

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
ВИВЧЕННЯ ПРОБЛЕМ ЗЛОЧИННОСТІ
ІМЕНІ АКАДЕМІКА В. В. СТАШИСА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Монографія

За загальною редакцією
В. І. Борисова, О. О. Пащенко

Харків
«Право»
2024

DOI: <https://doi.org/10.31359/9786178518899>

УДК 343.3/.7:004.056:006.42

К84

Рецензенти:

Голіна Володимир Васильович – доктор юридичних наук, професор, головний науковий співробітник відділу кримінологічних досліджень Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, член-кореспондент НАПрН України, заслужений діяч науки і техніки України;

Фріс Павло Львович – доктор юридичних наук, професор, професор кафедри політики у сфері боротьби зі злочинністю та кримінального права Навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника, член-кореспондент НАПрН України, заслужений діяч науки і техніки України

*Рекомендовано до друку вченою радою
Науково-дослідного інституту вивчення проблем злочинності
імені академіка В. В. Сташиса
Національної академії правових наук України
(постанова № 3/3 від 27 листопада 2024 р.)*

Кримінально-правова охорона інформаційної безпеки в Україні:
К84 монографія / [В. І. Борисов, О. О. Пашенко, Д. П. Євтєєва та ін.]; за заг. ред. В. І. Борисова, О. О. Пашенка ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. – Харків : Право, 2024. – 328 с. – DOI: <https://doi.org/10.31359/9786178518899>.

ISBN 978-617-8518-89-9

Монографія присвячена розгляду актуальних питань кримінально-правової охорони інформаційної безпеки в Україні. У виданні запропоновано класифікацію суспільно небезпечних діянь, вчинення яких супроводжується спричиненням шкоди інформаційній безпеці України або містить можливість заподіяння такої шкоди. На підставі цього поділу здійснено аналіз інформаційних кримінально-протиправних діянь, що посягають на основи національної безпеки України; кримінальних правопорушень у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави; суспільно небезпечних діянь у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електровз'язку; інформаційних кримінально-протиправних діянь, що посягають на мир, безпеку людства та міжнародний правопорядок.

Книга розрахована на науковців, викладачів права, народних депутатів України, працівників правоохоронних і судових органів, аспірантів (ад'юнктів), студентів, слухачів закладів вищої освіти, а також усіх інших осіб, хто цікавиться цією проблематикою.

УДК 343.3/.7:004.056:006.42

© Борисов В. І., Пашенко О. О.,
Євтєєва Д. П. та ін., 2024

© Науково-дослідний інститут вивчення
проблем злочинності імені академіка
В. В. Сташиса НАПрН України, 2024

ISBN 978-617-8518-89-9

ЗМІСТ

ПЕРЕДМОВА	8
-----------------	---

Розділ І.

ІНФОРМАЦІЙНІ КРИМІНАЛЬНО-ПРОТИПРАВНІ ДІЯННЯ, ЩО ПОСЯГАЮТЬ НА ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Вступні положення

(<i>В. І. Борисов, О. О. Пащенко</i>)	9
---	---

1.1. Інформаційні кримінально-протиправні діяння, що посягають на суверенітет, територіальну цілісність, недоторканність України (ст.ст. 109, 110 КК України) (<i>О. О. Пащенко</i>)	11
1.1.1. Публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (ч. 2 ст. 109 КК України)	12
1.1.2. Публічні заклики чи розповсюдження матеріалів із закликами до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України (ч. 1 ст. 110 КК України)	34
1.2. Інформаційні кримінально-протиправні діяння, що посягають на зовнішню безпеку України (ст.ст. 111, 114 КК України) (<i>В. І. Борисов</i>)	39
1.3. Інформаційні кримінально-протиправні діяння, що передбачають співпрацю з державою-агресором (ст.ст. 111 ¹ , 111 ² КК України) (<i>Н. В. Нетеса</i>)	59
1.3.1. Інформаційна колабораційна діяльність: загальні положення ..	59
1.3.2. Кримінально-правова характеристика колабораційної діяльності в інформаційній сфері (частини 1, 3 та 6 ст. 111 ¹ КК України)	66
1.3.3. Пособництво державі-агресору в інформаційній сфері (ст. 111 ² КК України)	94

1.4. Інформаційні кримінально-протиправні діяння, що посягають на обороноздатність України (ст. 114 ² КК України) (<i>В. В. Федосєєв</i>)	101
1.4.1. Загальні положення	101
1.4.2. Незаконне поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну (ч. 1 ст. 114 ² КК України)	105
1.4.3. Незаконне поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань (ч. 2 ст. 114 ² КК України)	114
Висновки ро розділу I.....	125

Розділ II.

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА ІНШОЇ ІНФОРМАЦІЇ, ЩО ЗАБЕЗПЕЧУЄ ОБОРОНОЗДАТНІСТЬ ДЕРЖАВИ

Вступні положення (<i>Д. П. Євтєєва, В. В. Базелюк, Д. О. Куковинець</i>)	129
2.1. Кримінальні правопорушення у сфері охорони державної таємниці (ст.ст. 328, 329, 422 КК України) (<i>Д. П. Євтєєва, Д. О. Куковинець</i>)	130
2.1.1. Розголошення державної таємниці (ст. 328 КК України)	130
2.1.2. Втрата документів, що містять державну таємницю (ст. 329 КК України)	143
2.1.3. Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422 КК України)	150
2.2. Кримінальні правопорушення у сфері охорони іншої інформації, що забезпечує обороноздатність держави (ст. 330 КК України) (<i>В. В. Базелюк</i>)	152
Висновки до розділу II	163

Розділ III.

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ
ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ),
СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Вступні положення (М. В. Карчевський, В. В. Федюк) 165

- 3.1. Кримінальні правопорушення в сфері використання
інформаційних технологій
(ст.ст. 361 – 363¹ КК України)
(М. В. Карчевський, В. В. Федюк) 167
- 3.1.1. Статистичні дані та дослідження судової практики 170
- 3.1.2. Родовий об'єкт кримінальних правопорушень
у сфері використання електронно-обчислювальних
машин (комп'ютерів), систем та комп'ютерних мереж
і мереж електрозв'язку 187
- 3.1.3. Несанкціоноване втручання в роботу інформаційних
(автоматизованих), електронних комунікаційних,
інформаційно-комунікаційних систем,
електронних комунікаційних мереж (ст. 361 КК України) 198
- 3.1.4. Створення з метою протиправного використання,
розповсюдження або збуту шкідливих програмних
чи технічних засобів, а також їх розповсюдження або збут
(ст. 361¹ КК України) 214
- 3.1.5. Несанкціоновані збут або розповсюдження інформації
з обмеженим доступом, яка зберігається
в електронно-обчислювальних машинах (комп'ютерах),
автоматизованих системах, комп'ютерних мережах
або на носіях такої інформації (ст. 361² КК України) 219
- 3.1.6. Несанкціоновані дії з інформацією, яка оброблюється
в електронно-обчислювальних машинах (комп'ютерах),
автоматизованих системах, комп'ютерних мережах
або зберігається на носіях такої інформації, вчинені особою,
яка має право доступу до неї (ст. 362 КК України) 224
- 3.1.7. Порушення правил експлуатації
електронно-обчислювальних машин (комп'ютерів),
автоматизованих систем, комп'ютерних мереж
чи мереж електрозв'язку або порядку чи правил захисту
інформації, яка в них оброблюється (ст. 363 КК України) 229

3.1.8. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363 ¹ КК України)	234
3.2. Перспективи кримінально-правового регулювання в контексті розвитку інформаційних технологій (М. В. Карчевський, В. В. Федюк)	237
Висновки до розділу III	256

Розділ IV.

ІНФОРМАЦІЙНІ КРИМІНАЛЬНО-ПРОТИПРАВНІ ДІЯННЯ, ЩО ПОСЯГАЮТЬ НА МИР, БЕЗПЕКУ ЛЮДСТВА ТА МІЖНАРОДНИЙ ПРАВОПОРЯДОК

Вступні положення (В. І. Борисов, М. В. Шепітько)	260
4.1. Інформаційні кримінально-протиправні діяння, що посягають на мир шляхом поширення пропаганди, виправдовування та глорифікації тоталітарних режимів та їх представників (ст.ст. 436, 436 ¹ , 436 ² КК України) (К. А. Новікова).....	262
4.2. Інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок шляхом планування, розв'язування та ведення агресивної війни (ст. 437 КК України) (М. В. Шепітько).....	292
4.3. Інформаційні кримінально-протиправні діяння, що посягають на мир та міжнародний правопорядок шляхом порушення законів та звичаїв війни (ст. 438 КК України) (В. І. Борисов, М. В. Шепітько)	299
4.4. Інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок шляхом здійснення публічних закликів до геноциду (ч. 2 ст. 442 КК України) (М. В. Шепітько).....	306

4.5. Інформаційні кримінально-протиправні діяння, що посягають на міжнародний правопорядок шляхом незаконного використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала (ст. 445 КК України) (<i>М. В. Шепітько, В. В. Базелюк</i>).....	316
Висновки до розділу IV	321
Авторський колектив	324

Передмова

Наукове дослідження, виконане колективом науковців, присвячене всебічному аналізу однієї з найгостріших і найактуальніших проблем буття сучасної України – кримінально-правовому забезпеченню інформаційної безпеки. Остання може зазнавати шкоди внаслідок вчинення кримінально-протиправного діяння. «Ядром» (субстратом, основою) відповідних суспільних відносин є вкрай важлива інформація, з приводу якої ці відносини формуються. У виданні запропоновано класифікацію суспільно небезпечних діянь, вчинення яких супроводжується спричиненням істотної шкоди інформаційній безпеці України або містить можливість заподіяння такої шкоди. На підставі цього поділу здійснено виділення та аналіз інформаційних кримінально-протиправних діянь, що посягають на основи національної безпеки України; кримінальних правопорушень у сфері охорони державної таємниці й іншої інформації, що забезпечує обороноздатність держави; та інформаційних кримінально-протиправних діянь, що посягають на мир, безпеку людства та міжнародний правопорядок. Також у контексті забезпечення інформаційної безпеки здійснено аналіз суспільно небезпечних діянь у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Наукова праця ґрунтується на широкому колі джерел, до яких, зокрема, належать офіційні документи, матеріали судової практики, наукові публікації та статистична інформація. Особливу цінність для дослідження являють результати, отримані за допомогою використання даних інтерактивного довідника «Протидія злочинності в Україні: інфографіка», що знаходиться у відкритому доступі на аналітичній платформі CrimeDataLab.

Пропонована монографія є не лише спробою комплексного правового дослідження проблем кримінально-правової протидії найнебезпечнішим посяганням в інформаційній сфері, а й може бути інструментом для розуміння й ефективного застосування відповідного законодавства про кримінальну відповідальність.

Розділ I

ІНФОРМАЦІЙНІ КРИМІНАЛЬНО-ПРОТИПРАВНІ ДІЯННЯ, ЩО ПОСЯГАЮТЬ НА ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Вступні положення

Норми законодавства про кримінальну відповідальність, що забезпечують інформаційну безпеку, розташовано законодавцем в багатьох розділах Особливої частини КК. Не є виключенням і розділ I «Злочини проти основ національної безпеки України». В доктрині кримінального права загальноновизнано, що у цьому розділі зосереджено такі «безпекові» злочини, вчинення яких ставить під загрозу саме існування Української держави як гаранта захисту прав і свобод громадян України, іноземців та осіб без громадянства. В диспозиції ст. 111 КК йдеться про державну, економічну та інформаційну безпеку. Аналіз Особливої частини КК дозволяє виокремити ще, принаймні, такі види безпеки: екологічну, громадську, безпеку виробництва, безпеку руху та експлуатації транспорту, безпеку державної таємниці та безпеку людства. Водночас, в розділ I Особливої частини КК «зібрано» посягання на всі можливі види безпеки, які, як зазначалося, об'єднує те, що їх учинення ставить під загрозу існування держави. Деякі з них вчиняються у такій сфері безпеки як інформаційна¹.

В цьому розділі послідовно розглянуті інформаційні кримінально-протиправні діяння, що посягають на суверенітет, територіальну цілісність, недоторканність України (ст.ст. 109, 110 КК), зовнішню безпеку України (ст.ст. 111, 114 КК), такі, що передбачають спів-

¹ Пашенко О. О. Кримінально-правова охорона інформаційної безпеки нормами Розділу I Особливої частини КК України. *Питання боротьби зі злочинністю*. Харків. 2024. Вип. 47. С. 12.

працю з державою-агресором (ст.ст. 111¹, 111² КК), посягають на обороноздатність України (ст. 114² КК).

Серед цих кримінальних правопорушень:

- **стаття 109 КК** «Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади»;
- **стаття 110 КК** «Посягання на територіальну цілісність і недоторканність України»;
- **стаття 111 КК** «Державна зрада»;
- **стаття 114 КК** «Шпигунство»;
- **стаття 111¹ КК** «Колабораційна діяльність»;
- **стаття 111² КК** «Пособництво державі-агресору»;
- **стаття 114² КК** «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».

Дослідженню основ національної безпеки України як родового об'єкта злочинів, передбачених розділом I Особливої частини КК України, присвячені праці значної кількості вітчизняних правників. Серед них слід виокремити роботи таких науковців як О. Ф. Бантишев, В. К. Гіжевський, В. О. Глушков, Н. О. Гуторова, М. В. Даньшин, І. В. Діордіца, М. Д. Дякур, О. Ю. Звонарьов, І. В. Зозуля, Є. М. Кислюк, М. Й. Коржанський, В. О. Кузнєцов, Я. О. Лантінов, В. А. Ліпкан, В. К. Матвійчук, Л. В. Мошняга, В. О. Навроцький, Ю. О. Найдзон, Д. О. Олейніков, В. І. Павликівський, М. А. Рубашенко, А. В. Савченко, Є. В. Сичевський, Є. Д. Скулиш, О. В. Сотула, В. Я. Тацій, Є. І. Харитонов, Р. Л. Чорний, О. А. Чуваков, О. В. Шамара, А. В. Шевчук та ін. Водночас до аналізу того, які із відповідних норм, передбачених цим розділом, мають своїм призначенням захист саме інформаційної безпеки, зазначені правники у своїх наукових пошуках не вдавалися¹, що зумовило необхідність проведення цього дослідження.

¹ Пашенко О. О. Кримінально-правова охорона інформаційної безпеки нормами Розділу I Особливої частини КК України. С. 12.

1.1. Інформаційні кримінально-протиправні діяння, що посягають на суверенітет, територіальну цілісність, недоторканність України (ст.ст. 109, 110 КК України)

Ступінь захищеності суспільства та держави від згубного використання інформації напряму залежить від якості правової регламентації суспільних відносин у сфері обігу інформації, у тому числі й від якості кримінально-правової охорони цих відносин¹.

У розділі І Особливої частини КК містяться дві статті – 109 і 110, які передбачають відповідальність за вчинення публічних закликів, а також розповсюдження матеріалів із закликами до вчинення визначених статтями дій².

Кримінальна відповідальність за публічні заклики до посягання на суверенітет Українського народу або розповсюдження відповідних матеріалів є досить ефективним засобом протидії інформаційній агресії³.

Надійною основою у забезпеченні сучасної кримінально-правової політики у сфері протидії злочинам проти державного суверенітету має стати кримінально-правова доктрина⁴. Тому дослідження проблеми кримінальної відповідальності за злочини, передбачені ст.ст. 109, 110 КК є вельми актуальними.

¹ Тарасенко Д. І. Комп'ютерна інформація як предмет злочинів проти основ національної безпеки України та джерело доказів. *Наука кримінального права в системі міждисциплінарних зв'язків*: матеріали міжнар. наук.-практ. конф. (Харків, 9–10 жовт. 2014 р.) ; редкол.: В. Я. Тацій, В. І. Борисов, А. П. Гетьман та ін. Харків: Право, 2014. С. 468.

² Там само. С. 468.

³ Янко В. М. Кримінальна відповідальність за злочини проти основ суверенітету українського народу: дис. ... к.ю.н. Северодонецьк, 2018. С. 132.

⁴ Кубальський В. Н. Проблеми кримінальної відповідальності за публічні заклики до вчинення злочинів проти державного суверенітету. *Судова апеляція*. 2018. № 2 (51). С. 68.

1.1.1. Публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (ч. 2 ст. 109 КК України)

Більшість науковців пов'язує визначення *основного безпосереднього об'єкта* цього злочину із такими поняттями як «конституційний лад» та «державна влада». Тому дослідження є сенс розпочати із аналізу наявних підходів до визначення цих понять.

Група науковців вважає, що категорія «конституційний лад» вживається у праві як усталена, проте це не позбавляє її бланкетного навантаження. Проблема в тому, що цей термін використовується в конституціях багатьох держав без офіційного визначення змісту відповідного поняття. Конституційний лад в Україні закріплюється Конституцією України. На підставі аналізу теорії конституційного права, положень Конституції України науковці визначають такі складові конституційного ладу: суверенітет держави, форма правління, державний устрій, державний режим¹.

З точки зору В. Я. Тація конституційний лад – це устрій держави і суспільства, а також їх інститутів відповідно до конституційно-правових норм². Є. В. Сичевський, Є. І. Харитонов, Д. О. Олей-

¹ Яремко Г. З. Бланкетна диспозиція ст. 109 КК України «Дії спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади». Актуальні проблеми юридичної науки: збірник тез Міжнародної наукової конференції «Восьмі осінні юридичні читання» (Хмельницький, 13–14 листоп. 2009 р.): у 4-х ч. Ч. 4-та. Хмельницький: Вид-во Хмельницьк. ун-та управління та права. С. 126; Мошняга Л. В. Склади злочинів, що посягають на конституційні основи національної безпеки України: поняття та шляхи вдосконалення. *Наук. вісн. Дніпропетров. держ. ун-ту внутр. справ.* 2010. № 1. С. 209, 210; Бангишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації): моногр. 3-тє вид., перероб. і допов. Луганськ: Віртуальна реальність, 2014. С. 139, 140; Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу I Особливої частини Кримінального кодексу України (Злочини проти основ національної безпеки України). Харків: Право, 2016. С. 8, 9.

² Тація В. Я. Злочини проти основ національної безпеки України. *Кримінальне право України. Особлива частина: підручник / за ред.: В. Я. Тація, В. І. Борисова, В. І. Тютюгіна.* 6-тє вид., перероб. і допов. Харків: Право, 2020. Розд. II. С. 30.

ніков зазначають, що конституційний лад – це сукупність найбільш усталених конституційних принципів, положень і правовідносин, що складаються на їх базі¹. Більш розгорнуте визначення надають О. Ф. Бантишев та В. С. Картавцев – це засновані на Конституції України: повновладдя Українського народу як носія і єдиного джерела влади в Україні, суверенітет держави, її територіальна цілісність і недоторканість державних кордонів, демократизм, республіканська форма правління, принципи і форми організації і діяльності органів державної влади та органів місцевого самоврядування, рівність всіх націй і народностей, права і свободи людини і громадянина, взаємовідносини громадян і держави². Це визначення поділяють В. А. Ліпкан і О. С. Ліпкан водночас виокремлюючи друге значення цього поняття: *цілісна система основоположних суспільних відносин і відповідних їм інститутів суспільства і держави*, які закріплені нормами конституційного законодавства³. Аналізуючи наведені визначення можна зауважити, що все те, що було перелічено у першому (суверенітет держави, її територіальна цілісність, демократизм, республіканська форма правління тощо) також входить у «цілісну систему основоположних суспільних відносин», більш того, є «ядром» навколо якого ці відносини формуються. Тому всі перелічені загальнонаціональні цінності (крім взаємовідносин людини і держави) утворюють предмет відповідних суспільних відносин. Остання ж наведена у першому визначенні складова ілюструє вже не предмет, а соціальний зв'язок між суб'єктами таких відносин з приводу відповідного предмета. Такий зв'язок є динамічним, оскільки відбиває *діяльність* громадян і держави, їх активну позицію щодо одне одного⁴.

¹ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 8, 9.

² Бантишев О. Ф., Картавцев В. С. Злочини проти основ національної безпеки України. *Науково-практичний коментар до Кримінального кодексу України*: у 2-х т. ; за заг. ред. П. П. Андрушка, В. Г. Гончаренка, Є. В. Фесенка. 3-тє вид., перероб. та доп. Київ: Правова єдність, 2009. Т. 1. Особлива частина. Розд. І. С. 264.

³ Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях і поняттях: словник. Вид. 2-ге, допов. і перероб. Київ: Текст, 2008. С. 169, 170.

⁴ Пащенко О. О. Конституційний лад та інформаційна безпека як об'єкти злочину, передбаченого ч. 2 ст. 109 КК України. Реалії та перспективи розбудови правової

На відміну від наведених позицій, дослідження А. Ю. Швед призвело її до висновку, що «значення, в яких вживається термін конституційний лад в Основному законі України, не дає підстав визначити його правову природу, встановити зміст вказаного поняття або ж визначити його складові елементи»¹. З цього приводу варто зазначити, що відповідний висновок може і є актуальним для порівняльно-правових досліджень (оскільки правниця здійснювала порівняльний аналіз злочинів проти конституційних засад національної безпеки за законодавством України та Скандинавських країн), проте не має практичної значущості для застосування законодавства про кримінальну відповідальність. Якщо притримуватися наведеної точки зору, то тоді кримінально-правова охорона стає безпредметною – невідомо що саме охороняє відповідна норма кримінального закону. Як було показано на початку, група науковців також наголошує на відсутності офіційного визначення змісту досліджуваного поняття, проте це не завадило їм виокремити складові елементи конституційного ладу не стикаючись при цьому ні з якими складнощами. Крім того, викликає заперечення думка, наведена дисертанткою у висновках свого дослідження. З її точки зору, конституційний лад «співвідноситься з державним та суспільним ладом як ціле та його частина»². Така побудова речення свідчить про те, що конституційний лад визнається правницею цілим, а державний і суспільний лад – частиною. З нашої точки зору це зовсім не так. Передусім, слід вести мову не про частину, а частини, адже державний і суспільний лад – не одне і те саме, і розглядатися в межах однієї «частини» не можуть. По суті ж питання, вважаємо, що навпаки, конституційний лад є частиною державного, оскільки визначає механізм державного регулювання, державного устрою та

держави в Україні та світі: матеріали VII Міжнар. наук.-практ. конф. (Суми, 31 трав. – 1 черв. 2024 р): У 2-х т. Суми: СумДПУ ім. А. С. Макаренка, 2024. Т. 2. С. 55.

¹ Швед А. Ю. Злочини проти конституційних засад національної безпеки за законодавством України та Скандинавських країн: порівняльна характеристика: автореф. дис. канд. юрид. наук ; Нац. ун-т «Одеська юридична академія». Одеса, 2021. С. 6, 7.

² Швед А. Ю. Злочини проти конституційних засад національної безпеки за законодавством України та Скандинавських країн. С. 11.

інші найважливіші елементи діяльності держави. Водночас державний лад цим не вичерпується, оскільки багато його складових знаходяться поза межами безпосереднього регулювання Конституції України, а значить і конституційного ладу. Водночас сам державний лад є часткою суспільного ладу, адже держава – продукт діяльності суспільства, без суспільства держава не може існувати і, навіть, виникнути. Слід відзначити, що в подальшому А. Ю. Швед фактично це визнає зазначаючи, що у разі сформованого суспільного ладу настають передумови для виникнення державного ладу, а в разі його належного функціонування стає можливим утворення в подальшому конституційного ладу¹.

Питання щодо визначення сутності та змісту *державної влади* є вічною проблемою, яку намагалися досліджувати та вирішувати багато вчених, серед яких правознавці, філософи, соціологи тощо. Незважаючи на це, і на теперішній час цю фундаментальну юридичну категорію визначають та тлумачать по-різному².

Саме на державну владу покладається реалізація найважливіших функцій держави спрямованих на досягнення в суспільстві стану законності та правопорядку³. В. Я. Тацій зазначав, що *державна влада* – це головна складова публічної влади, яка належить тільки державі й реалізується нею шляхом прийняття компетентними органами обов'язкових для виконання усіма рішень (правових актів) та застосування у разі необхідності державного примусу⁴. Л. В. Мошняга пише, що це – система органів законодавчої, виконавчої і судової влади, що здійснюють свої повноваження у встановлених

¹ Швед А. Ю. Злочини проти конституційних засад національної безпеки за законодавством України та Скандинавських країн. С. 11; Пашенко О. О. Конституційний лад та інформаційна безпека як об'єкти злочину, передбаченого ч. 2 ст. 109 КК України. С. 56, 57.

² Балаклицький А. І. Поняття та значення державної влади для забезпечення прогресивного розвитку суспільства. *Сучасні проблеми правової системи України: збірник матеріалів III Міжнар. наук.-прак. конф.* (Київ, 24 листоп. 2011 р.). Вип. 3. Київ: Вид-во Європ. ун-ту, 2011. С. 83.

³ Балаклицький А. І. Поняття та значення державної влади для забезпечення прогресивного розвитку суспільства. С. 84.

⁴ Тацій В. Я. Злочини проти основ національної безпеки України. С. 30, 31.

Конституцією межах і відповідно до законів України¹. Таке визначення поділяють О. Ф. Бантишев, В. С. Картавцев, О. О. Шамара², які з цього роблять висновок, що державна влада є похідною від конституційного ладу³, є його частиною⁴. Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков вважають, що *державна влада* – це здатність народу України безпосередньо і через органи державної влади і органи місцевого самоврядування приймати відповідні рішення, які стосуються найважливіших засад суспільного та політичного життя, і впроваджувати їх на території держави⁵.

Натомість цей підхід до визначення основного безпосереднього об'єкта злочину, передбаченого ч. 2 ст. 109 КК, не є єдиним в кримінально-правовій доктрині. Так, зокрема, М. В. Даньшин та Я. О. Лантінов визнають ним (а точніше ними, оскільки вони цілком обґрунтовано розглядають два окремі злочини, передбачені у цій частині – публічні заклики та розповсюдження матеріалів) безпеку політичного устрою України⁶.

З нашої точки зору, для визначення основного безпосереднього об'єкту злочину, передбаченого ч. 2 ст. 109 КК, слід звернутися до назви цієї статті та її диспозиції. Там зазначаються такі загальнонаціональні цінності як конституційний лад та державна влада. Тому цілком логічним вбачається висновок, що відповідним об'єктом є суспільні відносини з приводу охорони саме цих соціальних цінностей, які, своєю чергою, виступають як предмет названих суспіль-

¹ Мошняга Л. В. Склади злочинів, що посягають на конституційні основи національної безпеки України: поняття та шляхи вдосконалення. С. 210.

² Бантишев О. Ф., Картавцев В. С. Злочини проти основ національної безпеки України. С. 264; Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 140.

³ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 140.

⁴ Бантишев О. Ф., Картавцев В. С. Злочини проти основ національної безпеки України. С. 264.

⁵ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 9.

⁶ Злочини проти основ національної безпеки України: альбом схем / уклад.: М. В. Даньшин, Я. О. Лантінов. Харків: Харків юридичний, 2012. С. 7, 8.

них відносин. З приводу цього предмету (який за своїми властивостями є нематеріальним), а точніше для його захисту, і формуються відповідні суспільні відносини, структурними елементами яких є також їх суб'єкти (учасники) та соціальний зв'язок між ними з приводу зазначеного предмету. Суб'єктами цих відносин є фізичні, юридичні особи та суспільство в цілому, тобто коло учасників є дуже широким, оскільки інтерес у нормальному функціонуванні конституційного ладу та державної влади мають усі учасники суспільного процесу. При цьому соціальний зв'язок між цими суб'єктами має форму статички – тобто всі вони мають утримуватися від дій, спрямованих на насильницьку зміну чи повалення конституційного ладу, а також на захоплення державної влади.

Додатковим обов'язковим об'єктом злочину, передбаченого ч. 2 ст. 109 КК, є суспільні відносини, що забезпечують інформаційну безпеку. Такий висновок слідує із сутності діянь, що утворюють його об'єктивну сторону, оскільки і заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (1), і розповсюдження матеріалів із відповідними закликами (2) обов'язково спричиняють негативні зміни в інформаційному просторі¹.

Предмет. На думку В. Я. Тація, предметом злочину у формі публічних закликів є *інформація*, що містить хоч один заклик відповідного змісту, а формі розповсюдження матеріалів – *певний рухомий носій інформації* (в тому числі й в електронній формі), що містить такий заклик². Прихильником такої точки зору фактично є також Д. І. Тарасенко, який визнаючи предметом публічних закликів інформацію³, одночасно визнає предметом іншої аналізованої форми діяння *матеріали із закликами*⁴. Як зауважує Р. Л. Чорний, предме-

¹ Пашенко О. О. Конституційний лад та інформаційна безпека як об'єкти злочину, передбаченого ч. 2 ст. 109 КК України. С. 57, 58.

² Тація В. Я. Злочини проти основ національної безпеки України. С. 31.

³ Тарасенко Д. І. Комп'ютерна інформація як предмет злочинів проти основ національної безпеки України та джерело доказів. С. 467.

⁴ Тарасенко Д. І. Комп'ютерна інформація як предмет злочинів проти основ національної безпеки України та джерело доказів. С. 469.

ти злочину, передбаченого ч. 2 ст. 109 КК, чітко визначені в законі¹. З цього випливає, що такими предметами науковець визнає лише матеріали із закликами, адже ніяких інших предметів у диспозиції ч. 2 ст. 109 КК не зазначено.

На противагу цьому, інші науковці в останній формі виділяють не предмет злочину, а засоби його вчинення – *матеріали*², під якими зокрема О. А. Чуваков розуміє письмові чи зафіксовані на іншому носії інформації (дискети, аудіо-, відеокасети) звернення, листівки, плакати, газети, журнали тощо. Обґрунтовує він це тим, що «вони перебувають в динамічному (а не статичному, на відміну від предмета злочину, стані) й за їх допомогою суб'єкт впливає на об'єкт даного злочину»³.

Об'єктивна сторона. Якщо фізичні дії є типовими видами кримінально-протиправної поведінки, то природа й особливості інформаційних діянь стали предметами цілеспрямованих досліджень фахівців у галузі кримінального права лише з початком інформаційного буму в середині 2000-х років⁴. Інформаційні дії полягають у передаванні інформації іншим особам і завжди виражаються у словесній (вербальній) формі, а також у яких-небудь інших діях, що несуть інформацію: смислових жестах (конклюдентні дії), різних рухах (міміка)⁵. Одним із різновидів інформаційних дій є пу-

¹ Чорний Р. Л. Поняття, система та кримінально-правова характеристика складів злочинів проти основ національної безпеки України: автореф. дис. д-ра юрид. наук. Харк. нац. ун-т внутр. справ. Харків, 2021. С. 12.

² Злочини проти основ національної безпеки України: альбом схем. С. 7, 8; Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. *Проблеми кримінально-правової кваліфікації*: навч. посібник / М. Г. Арманов, О. З. Гладун, О. О. Книженко та ін. Київ: Нац. акад. прокуратури України, 2017. Розд. 4. С. 68; Чуваков О. А. Злочини проти основ національної безпеки України. С. 236.

³ Чуваков О. А. Злочини проти основ національної безпеки України: проблеми кримінально-правової теорії та практики: монографія. Одеса: Фенікс, 2017. С. 236.

⁴ Рубашенко М. А. Особливості кваліфікації публічних закликів та заперечень як інформаційних діянь. *Право України*. 2022. № 11. С. 77.

⁵ Панов М. І. Об'єктивна сторона кримінального правопорушення. *Кримінальне право України: Загальна частина*: підручник ; за ред. В. Я. Тація, В. І. Тютюгіна, В. І. Борисова. 6-те вид., перероб. і допов. Харків: Право, 2020. Розд. VIII. С. 140.

блічні заклики¹, про які йдеться, зокрема, у ч. 2 ст. 109 КК², а також у ч. 1 ст. 110 КК.

Більшість науковців виділяють такі форми об'єктивної сторони злочину, передбаченого ч. 2 ст. 109 КК: публічні заклики до насильницької зміни чи повалення конституційного ладу або захоплення державної влади; розповсюдження матеріалів із закликами до вчинення таких дій³.

Схожу точку зору висловлюють О. Ф. Бантишев та О. О. Шама-ра, які виокремлюють: публічні заклики до насильницької зміни конституційного ладу України (1); публічні заклики до насильницького повалення конституційного ладу України (2); публічні заклики до насильницького захоплення державної влади (3); розповсюдження матеріалів із закликами до здійснення таких дій (4), а саме до насильницької: а) зміни конституційного ладу; б) повалення консти-

¹ Мошняга Л. В. Суб'єктивна сторона злочинів проти конституційних основ національної безпеки України. *Бюлетень Міністерства юстиції України*. 2012. № 5. С. 79; Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканість України: монографія. Харків: Право, 2016. С. 127; Кубальський В. Н. Проблеми кримінальної відповідальності за публічні заклики до вчинення злочинів проти державного суверенітету. С. 70; Кривоускова К. Л. Кримінальна відповідальність за публічні заклики до вчинення злочинів проти основ національної безпеки за законодавством іноземних держав та України. *Часоп. Київ. ун-ту права*. 2021. № 2. С. 290.

² Пашенко О. О. Деякі особливості публічних закликів як інформаційних діянь, передбачених ч. 2 ст. 109 КК України. *Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення* : матер. IV Міжнар. наук.-практ. конф. (Дніпро, 21 черв. 2024 р.). Дніпро: Дніпров. гуманітар. ун-т. С. 86.

³ *Науково-практичний коментар до Кримінального кодексу України від 5 квітня 2001 р.* / за ред. М. І. Мельника, М. І. Хавронюка). Київ: Канон, А.С.К., 2001. С. 244; Мошняга Л. В. Об'єктивна сторона злочинів проти конституційних основ національної безпеки України. *Вісн. Запорізьк. юрид. ін-ту Дніпропетров. держ. ун-ту внутр. справ*. 2010. № 1. С. 206; Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 10; Денисов С. Ф., Багіров С. Р. Логіко-системний аналіз конструкцій деяких статей розділу І «Злочини проти основ національної безпеки України». *Актуальні проблеми кримінально-правової охорони основ національної безпеки України: матеріали кругл. столу* (Харків, 26 трав. 2017 р.). Харків: Право, 2017. С. 21; Янко В. М. Кримінальна відповідальність за злочини проти основ суверенітету українського народу: монографія. Сєверодонецьк: Луган. держ. ун-т внутр. справ, 2019. С. 74; Тацій В. Я. Злочини проти основ національної безпеки України. 2020. С. 31.

туційного ладу; в) захоплення державної влади¹. Схожою є позиція В. К. Матвійчука, а також О. О. Книженко, які щодо публічних закликів висловлюють подібну точку зору, а от все, що стосується розповсюдження матеріалів виділяють як окремі форми прояву об'єктивної сторони досліджуваного злочину: 4) розповсюдження матеріалів із закликами до насильницької зміни конституційного ладу; 5) розповсюдження матеріалів із закликами до повалення конституційного ладу України; 6) розповсюдження матеріалів із закликами до захоплення державної влади України².

Наведені позиції слід визнати цілком послідовними, оскільки вони повною мірою узгоджується із диспозицією ч. 2 ст. 109 КК. Проте, вони не є єдиними у вітчизняній кримінально-правовій доктрині. Так, І. В. Діордіца вважає, що це публічні заклики до *незаконної* зміни конституційного ладу України або до *незаконного здобуття* державної влади в Україні (1) та розповсюдження матеріалів із закликами до вчинення таких дій (2)³. З цього приводу слід зауважити, що правник здійснює досить довільне тлумачення тексту досліджуваного закону про кримінальну відповідальність. Справа у тому, що поняття «насильницька зміна» та «незаконна зміна» є далеко не рівнозначними: друге поняття є значно ширшим за своїм обсягом. Насильницька зміна конституційного ладу завжди є незаконною, а от незаконна зміна – не завжди має відбуватися насильницьким шляхом. Так, незаконною є зміна за допомогою використання обману, наприклад шляхом фальсифікації результатів всеукраїнського референдуму з питань зміни відповідних положень Конституції

¹ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 70.

² Матвійчук В. К. Форми вияву злочину «дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади», передбачені частинами 1, 2, 3 статті 109 КК України. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності: тези II Всеукр. наук.-практ. конф.* (Хмельницький, 2 берез. 2018 р.). Хмельницький: Нац. акад. держ. прикордон. служби України, 2018. С. 68; Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 65.

³ Діордіца І. В. Кримінально-правова відповідальність за дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади: дис. ... к.ю.н. Київ: Київ. міжнар. ун-т, 2008. С. 168, 169.

України. І навпаки, *незаконне здобуття* державної влади в Україні може відбуватися без застосування насильства, тоді як використаний законодавцем термін «захоплення» орієнтує на його обов'язкове застосування. Саме тому законодавець при конструюванні диспозиції не вказує на насильницький характер захоплення (державної влади), оскільки він є іманентним останньому. Подібної помилки припускається і О. В. Ковальська, пишучи про зміну конституційного ладу в *«неконституційний спосіб»*. Вочевидь таким є будь-який спосіб, не передбачений у Конституції України, а не лише насильницький, як того вимагає диспозиція ч. 2 ст. 109 КК¹.

Слід зауважити, що позицію І. В. Діордіці згодом підтримала Л. В. Мошняга, зауваживши при цьому, що в ст. 110 КК «також немає вказівок на насильницький характер передбачених тут дій»². Вочевидь дослідниця апелює до принципу системності побудови кримінального законодавства, тим паче, що вона є прихильницею об'єднання злочинів, передбачених ст.ст. 109, 110 (а також ст. 112) КК в одну класифікаційну групу з назвою «Злочини проти конституційних основ національної безпеки України»³. З нашої точки зору вимогу системності законодавства не слід тлумачити аж настільки буквально. Злочини, що входять до однієї класифікаційної групи і мають спільний видовий об'єкт не обов'язково повинні мати абсолютно ідентичні об'єктивні і суб'єктивні ознаки (у даному разі спосіб їх учинення). Тому відсутність вказівки на насильницький характер дій у диспозиції ст. 110 КК сама по собі не може слугувати аргументом на користь критики передбачення такого способу в ст. 109 КК. Інших аргументів щодо такого вирішення питання науковець нажалі не наводить⁴.

¹ Ковальська О. В. Кримінально-правова охорона *основ* національної безпеки України та диференціація злочинів проти основ національної безпеки України в сучасних умовах. *Юридична Україна*. 2022. № 5. С. 18.

² Мошняга Л. В. Об'єктивна сторона злочинів проти конституційних основ національної безпеки України. С. 206.

³ Там само. С. 204.

⁴ Пащенко О. О. Деякі особливості публічних закликів як інформаційних діянь, передбачених ч. 2 ст. 109 КК України. С. 86, 87.

Інакшу позицію з цього приводу займають Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков. З їхньої точки зору термін «насильницька» стосується лише зміни конституційного ладу¹. Крім того, вони стверджують, що його можна розглядати в двох аспектах: 1) зміна конституційного ладу України із застосуванням фізичного насильства; 2) зміна конституційного ладу всупереч встановленому законом порядку його зміни. Друге твердження дослідники аргументують тим, що «оскільки законом передбачений порядок зміни конституційного ладу України, то зміна конституційного ладу з його порушенням і буде вважатися насильницькою»². Така точка зору викликає заперечення. По-перше, досліджуваний термін обмежується чомусь лише фізичним насильством, тоді як можливість застосування іншого виду насильства – психічного, – не досліджується взагалі. По-друге, тезу щодо того, що зміна конституційного ладу з порушенням порядку «буде вважатися насильницькою» неможна обґрунтувати взагалі нічим. У такому випадку у назві статті та тексті її диспозиції варто було би зазначити про «порушення порядку зміни конституційного ладу», а не його насильницьку зміну, як має місце насправді. Крім того, слід зауважити, що Особлива частина КК містить значну кількість кримінальних правопорушень, об'єктивна сторона яких полягає у порушенні певного порядку (порушенні порядку здійснення певної діяльності): ст. 143 «Порушення встановленого законом порядку трансплантації анатомічних матеріалів людини», ст. 159¹ «Порушення порядку фінансування політичної партії, передвиборної агітації чи агітації референдуму», ст. 213 «Порушення порядку здійснення заготівлі металобрухту та операцій з металобрухтом», 321² «Порушення встановленого порядку доклінічного вивчення, клінічних випробувань і державної реєстрації лікарських засобів», ст. 333 «Порушення порядку здійснення міжнародних передач товарів, що підлягають державному експортному контролю» та ін. За логікою правників, усі ці суспільно небезпечні

¹ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 11.

² Там само. С. 11.

діяння мають бути визнані насильницькими, що, вочевидь, не є послідовним.

Зважаючи на викладене, об'єктивну сторону досліджуваного злочину становлять лише публічні заклики до *насильницької* зміни конституційного ладу або до захоплення державної влади. При цьому характер насильства, до якого закликає суб'єкт злочину, може бути як фізичним, так і психічним (або взагалі без конкретизації його виду)¹.

На думку В. Я. Тація, передбачені у ч. 2 ст. 109 КК *публічні заклики* – це доведення широкому (значному) колу осіб інформації в будь-якій формі, спрямованої викликати в них бажання вчинити дії з метою насильницької зміни конституційного ладу або захоплення державної влади². О. Ф. Бантишев та В. С. Картавцев вважають, що *заклик* – це активний вплив на невизначену кількість людей або членів певної партії, організації чи інше угруповання, пов'язаний із схиленням їх до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади. Такий заклик має бути *публічним*, тобто бути звернений не до однієї, а до декількох осіб, які реально сприймають його або, на думку розповсюджувача, можуть сприймати ці заклики³. З точки зору Д. І. Тарасенка, *закликом* є така психолінгвістична конструкція, яка створює у людини мотивацію для жаданої поведінки⁴. *Публічність* ж закликів, з його точки зору, передбачає доведення їх змісту до багатьох осіб, що може відбуватися як під час публічних виступів на різноманітних зібраннях і трансляціях, так і за допомогою мережі Інтернет⁵. На переконання О. О. Книженко, *заклики* є формою впливу на свідомість і волю людини, коли формується чітке спонукання до певного виду діяльнос-

¹ Пащенко О. О. Деякі особливості публічних закликів як інформаційних діянь, передбачених ч. 2 ст. 109 КК України. С. 87, 88.

² Тацій В. Я. Злочини проти основ національної безпеки України. С. 31.

³ Бантишев О. Ф., Картавцев В. С. Злочини проти основ національної безпеки України. С. 265.

⁴ Тарасенко Д. І. Комп'ютерна інформація як предмет злочинів проти основ національної безпеки України та джерело доказів. С. 468, 469.

⁵ Там само. С. 469.

ті¹. *Публічність*, з її точки зору, означає, що заклики мають відкритий, доступний для усвідомлення і розуміння характер та звернені до широкого, невизначеного кола людей². О. А. Чуваков зазначає, що під *публічними закликами* до зазначених дій слід розуміти цілий комплекс різноманітних дій: 1) активний вплив на невизначену кількість людей або на членів певної партії, організації чи іншого угруповування, з'єднаний із схилинням їх до насильницької зміни чи повалення конституційного ладу чи до захоплення державної влади; 2) публічний характер, тобто має проголошуватися відкрито, в присутності багатьох громадян; 3) це форма впливу на свідомість, волю та поведінку людей, що полягає в безпосередньому зверненні до них для формулювання спонукання до певної діяльності; вони мають загальний характер, вони не звернені до конкретної особи чи групи осіб, не містять конкретної вказівки про місце, час і спосіб учинення злочину; 4) можуть бути звернені до громадян взагалі, але можуть бути цілеспрямовано звернені до тих чи інших верств населення, етнічних груп, релігійних конфесій, членів тих або інших рухів, партій, інших громадських організацій, але в будь-якому разі вони пов'язані із цілеспрямованим схилинням невизначеного кола осіб; цінною є вказівка на відмежування таких публічних закликів від «балаканини» з одного боку і від підбурювання до конкретного злочину – з другого; 5) це хоча б одне відкрите звернення до невизначеного, але значного кола осіб, у якому виражені ідеї, погляди чи вимоги, спрямовані на те, щоб шляхом поширення їх серед населення чи його окремих категорій схилити певну кількість осіб до певних дій³. На наш погляд, у цьому «комплексі різноманітних дій», про які пише правознавець, деякі з них «перехрещуються» або повторюються, а то і явно мають протилежний за значенням зміст. Вочевидь тут йдеться не про «комплекс дій», а про різні підходи до їх визначення, які вдалося відшукати правознавцеві в доктрині кримінального права.

¹ Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 67.

² Там само. С. 68.

³ Чуваков О. А. Злочини проти основ національної безпеки України. С. 235.

З точки зору Є. В. Сичевського, Є. І. Харитонова та Д. О. Олейнікова публічні заклики – це виражені в будь-якій формі звернення до інших осіб, вчинені у відкритий спосіб у місці, яке дозволяє сприймати їх необмеженому колу осіб, розраховані на спонукання цих осіб до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, здійснювані шляхом поширення відомостей про доцільність, необхідність чи бажаність цього¹. При цьому публічність правники розглядають в декількох аспектах. По-перше, заклики адресуються невизначеному широкому колу осіб (хоча можливим є звернення і до однієї особи, проте, в присутності інших, коло яких не обмежене персональними рамками). Якщо ж заклики до вчинення злочинних дій стосуються лише конкретних осіб, їх обмеженого кола, то такі дії мають кваліфікуватися як підбурювання до злочину, передбаченого ч. 1 ст. 109 КК. Визначальними, на думку дослідників, тут слід вважати випадковий склад аудиторії та вільну можливість інших осіб підключитися до неї². Вважаємо, що такий критерій розмежування злочинів, передбачених ч. 1 та ч. 2 ст. 109 КК, слід підтримати. По-друге, переконують правники, невід’ємною ознакою закликів є їх здатність спонукати свідомість та волю особи на вчинення певних дій, про що можуть свідчити спеціальні лінгвістичні чи психолого-лінгвістичні конструкції, призначення яких полягає не тільки у доведенні певної інформації до відома іншої особи, а й її спонуканні до вчинення певних дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади³. З точки зору К. Л. Кривопускової, публічні заклики – це доведення до значної кількості людей (публіки) в будь-якій формі інформації, зміст якої спрямований викликати в них бажання (намір) учинити дії з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади⁴.

¹ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 16, 17.

² Там само. С. 17.

³ Там само. С. 17.

⁴ Кривопускова К. Л. Кримінальна відповідальність за публічні заклики до вчинення злочинів проти основ національної безпеки за законодавством іноземних держав та України. С. 290.

О. О. Кваша та В. В. Гапончук шляхом аналізу Конвенції Ради Європи про запобігання тероризму дійшли висновку, що за змістом поняття «публічні заклики» є тотожним поняттю «публічне підбурювання». Останнього КК України не містить ні в Загальній, ні в Особливій частині, але це поняття зустрічається ще принаймні в двох міжнародно-правових документах¹. Співучасть у виді підбурювання має, як правило, не публічний характер та спрямована до певної особи, на відміну від публічних закликів, які спрямовані до невизначеного кола осіб. Традиційно саме публічність/не публічність вважається основною розмежувальною рисою цих понять². Тому публічне підбурювання і є закликком (закликами)³.

Аналізуючи п. 1 примітки до ст. 111¹ КК М. А. Рубашенко зазначив, що законодавець уперше закріпив визначення *публічності* безпосередньо у кримінальному законі, поклавши в основу традиційний для кримінального права підхід, що базується на критерії невизначеного кола осіб, (зокрема в мережі Інтернет або за допомогою засобів масової інформації)⁴.

Слід зазначити, що в кримінально-правовій доктрині наявна точка зору, згідно якої публічність виокремлюється як окрема ознака об'єктивної сторони досліджуваного діяння – *обставини вчинення злочину*⁵.

Злочин у цій формі вважається закінченим з моменту вчинення (проголошення, висловлення) винною особою (особами) заклику, адресованого певній кількості осіб⁶. Майже так само вважає і М. А. Рубашенко зазначаючи, що такі інформаційні діяння вважа-

¹ Кваша О. О., Гапончук В. В. Публічні заклики до вчинення злочинів проти основ національної безпеки України (ч. 2, 3 ст. 109, ст. 110 КК України). *Держава і право*. Вип. 83. Київ: Юридична думка, 2019. С. 249.

² Там само. С. 249.

³ Там само. С. 250.

⁴ Рубашенко М. А. Особливості кваліфікації публічних закликів та заперечень як інформаційних діянь. С. 83.

⁵ Злочини проти основ національної безпеки України: альбом схем. С. 7.

⁶ Сичевський В. В., Харитонов С. І., Олейніков Д. О. Науково-практичний коментар до розділу I Особливої частини Кримінального кодексу України. С. 17; Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ наці-

ються закінченими з моменту доведення змісту закликів до відома так званого невизначеного кола осіб¹. Наведені визначення багато в чому схожі, але «проголошення» («висловлення») і «доведення змісту» не одне і те саме: довести зміст можна не лише шляхом проголошення (висловлення), а тому визначення М. А. Рубашенка за обсягом є ширшим².

Розповсюдження матеріалів із закликами до вчинення таких дій. В. Я. Тацій зауважує, що це їх поширення серед інших осіб або створення достатніх умов для ознайомлення з їх змістом (розклеювання листівок, розсилання повідомлень тощо)³. О. Ф. Бантишев та В. С. Картавцев вважають, що це доведення їх змісту – заклику до насильницької зміни чи повалення конституційного ладу чи до насильницького захоплення державної влади – до відома невизначеної чи визначеної групи людей⁴. О. А. Чуваков розширює це визначення додаючи до нього додаткові вимоги: має передбачатися ознайомлення з такими матеріалами інших осіб або створення умов для такого ознайомлення; а також, що це дії, метою яких є доведення змісту матеріалів до відома багатьох людей (невизначеної їх кількості чи певного кола)⁵. Останнє уточнення виглядає відверто зайвим, оскільки про визначену чи невизначену групу людей як адресатів заклику, вже йшлося в першому аспекті аналізованого визначення.

Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков під розповсюдженням відповідних матеріалів розуміють діяльність, яка ви-
ональної безпеки України. С. 68; Чуваков О. А. Злочини проти основ національної безпеки України. С. 236.

¹ Рубашенко М. А. Особливості кваліфікації публічних закликів та заперечень як інформаційних діянь. *Право України*. 2022. № 11. С. 84.

² Пащенко О. О. Свобода вираження поглядів vs публічні заклики до вчинення злочинів проти основ національної безпеки України в інформаційній сфері. *Інформаційна агресія в сучасному світі: правовий аналіз та протидія*: матеріали Всеукр. наук.-практ. круг. столу (Харків, 21 чер. 2024 р.). Харків: Право, 2024. С. 77.

³ Тацій В. Я. Злочини проти основ національної безпеки України. С. 31.

⁴ Бантишев О. Ф., Картавцев В. С. Злочини проти основ національної безпеки України. С. 266.

⁵ Чуваков О. А. Злочини проти основ національної безпеки України. С. 236.

ражається у поширенні відомостей, що містять заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, шляхом передачі їх іншим особам на матеріальних носіях чи з використанням аудіо-, відеопристроїв (записи промов), інформаційно-телекомунікаційних мереж¹.

У цій формі злочин є закінченим з моменту одержання адресатом хоча б частини зазначених підготовлених матеріалів² або з моменту, коли особа створила умови для отримання матеріалів із відповідними закликами, незалежно від того, яка кількість осіб встигла з ними ознайомитись³. Як бачимо, друге визначення моменту закінчення злочину не спростовує перше, оскільки зворот «незалежно від того, яка кількість осіб встигла з ними ознайомитись» при буквальному тлумаченні припускає, що якась кількість осіб із відповідними матеріалами все ж таки встигла ознайомитися. Водночас не виключеним є тлумачення наведеного судження і у такий спосіб, що сам факт ознайомлення значення немає. В такому випадку логічний наголос слід зробити на першій частині речення: «коли особа створила умови для отримання матеріалів із відповідними закликами». Вочевидь, створення умов означає лише наявність реальної можливості для ознайомлення, а не ознайомлення як таке. Тому правникам варто було би конкретизувати свою позицію з розглядуваного питання. Не дуже зрозумілою є також позиція О. Ф. Бантишева та В. С. Картавцева, які зазначають, що сам факт розповсюдження матеріалів із відповідними закликами є закінченим злочином⁴. Науковці повторюють назву суспільно небезпечного діяння, що визначене у ч. 2 ст. 109 КК не уточнюючи, коли саме це діяння є закінченим.

¹ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 18.

² Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 69; Чуваков О. А. Злочини проти основ національної безпеки України. С. 239.

³ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 19.

⁴ Бантишев О. Ф., Картавцев В. С. Злочини проти основ національної безпеки України. С. 266.

Суб'єктивна сторона. На переконання Л. В. Мошняги, обов'язковими ознаками суб'єктивної сторони злочинів, передбачених ст. 109 КК, виступають вина – в умисній формі та спеціальна мета – насильницька зміна або повалення конституційного ладу або захоплення державної влади¹. Вважаємо, що вжитий дослідницею зворот «злочинів» (у множині) переконує, що вона має на увазі не лише ті діяння, що містяться в ч. 1 ст. 109 КК, а й іншими частинами, зокрема 2 і 3. Слід погодитись із запропонованими нею визначеннями видів мети щодо кожного із діянь, передбачених ст. 109 КК: мета «насильницької зміни чи повалення конституційного ладу» полягає в уявленні таких змін у суспільному устрої на шкоду національній безпеці, за яких унеможлиблюється реалізація повновладдя українського народу, суверенітету держави, демократизму, республіканської форми правління, а мета «захоплення державної влади» – в уявленні таких змін у суспільному устрої на шкоду національній безпеці, за яких унеможлиблюється реалізація влади, яка є керівником і провідником волі народу в реалізації Конституції України, іншого законодавства і забезпечення добробуту людей, охорону людини, її життя та здоров'я, честі й гідності, недоторканості і безпеки². Як бачимо, останні уточнення характеризують можливу шкоду певним сферам національної безпеки, про яку зазначалося на початку обох визначень.

О. Ф. Бантишев, О. О. Шамара вважають, що, оскільки ч. 2 ст. 109 КК передбачає відповідальність за публічні заклики до насильницької зміни чи повалення конституційного ладу, до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій, – то це зумовлює наявність у винного відповідної мети. Її ігнорування може спричинити притягнення до кримінальної відповідальності інакодумців; притягнення громадян до кримінальної відповідальності за безпідставну балаканину як за злочин проти основ національної безпеки України. Відсутність та-

¹ Мошняга Л. В. Суб'єктивна сторона злочинів проти конституційних основ національної безпеки України. С. 81.

² Там само. С. 81.

кої мети у винного виключає можливість кваліфікації вчиненого за ст. 109 КК¹. В цьому ж аспекті висловлюються Є. Скулиш і О. Звонарьов². З точки зору В. К. Матвійчука, незважаючи на те, що така найсуттєвіша ознака як мета, у відповідній диспозиції не вказана, але вона сама по собі є зрозумілою із змісту у ч. 2 ст. 109 КК³. На думку В. Н. Кубальського, мета публічних закликів до вчинення злочинів проти державного суверенітету полягає у доведенні до людей певних висловлювань з метою змінити їх поведінку, схилити до здійснення діяльності чи вчинення дій, які посягають на державний суверенітет України, завдаючи йому шкоди⁴. Не заперечуючи проти такої дефініції по суті, водночас відзначаємо, що у тут мета визначається, знов таки, через мету, що навряд чи є послідовним.

З точки зору А. Ю. Швед, «обов'язковими ознаками суб'єктивної сторони складів злочинів, передбачених ст. 109 КК, виступають вина в формі прямого умислу і спеціальна мета – насильницька зміна чи повалення конституційного ладу; захоплення державної влади»⁵. Як бачимо, вона не диференціює значення мети для різних форм суспільно небезпечних діянь, передбачених ст. 109 КК, а отже визнає її обов'язковою ознакою публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади та розповсюдження матеріалів із закликами до вчинення таких дій. У такий самий спосіб слід тлумачити позицію В. М. Янка⁶.

¹ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 128.

² Скулиш Є., Звонарьов О. Злочини проти основ національної безпеки України: навч. посібник. Київ: Нац. акад. СБУ, 2011. С. 99.

³ Матвійчук В. К. Форми вияву злочину «дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади», передбачені частинами 1, 2, 3 статті 109 КК України. С. 68.

⁴ Кубальський В. Н. Проблеми кримінальної відповідальності за публічні заклики до вчинення злочинів проти державного суверенітету. С. 72.

⁵ Швед А. Ю. Злочини проти конституційних засад національної безпеки за законодавством України та Скандинавських країн. С. 10.

⁶ Янко В. М. Кримінальна відповідальність за злочини проти основ суверенітету українського народу. С. 86; Пащенко О. О. Щодо мети публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення дер-

На противагу цьому, Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков також вважають наявність мети обов'язковою лише для першої та другої форм об'єктивної сторони злочину, передбаченого ч. 1 ст. 109 КК, у випадку ж свідомого розповсюдження матеріалів, на їх думку, особа підлягає кримінальній відповідальності незалежно від мотивів, які спонукали її на вчинення злочину, та мети, яку вона переслідувала¹. В. А. Ліпкан, І. В. Діордіца, Р. В. Стецишин, М. І. Хавронюк, М. І. Рубащенко та інші науковці зазначають, що чинна редакція ч. 2 ст. 109 КК не вимагає встановлення спеціальної мети насильницької зміни чи повалення конституційного ладу чи захоплення державної влади. У випадку поширення публічних закликів чи розповсюдження певних матеріалів, суб'єктивна сторона злочину передбачає лише наявність вини у формі прямого умислу².

Не дуже послідовною є позиція О. О. Книженко. Аналізуючи злочин, передбачений ч. 2 ст. 109 КК у формі публічних закликів, вона зазначає, що «заклики мають визначену мету, що полягає у бажанні об'єднати громадян, активізувати їхню волю та стимулювати у них поведінку прямого захоплення державної влади, повалення

державної влади як злочину проти основ інформаційної безпеки України. *Захист прав людини в українській моделі перехідного правосуддя*: матеріали наук.-практ. кругл. столу (Харків, 14 чер. 2024 р.). Харків: Право, 2024. С. 159, 160.

¹ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 20, 24; Пащенко О. О. Щодо мети публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади як злочину проти основ інформаційної безпеки України. С. 161.

² Ліпкан В. А., Діордіца І. В. Національна безпека України: кримінально-правова охорона: навч. посіб. Київ: КНТ, 2007. С. 140; Стецишин Р. В. Мета як ознака суб'єктивної сторони складу злочину, передбаченого ст. 109 КК України. *Актуальні проблеми юридичної науки*: збірник тез Міжнародної наукової конференції «Восьмі осінні юридичні читання» (Хмельницький, 13–14 листоп. 2009 р.): у 4-х ч. Ч. 4-та. Хмельницький: Вид-во Хмельницьк. ун-та управління та права. С. 104; *Науково-практичний коментар Кримінального кодексу України*. 6-те вид., перероб. та допов. / за ред. М. І. Мельника, М. І. Хавронюка. Київ: Юрид. думка, 2009. С. 228; Злочини проти основ національної безпеки України: альбом схем. С. 7, 8; Рубащенко М. А. Особливості кваліфікації публічних закликів та заперечень як інформаційних діянь. *Право України*. 2022. № 11. С. 79.

чи насильницької зміни конституційного ладу»¹. Натомість, підсумовуючи цю частину дослідження, науковець звертає увагу на те, що «спеціальної мети, визначеної у ч. 1 ст. 109 КК України, суб'єкт публічних закликів чи розповсюдження матеріалів із таким закликами не має. Мета, як і мотиви, можуть бути корисливого, особистого характеру, полягати в бажанні змінити життя на краще тощо»². Останнє, з нашої точки зору, може стосуватися лише мотиву, але аж ніяк не мети, оскільки ні корисливий, ні особистий характер, ні бажання змінити життя на краще не може характеризувати той уявний результат, якого прагне досягти суб'єкт, вчиняючи відповідне діяння.

На думку О. А. Чувакова, мета не є обов'язковою ознакою розглянутого складу злочину, «про що в принципі свідчить законодавче формулювання такого складу злочину»³. Цю думку розвиває Р. Л. Чорний, зазначаючи, що висновок щодо обов'язковості наявності мети у досліджуваних випадках не впливає із безпосереднього тлумачення відповідної норми закону, оскільки у диспозиції ст. 109 КК чітко вказано, що «зазначені дії не охоплюють публічних закликів до їх вчинення чи розповсюдження матеріалів із відповідними закликами»⁴. Така побудова аргументації свідчить про те, що дослідник обґрунтовує свою точку зору щодо відсутності мети у ч. 2 ст. 109 КК тим, що вона текстуально наявна лише у ч. 1 цієї статті, де, своєю чергою, не передбачено таких діянь як «публічні заклики» та «розповсюдження матеріалів». Така позиція не виглядає послідовною, тим паче, що прихильники протилежної точки зору не обґрунтовують обов'язковість мети у ч. 2 ст. 109 КК тим, що вона передбачена у ч. 1 цієї статті, а також не вказують, що у ч. 1 встановлено відповідальність за «публічні заклики» і «розповсюдження матеріалів». Тому наведені міркування аж ніяк не спросто-

¹ Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 67.

² Там само. С. 69.

³ Чуваков О. А. Злочини проти основ національної безпеки України. С. 291.

⁴ Чорний Р. Л. Проблемні питання мети і мотивів у складах злочинів проти основ національної безпеки України. *Вісник кримінального судочинства*. 2019. № 4. С. 93.

вують правильність протилежної точки зору. Підсумовуючи викладене, Р. Л. Чорний вказує, що законодавець визначив, що вчиняючи досліджувані діяння «особа може керуватися, наприклад, корисливою метою, бажанням спровокувати масові заворушення з подальшими вигідними для себе політичними наслідками тощо»¹. З цього приводу вважаємо за необхідне зазначити, що, з нашої точки зору, мета є іманентною досліджуваним діянням. Так само як крадіжку неможна вчинити без мети заволодіння майном (обертання майна), так і вчиняти публічні заклики та поширювати матеріали із такими закликами *неможливо без прагнення на досягнення того, що утворює зміст таких закликів*. Наявність прямого умислу в цих випадках обов'язково свідчить і про наявність спеціальної мети – насильницької зміни чи повалення конституційного ладу чи захоплення державної влади. Бажаючи вчиняти передбачені ч. 2 ст. 109 КК суспільно небезпечні діяння суб'єкт злочину обов'язково уявляє собі результат такої поведінки – у адресатів закликів має сформуватися прагнення поводити себе у чітко визначений спосіб – змінити чи повалити насильницьким шляхом конституційний лад або захопити державну владу. Інша річ, що спонукати особу до вчинення відповідних діянь може не саме по собі прагнення насильницької зміни чи повалення конституційного ладу або захоплення державної влади, а інші мотиви (але не мета, як про це зазначають, зокрема, О. О. Книженко та Р. Л. Чорний), скажімо користь, оскільки «спонукання» – це не мета вчинення кримінального правопорушення, а його мотив².

¹ Там само. С. 93, 99.

² Кривоченко Л. М. Мотив і мета злочину. *Кримінальне право України: Загальна частина*: підручник ; за ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. Київ – Харків: Юрінком Інтер – Право, 2001. Розд. X, §6. С. 162; Сухонос В. В., Сухонос В. В. (мол.) *Склад злочину: закон, теорія та практика*: монографія. Суми: Університетська книга, 2018. С. 89; Ломако В. А., Панов М. І. Мотив та мета кримінального правопорушення. *Кримінальне право України: Загальна частина*: підручник ; за ред. В. Я. Тація, В. І. Тютюгіна, В. І. Борисова. 6-те вид., перероб. і допов. Харків: Право, 2020. Розд. X, §6. С. 200; Пашенко О. О. Щодо мети публічних закликів до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади як злочину проти основ інформаційної безпеки України. С. 161, 162.

Суб'єкт. О. Ф. Бантишев, О. О. Шамара, О. О. Книженко вважають, що за чч. 1, 2 ст. 109 КК – будь-яка фізична осудна особа, яка досягла шістнадцятирічного віку¹. Натомість М. В. Даньшин, Я. О. Лантінов, Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков пишуть, що суб'єкт досліджуваного злочину загальний², В. Я. Тацій зауважував, що ним може бути «будь-яка особа, що досягла 16-річного віку»³.

1.1.2. Публічні заклики чи розповсюдження матеріалів із закликами до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України (ч. 1 ст. 110 КК України)

Охорона основ національної безпеки України як одну із основоположних своїх складових передбачає охорону цілісності й недоторканості території нашої держави, непорушності існуючого державного кордону України⁴.

Основний безпосередній об'єкт злочину, передбаченого ч. 1 ст. 110 КК у кримінально-правовій доктрині визначається як: основні інтереси України у сфері забезпечення її суверенітету над своєю

¹ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 116; Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 70.

² Злочини проти основ національної безпеки України: альбом схем. С. 7, 8; Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу I Особливої частини Кримінального кодексу України. С. 24.

³ Тацій В. Я. Злочини проти основ національної безпеки України. С. 32.

⁴ Пономаренко Ю. А. Про деякі кримінально-правові наслідки окупації та деокупації території України. *Актуальні проблеми кримінально-правової охорони основ національної безпеки України*. С. 33.

територією і недоторканості її державного кордону¹; встановлений Конституцією України порядок зміни меж території України²; суспільні відносини у сфері охорони територіальної цілісності й недоторканості України³; безпеку територіальної цілісності України⁴; суспільні відносини суверенітету Українського народу в частині забезпечення територіальної цілісності⁵, безпеку держави у політичній і воєнній сферах⁶, суспільні відносини щодо забезпечення територіальної цілісності України в межах встановлених державних кордонів⁷.

Окремо визначає основний безпосередній об'єкт розглядуваного злочину у третій та четвертій формах М. А. Рубашенко: суспільні відносини, які забезпечують охорону територіальної цілісності України у сфері реалізації конституційного права вільно поширювати інформацію⁸.

Предмет. Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков – відповідна ділянка території України, на яку здійснюється посягання (прикордонний район, адміністративно-територіальна одиниця, населений пункт)⁹. М. А. Рубашенко: у третій формі – інформація, зміст якої характеризується спрямованістю інформаційного впливу на те, щоб викликати в людей яким інформація повідомляється, бажання (намір) учинити дії з метою зміни меж території або державного кор-

¹ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 150.

² Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу I Особливої частини Кримінального кодексу України. С. 33.

³ Чуваков О. А. Злочини проти основ національної безпеки України. С. 169.

⁴ Злочини проти основ національної безпеки України: альбом. С. 10, 11.

⁵ Янко В. М. Кримінальна відповідальність за злочини проти основ суверенітету українського народу. С. 73.

⁶ Бантишев О. Ф., Картацев В. С. Злочини проти основ національної безпеки України. С. 267; Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 74.

⁷ Тацій В. Я. Злочини проти основ національної безпеки України. С. 32.

⁸ Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканість України: монографія. Харків: Право, 2016. С. 68.

⁹ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу I Особливої частини Кримінального кодексу України. С. 34.

дону України на порушення порядку, встановленого Конституцією України¹; у четвертій формі – матеріали, у яких зафіксована така інформація². В. Я. Тацій – у формі публічних закликів – інформація, що містить хоча б один заклик відповідного змісту; у формі розповсюдження матеріалів – певний рухомий носій інформації (газета, листівка, електронне повідомлення тощо), що містить такий заклик³.

Об'єктивна сторона злочину передбачає два альтернативні суспільно небезпечні діяння: *публічні заклики* до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України (1) та *розповсюдження матеріалів із закликами* до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України (2).

Публічні заклики до вчинення визначених у ст. 110 КК дій – це спроба активно впливати на свідомість і волю інших людей із метою їхнього схвалення до бажаної для винного поведінки. Висловлення своїх думок, переконань, бажань не може розцінюватися як публічні заклики. Заклики – це активне нав'язування своїх ідей іншим особам, коли обов'язково вказується, як варто діяти, що робити, щоб досягти конкретного результату, якого прагне особа, яка виголошує такі заклики⁴.

М. А. Рубашенко відзначає, що заклик – це повідомлення адресату в будь-якій формі інформації, зміст якої спрямований викликати в іншої особи (осіб) бажання (намір) учинити дії з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України⁵. Способом учинення самого заклику є публічність – у випадках, коли значна кількість людей

¹ Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканість України. С. 68.

² Там само. С. 68, 69.

³ Тацій В. Я. Злочини проти основ національної безпеки України. С. 32.

⁴ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 83.

⁵ Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканість України. С. 158.

(публіка) виступає адресатом інформаційного впливу та інформаційного повідомлення¹. Словосполучення «на порушення порядку, встановленого Конституцією України» пропонується розуміти як на порушення порядку, встановленого ч. 3 ст. 5 та ст. 73 Конституції, тобто без згоди Українського народу, вираженої на всеукраїнському референдумі. Це можливе шляхом *фальсифікації* останнього або *без його проведення* (в будь-який інший спосіб)². Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков тлумачать поняття заклик як виражені в будь-якій формі (усній, з використанням технічних засобів, інформаційно-телекомунікаційних мереж) звернення до інших осіб, вчинені у відкритий спосіб у місці, яке дозволяє вільно сприймати їх необмеженому колу осіб, розраховані на спонування цих осіб до вчинення дій, спрямованих на зміну меж території України на порушення порядку, встановленого Конституцією України, здійснювані шляхом розповсюдження відомостей про доцільність, необхідність чи бажаність посягання на територіальну цілісність і недоторканість України³. З точки зору О. О. Книженко – це хоча б одне відкрите звернення до невизначеного, але значного кола осіб, в якому висловлюються ідеї погляди чи вимоги, спрямовані на те, щоб шляхом поширення їх серед населення чи його окремих категорій (представників влади, військовослужбовців тощо) схилити його (населення) до певних дій⁴.

Розповсюдження матеріалів із закликами, про які мова йде в диспозиції ст. 110 КК полягає в ознайомленні багатьох людей (невизначеної кількості або певного кола) із друкowanими, фотографічними матеріалами, відео- й аудіо-записами, в яких містяться такі заклики⁵. М. А. Рубашенко відзначає, що під «розповсюдженням...» у ст. 110 КК слід розуміти індивідуалізоване поширення (надання-

¹ Там само. С. 159.

² Там само. С. 157.

³ Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 43, 44.

⁴ Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 79.

⁵ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 84.

одержання) або інше відчуження значної кількості «матеріалів...»¹. Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков – це діяльність, яка виражається у поширенні відомостей, що містять заклики до зміни меж території України на порушення порядку, встановленого Конституцією України, шляхом передачі їх іншим особам на матеріальних носіях (розповсюдження листівок, прокламацій, поліграфічної продукції) чи з використанням аудіо-, відеопристроїв (записи промов), інформаційно-телекомунікаційних мереж (розміщення та поширення текстових чи графічних матеріалів із необхідними поясненнями в соціальних мережах, на сайтах, форумах мережі Інтернет)². О. О. Книженко – це дії, метою яких є доведення змісту відповідних матеріалів до відома багатьох людей (невизначеної їх кількості або певного кола)³.

Суб'єктивна сторона. В. Я. Тацій, В. А. Ліпкан, І. В. Діордіца, М. В. Даньшин, Я. О. Лантінов, а також О. Ф. Бантишев, В. С. Картавцев, О. О. Шамара вважають, що цей елемент складу досліджуваного кримінального правопорушення утворюють такі ознаки: *вина* – прямий умисел та спеціальна *мета* – зміна меж території або державного кордону України на порушення порядку, встановленого Конституцією України⁴. О. А. Чуваков, В. М. Янко – *вина* в формі прямого умислу та спеціальна *мета*⁵. М. А. Рубашенко, а також

¹ Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканість України. С. 159.

² Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 44.

³ Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 79.

⁴ Тацій В. Я. Злочини проти основ національної безпеки України. С. 33; Ліпкан В. А., Діордіца І. В. Національна безпека України: кримінально-правова охорона. С. 160; Бантишев О. Ф., Картавцев В. С. Злочини проти основ національної безпеки України. С. 267; Злочини проти основ національної безпеки України: альбом схем. С. 9; Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 128.

⁵ Чуваков О. А. Злочини проти основ національної безпеки України. С. 299; Янко В. М. Кримінальна відповідальність за злочини проти основ суверенітету українського народу. С. 86.

Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков, О. О. Книженко – лише вина у формі прямого умислу¹.

Суб'єкт. О. Ф. Бантишев, О. О. Шамара, М. В. Даньшин, Я. О. Лантінов, Є. В. Сичевський, Є. І. Харитонов, Д. О. Олейніков, О. О. Книженко, В. Я. Тацій зазначають, що за ч. 1 ст. 110 КК ним може бути будь-яка фізична осудна особа, яка досягла шістнадцятирічного віку².

Вважаємо за необхідне підтримати уточнення ознак суб'єкта розглядуваного злочину (ч. 1 ст. 110 КК), зроблене М. А. Рубашенком: він є загальним – фізична осудна особа, яка досягла шістнадцятирічного віку і водночас характеризується обмеженням кола осіб ознакою «крім представників влади»³.

1.2. Інформаційні кримінально-протиправні діяння, що посягають на зовнішню безпеку України (ст.ст. 111, 114 КК України)

Державна зрада та шпигунство належать до кримінальних правопорушень, що мають високий ступінь суспільної небезпечності. Відповідальність за державну зраду передбачена ст. 111 КК. За нормою ч. 1 цієї статті державна зрада є діянням, яке умисно вчиняється

¹ Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканість України. С. 180, 181; Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 46; Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 80.

² Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації). С. 117; Злочини проти основ національної безпеки України: альбом. С. 10, 11; Сичевський В. В., Харитонов Є. І., Олейніков Д. О. Науково-практичний коментар до розділу І Особливої частини Кримінального кодексу України. С. 49; Книженко О. О. Кваліфікація діянь, що містять ознаки злочинів проти основ національної безпеки України. С. 80; Тацій В. Я. Злочини проти основ національної безпеки України. С. 33.

³ Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканість України. С. 181.

громадянином України на шкоду суверенітету, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в період збройного конфлікту (далі – «перехід на бік ворога»), шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України (далі – «надання допомоги»). Не менш небезпечним кримінальним правопорушенням є шпигунство, що вчиняється іноземцем або особою без громадянства. Відповідальність за вчинення такими особами шпигунства передбачена ст. 114 КК. За нормою ч. 1 цієї статті шпигунством є передача або збирання з метою передачі іноземній державі, іноземній організації або їх представника відомостей, що становлять державну таємницю. Зазначене визначення є однаковим за об'єктом, предметом, формами вчинення і видом вини також і для шпигунства, що визначене у ст. 111 КК.

Згідно з ч. 6 ст. 12 КК державна зрада і шпигунство (за ст. 114 КК) є особливо тяжкими злочинами¹. Значну небезпеку ці діяння набувають у часи вирішальних випробувань для існування України як незалежної держави. На сьогодні це воєнний стан, в якому перебуває Україна з 24 лютого 2022 року.

Одним із показників такої небезпеки є поширеність злочинів проти основ національної безпеки України. Так, якщо термін дії чинного КК, починаючи з 2001 р., розподілити умовно на три періоди, зв'язавши їх із соціально-політичним станом України та вчиненням у ці періоди її громадянами *державної зради*, то показники поширеності цього злочину виглядають так:

– з 2001 р. по 2013 р., час, коли розвиток держави Україна був відносно спокійним. Цей період характеризується поодинокими випадками вчинення суспільно небезпечних діянь, кваліфікованих за

¹ Відповідно до Закону України № 2617-VIII від 22.11.2018 р. в КК як загальне використовується поняття «кримінальне правопорушення» (див. ст. 11 КК). Однак, оскільки згідно зі ст. 12 КК «Класифікація кримінальних правопорушень» і з назвою розділу I Особливої частини КК «Злочини проти основ національної безпеки України» діяння «Державна зрада» і «Шпигунство» визнані злочином, то й безпосередня характеристика його ознак пов'язується з цим видом кримінального правопорушення.

ст. 111 КК. Однак за ступенем тяжкості такі випадки відрізнялися особливо істотною шкодою, що була або могла бути спричинена інтересам національної безпеки України. Так, апеляційний суд Житомирської області визнав трьох колишніх військовослужбовців-співробітників запорізького держпідприємства «Мігремонт» винними в державній зраді. Ці працівники за завданням спецслужб іноземної держави збирали секретну військово-технічну інформацію. За передачу інформації їм було обіцяно 800 тис. доларів США винагороди. У разі витоку цієї інформації Україна могла б зазнати надзначних збитків в економічній і оборонній сферах своєї життєдіяльності¹;

– з 2014 р. по 2021 р., період активного проведення на сході нашої країни антитерористичної операції та операції Об'єднаних сил. У цей період поширення набуло вербування спецслужбами Російської Федерації (далі – РФ) українських військових для вчинення ними зрадницьких дій. Зокрема, приклад державної зради військовослужбовцем містить вирок Старокостянтинівського районного суду Хмельницької області від 22 червня 2016 року. К., будучи льотчиком Збройних Сил України, був завербований спецслужбами РФ. Маючи доступ до інформації зі ступенем секретності «Цілком таємно» та «Таємно», він завчасно повідомляв представників ворожої сторони про обставини проведення спеціальних розвідувальних польотів (час та маршрут польоту вздовж державного кордону України), відомості про які становлять державну таємницю. Дії К. були кваліфіковані за ст. 111 КК². Кількість випадків державної зради у цей період стала сягати до декількох десятків, а то й більше ста на рік. Так, у тому ж 2016 році було занесено до первинного обліку злочинів 126 фактів вчинення громадянами України державної зради³, засуджено 3 осо-

¹ Юридичний вісник України. Вип. від 6–12 лютого 2012 р. № 6 (762). С. 3.

² Вирок Старокостянтинівського районного суду Хмельницької області від 22 червня 2016 року (справа № 683/2848/15-к; провадження № 1-кп/683/18/2016). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/58673008> (дата звернення: 04.11.2024)

³ Єдиний звіт про кримінальні правопорушення за січень-грудень 2016 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/>

би¹. Всього за цей період таких випадків було обліковано 964², засуджено за їх вчинення 28 осіб³.

pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 04.11.2024)

¹ 2016 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/2016_zvit (дата звернення: 04.11.2024)

² Єдиний звіт про кримінальні правопорушення за січень-грудень 2014 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2015 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2016 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2017 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2018 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2019 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2020 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2021 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата звернення: 04.11.2024).

³ 2014 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/lkflghkjlh; 2015 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/Sud_statustuka/Zvit_2015; 2016 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/2016_zvit; 2017 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2017; 2018 рік. Форма № 7 «Звіт про склад засуджених». *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2018; 2019 рік. Форма № 7 Звіт про склад засуджених за 2019 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2019; 2020 рік. Форма № 7 Звіт про склад засуджених за 2020 рік. *Судова влада України*:

Варто зазначити, що в ці роки набули певного поширення й інші посягання проти основ національної безпеки України, а тому законодавець, оцінюючи обстановку, що склалася в державі, заважав необхідним посилити караність діянь, визначених у нормах розділу І «Злочини проти основ національної безпеки». Зокрема, Законом України від 8 квітня 2014 р. були скасовані строки давності за ці злочин¹. Що стосується ст. 111 КК, то у санкції її ч. 1 була підвищена мінімальна межа позбавлення волі з 10 до 12 років² та встановлено додаткове факультативне покарання у виді конфіскації майна³. Також була змінена санкція ч. 1 ст. 114 КК. Наразі вона передбачає покарання позбавленням волі на строк від 10 до 15 років з конфіскацією майна або без такої⁴;

– з 2022 по 2024 р. 24 лютого 2022 р. почалося повномасштабне вторгнення військ Російської Федерації до України. Указом Президента України № 64/2022 було введено воєнний стан, затверджений у цей же день Верховною Радою України⁵. У цьому надзвичайно-

оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2020; 2021 рік. Форма № 7 Звіт про склад засуджених за 2021 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvitnist_21 (дата звернення: 04.11.2024).

¹ Про внесення змін до Кримінального кодексу України: Закон України від 08.04.2014 р. № 1183-VII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/1183-18#Text> (дата звернення: 04.11.2024).

² Там само.

³ Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо невідворотності покарання за окремі злочини проти основ національної безпеки, громадської безпеки та корупційні злочини: Закон України від 07.10.2014 р. № 1689-VII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/1689-18#Text> (дата звернення: 04.11.2024).

⁴ Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо невідворотності покарання за окремі злочини проти основ національної безпеки, громадської безпеки та корупційні злочини: Закон України від 07.10.2014 р. № 1689-VII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/1689-18#n14> (дата звернення: 04.11.2024).

⁵ Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 р. № 64/2022. *Верховна Рада України. Законодавство України*: оф.

му стані, що неодноразово подовжувався, Україна знаходиться й дотепер. Характерним для означеного періоду є значне зростання більшості злочинів проти основ національної безпеки України, включно з державною зрадою. Так, у 2022 році за ст. 111 КК було занесено до первинного обліку 1957 зрадницьких дій¹, у 2023 році показник таких дій сягнув 3207². Суттєво збільшилися й показники засудження за цей злочин. У 2022 році за ст. 111 КК було засуджено 111 осіб³, у 2023 році – 179⁴. Показовим убачається наступний приклад вчинення державної зради. Вінницьким міським судом Вінницької області було 11 травня 2022 р. засуджено за державну зраду громадянина України Особа_5, уродженця м. Макіївка Донецької області. Особа_5 у перший день початку збройно агресії РФ проти України, достовірно знаючи про свій громадянський статус, добровільно звернувся до військомату терористичної організації «ДНР» у м. Макіївка, де отримав звання «рядовий» та відразу був зарахований до військового підрозділу армії так званої «ДНР» у складі Збройних Сил РФ. У подальшому він виконував за наказом ворога бойові завдання на території Миколаївської області, де й був затриманий військовослужбовцями збройних сил України⁵.

вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/64/2022#Text> (дата звернення: 04.11.2024).

¹ Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-1> (дата звернення: 04.11.2024).

² Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата звернення: 04.11.2024).

³ 2022 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2022 (дата звернення: 04.11.2024).

⁴ 2023 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2023 (дата звернення: 04.11.2024).

⁵ Вирок Вінницького міського суду Вінницької області від 11.05.2022 року (справа № 127/7728/22; провадження № 1-кп/127/201/22. *Єдиний державний реєстр*

Значно непоказною виглядає статистика щодо *шпигунства*, вчиненого іноземцями або особами без громадянства. У роки з 2001 по 2013 – це були вкрай поодинокі випадки реєстрації таких діянь та засудження за їх вчинення. У роки з 2014 по 2021 показники обліку шпигунства за ст. 114 КК дещо збільшилися. Зазвичай вони складали 2–9 випадків на рік¹. Однак кількість засуджених становила не більше однієї особи, та й то не кожний рік². Так, у 2016 році було

судових рішень: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/104251862> (дата звернення: 04.11.2024).

¹ Єдиний звіт про кримінальні правопорушення за січень-грудень 2014 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2015 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2016 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2017 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2018 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2019 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2020 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2021 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2> (дата звернення: 04.11.2024).

² 2014 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/lkfghkjllh; 2015 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/Sud_statustuka_Zvit_2015; 2016 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/2016_zvit; 2017 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2017; 2018 рік. Форма № 7 «Звіт про склад засуджених». *Судова вла-*

обліковано 2 випадки шпигунства, кваліфікованого за ст. 114 КК¹, не засуджено жодної особи². Шпигунство, вчинене в умовах воєнного стану набуло таких показників: у 2022 р. було обліковано 40 випадків, не засуджено жодного³; у 2023 р. обліковано 38 випадків, засуджено одну особу⁴. Порівнюючи зазначені показники щодо шпи-

да України: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2018; 2019 рік. Форма № 7 Звіт про склад засуджених за 2019 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2019; 2020 рік. Форма № 7 Звіт про склад засуджених за 2020 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2020; 2021 рік. Форма № 7 Звіт про склад засуджених за 2021 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvitnist_21 (дата звернення: 04.11.2024).

¹ Єдиний звіт про кримінальні правопорушення за січень-грудень 2016 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/prozareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата звернення: 04.11.2024).

² 2014 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/lkflghkjlh; 2015 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/Sud_statustuka_Zvit_2015; 2016 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/2016_zvit; 2017 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2017; 2018 рік. Форма № 7 «Звіт про склад засуджених». *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2018; 2019 рік. Форма № 7 Звіт про склад засуджених за 2019 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2019; 2020 рік. Форма № 7 Звіт про склад засуджених за 2020 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2020; 2021 рік. Форма № 7 Звіт про склад засуджених за 2021 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvitnist_21 (дата звернення: 04.11.2024).

³ Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/prozareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; 2022 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2022 (дата звернення: 04.11.2024).

⁴ Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/prozareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; 2023 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф.

гунств, кваліфікованих за ст. 111 КК та ст. 114 КК, можна зробити невтішний висновок про те, що потреби інших держав в отриманні протиправними способами відомостей, що становлять державну таємницю в Україні, вирішується здебільшого через зрадницькі дії громадян України.

Після 22 лютого 2022 р. в Україні склалася непроста ситуація, на яку законодавець доволі швидко зреагував. Вже 3 березня 2022 р. Законом України № 2113-ІХ до КК були внесені численні зміни та доповнення, що ураховували вчинення кримінальних правопорушень в умовах воєнного стану¹. Була піддана змінам й норма ст. 111 КК шляхом доповнення її тексту частиною 2: «Ті самі діяння, вчинені в умовах воєнного стану, – караються позбавленням волі на строк п'ятнадцять років або довічним позбавленням волі, з конфіскацією майна». Варто зауважити, що наведена новела «в умовах воєнного стану» є обставиною, яка суттєво обтяжила кримінальну відповідальність за державну зраду. Натепер (умови воєнного стану) всі зрадницькі діяння, вчинені після набрання чинності Законом № 2113-ІХ, незалежно від форми їх здійснення та ступеня тяжкості, підлягають кваліфікації за ч. 2 ст. 111 КК. Наведене доповнення очевидне, воно прямо визначене в тексті Закону. Більш складними є зміни змістовного характеру, встановлення яких потребує різного рівня наукових розвідок, відповідно до ознак складу злочину «Державна зрада». Що стосується норми ст. 114 КК У, то вона не була піддана змінам, спрямованим на посилення відповідальності за шпигунство, що вчиняється іноземцями або особами без громадянства. Уявляється, що таке рішення було пов'язане з доволі суворою санкцією на той час (як і натепер) за це діяння, а, отже, сенсу змінювати її з урахуванням явно незначної поширеності цього виду шпигунства не було.

вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2023 (дата звернення: 04.11.2024).

¹ Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за злочини проти основ національної безпеки України в умовах дії режиму воєнного стану: Закон України від 03.03.2022 р. № 2113-ІХ. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2113-20#Text> (дата звернення: 04.11.2024).

Об'єкт злочину. Виходячи з назви розділу «Злочини проти основ національної безпеки України» та складових цієї сфери суспільних відносин, що безпосередньо зазначені в диспозиції норми ч. 1 ст. 111 КК, можна зробити висновок, що *основним безпосереднім об'єктом державної зради є суспільні відносини, що забезпечують основи зовнішньої безпеки України*¹, як і шпигунства, передбаченого ст. 114 КК. Взаємопов'язаними компонентами цих відносин є такі загальнонаціональні цінності: суверенітет України, територіальна цілісність та недоторканність; обороноздатність; державна, економічна та інформаційна безпека. Державна зрада і шпигунство спричиняють або здатні спричинити шкоду одній або декільком зазначеним загальнонаціональним цінностям.

В умовах здійснення РФ збройної агресії проти України поширення набули зрадницькі діяння, спрямовані на спричинення шкоди інформаційній безпеці як безпосередньо, так і у поєднанні з обороноздатністю та економічною безпекою України. Також шкода інформаційній безпеці спричиняється у всіх випадках вчинення шпигунства, що кваліфікуються за нормою ст. 114 КК.

Інформаційна безпека в системі загальнонаціональних цінностей, зазначених у диспозиції норми ч. 1 ст. 111 КК, являє *стан захищеності* національних інтересів в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз, що відповідає принципу забезпечення національної безпеки в інформаційній сфері². Відразу треба зазначити, що наведене визначення, як і більшість інших, йому подібних, є широким, а тому його можна використовувати при характеристиці кримінально-протиправних діянь проти національної безпеки, здійснення яких спричиняє або може спричинити шкоду відповідним відносинам, функціонування яких пов'язано з інформа-

¹ Борисов В. І. *Правова модель складу злочину «Державна зрада» та інформація в системі її ознак*. *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.): Харків: Право, 2023. С. 90.

² Ніщименко О. А. *Інформаційна безпека України на сучасному етапі розвитку держави і суспільства*. *Наше право*. 2016. № 1. С. 17–23.

цією¹. Наприклад, одним із таких діянь можуть бути публічні заклики до вчинення терористичного акту з метою провокації воєнного конфлікту чи міжнародного ускладнення (ст. 258² КК).

Наведене дозволяє зазначити, що інформаційна безпека для кожного діяння, визнаного кримінальним правопорушенням та пов'язаного з інформацією, обмежується певною сферою, у межах якої відбувається посягання. Це різноманітні суспільні відносини, що забезпечують ті або інші інтереси особи, інтереси суспільства та держави. Якщо звернутися до диспозиції ч. 1 ст. 111 КК, то три форми діянь, що в ній визначені: «перехід на бік ворога»; шпигунство; «надання допомоги», по-різному пов'язані з інформацією. Так, «перехід на бік ворога» та «надання допомоги» можуть бути здійснені з використанням інформації, але така прив'язка не є обов'язковою. У тих же випадках, коли при вчиненні зазначених діянь застосовується інформація, внаслідок чого спричиняється або може бути спричинена шкода інформаційній безпеці, цей сегмент ураження в межах відносин, що складають основи зовнішньої безпеки України, не є, як правило, домінуючим чинником. Такими є зазвичай шкода, що спричиняється або може бути спричинена обороноздатності, економічній безпеці та іншим загальнонаціональним цінностям, що безпосередньо впливає із цілеспрямованості здійсненого суспільно небезпечного діяння. А, отже, «перехід на бік ворога» та «надання допомоги», навіть якщо вони здійснюються з використанням інформації, не можуть визнаватися інформаційними кримінальними правопорушеннями. Таким правопорушенням є шпигунство, вчинене громадянином України відповідно до ознак, зазначених у ч. 1 ст. 111 КК². Так само інфор-

¹ Борисов В. І. Вибрані твори. Книга 2 / уклад.: М. В. Шепітько, О. О. Пашченко, Д. П. Євтеєва, Д. О. Куковинець; відп. за вип. М. В. Шепітько. Харків: Право, 2023. 840 с.

² Борисов В. І. Забезпечення охорони інформаційної безпеки нормою ст. 111 «Державна зрада». Цифровізація кримінального провадження: стан та перспективи: матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш]; НДІ вивч. проблем злочинності ім. акад. Сташиса НАПрН України; Від. дослідж. проблем кримін. процесу та судоустрою. Харків: Право, 2024. С. 26.

маційним кримінальним правопорушення є шпигунство, суб'єктом вчинення якого є іноземець або особа без громадянства (ст. 114 КК).

Предмет злочинів, передбачених нормами ст.ст. 111 та 114 КК. Поряд з об'єктом кримінального правопорушення теорія кримінального права виділяє потерпілого та предмет. Варто зауважити, що питання стосовно змісту таких ознак саме складу державної зради (ст. 111 КК), як правило, не порушуються¹. Однак, якщо звернутися до діяння у формі шпигунство, то воно завжди пов'язано з предметом, а саме державною таємницею. Традиційно зміст поняття *державна таємниця* розглядається при аналізі шпигунства, як окремого злочину, передбаченого ст. 114 КК². Втім, напрацювання щодо розуміння цього предмета є однаковими як для норми ст. 111 КК, так і норми ст. 114 КК.

Державна таємниця складається із відомостей, що загальним чином перераховані в Законі України «Про державну таємницю» від 21 січня 1994 р. № 3855-ХІІ³ та конкретизовані в підзаконних нормативно-правових актах Кабінету Міністрів України, міністерств, комітетів, інших відомств. Згідно зі ст. 1 зазначеного Закону державною таємницею визнається певний вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державною⁴. Спеціальним уповноваженим органом державної влади в сфері забезпечення охорони державної таємниці є Служба безпеки України⁵. Процедуру засекре-

¹ Тацій В. Я., Рубашенко М. А. Види злочинів проти основ національної безпеки. Кримінальне право України: Особлива частина: підручник / В. Я. Тацій, В. І. Борисов, В. І. Тютюгін та ін.; за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна, 6-те вид., перероб. і допов. Харків: Право, 2020. 786 с. С. 35.

² Там само. С. 39.

³ Про державну таємницю: Закон України від 21.01.1994 р. № 3855-ХІІ. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text> (дата звернення: 04.11.2024).

⁴ Там само.

⁵ Відомості Верховної Ради України. 1994. № 16. Ст. 97.

чення здійснюють державні експерти з питань таємниць¹. Такими експертами за посадами, наприклад, у сфері оборони, відповідно до Зводу відомостей, що становлять державну таємницю, затвердженого Наказом Центрального управління Служби безпеки України 23.12.2020 р. № 383², є державні експерти з питань таємниць Державної прикордонної служби України, Збройних Сил України, Служби зовнішньої розвідки України тощо. Засекречення матеріальних носіїв інформації здійснюється шляхом надання відповідному документу, виробу чи іншому матеріальному носію інформації грифа секретності («особливої важливості», «цілком таємно», «таємно»)³.

Інформація, як предмет цих злочинів (так само, як і інформація, що є предметом кримінальних правопорушень, передбачених нормами ст.ст. 328, 329, 422 КК), за своїм змістом, значущістю для інтересів суспільства й держави та цілеспрямованого злочинного поводження з нею (збирання, передача – ст.ст. 111, 114 КК) на користь іноземної держави, іноземної організації або їх представників, дає можливість виділити її як особливий предмет підвищеного захисту з боку держави та уповноважених на то органів спеціального призначення. Зазначене дозволяє зробити висновок, що в межах системи суспільних відносин, які охороняються нормами ст.ст. 111 та 114 КК, додатково-обов'язковим безпосереднім об'єктом саме шпигунства слід визнавати спеціальний вид інформаційної безпеки, а саме

¹ Борисов В. І. Забезпечення охорони інформаційної безпеки нормою ст. 111 «Державна зрада». *Цифровізація кримінального провадження: стан та перспективи*: матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 27.

² Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ від 23.12.2020 № 383. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/z0052-21#Text> (дата звернення: 04.11.2024).

³ Кримінальне право України: Особлива частина: навч. посіб. / за ред. д.ю.н., проф. В. К. Грищука, д.ю.н., проф. О. М. Омельчука. Хмельницький: Хмельницький університет управління і права. 2016. С. 34.

*основи інформаційної безпеки*¹. Що стосується вчинення діянь «перехід на бік ворога» та «надання допомоги», то спричинення шкоди відносинам по забезпеченню інформаційної безпеки, як вже було зазначено, не є для них обов'язковою ознакою. Більш того, можливість вчинення діянь «перехід на бік ворога» і «надання допомоги», пов'язаних саме із інформацією, різко зменшилася в останні роки, через те, що законодавець увів до КК ст. 111¹ (з 03.03.2022 р.), ст. 111² (з 14.04.2022 р.) та ст. 114² (з 24.03.2022 р.), у нормах яких зазначені діяння, що до часу їх переміщення до нових статей кваліфікувалися як державна зрада.

Зазначене дозволяє стверджувати, що шпигунство за ст. 111 КК, незважаючи на єдність основного безпосереднього об'єкта кримінально-правової охорони – основи зовнішньої безпеки України, не є діянням суміжним з іншими, що визначені в диспозиції норми ч. 1 ст. 111 КК². Мабуть, міркування щодо особливостей об'єкта, поставленого під охорону нормами ст.ст. 111 та 114 КК, специфіки предмета, щодо якого здійснюються шпигунські діяння, та їх прихованості тощо, дало підстави авторам проекту нового КК запропонувати в розділі 9.1. «Злочини проти національної безпеки України» окрему норму «Шпигунство» (ст. 9.1.8.) поряд із нормою «Зрада Україні» (ст. 9.1.5.), в якій діяння «шпигунство» не зазначене³.

Об'єктивна сторона. Диспозицією норми ч. 1 ст. 111 КК передбачена можливість вчинення державної зради у трьох самостійних

¹ Борисов В. І. Забезпечення охорони інформаційної безпеки нормою ст. 111 «Державна зрада». *Цифровізація кримінального провадження: стан та перспективи*: матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 27.

² Борисов В. І. Правова модель складу злочину «Державна зрада» та інформація в системі її ознак». *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.): Харків: Право, 2023. С. 91.

³ Текст проекту нового Кримінального кодексу України (станом на 01.08.2024 р.). Робоча група з питань розвитку кримінального права: оф. вебсайт. URL: <https://newcriminalcode.org.ua/criminal-code> (дата звернення: 04.11.2024).

формах: «перехід на бік ворога», шпигунство, «надання допомоги». Що стосується об'єктивної сторони шпигунства, передбаченого нормою ст. 114 КК, то вона полягає в діях, які можуть бути вчинені у двох формах: передача іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю; збирання з метою передачі таких відомостей із метою передачі зазначеним адресатам. Поділ шпигунства на дві форми характерний не тільки для злочину, передбаченого ст. 114 КК, але й для шпигунства, визначеного узагальнено в ст. 111 КК. Для наявності об'єктивної сторони цих злочинів достатньо вчинення одного із діянь, зазначених у диспозиції ч. 1 ст. 111 КК або ч. 1 ст. 114 КК. Перелік наведених діянь у диспозиціях цих норм є вичерпним, кожне з них є обов'язковою і водночас самостійною ознакою об'єктивної сторони злочину. Усі діяння визнаються закінченими з моменту їх здійснення. Таким чином, з об'єктивної сторони державна зрада та шпигунство належать до кримінальних правопорушень з формальним складом¹.

Обов'язковими ознаками, пов'язаними з вчиненням діянь, зазначених у диспозиції норми ст. 111 КК, є також обстановка та час їх вчинення². Для діяння «перехід на бік ворога» – це період збройного конфлікту. У разі вчинення такого діяння в умовах воєнного стану дії винного кваліфікуються за ч. 2 ст. 111 КК. Кожна із зазначених обставин характеризується певною небезпечністю обстановки та має обмеження в часі³. Наявність воєнного стану суворо регламентована українським законодавством, відповідно до якого воєнний стан

¹ Борисов В. І. Правова модель складу злочину «Державна зрада» та інформація в системі її ознак». *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.): Харків: Право, 2023. С. 91.

² Матвійчук В. К. Злочини проти основ національної безпеки України: поняття та загальна характеристика. *Юридична наука*. 2013. № 9. С. 80–87.

³ Борисов В. І. Правова модель складу злочину «Державна зрада» та інформація в системі її ознак». *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.): Харків: Право, 2023. С. 92.

має час його введення та час припинення або скасування¹. Розуміння збройного конфлікту впливає із Стратегії воєнної безпеки України, затвердженої Указом Президента України 25 березня 2021 р.², в якій передбачені ймовірні сценарії таких конфліктів: 1) спровокований та підтриманий ззовні збройний конфлікт у межах території України; 2) втягнення України в міжнародний збройний конфлікт; 3) збройний конфлікт на державному кордоні. Із наведеного випливає, що збройний конфлікт може бути міжнародним і внутрішнім (неміжнародним)³.

Визначальною рисою цієї ознаки є обстановка, що може виникнути в державі, наявність та протидія якій на певний момент (період, час) повинні бути встановлені державними органами. Однак збройному конфлікту притаманний і час, пов'язаний із його виникненням, локалізацією або переведенням у воєнний стан⁴.

Після змін, внесених 3 березня 2022 року до ст. 111 КК, виникли також питання щодо правової оцінки діяння «надання допомоги». Потрібно зауважити, що за зовнішнім проявом вчинення цього діяння багато в чому сходиться з «переходом на бік ворога», а тому знання про час вчинення цих діянь набуває вирішального значення для їх правової оцінки.

¹ Конституція України (ст.ст. 64, 83, 85 та ін.), Закон України від 12 травня 2015 р. № 389-VIII «Про правовий режим воєнного стану» (у редакції від 13 грудня 2022 р.), Закон України від 6 грудня 1991 р. № 1932-XII «Про оборону України» (у редакції від 2 жовтня 2018 р.)

² Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України»: Указ Президента України від 25.03.2021 р. № 121/2021. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/121/2021#Text>. (дата звернення: 04.11.2024).

³ Бантишев О. Ф., Шамара О. В. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації): монографія. 3-вид., перероб. і допов. Луганськ, Віртуальна реальність. 2014. С. 90.

⁴ Борисов В. І. Правова модель складу злочину «Державна зрада» та інформація в системі її ознак». *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.): Харків: Право, 2023. С. 92.

У ч. 2 ст. 111 КК встановлена відповідальність за діяння, зазначені у ч. 1 цієї статті, якщо вони вчинені в умовах воєнного стану. Мова йде про всі три діяння, наведені в ч. 1. Однак, якщо розглядати вчинення таких діянь у їх безпосередньому сполученні з умовами воєнного стану, то таке поєднання діяння з цією обтяжуючою обставиною можливе лише для «переходу на бік ворога» та шпигунства.

Щодо «надання допомоги». Тут варто ще раз підкреслити, що з доповненням розділу І Особливої частини КК ст. 111¹, ст. 111² та ст. 114², значна частина діянь, які охоплювалися цим поняттям, була переміщена до норм означених статей. На відміну від поняття «надання допомоги», що вкрай узагальнено охоплювало значний масив зрадницьких діянь, у нових нормах КК діяння викладені конкретизовано й деталізовано до такої міри, яка дозволяє правозастосувачу більш упевнено підводити певний реальний випадок з ознакою суспільної небезпечності під ознаки діяння, наведеного в нормі закону про кримінальну відповідальність.

Що стосується діяння шпигунство, зазначеного в ч. 1 ст. 111 КК, то слід зазначити, що до 03.03.2022 р. воно могло бути вчинене як у період збройного конфлікту, так і в мирний час. Тобто час вчинення діяння для шпигунства не був обов'язковою ознакою складу злочину. Однак, після зміни редакції цієї статті,¹ ознака часу також стала обов'язковою для шпигунства. У мирний час, а також у період збройного конфлікту шпигунство кваліфікується за ч. 1 ст. 111 КК, а за умов воєнного стану – за ч. 2 цієї статті².

Як уже зазначалося, діяння у формі «перехід на бік ворога» та «надання допомоги» за характером впливу на об'єкт злочину поді-

¹ Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за злочини проти основ національної безпеки України в умовах дії режиму воєнного стану: Закон України від 03.03.2022 р. № 2113-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2113-20#Text> (дата звернення: 04.11.2024).

² Борисов В. І. Правова модель складу злочину «Державна зрада» та інформація в системі її ознак». *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.): Харків: Право, 2023. С. 92.

ляються на фізичні та інформаційні. До виключно інформаційних діянь належать шпигунство, зазначене у ч. 1 ст. 111¹ КК, та шпигунство як окремий вид злочину, визначення якого наведено в ст. 114 КК. Що стосується «переходу на бік ворога» та «надання допомоги», то інформаційність цих діянь може бути пов'язана з предметом використання або знаряддям чи засобами їх вчинення. Так, це може бути збір і передача представнику іноземної держави інформації з обмеженим доступом, що, однак, не становить державної таємниці (предмет кримінально-протиправної діяльності). В іншому випадку зрадник на виконання отриманого завдання поширює вкрай неправдиву інформацію (знаряддя вчинення діяння). Наведені приклади, як і множина інших, їм подібним, пов'язаних із широким використанням особою інформації, ускладнює однозначне розуміння таких діянь, призводить до можливості їх суб'єктивного оцінювання правозастосувачем¹. До того ж у поведінці зрадника можуть сполучатися інформаційні дії з фізичними. За таких умов (різноманіття) інформація не може бути уведена до складу діянь «перехід на бік ворога» і «надання допомоги» як їх обов'язкова ознака, хоча, безсумнівно, при формулюванні обвинувачення вказівка на те, що конкретно являла собою інформація при їх здійсненні, є необхідною складовою визначення ступеня тяжкості вчиненого².

Суб'єктивна сторона кримінально-протиправних діянь, зазначених у ст. 111 КК та ст. 114 КК, відображає процес свідомості й волі особи, яка їх вчиняє. Оскільки в законі об'єктивна сторона обмежена фактом вчинення суспільно небезпечного діяння, то й суб'єктивна сторона складу цього злочину повинна бути обмежена змістом відповідного діяння. Обов'язковою ознакою державної зради та шпигунства є *вина*. Вид вини – прямий умисел. Зміст прямого умислу

¹ Слюсарчук І., Вареня Н. Сутність підривної діяльності. *Підприємництво, господарство і право*. 2019. № 9. С. 221.

² Борисов В. І. Правова модель складу злочину «Державна зрада» та інформація в системі її ознак». *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.)*: Харків: Право, 2023. С. 95.

узагальнено для всіх форм зрадницької діяльності та шпигунства таких: особа усвідомлює, що її дії вчиняються на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці, і бажає їх вчинити¹.

Мотиви, якими керуються злочинці, можуть бути різними: помста, користь, бажання отримати громадянство країни, на яку особа починає працювати, тощо. На кваліфікацію вони не впливають. У силу такого різноманіття не є доцільним вводити мотив до системи обов'язкових ознак складу державної зради та шпигунства².

У зв'язку зі зростанням, починаючи з 2014 р., кількості кримінальних проваджень за ст. 111 КК, набуло актуальності питання щодо визнання *мети* обов'язковою ознакою вчинення таких діянь, як «перехід на бік ворога» та «надання допомоги». Більшість науковців вважають можливим визнавати мету обов'язковою ознакою цих діянь. Варто зазначити, що й суди цій ознаці суб'єктивної сторони державної зради стали останнім часом приділяти більше уваги. О. В. Зайцев та В. Р. Філіпенко, проаналізувавши практику, з'ясували, що в кожному обвинувальному вирокі указується на мету надання підривної діяльності проти України – «на шкоду суверенітетові, територіальній цілісності та недоторканності, державній, економічній та інформаційній безпеці України». Мета державної зради в зазначеній формі, зазначають автори, прямо не відбита в диспозиції норми ч. 1 ст. 111 КК, проте вираз «на шкоду» опосередковано на неї вказує, що доводить обов'язковість її встановлення³. Наведене дає підстави

¹ Тацій В. Я., Рубашенко М. А. Види злочинів проти основ національної безпеки. Кримінальне право України: Особлива частина: підручник / В. Я. Тацій, В. І. Борисов, В. І. Тютюгін та ін.; за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна, 6-те вид., перероб. і допов. Харків: Право, 2020. 786 с. С. 36.

² Борисов В. І. Правова модель складу злочину «Державна зрада» та інформація в системі її ознак». *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.): Харків: Право, 2023. С. 94.

³ Зайцев О. В., Філіпенко В. Р. Надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України як форма державної зради (ст. 111 КК України). *Вісник Луганського державного*

для висновку, що для діянь «перехід на бік ворога» та «надання допомоги» мета спричинення шкоди є обов'язковою ознакою, яка й має бути уведена до системи ознак складу цього злочину.

Суб'єкт злочину. Одностайно визнається, що суб'єкти державної зради та шпигунства – спеціальні. Цей висновок випливає безпосередньо з тексту диспозиції ч. 1 ст. 111 КК, де зазначено, що державна зрада є діянням, яке «вчинене громадянином України». Відповідно до ст. 1 Закону України від 18 січня 2001 року «Про громадянство України»¹ громадянином України є особа, яка набула громадянство України в порядку, передбаченому законами України та міжнародними договорами України. У диспозиції ч. 1 ст. 114 КК також вказано на суб'єкта злочину. Зазначено, що шпигунство вчиняється «іноземцем або особою без громадянства». Згідно з положеннями ст.ст. 18, 19, 22 Загальної частини КК суб'єктами державної зради та шпигунства можуть бути фізичні осудні особи, які вчинили ці діяння у віці з 16 років.

Відносно суб'єкта шпигунства за ст. 114 КК, яким є іноземці або особи без громадянства, то варто додати, що протиправній діяльності таких суб'єктів, пов'язаних із шпигунством, приділена увага в міжнародних конвенціях, зокрема, у випадках, коли нею займаються військовослужбовці воюючих сторін. Так, у п. 1 ст. 46 Додаткового протоколу (I) до Женевських конвенцій від 12 серпня 1949 р., що стосуються захисту жертв міжнародних збройних конфліктів, зазначено: «...будь-яка особа із складу збройних сил сторони, що перебуває у конфлікті, яка потрапляє під владу супротивної сторони в той час, коли вона займається шпигунством, не має права на статус військовополоненого, і з нею можуть поводитися як зі шпигуном». Однак у п. 2 цього протоколу уточнюється: «Особа із складу збройних сил сторони, що перебуває в конфлікті, яка від імені цієї сторони збирає або намагається зібрати інформацію на терито-

університету внутрішніх справ імені Е. О. Дідоренка. Северодонецьк, 2019. Вип. 3 (87). С. 249.

¹ Про громадянство України: Закон України від 18.01.2001 р. № 2235-III. *Верховна Рада України. Законодавство України:* оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2235-14#Text> (дата звернення: 04.11.2024).

рії, що контролюється супротивною стороною, не вважається особою, яка займається шпигунством, якщо, діючи таким чином, вона носить формений одяг своїх збройних сил»¹. Наведене засвідчує важливість дослідження питань, пов'язаних із шпигунством з боку військовослужбовців, що набуває особливої актуальності в умовах, коли Україна веде безкомпромісну боротьбу з воєнною агресією, розв'язаною РФ.

1.3. Інформаційні кримінально-протиправні діяння, що передбачають співпрацю з державою-агресором (статті 111¹, 111² КК України)

1.3.1. Інформаційна колабораційна діяльність: загальні положення

Російська військова агресія проти України нерозривно пов'язана з інформаційною війною, головною метою якої є підрив інформаційної безпеки нашої держави. Ця стратегія спрямована, зокрема, на ураження національної свідомості українців шляхом формування викривленої оцінки реальних подій (починаючи з 2014 року) та спроби схилити населення України до підтримки проросійського політичного курсу й співпраці з агресором. Остання є складним соціальним феноменом, який набуває неоднозначної оцінки в суспільстві через зумовленість різними чинниками, найвагомішим з яких є окупація українських територій.

З одного боку, самі по собі умови окупації накладають відбиток на повсякденне життя та можливість людей вільно обирати варіант поведінки, які незалежно від своїх поглядів і цінностей змушені

¹ Додатковий протокол (I) до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів. (ООН, від 08.06.1977). URL: <http://zakon5.rada.gov.ua/laws/show/995-199>. Прочитовано із джерела: Антипов В. І. Кримінальний кодекс України в контексті міжнародного права та практики Європейського суду з прав людини: правові норми, судова практика, науково-практичний коментар. Харків: Право, 2019. С. 266.

приспосовуватися (добровільно чи примусово, свідомо чи несвідомо) і в такий спосіб ставати складовою колабораційних практик, що обумовлено гострою потребою забезпечити свою життєдіяльність на окупованих територіях¹. Однак, з другого боку, колаборація місцевого населення з державою-агресором стає ключовим елементом, який дозволяє окупантам утвердитися на захоплених територіях. Це сприяє створенню системи окупаційної влади, зокрема її силового блоку, а також забезпеченню життєдіяльності цих регіонів. В умовах війни така співпраця, особливо якщо вона ініціативна та добровільна, становить серйозну загрозу для національної безпеки, адже вона підриває державний суверенітет, загрожує територіальній цілісності, конституційному ладу та іншим національним інтересам країни, що зазнала агресії. Саме тому подібне явище вимагає рішучої реакції з боку держави заради недопущення розростання його масштабів.

Звісно, що форми, характер і ступінь взаємодії місцевого населення з окупантами можуть суттєво відрізнятись, як і мотивація та обставини, за яких така співпраця здійснюється. Так, залежно від сфери, у якій проявляється колабораціонізм, його формами (видами) можуть бути воєнний, адміністративний, економічний, культурний (духовний), побутовий тощо². Водночас визначити всі можливі види такого явища складно, та й не завжди доцільно, оскільки колабораціонізм є динамічною, відкритою системою, здатною змінюватися та набувати нових форм по мірі розвитку суспільних процесів. Одним із яскравих підтверджень цього є виникнення окремої форми інформаційного колабораціонізму, масштаби та наслідки якого зростають

¹ Букреєв О. І., Нетеса Н. В. Колабораціонізм у гуманітарній сфері: пошук оптимального законодавчого рішення та реалії практики застосування ст. 111¹ КК України. *Ретроспектива військової агресії рф в Україні: злочини проти миру, безпеки людства та міжнародного правопорядку в сучасному вимірі*: матеріали міжнар. наук.-практ. круглого столу 22–23 червня 2023 р. Київ: Алерта, 2023. С. 59.

² Гончаренко О. Проблеми інституційного визначення терміна колабораціонізму, його видів та ознак у сучасній вітчизняній історіографії. *Військово-історичний меридіан*. 2019. Вип. 1 (23). С. 20. URL: https://vim.gov.ua/pages/ua/archive/number.php?archive_number=23.05.2019; Радутний О. Е. Публічні заклики та заперечення як форми інформаційної колабораційної діяльності за Кримінальним кодексом України. *Інформація і право*. 2022. № 2(41). С. 104. DOI: [https://doi.org/10.37750/2616-6798.2022.2\(41\).270372](https://doi.org/10.37750/2616-6798.2022.2(41).270372).

за принципом геометричної прогресії, що пов'язано з тим, що інформація дедалі більше набуває статусу універсального інструментарію реалізації суспільно значущих практик (в тому числі протиправної поведінки).

Очевидно, що на різних етапах суспільно-історичного розвитку, з огляду на воєнно-політичну обстановку в державі та систему морально-етичних цінностей, згадані форми колабораціонізму не можуть піддаватися однаковій суспільній чи правовій оцінці, а тим більше кримінально-правовій. Не викликає сумнівів, що найвищий рівень суспільної небезпечності властивий воєнному, політичному та адміністративному колабораціонізму, які нерідко супроводжуються вчиненням воєнних злочинів чи інших кримінально караних діянь. Такі форми співпраці з агресором потребують найсуворішої реакції з боку держави. Водночас існує й колабораціонізм у гуманітарній сфері, яким охоплюється, зокрема, діяльність у галузях медицини, надання комунальних послуг, забезпечення правопорядку, захисту прав людини, тобто тих сфер, які забезпечують життєдіяльність цивільного населення на окупованих територіях. Частково до цього можна віднести й співпрацю в освітній сфері, адже право на освіту гарантується як Конституцією України, так і Європейською конвенцією з прав людини, а також окремі форми економічної взаємодії з ворогом, пов'язані з постачанням харчових продуктів, побутових товарів, послуг та інших необхідних ресурсів. При цьому важливо враховувати, що населення окупованих територій чи територій, де відбувається збройний конфлікт, потрапляє під безпосередній захист норм міжнародного гуманітарного права (зокрема, Женевської конвенції про захист цивільного населення під час війни¹), що не може ігноруватися під час кримінально-правової оцінки таких діянь, що, на жаль, має місце на практиці насамперед через відсутність в Україні правового механізму узгодження положень міжнародного гуманітарного права та національного законодавства. Вочевидь, що такі форми колабораційної діяльності слід визнавати вимушеними

¹ Про захист цивільного населення під час війни: Женевська Конвенція від 12.08.1949 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_154#Text (дата звернення: 25.10.2024).

та соціально виправданими з огляду на потребу забезпечення життєдіяльності цивільного населення на таких територіях. Крім того, є окремі колабораційні прояви (як-от, побутовий колабораціонізм), які взагалі мають перебувати поза межами правового регулювання, оскільки вони знаходяться в системі координат інших соціальних норм – морально-етичних, а отже, можуть зазнавати хіба що неправових видів соціального реагування, зокрема, морального осуду.

Що ж стосується колабораціонізму в інформаційній сфері, то тут слід зазначити, що в умовах воєнного стану його суспільна небезпечність значно зростає. Це пов'язано з тим, що складовою частиною воєнної доктрини країни-агресора завжди виступає інформаційно-психологічна війна, спрямована на знищення не лише державності, а й національної ідентичності населення країни, яка зазнає агресії, шляхом нав'язування ворожої ідеології з одночасним впровадженням цензури, придушенням продержавницьких позицій, зокрема в освіті та культурі, здійсненням репресій щодо прихильників опозиційних рухів та ін. За таких умов культура, освіта, національно-державницька ідеологія стають найуразливішими ланками системи, на якій тримається консолідація українського суспільства, а співпраця населення з ворогом у культурній, духовній, ідеологічній сферах ставить під загрозу знищення національної пам'яті, української самобутності та громадянської ідентичності¹.

Отже, *інформаційна колабораційна діяльність*, по суті, являє собою різні форми усвідомленої добровільної взаємодії громадян України з ворогом в інформаційній сфері, що мають своїм змістом будь-які прояви циркуляції інформації на шкоду національній безпеці України. При цьому колабораціонізм в інформаційній сфері може розглядатися як родове поняття, що охоплює певні його види, в основу виокремлення яких може бути покладений характер такої інформаційної співпраці з ворогом. Остання може здійснюватися

¹ Нетеса Н. В. Колабораціонізм в інформаційній сфері як загроза безпековій ситуації в Україні в умовах гібридної агресії. *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки*: матеріали Всеукр. наук.-практ. конф. (м. Київ, 27 верес. 2024 р.) / редкол.: Вербенський М. Г., Опришко І. В., Лісниченко Л. В. та ін. Вінниця: ТВОРИ, 2024. С. 128.

або в *інформаційно-психологічній сфері*, за якої вчиняються інформаційні діяння, пов'язані зі здійсненням впливу на психіку й поведінку окремих осіб та їх груп, або ж в *інформаційно-технічній сфері*, коли мета маніпулювання громадською свідомістю не ставиться¹. У першому випадку, враховуючи спрямованість інформаційно-психологічної співпраці на ураження національної свідомості українців (що може здійснюватися через зміну ідеології, культури, стандартів освіти), цілком виправданим уявляється виокремлення ідеологічного, культурного, освітнього колабораціонізму як його підвидів. Щодо другого випадку – інформаційно-технічного колабораціонізму, то тут можна говорити про інформаційний колабораціонізм у тісному сенсі слова, за якого співпраця зводиться до окремих форм оперування інформацією в інтересах ворога, а також про кібернетичний колабораціонізм, що передбачає надання допомоги у здійсненні впливу на інформаційно-технічне середовище (інформаційно-комунікаційні системи та мережі тощо). Указані види інформаційного колабораціонізму відрізняються між собою метою здійснення, засобами, сферою застосування, наслідками, але у реальній дійсності вони нерідко набувають гібридних форм (як-от, культурно-ідеологічний, інформаційно-кібернетичний та ін.)².

Переміщуючи цю матрицю на ґрунт кримінально-правової матерії, можна констатувати, що кримінально-правовими засобами реагування на явище колабораціонізму в інформаційній сфері є положення частин 1, 3 та 6 ст. 111¹ КК. При цьому частина 1 зазначеної статті розрахована здебільшого на протидію ідеологічному колабораціонізму, адже, по суті, в основі заперечення збройної агресії лежить проросійський світогляд, а публічні заклики на підтримку рішень країни-агресора є типовою формою поширення ворожої ідеології та

¹ Нетеса Н. В., Мокляк В. В. Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм. *Інформація і право*. 2023. № 3(46). С. 102. DOI: [https://doi.org/10.37750/2616-6798.2023.3\(46\).287168](https://doi.org/10.37750/2616-6798.2023.3(46).287168).

² Більш докладно див.: Нетеса Н. В. Інформаційний колабораціонізм: деякі проблемні аспекти тлумачення та застосування кримінально-правових норм. *Інформація і право*. 2024. № 4(51). С. 223. DOI: [https://doi.org/10.37750/2616-6798.2024.4\(51\).318138](https://doi.org/10.37750/2616-6798.2024.4(51).318138).

проросійського політичного курсу. Щодо частини 3 ст. 111¹ КК, то вона передбачає кримінальну відповідальність за освітній колабораціонізм, за якого в процесі набуття освітніх компетентностей відбувається комплексний вплив на свідомість майбутніх поколінь через формування у них ворожої ідеології, культури, морально-етичних цінностей. І, нарешті, ч. 6 аналізованої статті, за якою кримінально караними визнаються організація та проведення заходів політичного характеру, а також здійснення інформаційної діяльності у співпраці з державою-агресором, є нормою з найширшим діапазоном видів колабораціонізму – від суто інформаційно-технологічного до ідеологічного¹. І дійсно, організація та проведення заходів політичного характеру має розглядатися в контексті ідеологічного колабораціонізму, адже будь-який політичний захід ґрунтується на насаджуваних аудиторії відповідній ідеології. Що ж стосується здійснення інформаційної діяльності, то нею, виходячи зі змісту п. 3 примітки до ст. 111¹ КК, охоплюються як форми інформаційної колаборації, що самі по собі не пов'язані з інформаційно-психологічними впливами на суспільну свідомість (як-от, створення, збирання, одержання, зберігання інформації), так і власне ідеологічний колабораціонізм, коли співпраця з ворогом здійснюється у форматі масового поширення інформації (наприклад, інформаційна діяльність блогерів, публічних осіб держави, інших лідерів громадської думки, суб'єктів у сфері медіа тощо).

Разом із тим, зауважимо, що окремі елементи інформаційного колабораціонізму у різних його проявах так само містяться й в інших нормах ст. 111¹ КК, зокрема у ч. 5, де згадується про таку форму, як публічні заклики до проведення незаконних виборів та референдумів на тимчасово окупованій території, а також у ч. 7, де йдеться про надання незаконним збройним чи воєнізованим формуванням, створеним на тимчасово окупованій території, та збройним формуванням держави-агресора допомоги (у тому числі інформаційної) у веденні бойових дій проти Збройних Сил України та інших військових

¹ Нетеса Н. В. Інформаційний колабораціонізм: деякі проблемні аспекти тлумачення та застосування кримінально-правових норм. *Інформація і право*. 2024. № 4(51). С. 224. DOI: [https://doi.org/10.37750/2616-6798.2024.4\(51\).318138](https://doi.org/10.37750/2616-6798.2024.4(51).318138).

формувань, утворених відповідно до законів України. Як приклад останнього випадку можна навести рішення Красногвардійського районного суду м. Дніпропетровська, відповідно до якого за ч. 7 ст. 111¹ КК як надання інформаційної допомоги були кваліфіковані дії особи, яка з використанням мобільного телефону поширила інформацію представнику незаконного збройного формування «ДНР» про переміщення військової техніки й особового складу ЗСУ, а також місця постійної і тимчасової дислокації підрозділів ЗСУ¹.

Отже, викладене підтверджує, що чимало кримінальних правопорушень, пов'язаних із колабораційною діяльністю, можуть мати форму інформаційних діянь, що тим не менше не перетворює їх автоматично на інформаційний колабораціонізм. Такого висновку фактично доходить й М. А. Рубашенко, хоча його бачення переліку тих кримінальних правопорушень, які становлять, за його термінологією, «інформаційне колаборанство», на наше переконання, є неповним, адже до цієї класифікаційної групи він включає лише діяння, указані в ч. 1 ст. 111¹ КК, та здійснення інформаційної діяльності, передбачене ч. 6 цієї статті². При цьому суперечливими виглядають його судження щодо публічних закликів до проведення незаконних виборів та референдумів, адже наголошуючи на тому, що такі заклики володіють аналогічними з передбаченими ч. 1 ст. 111¹ КК закликами особливостями в характері діяння³ (напевно, йдеться про їх інформаційну природу), він водночас не відносить їх до інформаційного колаборанства, що загалом то є правильним, але в даному випадку недостатньо аргументованим. Крім того, взагалі поза увагою дослідника залишилося надання інформаційної допомоги воєнізованим та збройним формуванням, що охоплюється ч. 7 цієї статті, адже це діяння також є типовим прикладом інформаційних

¹ Вирок Красногвардійського районного суду м. Дніпропетровська від 29.03.2023 року (справа № 204/80/23, провадження № 1-кп/204/516/23). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/109869204/> (дата звернення: 25.10.2024).

² Рубашенко М. А. Кримінально-правова класифікація колабораційної діяльності (ст. 111-1 КК). *Юридичний науковий електронний журнал*. 2023. № 10. С. 506. URL: http://lsej.org.ua/10_2023/122.pdf.

³ Там само. С. 505.

діянь, так само як і здійснення пропаганди у закладах освіти (ч. 3), в якому він чомусь теж не вбачає інформаційної сутності. Вочевидь, що невизнання інформаційним колабораціонізмом діянь, указаних у частинах 5 та 7 ст. 111¹ КК, незважаючи на беззаперечну присутність в них його елементів, пов'язано з тим, що в цих випадках інформаційний колабораціонізм має субсидіарний характер стосовно інших його форм – політичного та воєнного, що означає спрямованість цих проявів колабораційної діяльності не на інформаційну безпеку як таку, а на інші складові національної безпеки, приміром, воєнної безпеки, на захист якої й орієнтована норма ч. 7 аналізованої статті. Саме тому у межах цього дослідження у фокусі нашої уваги перебуватимуть проблемні аспекти лише тих форм кримінально караної колабораційної діяльності, які мають безпосереднє відношення до інформаційної безпеки – частини 1, 3 та 6 ст. 111¹ КК.

1.3.2. Кримінально-правова характеристика колабораційної діяльності в інформаційній сфері (частини 1, 3 та 6 ст. 111¹ КК України)

З початком повномасштабного вторгнення РФ в Україні з'явилася достатньо потужна нормативно-правова платформа для протидії колабораційній діяльності у вигляді встановлення кримінальної відповідальності за різні її прояви, в тому числі в інформаційній сфері (Закон України «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність» від 03 березня 2022 р. № 2108-IX, набрав чинності з 15 березня 2022 р.¹). Відтоді постало чимало непростих у доктринальному сенсі питань, зумовлених появою нових термінів та потребою їх тлумачення, а також виникли проблеми правозасто-

¹ Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність: Закон України від 03.03.2022 р. № 2108-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2108-20#Text> (дата звернення: 25.10.2024).

сування нових норм, пов'язані з труднощами кваліфікації вчинюваних діянь та розмежування суміжних складів кримінальних правопорушень.

Слід зазначити, що колабораційна діяльність в інформаційній сфері є типовим прикладом кримінально караних суспільно небезпечних інформаційних діянь і як будь-яке інформаційне діяння являє собою певну форму соціальної комунікації, за якої відповідні суб'єкти вступають у соціальні зв'язки з приводу предмета комунікації, яким є інформація, виражена у певній формі. При цьому характер таких зв'язків може бути різним залежно від аудиторії, яка виступає реципієнтом такої інформації (від однієї особи до необмеженого, індивідуально невизначеного кола осіб), а також від форми діяння. Крім того, різною може бути й форма донесення інформації при колабораційній діяльності – від публічних закликів (ч. 1 ст. 111¹ КК) до власне пропаганди (ч. 3 ст. 111¹ КК), заперечення певних фактів (ч. 1 ст. 111¹ КК), здійснення інформаційної діяльності (ч. 6 ст. 111¹ КК).

Не ставлячи собі за завдання надання повної характеристики колабораційних кримінальних правопорушень в інформаційній сфері, у межах даного підрозділу розглянемо лише ті питання, які, на наш погляд, мають істотне значення для забезпечення правильної кваліфікації аналізованих кримінальних правопорушень та вирішення складних питань подолання колізії суміжних кримінально-правових норм і які дотепер не отримали достатньої науково-правової оцінки або досі викликають жваві дискусії. Одним із таких питань, на наше переконання, є визначення об'єкта кримінальних правопорушень, пов'язаних із колабораційною діяльністю в інформаційній сфері.

На сьогодні більшість дослідників, посилаючись на розміщення ст. 111¹ у розділі I КК серед злочинів проти основ національної безпеки, просто констатують, що родовим та безпосереднім об'єктом цих кримінальних правопорушень є суспільні відносини у сфері національної безпеки¹. Здавалося б, питання вирішене самим

¹ Василенко Ю. В. Колабораційна діяльність: кримінально-правова характеристика складу кримінального правопорушення. *Часопис Київського інституту інтелектуальної власності та права*. 2022. Вип. 1. С. 4; Злочинна колаборація в умовах збройної агресії: практичний poradnik з кримінально-правової оцінки та

законодавцем, але специфіка інформаційних діянь змушує науковців шукати способи конкретизації об'єкта аналізованих суспільно небезпечних діянь. Так, окремі науковці висловлюють думку про притаманність кримінальним правопорушенням, передбаченим частинами 1, 3 та 6 ст. 111¹ КК, додаткового об'єкта, який, на їх думку, можуть становити інформаційна безпека, а також мир і безпека людства, політична безпека, нормальний соціальний розвиток неповнолітніх¹. Убачається, що така позиція породжує, принаймні, декілька застережень.

По-перше, у контексті вказаних положень ст. 111¹ КК інформаційна безпека, вочевидь, має визнаватися складовою національної безпеки, що означає перебування безпосереднього об'єкта у межах родового. Визнання протилежного фактично заперечує усталену в теорії кримінального права позицію про те, що додатковий безпосередній об'єкт завжди існує поряд із основним об'єктом і, як правило, перебуває у межах інших родових об'єктів. По-друге, виникають сумніви й щодо можливості визнання додатковим об'єктом інформаційної колабораційної діяльності політичної безпеки, адже таким терміном не оперує навіть базовий Закон України «Про національну безпеку України»², де використовується термін «зовнішньополітична безпека». По-третє, говорячи про можливість визнання додатковим безпосереднім об'єктом кримінальних правопорушень, передбачених частинами 1, 3 та 6 ст. 111¹ КК, суспільних відносин, які

розмежування / за заг. ред. В. В. Малюка. Київ: Алерта, 2023. С. 105; Кравчук О. О., Бондаренко М. С. Колабораційна діяльність: науково-практичний коментар до нової статті 111-1 КК. *Юридичний науковий електронний журнал*. 2022. № 3. С. 199. URL: http://lsej.org.ua/3_2022/45.pdf.

¹ Письменський Є. О. Ідеологічний та культурно-освітній колабораціонізм як посягання на інформаційну безпеку. *Кримінально-правова охорона інформаційної безпеки*: матеріали VI міжнар. наук.-практ. конференції, м. Харків, 12 трав. 2022 р. / [редкол.: Л. М. Демидова (голов. ред.) та ін.] ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України ; Нац. юрид. ун-т ім. Ярослава Мудрого ; громад.організація «Всеукраїнська асоціація кримінального права». – Харків : Право, 2022. С. 81.

² Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 25.10.2024).

поставлені під охорону розділу XX КК (миру та безпеки людства), варто враховувати, що тут, скоріше за все, виникає питання щодо правильної кваліфікації вчиненого діяння та розмежування суміжних діянь шляхом подолання наявної конкуренції кримінально-правових норм, а отже, насамперед правильного визначення родового об'єкта кримінального правопорушення. Дійсно, на сьогодні склалася парадоксальна ситуація, коли однотипні форми суспільно небезпечної поведінки законодавцем розцінюються як різнородові посягання. Йдеться насамперед про ідеологічний колабораціонізм у формі заперечення громадянином України здійснення збройної агресії проти України та встановлення чи утвердження тимчасової окупації частини території України (ч. 1 ст. 111¹ КК), який визнається кримінальним правопорушенням проти основ національної безпеки, та про діяння, пов'язане з виправдовуванням, визнанням правомірною, запереченням збройної агресії Російської Федерації проти України та глорифікацією учасників (ст. 436² КК), яке розміщене у розділі XX КК серед кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку. Надмірна подібність зазначених норм, що, безумовно, є вадою чинного законодавства, спонукає окремих дослідників до думки про нагальну потребу у виключенні ч. 1 зі ст. 111¹ КК¹ через охоплення таких діянь нормою ст. 436² КК. Але така пропозиція, на наше переконання, є прикладом половинчастого підходу до розв'язання наявної проблеми, оскільки не надає відповіді на запитання про те, загрозу яким саме суспільним відносинам становлять діяння, пов'язані із запереченням збройної агресії проти України, і чи соціально зумовленим є розташування діяння, передбаченого ст. 436² КК, саме серед кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку. Цілком погоджуючись із тим, що наведена ситуація вимагає якомога скорішого подолання очевидної законодавчої вади та усунення невиправданої

¹ Письменський С., Мовчан Р. Ідеологічний та культурно-освітній колабораціонізм: окремі проблеми тлумачення та вдосконалення законодавства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 2. С. 12; Мовчан Р. О. Воєнні новели Кримінального кодексу України: правотворчі та правозастосовні проблеми: монографія. Київ: Норма права, 2022. С. 200.

конкуренції кримінально-правових норм, все ж таки вважаємо, що ця проблема має вирішуватися системно, з переглядом змісту споріднених норм не лише на предмет їх правової визначеності, а й на предмет їх розташування в КК, адже вбачається, що конкретизація у диспозиції ст. 436² КК суб'єкта та об'єкта збройної агресії є аргументом на користь того, що при вчиненні описаних у ній діянь під загрозу заподіяння шкоди насамперед потрапляють суспільні відносини у сфері забезпечення національної безпеки України. Такий умовивід загалом кореспондує позиції міжнародної спільноти у визнанні цієї категорії кримінальних правопорушень політичними, а отже, такими що вчиняються проти держави та становлять загрозу не міжнародному правопорядку, а насамперед національній безпеці конкретної держави¹. До речі, фактично такої позиції дотримуються й розробники проекту нового Кримінального кодексу, які не визнаючи виправдовування, заперечення збройної агресії колабораційною діяльністю (ст. 9.1.6), передбачили її як окрему форму кримінально протиправної поведінки (ст. 9.1.12) у розділі 9.1 Проекту «Злочини проти національної безпеки та держави»².

Враховуючи викладене, вважаємо, що *безпосередній об'єкт* розглядуваних кримінальних правопорушень може бути визначений як *суспільні відносини у сфері інформаційної безпеки як складової національної безпеки*. Така конкретизація має принципове значення, адже у разі вчинення таких діянь насамперед має місце посягання на інформаційні відносини, сутність яких полягає у реалізації закріпленого в ст. 34 Конституції України права на свободу думки і слова, на вільне вираження своїх поглядів і переконань, права вільно збирати, зберігати, використовувати й поширювати інформацію, які, разом із тим, можуть бути обмежені законом, зокрема в інтересах національної безпеки та територіальної цілісності. При цьо-

¹ Нетеса Н. В. Інформаційний колабораціонізм: деякі проблемні аспекти тлумачення та застосування кримінально-правових норм. *Інформація і право*. 2024. № 4(51). С. 225. DOI: [https://doi.org/10.37750/2616-6798.2024.4\(51\).318138](https://doi.org/10.37750/2616-6798.2024.4(51).318138).

² Текст проекту нового Кримінального кодексу України: контрольний текст (станом на 01.08.2024). Робоча група з питань розвитку кримінального права. URL: <https://newcriminalcode.org.ua/criminal-code> (дата звернення: 01.11.2024).

му суспільні відносини у сфері інформаційної безпеки як безпосередній об'єкт досліджуваних кримінальних правопорушень слід розуміти як стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави від негативних інформаційних (інформаційно-психологічних) впливів на свідомість особи та суспільства, а також від неповноти та несвоечасності поширення інформації, порушення її цілісності та доступності, поширення інформації зі суспільно шкідливим контентом (в тому числі від скоординованого поширення недостовірної інформації та деструктивної пропаганди).

Щодо виокремлення *додаткових об'єктів* цих кримінальних правопорушень, то оскільки норми про колабораційну діяльність в інформаційній сфері не сконструйовані за правилами врахованої законодавцем сукупності кримінальних правопорушень чи кримінальних правопорушень, поєднаних з настанням суспільно небезпечних наслідків, що лежать у площині родових об'єктів інших кримінальних правопорушень, то їх виокремлення вбачається недоречним. Як ілюстрацію непереконливої спроби виокремити додатковий об'єкт колабораційної діяльності у формі впровадження стандартів освіти держави-агресора (ч. 3 ст. 111¹ КК) можна навести висловлену у колі правознавців пропозицію визнавати ним гарантоване кожному конституційне право на освіту (ст. 53 Основного Закону)¹. Така позиція вбачається логічно суперечливою, адже якраз право на освіту у такому разі реалізовується, оскільки заклади освіти на окупованих територіях функціонують, але освітній процес відбувається за стандартами країни-агресора, окремі компоненти яких (ідеологічний, світоглядний, ціннісно-орієнтаційний) суперечать національному складнику освітніх програм України, а отже, й меті освіти в Україні через подання інформації у фальсифікованому вигляді, що свідчить про те, що шкода і в цьому випадку заподіюється

¹ Кравчук О., Бондаренко М. Колабораціонізм в освіті: аналіз рішень судів щодо впровадження стандартів держави-агресора. *Українська Гельсінська група*: вебсайт. URL: <https://www.helsinki.org.ua/articles/kolaboratsionizm-v-osviti-analiz-rishen-sudiv-shchodo-vprovadzhennia-standartiv-derzhavy-ahresora/> (дата звернення: 25.10.2024).

ся саме інформаційним відносинам, які є основним безпосереднім об'єктом колабораційної діяльності у цій формі.

У контексті розгляду об'єкта інформаційних форм колабораційної діяльності варто також приділити окрему увагу визначенню *предмета* цих кримінальних правопорушень, який є обов'язковою ознакою їх складів. У ролі такого виступає відповідна інформація, специфікою якої є шкідливий протиправний контент, який або чітко визначається відповідними нормами статей Особливої частини КК (як у випадку ч. 1 ст. 111¹ КК), або описується у загальних рисах (у випадку ч. 3 та ч. 6 ст. 111¹ КК). Так, предметом кримінального правопорушення, передбаченого ч. 1 аналізованої статті, є інформація, що містить заперечення вказаних у ній суспільно значущих фактів або заклик до суспільно небезпечних дій як певний набір символів (текстових, звукових, візуальних); предметом кримінального правопорушення, передбаченого ч. 3 ст. 111¹ КК, – інформація у вигляді певних шкідливих ідей, поглядів, знань, що поширюються з метою здійснення ідейного впливу на широкі маси або певні групи людей; предметом кримінального правопорушення, передбаченого ч. 6 цієї статті, може бути будь-яка інформація, що є свідченням підтримки держави-агресора, її окупаційної адміністрації чи збройних формувань або сприяння уникненню нею відповідальності за збройну агресію проти України. Така особливість інформації як предмета кримінального правопорушення у складах інформаційної колабораційної діяльності свідчить про те, що цей предмет не входить до структури суспільних відносин у сфері інформаційної безпеки як об'єкта кримінально-правової охорони, оскільки, як справедливо наголошує М. А. Рубашенко, останні не можуть виникати з приводу предметів, що мають явно виражені соціально негативні властивості¹. Це дозволяє констатувати, що інформація тут є предметом, відсутність якого свідчить про нормальне функ-

¹ Рубашенко М. Особливості публічних закликів і розповсюдження матеріалів із закликами як суспільно небезпечних діянь. *JURNALUL JURIDIC NAȚIONAL: TEORIE ȘI PRACTICĂ*. Decembrie 2019 (6). С. 163. URL: <http://jurnaluljuridic.in.ua/archive/2019/6/37.pdf>.

ціонування суспільних відносин у сфері забезпечення інформаційної безпеки.

З *об'єктивної сторони* всі форми інформаційного колабораціонізму належать до кримінальних правопорушень із формальним складом, коли суспільно небезпечні наслідки не є обов'язковою ознакою об'єктивної сторони складу кримінального правопорушення, яке вважається закінченим із моменту вчинення суспільно небезпечного діяння. Звісно, що в реальній дійсності наслідки інформаційних діянь завжди мають місце, але їх наявність не впливає на кваліфікацію вчиненого за ознаками частин 1, 3, 6 ст. 111¹ КК, відповідно, вони не є предметом доказування у кримінальному процесі. Отже, розглянемо об'єктивну сторону окремих форм інформаційної колабораційної діяльності більш детально, розпочавши цей аналіз із кримінального правопорушення, передбаченого ч. 1 ст. 111¹ КК.

Як уже зазначалося, в *ч. 1 ст. 111¹ КК* встановлена кримінальна відповідальність за так званий *ідеологічний колабораціонізм*, що полягає у вчиненні інформаційного діяння в одній з форм, що вказані в законі як альтернативні: *1) публічне заперечення: а) здійснення збройної агресії проти України, б) встановлення та утвердження тимчасової окупації частини території України; або 2) публічні заклики до: а) підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, б) до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, в) до невизнання поширення державного суверенітету України на тимчасово окуповані території України.*

Щодо *заперечення*, то зазначимо, що цей термін є своєрідною новелою воєнного часу, що зумовлює потребу не лише встановлення його змісту, а й визначення співвідношення з іншими інформаційними діяннями – як тими, що є усталеними для кримінального законодавства (як-от, заклики, пропаганда), так і з тими, що з'явилися у кримінальному законодавстві одночасно з цим терміном (виправдовування, визнання правомірними певних діянь). Для вирішення цього завдання насамперед звернемося до етимології

слова «заперечення», яке означає дію за значенням заперечити; заяву про незгоду з ким-, чим-небудь, доказ проти чогось; спростування чого-небудь; невизнання існування, значення, доцільності чого-небудь¹. Виходячи з цього, в доктрині кримінального права під публічним запереченням зазвичай пропонується розуміти таку поведінку, яка полягає у відкритому вираженні думки про те, що визначені у диспозиції ч. 1 ст. 111¹ КК факти не встановлені або відсутні, а також у відкритому спростуванні цих фактів². Водночас нерідко публічне заперечення науковцями пов'язується не лише із невизнанням чи спростуванням певних фактів та подій, а й з публічним применшенням їх значення, а так само й з їх виправдовуванням³. Одразу зазначимо, що чимало науковців вважають останню позицію такою, що не відповідає принципу правової визначеності норми через непередбаченість у законі інших окрім публічного заперечення та публічних закликів форм, а отже, якщо особа публічно виправдовує чи визнає правомірною збройну агресію РФ проти України, то її дії мають кваліфікуватися за іншою нормою – ст. 436² КК⁴, в диспозиції якої такі форми суспільно небезпечної поведінки прямо зазначені. Але тут виникає одразу декілька непростих запитань. Чи варто абсолютизувати у даному

¹ Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. Київ: Перун, 2005. С. 411.

² Мовчан Р. О. Воєнні новели Кримінального кодексу України: правотворчі та правозастосовні проблеми: монографія. Київ: Норма права, 2022. С. 26.

³ Злочинна колаборація в умовах збройної агресії: практичний порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ: Алерта, 2023. С. 106; Кравчук О. О., Бондаренко М. С. Колабораційна діяльність: науково-практичний коментар до нової статті 111-1 КК. *Юридичний науковий електронний журнал*. 2022. № 3. С. 199. URL: http://lsej.org.ua/3_2022/45.pdf; Хавронюк М. Кримінальна відповідальність за колабораціонізм. *Центр політико-правових реформ*: вебсайт. URL: <https://pravo.org.ua/blogs/kolaboratsijna-diyalnist-nova-stattya-kryminalnogo-kodeksu/>.

⁴ Мовчан Р. О. Воєнні новели Кримінального кодексу України: правотворчі та правозастосовні проблеми: монографія. Київ: Норма права, 2022. С. 26; Письменський Є., Мовчан Р. Ідеологічний та культурно-освітній колабораціонізм: окремі проблеми тлумачення та вдосконалення законодавства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 2. С. 9.

випадку принцип правової визначеності і чи завжди законодавець дотримується системного підходу під час законодавчого формулювання положень подібних за змістом норм КК? Невже колабораційна діяльність не може здійснюватися, наприклад, у формі виправдовування збройної агресії або ж остання є менш небезпечною формою поведінки порівняно із запереченням і тому не передбачена як кримінально карана? Або ж ще парадоксальніше – невже припустимою можна визнавати кваліфікацію заперечення збройної агресії як кримінального правопорушення проти основ національної безпеки, а виправдовування такої агресії за таких самих обставин вже як кримінального правопорушення проти миру, безпеки людства та міжнародного правопорядку, лише тому, що слідуючи принципу правової визначеності, необхідно застосовувати норму, в якій така форма прямо передбачена, у даному разі ч. 1 ст. 436² КК? Вочевидь, що відповідь на всі поставлені запитання має бути негативною.

Вбачається, що принцип правової визначеності норми не повинен підміняти собою потреби у з'ясуванні адекватного змісту вживаних у законі термінів, що особливо актуально в умовах відсутності легального їх визначення. На жаль, на сьогоднішній день не сформульоване не лише законодавче визначення термінів «заперечення», «виправдовування» та «визнання правомірною», а й базові дефініції «колабораційна діяльність», «держава-агресор», «органи держави-агресора» та ін., не зрозумілим є співвідношення термінів «співпраця» та «взаємодія», які одночасно вживаються в тексті ст. 111¹ КК, не визначеним є питання щодо тих рішень або дій, підтримка яких може розцінюватися як колабораційна діяльність, пособництво державі-агресору тощо. Все це значно ускладнює реалізацію принципу правової визначеності через універсальність таких термінологічних конструкцій. Більше того, наразі ми вимушені констатувати різний ступінь деталізації законодавцем форм суспільно небезпечної поведінки під час формулювання положень норм (в тому числі тих, що передбачені ч. 1 ст. 111¹ КК та ч. 1 ст. 436² КК). У цьому сенсі ми підтримуємо висловлену в літературі тезу про те, що законодавець не мав на меті сконструювати норми,

які б конкурували між собою, а виявлена суперечність – це законодавчий дефект з притаманною йому неузгодженістю розглядуваних кримінально-правових норм, що не ґрунтується на припущенні розумності законодавства¹.

І дійсно, якщо проаналізувати процедуру законопроектної роботи з доповнення КК нормами про колабораційну діяльність та про виправдовування, визнання правомірною, заперечення збройної агресії РФ проти України, то іншого висновку, як про безсистемність, поспішність та розбалансованість у законотворчому процесі, навряд чи можна дійти. Річ у тім, що обидва законопроекти про внесення змін до КК (Проект Закону про внесення змін до деяких законодавчих актів (щодо встановлення кримінальної відповідальності за колабораційну діяльність) (реєстр. № 5144 від 24.02.2021 р.)² та Проект Закону про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції) (реєстр. № 5102 від 18.02.2021 р.)³ розглядалися в одному головному Комітеті Верховної Ради України – Комітеті з питань правоохоронної діяльності. Крім того, вони готувалися й обговорювалися фактично паралельно (текст законопроекту 5144 та супровідні документи до нього датовані 25 лютого 2021 р., а законопроекту 5102 – 19 лютого 2021 р.) і, що показово, окремі народні депутати, що виступили суб'єктами

¹ Письменський Є., Мовчан Р. Ідеологічний та культурно-освітній колабораціонізм: окремі проблеми тлумачення та вдосконалення законодавства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 2. С. 11.

² Проект Закону про внесення змін до деяких законодавчих актів (щодо встановлення кримінальної відповідальності за колабораційну діяльність) (реєстр. № 5144 від 24.02.2021). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5144&conv=9> (дата звернення: 25.10.2024).

³ Проект Закону про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції) (реєстр. № 5102 від 18.02.2021 р.). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5102&conv=9> (дата звернення: 25.10.2024).

законодавчої ініціативи, були членами авторських колективів обох законопроектів. Так само викликає подив й те, що в жодному висновку на вказані законопроекти (ані у висновках Головного науково-експертного управління Апарату Верховної Ради України, ані у висновках головного Комітету) не була помічена явно закладена колізія норм ч. 1 ст. 111¹ КК та ст. 436² КК, тоді як проміжок часу між поданням цих законопроектів та їх прийняттям (більше року) більш ніж достатній для того, щоб виявити наявні неузгодженості та усунути ці вади. Не було це зроблено й Верховною Радою України, яка прийняла обидва Закони – «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції»¹ та «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність»² на одному засіданні – 03 березня 2022 р. Наслідком відсутності системного уніфікованого підходу до законотворення стала потреба розв’язання цієї проблеми на рівні правозастосування, де гостро постало питання можливості застосування різних обсягів одних і тих самих законодавчих термінів, що, на наш погляд, є припустимим у випадках, коли того вимагає конкретна життєва ситуація та принцип справедливості. Безумовно, в ідеалі в законі, в тому числі про кримінальну відповідальність, мають вживатися терміни в однаковому значенні та обсязі, проте доти, поки законотворець не виправить очевидних законодавчих вад, це питання потребує свого розв’язання на рівні правозастосування, зокрема шляхом вироблення правової позиції Верховного суду з розглядуваного питання, де,

¹ Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції: Закон України від 03.03.2022 р. № 2110-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2110-20#Text> (дата звернення: 25.10.2024).

² Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність: Закон України від 03.03.2022 р. № 2108-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2108-20#Text> (дата звернення: 25.10.2024).

на наш погляд, з огляду на вище наведені аргументи доцільніше віддати перевагу у контексті ч. 1 ст. 111¹ КК саме розширювальному тлумаченню терміна «заперечення» як такого, що охоплює й виправдовування та визнання правомірною збройної агресії.

Другою формою інформаційної колабораційної діяльності, що передбачена ч. 1 ст. 111¹ КК, є публічні заклики, які, за справедливим твердженням М. А. Рубашенка, наділені специфічними ознаками, що відрізняють їх від інших діянь, яким властива інформаційна природа. Такими ознаками є наявність у структурі закликів двох обов'язкових компонентів – повідомлення основних відомостей про діяння, на вчинення яких указує суб'єкт заклику, та спонукання до вчинення такого діяння¹. Останнє є тим елементом, який якраз і відрізняє заклик від простого ознайомлення адресата з відповідною інформацією. При цьому його відмінність від підбурювання до кримінального правопорушення полягає в тому, що тут відсутній характерний для співучасті двосторонній зв'язок між співучасниками.

Разом із тим, те діяння, до якого спонукає правопорушник, саме по собі є кримінальним правопорушенням за чинним КК, у даному разі це вчинення дій, спрямованих на реалізацію чи підтримку рішень або дій держави-агресора, збройних формувань та окупаційної адміністрації держави-агресора, кримінальна відповідальність за які передбачена ст. 111² КК, вчинення інших форм колабораційної діяльності, що передбачені іншими частинами ст. 111¹ КК. Водночас однією з проблем застосування всіх цих норм є відсутність чіткого розуміння того, до яких саме рішень чи дій на підтримку держави-агресора чи до якої саме співпраці закликає особа? На це, до речі, цілком справедливо вказано й у висновку Головного науково-експертного управління Апарату Верховної Ради на законопроект 5144 від 24.02.2021 р., в якому як такі, що потребують відповідей, вказані запитання: чи підпадатимуть під публічні заклики дії громадянина України, який публічно закликає до обміну полоненими, до заку-

¹ Рубашенко М. А. Особливості кваліфікації публічних закликів та заперечень як інформаційних діянь. *Право України*. 2022. № 11. С. 78–79.

півлі електроенергії з РФ, який виступає на радіостанції держави-агресора тощо? У чому полягає відмінність публічних закликів до дій, указаних в ч. 1 ст. 111¹ КК, від публічних закликів до проведення незаконних виборів або референдумів на тимчасово окупованій території (ч. 5 ст. 111¹ КК)?¹ Звісно, ці питання не повинні визнаватися предметом регулювання законодавства про кримінальну відповідальність, адже його головним призначенням є забезпечення охорони тих суспільних відносин, які впорядковані регуляторним законодавством, що дає нам підстави запропонувати два можливих шляхи виходу з наявної ситуації – або розробка спеціального закону про протидію колабораційній діяльності, або внесення змін до Закону України «Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України» від 15 квітня 2014 року № 1207-VII². Але в будь-якому разі слід погодитися з висловлюваною в юридичній літературі думкою про те, що кримінальна караність публічних закликів має обмежуватися лише закликами до підтримки тих рішень або дій держави-агресора, а також до співпраці з нею, які не направлені на виконання державою-агресором своїх зобов'язань, передбачених міжнародним гуманітарним правом³, зокрема Женевською Конвенцією про поведження з військовополоненими⁴ або Женевською Конвенцією про захист цивіль-

¹ Проект Закону про внесення змін до деяких законодавчих актів (щодо встановлення кримінальної відповідальності за колабораційну діяльність) (реєстр. № 5144 від 24.02.2021). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5144&conv=9> (дата звернення: 25.10.2024).

² Нетеса Н., Федосєєв В. Щодо деяких аспектів удосконалення кримінальної відповідальності за окремі види колабораційної діяльності. *Проблеми протидії колабораційній діяльності в умовах збройної та інформаційної агресії рф проти України*: зб. матер. наук.-практ. сем. (м. Київ, 4 квіт. 2024 р.) / упоряд.: Ю. О. Найдьон, В. Г. Пилипчук, М. О. Теплох, Т. О. Давидова, В. С. Зубенко. Київ : НА СБУ, ДНУ ПБП НАПрН України, 2024. С. 128.

³ Злочинна колаборація в умовах збройної агресії: практичний poradник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ: Алерта, 2023. С. 108-110.

⁴ Про поведження з військовополоненими: Женевська Конвенція від 12.08.1949 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_153#Text (дата звернення: 25.10.2024).

ного населення під час війни¹ від 12 серпня 1949 року, низкою норм якої (статті 50, 51, 56, 63 та ін.) передбачено обов'язок окупаційної держави у співробітництві з державними та місцевими органами влади забезпечувати та підтримувати життєдіяльність населення на захоплених територіях (зокрема, громадський порядок, діяльність медичних та освітніх установ, основних служб громадського користування, розподілення допомоги та організації рятувальних операцій тощо).

Ще один момент, який кидається в око навіть при первісному ознайомленні зі змістом диспозиції ч. 1 ст. 111¹ КК в аспекті повноти опису у ній ознак об'єктивної сторони складу кримінального правопорушення, це відсутність поряд із указаними формами інформаційних дій спорідненої для них форми – розповсюдження матеріалів, що містять заперечення збройної агресії та заклики до вказаних у диспозиції ч. 1 ст. 111¹ КК дій. Вочевидь, що логічно пояснити таку позицію неможливо, адже вона порушує як принцип системності кримінального законодавства, так і уявлення про соціально зумовлені форми кримінально протиправної поведінки, коли рух інформації визнається кримінальним правопорушенням, а щодо руху матеріальних носіїв з такою інформацією – законодавець не визначився, що змушує правозастосувача або взагалі констатувати некараність таких діянь (якщо чітко слідувати принципу правової визначеності норми), або шукати підстави для застосування інших кримінально-правових норм, зокрема, ч. 2 ст. 436² КК (де розповсюдження матеріалів визнається обставиною, що обтяжує кримінальну відповідальність, з набагато суворішою санкцією, що також є нетиповим способом конструювання норм КК і само по собі викликає чимало запитань), або ж вдаватися до розширювального тлумачення законодавчих термінів «заперечення» та «публічні заклики» як таких, якими охоплюється в тому числі розповсюдження матеріалів, змістом яких є заперечення або ж публічні заклики. Останній підхід, який підтримується й окремими науковцями

¹ Про захист цивільного населення під час війни: Женевська Конвенція від 12.08.1949 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_154#Text (дата звернення: 25.10.2024).

(зокрема, О. Е. Радутним¹), за наведених умов убачається найбільш прийнятним у ситуації, що склалася, адже дозволяє заповнити законодавчі прогалини і водночас не допустити невиправданої конкуренції норм.

Завершуючи розгляд окремих аспектів об'єктивної сторони форм інформаційної колабораційної діяльності, передбачених ч. 1 ст. 111¹ КК, слід також вказати на притаманність їм такої обов'язкової ознаки, як публічність. Легальне визначення у кримінальному законодавстві терміна «публічний» з'явилося лише після прийняття Закону України «Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність» від 03.03.2022 р., хоча сам цей термін й раніше вживався у тексті закону про кримінальну відповідальність у низці норм (статті 109, 110, 258², 258⁵, 295, 316, 338, 436, 436¹, 442 КК). До цього часу роз'яснення терміна містилося у постанові Пленуму Верховного Суду України «Про застосування судами законодавства, що передбачає відповідальність за посягання на життя, здоров'я, гідність та власність суддів і працівників правоохоронних органів» від 26 червня 1992 р. № 8, у п. 7 якої зазначалося, що «публічними є заклики у будь-якій формі до громадян або хоча б до однієї особи, але в присутності інших громадян...»². Наразі у п. 1 примітки до статті 111¹ КК вказується, що публічним є поширення закликів або висловлення заперечення до невизначеного кола осіб, зокрема у мережі Інтернет або за допомогою засобів масової інформації. При цьому, як справедливо зауважує О. Е. Радутний, формулювання «у мережі Інтернет або за допомогою засобів масової інформації» не повинно тлумачитися як таке, що акцентує увагу на самому факті використання засобу поширення інформації (наприклад, відповідне заперечення або

¹ Радутний О. Е. Публічні заклики та заперечення як форми інформаційної колабораційної діяльності за Кримінальним кодексом України. *Інформація і право*. 2022. № 2(41). С. 111. DOI: [https://doi.org/10.37750/2616-6798.2022.2\(41\).270372](https://doi.org/10.37750/2616-6798.2022.2(41).270372).

² Про застосування судами законодавства, що передбачає відповідальність за посягання на життя, здоров'я, гідність та власність суддів і працівників правоохоронних органів: постанова Пленуму Верховного Суду України від 26 червня 1992 р. № 8. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/v0008700-92#Text> (дата звернення: 25.10.2024).

заклик може міститися в особистому повідомленні, відправленому електронною поштою через ту ж саму мережу Інтернет, або у месенджері (WhatsApp, Viber, Telegram), що виключає ознаку публічності та відповідно можливість кваліфікації таких дій за ч. 1 ст. 111¹ КК)¹. Тут ознака публічності, так само як і в інших випадках, має оцінюватися комплексно, виходячи з сукупності обставин, що характеризують відповідну обстановку вчинення діяння – місце, час, спосіб, кількісна ознака аудиторії тощо. Втім, на наше переконання, наведене у п. 1 примітки до ст. 111¹ КК уточнення («зокрема у мережі Інтернет або за допомогою засобів масової інформації») є зайвим, адже, з одного боку, воно не несе у собі жодного змістовного навантаження, а, з другого, створює непотрібну у даному разі конкуренцію з нормами, які передбачають використання засобів масової інформації як обставину, що обтяжує кримінальну відповідальність (та ж сама ч. 3 ст. 436² КК).

Щодо ч. 3 ст. 111¹ КК, де передбачено кримінальну відповідальність за **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 за дії громадян України, спрямовані на впровадження стандартів освіти держави-агресора у закладах освіти** (так званий *освітній колабораціонізм*), то тут так само доречно розглядати проблемні аспекти щодо кожної з форм об'єктивної сторони окремо. Щодо першої форми, то, напевно, найбільше запитань виникає у світлі використання в законі терміна «пропаганда». На відміну від вище розглянутих термінологічних новел чинного закону про кримінальну відповідальність, її визначення пропонується у регуляторному законодавстві, зокрема, у Законах України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої

¹ Радутний О. Е. Публічні заклики та заперечення як форми інформаційної колабораційної діяльності за Кримінальним кодексом України. *Інформація і право*. 2022. № 2(41). С. 111. DOI: [https://doi.org/10.37750/2616-6798.2022.2\(41\).270372](https://doi.org/10.37750/2616-6798.2022.2(41).270372).

символіки» від 9 квітня 2015 р. № 317-VIII¹, «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну» від 22 травня 2022 р. № 2265-IX², «Про засудження та заборону пропаганди російської імперської політики в Україні і деколонізацію топонімії» від 21 березня 2023 р. № 3005-IX³.

Але, знов-таки, чи адекватним є зміст цього терміна, наданий у вище названих законодавчих актах? Так, якщо звернутися до Великого тлумачного словника української мови, то в ньому термін «пропаганда» пов'язується із поширенням і постійним, глибоким та детальним роз'ясненням яких-небудь ідей, поглядів, знань; з ідейним впливом на широкі маси або певні групи людей, що має політичний або релігійний характер; системою засобів масового поширення ідей, поглядів тощо⁴. Тобто, це дає підстави зробити висновок, що етимологія слова «пропаганда» вказує на те, що її некоректно зводити до більш простих форм інформаційних діянь – публічних закликів, звичайного поширення інформації, її передачі, заперечення, виправдовування тощо. Дійсно, не виключені випадки, коли, приміром, публічні заклики можуть набувати форму пропаганди, а заперечення чи виправдовування становлять її зміст. Але, все ж таки, пропаганда у кримінально-правовому сенсі, на відміну від ін-

¹ Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки: Закон України від 09.04.2015 р. № 317-VIII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/317-19#Text> (дата звернення: 25.10.2024).

² Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну: Закон України від 22.05.2022 р. № 2265-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2265-20#Text> (дата звернення: 25.10.2024).

³ Про засудження та заборону пропаганди російської імперської політики в Україні і деколонізацію топонімії» від 21.03.2023 р. № 3005-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/3005-20#Text> (дата звернення: 25.10.2024).

⁴ Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. Київ: Перун, 2005. С. 1162.

ших форм інформаційних дій, це діяння, яке може мати прихований характер, здійснюється систематично, протягом, як правило, тривалого проміжку часу та передбачає цілеспрямоване контрольоване нав'язування певних шкідливих за змістом поглядів та ідей з метою маніпулювання громадською думкою. Враховуючи викладене, не надаючи оцінку іншим нормам КК, де так само вживається термін «пропаганда», вважаємо, що застосування цього терміна в контексті норми про освітній колабораціонізм (ч. 3 ст. 111¹ КК) є цілком доречним, оскільки, як було зазначено вище, освітній процес – це система, яка пов'язана з формуванням не лише знань, а й світогляду та ціннісних уявлень та переконань, вихованням майбутніх поколінь українських громадян з чіткою громадянською позицією та усвідомленням своєї національної ідентичності¹.

Отже, здійснення пропаганди у контексті ч. 3 ст. 111¹ КК може бути визначене як цілеспрямоване, заздалегідь сформоване та узгоджене з ідеологічною концепцією держави-агресора² поширення у закладах освіти поглядів, уявлень та переконань, що обґрунтовують сприяння здійсненню збройної агресії проти України, встановленню та утворенню тимчасової окупації частини її території, а також уникненню відповідальності за таку агресію, кінцевою метою якого є маніпулювання свідомістю цільової аудиторії.

При цьому обов'язковою ознакою об'єктивної сторони аналізованого кримінального правопорушення є місце його вчинення, яке законодавцем визначене як заклад освіти. Останній, відповідно до п. 6) ч. 1 ст. 1 Закону України «Про освіту», визначається як юридична особа публічного чи приватного права, основним видом діяльності якої є освітня діяльність³, яка може здійснюватися на різних

¹ Нетеса Н. В. Інформаційний колабораціонізм: деякі проблемні аспекти тлумачення та застосування кримінально-правових норм. *Інформація і право*. 2024. № 4(51). С. 228. DOI: [https://doi.org/10.37750/2616-6798.2024.4\(51\).318138](https://doi.org/10.37750/2616-6798.2024.4(51).318138).

² Злочинна колаборація в умовах збройної агресії: практичний poradnik з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ: Алерта, 2023. С. 116.

³ Про освіту: Закон України від 05.09.2017 р. № 2145-VIII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text> (дата звернення: 25.10.2024).

рівнях та за різними видами освіти. Разом із тим, слід звернути увагу на те, що указаний Закон, поряд із зазначеним, містить й легальне визначення освітньої діяльності (п. 17: «освітня діяльність – діяльність суб’єкта освітньої діяльності, спрямована на організацію, забезпечення та реалізацію освітнього процесу у формальній та/або неформальній освіті») та визначає суб’єктів такої діяльності (п. 27: «суб’єкт освітньої діяльності – фізична або юридична особа (заклад освіти, підприємство, установа, організація, громадське об’єднання), що провадить освітню діяльність»). Отже, з наведеного випливає, що заклад освіти визнається одним, але не єдиним суб’єктом освітньої діяльності. Це дає підстави констатувати, що законодавець, формулюючи диспозицію ч. 3 ст. 111¹ КК, вдався до дещо звуженого підходу до визначення місця вчинення освітнього колабораціонізму, якщо оцінювати це в контексті положень Закону України «Про освіту». Водночас, застосовуючи правило адекватного тлумачення змісту закону, з якого випливає, що ознаки кримінального правопорушення можуть як прямо зазначатися в ньому, так і впливати з його змісту, такий підхід вбачається припустимим, оскільки, наприклад, у випадку організації закладом освіти культурних, спортивних та ін. заходів у межах освітньої діяльності, але поза межами закладу, це все одно буде складовою освітнього процесу. У протилежному випадку, якщо розширювати перелік можливих місць вчинення освітнього колабораціонізму, як це пропонується, наприклад, у законопроекті «Про внесення змін до Кримінального та Кримінального процесуального кодексу України щодо вдосконалення відповідальності за деякі злочини проти основ національної безпеки України» (реєстр. № 10136 від 09.10.2023 р.)¹, де поряд із закладами освіти вказано «заклади оздоровлення та відпочинку, місця, що використовуються для проведення навчальних, спортивних і культурних заходів», гіпотетично може виникнути ситуація, коли пропаганда здійснюється *поза*

¹ Проект Закону про внесення змін до Кримінального та Кримінального процесуального кодексу України щодо вдосконалення відповідальності за деякі злочини проти основ національної безпеки України» (реєстр. № 10136 від 09.10.2023 р.). Верховна Рада України. Законопроекти: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/42957> (дата звернення: 25.10.2024).

межами закладу освіти, не суб'єктами освітньої діяльності, щодо аудиторії, що не обмежується учнями. Підстави для такого умовиводу фактично дає й законодавче визначення суб'єкта цього кримінального правопорушення як громадянина України без його конкретизації за професійною ознакою (*педагог, вихователь*), родинними зв'язками (*батьки*), віковою ознакою (*неповнолітній*) тощо. До того ж, перелічені місця, якщо чітко слідувати положенням Закону України «Про освіту» або мають опосередковане відношення, або взагалі не мають відношення до здійснення освітньої діяльності. А це, у свою чергу, створює ситуацію правової невизначеності через «розмитість» меж розуміння освітньої діяльності, а отже, й освітнього колабораціонізму як такого, що матиме своїм наслідком конкуренцію норми ч. 3 ст. 111¹ КК з нормами, передбаченими ч. 1 ст. 111¹ КК та ст. 436² КК.

Щодо *впровадження стандартів освіти*, то тут ситуація виглядає таким чином, що ознаки об'єктивної сторони перебувають у нерозривній єдності з ознаками суб'єкта цього кримінального правопорушення, фактично визначаючи його. Враховуючи те, що «впровадження» – це насамперед організаційно-розпорядче рішення відповідної службової особи про перехід на стандарти освіти країни-агресора (від планування й розробки стандарту до його реалізації та складання освітніх програм та навчальних планів), то суб'єктом кримінального правопорушення у цій формі, на наше переконання, є лише службові особи, що наділені організаційно-розпорядчими функціями. До них передусім належать працівники незаконних органів влади в сфері освіти, а також службові особи закладів освіти, які виконують організаційно-розпорядчі функції (наприклад, завідувачі дошкільних навчальних закладів, директори та завучі шкіл, ректори та проректори внз та ін.), тобто ті, від кого безпосередньо залежить забезпечення навчання відповідно до вимог стандартів освіти країни-агресора. Щодо інших, так би мовити, пересічних педагогічних працівників, то не виключаючи можливість їх активної ініціативної участі у процесі впровадження стандартів освіти, вони можуть нести кримінальну відповідальність за колабораційну діяльність у розглядуваній формі лише як підбурювачі або пособники за правилами

кваліфікації співучасті загального суб'єкта у кримінальних правопорушеннях зі спеціальним суб'єктом, звісно, за наявності всіх необхідних для того ознак співучасті¹.

Так само не охоплюється цією нормою й безпосереднє виконання педагогічними працівниками своїх професійних функцій з власне викладання навчальних предметів на основі вже впроваджених стандартів, про що неодноразово зазначалося у науковій літературі². Така позиція, серед іншого, ґрунтується на тому, що здійснення освітньої діяльності на окупованих територіях є сферою, де у разі збройного конфлікту мають застосовуватися положення міжнародного гуманітарного права, зокрема, вже згадуваної вище Женевської конвенції, у ст. 50 якої прямо зазначається, що окупаційна держава повинна в співробітництві з державними та місцевими органами влади сприяти належному функціонуванню закладів, відповідальних за піклування про дітей і їхню освіту³. Тобто фактично норми міжнародного гуманітарного права сприяють забезпеченню реалізації на окупованих територіях права на освіту, яке гарантоване ст. 53 Конституції України, а також ст. 28 Конвенції про захист дитини та ст. 26 Загальної декларації прав людини.

¹ Нетеса Н. В. Впровадження стандартів освіти країни-агресора як форма кримінально протиправного освітянського колабораціонізму: проблемні аспекти тлумачення та правозастосування. *Питання боротьби зі злочинністю*: зб. наук. пр. / редкол. : В. С. Батиргарєєва та ін. Харків: Право, 2022. Вип. 44. С. 79.

² Букреев О. І., Нетеса Н. В. Колабораціонізм у гуманітарній сфері: пошук оптимального законодавчого рішення та реалії практики застосування ст. 111¹ КК України. *Ретроспектива військової агресії рф в Україні: злочини проти миру, безпеки людства та міжнародного правопорядку в сучасному вимірі*: матеріали міжнар. наук.-практ. круглого столу 22–23 червня 2023 р. Київ: Алерта, 2023. С. 62; Злочинна колаборація в умовах збройної агресії: практичний порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ: Алерта, 2023. С. 120; Нетеса Н. В. Впровадження стандартів освіти країни-агресора як форма кримінально протиправного освітянського колабораціонізму: проблемні аспекти тлумачення та правозастосування. *Питання боротьби зі злочинністю*: зб. наук. пр. / редкол. : В. С. Батиргарєєва та ін. Харків: Право, 2022. Вип. 44. С. 79.

³ Про захист цивільного населення під час війни : Женевська Конвенція від 12.08.1949 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_154#Text (дата звернення: 25.10.2024).

Викладене дає підстави для висновку, що співпраця з країною-агресором у здійсненні освітнього процесу може бути кримінально каранюю лише тоді, коли вона вбирає в себе елементи ідеологічного та (чи) культурного колабораціонізму, що має місце у випадку сприяння у набутті учнями компетентностей так званого національного складника освітніх програм (громадянські, соціальні, ідеологічні, світоглядні компетентності, компетентності володіння і спілкування державною мовою), і, за загальним правилом, не стосується співпраці у формуванні ключових компетентностей освіти впродовж життя, що рекомендовані Європейським Парламентом та Радою Європейського Союзу (загальні навчальні, математична компетентність; компетентності у галузі природничих наук, техніки і технологій; екологічна компетентність; інформаційно-комунікаційна компетентність; навчання впродовж життя) та узгоджені із визначеними ключовими компетентностями на рівні світового освітнього простору¹. Це актуалізує потребу в забезпеченні на правозастосовному рівні того, щоб кожен випадок піддавався індивідуальній оцінці на предмет відсутності в діяннях осіб, що надають освітні послуги, під час викладання ними навчальних предметів ознак іншої закріпленої у ч. 3 аналізованої статті форми освітнього колабораціонізму – пропаганди 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 за певних обставин – й ознак державної зради.

Аналізуючи зміст **ч. 6 ст. 111¹ КК**, де передбачена кримінальна відповідальність за організацію 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 адміністра-**

¹ Рекомендації Європейського Парламенту та Ради Європейського Союзу щодо формування ключових компетентностей освіти впродовж життя: Міжнародний документ від 18.12.2006 № 2006/962/ЄС. Верховна Рада України. Законодавство України: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/994_975#Text (дата звернення: 25.10.2024).

ції чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України, за відсутності ознак державної зради, а також за активну участь у таких заходах, слід відмітити, що незважаючи на те, що у примітці до ст. 111¹ КК надається тлумачення термінів «заходи політичного характеру» (п. 2 Примітки, де фактично просто наводиться їх відкритий перелік – з'їзди, збори, мітинги, походи, демонстрації, конференції, круглі столи тощо) та «здійснення інформаційної діяльності» (п. 3, де перелічуються види інформаційної діяльності – створення, збирання, одержання, зберігання, використання та поширення відповідної інформації), це аж ніяк не полегшує застосування цієї норми. Річ у тім, що за наведених обставин відкритим залишається питання, як розмежовувати не лише суміжні форми колабораційної діяльності (ч. 1 та ч. 3), а й суміжні склади кримінальних правопорушень, передбачених ст. 436², ст. 111², а так само ст. 111 КК, адже саме в ч. 6 законодавець прямо вказав на відсутність ознак державної зради, але яких саме так і не зрозуміло, що по-різному оцінюється фахівцями-правознавцями. Так, Г. М. Анісімов зауважує, що вказівка «за відсутності ознак державної зради» фактично свідчить про те, що діяння кваліфікуються за ч. 6 ст. 111¹ КК тільки тоді, коли вони вчиняються іноземцем чи особою без громадянства; якщо ж такі дії вчиняє громадянин України, то, на думку судді ККС Верховного суду, в них наявні ознаки державної зради¹.

З таким висновком, звісно, погодитися важко, адже те, що законодавець не вказав у ч. 6 ст. 111¹ КК на суб'єкта вчинення кримінального правопорушення, не змінює природи самої колабораційної діяльності, соціальна сутність якої полягає у співпраці з державою-агресором саме громадян країни, територія якої зазнала агресії та потрапила під окупацію. На наш погляд, наявна вада законодавчої техніки може бути цілком подолана, якщо виходити з того, що окремі ознаки складу кримінального правопорушення можуть не лише прямо зазначатися в законі, а й однозначно впливати з його змісту,

¹ Антонюк Н., Анісімов Г. Як розмежовувати колабораційну діяльність і суміжні склади кримінальних правопорушень? *Верховний Суд*: оф. вебсайт. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1299973/> (дата звернення: 25.10.2024).

що й має місце у даному випадку. У цьому контексті слухним виглядає зауваження З. А. Загинеї-Заболотенко, яка справедливо зазначає, що для тлумачення кримінально-правових норм особливо важливого значення набуває не лише лінгвістичний аналіз нормативних речень, а й логічний аналіз змісту кримінально-правових понять¹. З огляду на це більш переконливою вбачається позиція, коли розмежування з державною зрадою стосується форми інформаційної діяльності, що подібна до шпигунства, але за умови, що предметом кримінального правопорушення є інформація, яка не належить до категорії державної таємниці.

Не вдаючись до непростой дискусії про те, що мав на увазі законодавець, доповнюючи норму ч. 6 ст. 111¹ КК вказівкою на відсутність ознак державної зради (адже це, знов таки, може бути невдалою спробою законодавця закласти підстави для розмежування суміжних складів кримінальних правопорушень), вважаємо за доцільне більше уваги приділити тому аспекту, який стосується саме предмета нашого дослідження. Розуміючи те, що законодавець навряд чи ставив собі за мету створити колізію норм, тим більше у межах однієї статті про колабораційну діяльність, та враховуючи разючу різницю між ступенем тяжкості передбаченого ч. 6 ст. 111¹ КК діяння, яке законодавцем віднесено до категорії особливо тяжких злочинів, та іншими формами суміжних інформаційних діянь, що передбачені частинами 1 та 3 ст. 111¹ КК, ст. 436² КК, вважаємо, що ключовий момент для забезпечення правильної кваліфікації діянь за ознаками ч. 6 ст. 111¹ КК треба шукати саме в характері тієї протиправної діяльності, яка не може зводитися до спрощених її форм. Для підтвердження висунутої гіпотези ми звернулися до практики застосування ч. 6 ст. 111¹ КК, вивчення якої показало, що найчастіше за цією нормою в частині здійснення інформаційної діяльності кваліфікуються: адміністрування сайтів, які просувають наративи російської пропаганди; підготовка та розміщення у соцмережах з необмеженим доступом і кількістю користувачів статей та інших матеріалів на підтримку держави-агре-

¹ Загинеї З. А. Кримінально-правова герменевтика: монографія. Київ: Вид. дім «АртЕк», 2015. С. 107–108.

сора; діяльність головних редакторів, редакторів, військових кореспондентів та журналістів окупаційних друкованих та онлайн медіа; активна участь в інтерв'ю російських пропагандистських медіа видань представників незаконних органів влади та місцевого самоврядування на окупованих територіях. Крім того, аналіз практики підтвердив наше припущення, що проведення заходів політичного характеру, як правило, супроводжується здійсненням інформаційної діяльності у вигляді проведення пропагандистських заходів та їх масового висвітлення у медіа, насамперед російських та окупаційних, а також у мережі Інтернет, що певним чином пояснює передбачення цих форм об'єктивної сторони колабораційної діяльності у межах однієї норми КК.

Таким чином, можна констатувати, що слідча та судова практика здебільшого йдуть правильним шляхом у частині розуміння інформаційної діяльності як такої, що здійснюється систематично та цілеспрямовано, а не зводиться до одноразового факту передачі чи поширення інформації. Це дає підстави погодитися з висловленою в юридичній літературі позицією про те, що *інформаційна діяльність* у розумінні ч. 6 ст. 111¹ КК – це специфічна професійна, політична чи громадська діяльність відповідних суб'єктів, яка полягає в: а) інформаційній взаємодії з органами влади, об'єднаннями громадян, юридичними та фізичними особами; б) створенні та організації доступу до публічної інформації; в) впорядкуванні інформаційних ресурсів; г) формуванні інформаційно-комунікаційної інфраструктури, засобів зв'язку та засобів інформаційної безпеки¹. Враховуючи висловлене, на перспективу вдосконалення аналізованої норми можна запропонувати передбачити спеціального суб'єкта відповідальності за здійснення інформаційної діяльності, що дозволить зняти питання про розмежування з суміжними складами кримінальних правопорушень та виправдати достатньо суворе покарання за цю форму колабораційної діяльності. Крім того, зайвим видається згадування у тексті диспозиції ч. 6 ст. 111¹ КК про вчинення описаних у ній діянь

¹ Злочинна колаборація в умовах збройної агресії: практич. порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ : Алерта, 2023. С. 139.

«у співпраці з державою-агресором та/або його окупаційною адміністрацією», що, з одного боку, і так є іманентною ознакою колабораційної діяльності, а, з другого, створює хибне уявлення про те, що нібито для інших форм колабораційної діяльності (крім передбачених у частинах 4 та 6 ст. 111¹ КК) вона не є обов'язковою¹. Такий висновок суперечить сутності колабораційної діяльності, яка завжди віддзеркалює відповідну поведінку як елемент взаємодії (співпраці) з ворогом (окупантом)². Інша справа, що така взаємодія з ворогом може бути дистантною, що є специфічною рисою насамперед інформаційних діянь, вчинення яких на шкоду Україні є можливим як на тимчасово окупованій території, так і на території, що підконтрольна Україні, чи взагалі закордоном. Але навіть визнання можливості безконтактної взаємодії з ворогом, повторимося, не повинно змінювати соціально-правової природи колабораційної діяльності як такої, що як явище існує лише на окупованих територіях. На користь висловленої нами позиції про доцільність прив'язки колабораційної діяльності до території окупації свідчить й відображена в проєкті нового КК (ст. 9.6.1) пропозиція вважати колабораційною діяльністю добровільну співпрацю з державою-агресором громадянина України саме на тимчасово окупованій її території³.

Отже, на нашу думку, позиція законодавця, який не вказав у ч. 6 ст. 111¹ КК (так само як і в її ч. 4) не лише на місце вчинення кримінального правопорушення, а й на громадянина України як його суб'єкта, є законодавчою помилкою, яка має своїм наслідком не-

¹ Нетеса Н. В. Інформаційний колабораціонізм: деякі проблемні аспекти тлумачення та застосування кримінально-правових норм. *Інформація і право*. 2024. № 4(51). С. 229. DOI: [https://doi.org/10.37750/2616-6798.2024.4\(51\).318138](https://doi.org/10.37750/2616-6798.2024.4(51).318138).

² Письменський Є. О. Ідеологічний та культурно-освітній колабораціонізм як посягання на інформаційну безпеку. *Кримінально-правова охорона інформаційної безпеки*: матеріали VI міжнар. наук.-практ. конференції, м. Харків, 12 трав. 2022 р. / [редкол.: Л. М. Демидова (голов. ред.) та ін.]; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України; Нац. юрид. ун-т ім. Ярослава Мудрого; громад. організація «Всеукраїнська асоціація кримінального права». Харків: Право, 2022. С. 84.

³ Текст проєкту нового Кримінального кодексу України: контрольний текст (станом на 01.08.2024). Робоча група з питань розвитку кримінального права. URL: <https://newcriminalcode.org.ua/criminal-code> (дата звернення: 25.10.2024).

виправдану можливість визнання колаборантами не лише громадян України, які не проживають на окупованих територіях, а й іноземців та осіб без громадянства, що, до речі, нерідко зустрічається у юридичній літературі¹. Вбачається, що таке буквальне тлумачення законодавчих положень є неприпустимим, оскільки КК містить достатньо інструментів для кримінального переслідування останніх за іншими статтями, які передбачають, зокрема, відповідальність за державну зраду (коли суб'єктом є громадянин України) або пособництво державі-агресору (якщо кримінальне правопорушення вчинив іноземець чи особа без громадянства), звісно, за наявності ознак цих кримінальних правопорушень.

Підводячи підсумок розгляду форм колабораційної діяльності в інформаційній сфері, зазначимо, що всі вони є прямоумисними кримінальними правопорушеннями, для більшості з яких у законі передбачена спеціальна мета, яка або прямо зазначається в тексті диспозиції, як, наприклад, в ч. 3 ст. 111¹ КК (з метою сприяння здійсненню збройної агресії проти України, встановленню та утворенню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України), або випливає зі змісту закону, на що вказує вживання термінологічної конструкції «дії, спрямовані...», наприклад, на впровадження стандартів освіти держави-агресора (ч. 3 ст. 111¹ КК), на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або уникнення нею відповідальності за збройну агресію проти України (ч. 6 ст. 111¹ КК). Щодо мотивації поведінки «інформаційних» колаборантів, то вона може бути різною – ідеологічною, коли особа діє відповідно до своїх переконань та уявлень; політичною, якщо вона, наприклад, прагне зайняти керівні посади в органах окупаційної адміністрації чи незаконних органах місцевої влади або ж просунути по партійній

¹ Антонюк Н., Анісімов Г. Як розмежовувати колабораційну діяльність і суміжні склади кримінальних правопорушень? *Верховний Суд*: оф. вебсайт. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1299973/> (дата звернення: 25.10.2024); Мовчан Р. О. Воєнні новели Кримінального кодексу України: правотворчі та правозастосовні проблеми: монографія. Київ: Норма права, 2022. С. 41.

лінії; корисливою, коли її поведінка зумовлена лише прагненням до збагачення; тощо.

1.3.3. Пособництво державі-агресору в інформаційній сфері (ст. 111² КК України)

Відповідальність за пособництво державі-агресору, закріплена в ст. 111² КК, є новелою українського кримінального законодавства, поява якої пов'язана з прийняттям в умовах повномасштабної агресії РФ проти України Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки» від 14 квітня 2022 р. № 2198-IX¹. Поспішність у прийнятті цього Закону та фактична ідентичність обґрунтування доцільності запровадження кримінальної відповідальності за пособництво державі-агресору та за колабораційну діяльність (про що свідчить аналіз змісту Пояснювальних записок до обох законопроектів – реєстр. № 5144 від 24.02.2021 р.² (колабораційна діяльність) та реєстр. № 7186 від 21.03.2022 р.³ (пособництво державі-агресору)) разом із виділенням відповідного скла-

¹ Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки: Закон України від 14.04.2022 р. № 2198-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2198-20#Text> (дата звернення: 25.10.2024).

² Проект Закону про внесення змін до деяких законодавчих актів (щодо встановлення кримінальної відповідальності за колабораційну діяльність) (реєстр. № 5144 від 24.02.2021). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5144&conv=9> (дата звернення: 25.10.2024).

³ Проект Закону України про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливостей застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки (реєстр. № 7186 від 21.03.2022 р.). *Верховна Рада України. Законопроекти*: оф. вебсайт.

ду кримінального правопорушення зі складу державної зради очікувано спричинили низку труднощів у застосуванні норми ст. 111² КК. Ці проблеми, не в останню чергу, зумовлені суттєвими недоліками законодавчого конструювання досліджуваної норми, серед яких на-самперед занадто широкий зміст описаного в диспозиції ст. 111² КК діяння, яке сформульовано як «умисні дії, спрямовані на допомогу державі-агресору», що є дуже неконкретизованим і фактично охоплює будь-які дії, які за своєю природою можуть бути як фізичними, так і інтелектуальними, в тому числі й інформаційними. Навіть уточнення в законі про форми пособництва, такі як 1) підтримка чи реалізація рішень і дій держави-агресора, його збройних формувань або окупаційної адміністрації та 2) добровільний збір, підготовка і передача матеріальних ресурсів чи інших активів представникам агресора, не усувають цієї невизначеності.

Зокрема, одразу виникає запитання стосовно тих рішень держави-агресора, реалізація чи підтримка яких може становити склад аналізованого кримінального правопорушення, адже вони можуть стосуватися будь-яких питань – як загальних (збройна агресія під виглядом спеціальної воєнної операції, створення псевдодержавних утворень на окупованих територіях), так і локальних (призначення керівників незаконних органів, здійснення нормотворчої діяльності, забезпечення правопорядку на окупованих територіях, організація та здійснення освітнього процесу, наповнення бюджету псевдодержавних утворень тощо). Крім того, такі рішення можуть стосуватися різних сфер – військової, політичної, економічної, ідеологічної, освітньої, культурної та ін. Єдине, що можна з певною мірою впевненості стверджувати, це те, що зі змісту диспозиції ст. 111² КК, де міститься пряма вказівка на мету вчинення цього кримінального правопорушення, випливає, що такі рішення та дії мають бути спрямовані на шкоду Україні, що автоматично має виводити з-під юрисдикції цієї норми реалізацію чи підтримку тих рішень та дій, які або не здатні заподіювати шкоду саме державі (як-от, забезпечення благо-

URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=7186&conv=9> (дата звернення: 25.10.2024).

устрою окупованих територій), або ж спрямовані на виконання країною-агресором зобов'язань, передбачених нормами міжнародного гуманітарного права (зокрема, щодо обміну військовополоненими, проведення санітарно-епідеміологічних заходів, надання медичної допомоги цивільному населенню та ін.).

Так само значні труднощі виникають і з тлумаченням та встановленням обсягу понять «реалізація» та «підтримка» через очевидну розмитість їх меж. Так, реалізація рішень, хоча й традиційно асоціюється з організаційним аспектом забезпечення виконання певного рішення іншими особами¹, однак сама по собі є багатоступеневим процесом, участь в якому становитиме склад аналізованого злочину незалежно від досягнення необхідного результату – факту реалізації такого рішення. Що ж стосується підтримки, то вона взагалі передбачає невизначений спектр діянь – від схвалення конкретних ініціатив до добровільного виконання рішень та дій держави-агресора.

Певне розв'язання цієї проблеми, на наш погляд, лежить у площині визначення характеру інформаційних дій, які за своїм енергетичним змістом здатні заподіювати шкоду інтересам України та відповідно становити пособництво державі-агресору саме в інформаційній сфері. Вбачається, що у чистому вигляді інформаційні дії можуть становити склад аналізованого кримінального правопорушення насамперед тоді, коли допомога полягає у передачі агресору певної інформації, необхідної для реалізації його рішень. Наприклад, особа надає інформацію про людей, стосовно яких агресор планує нейтралізацію чи фізичне усунення з метою придушення супротиву (зокрема, щодо учасників АТО, ветеранів, активістів Революції Гідності, пенсіонерів Збройних Сил України чи патріотично налаштованих громадян та ін.). Або ж ще один приклад, коли особа, добре знаючи місцевість, інформує ворога про місця, які найкраще підходять для розміщення військової техніки чи особового складу збройних формувань держави-агресора, або надає відомості про оптимальні маршрути пересування, сприяючи тим самим реалізації їхніх логіс-

¹ Злочинна колаборація в умовах збройної агресії: практичний poradnik з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малука. Київ: Алерта, 2023. С. 154.

тичних завдань. Так само, як показав аналіз практики застосування ст. 111² КК в аспекті, що нас цікавить, як «чисте» інформаційне пособництво державі-агресору можна розцінювати кваліфіковани за ст. 111² КК випадки, коли суб'єкти надання інформаційно-комунікаційних послуг та зв'язку передають представникам російських спецслужб інформацію, яка міститься в належних їм мережах електронного зв'язку, що сприяє витоку чутливої для України інформації, або, приміром, блокують українські медіа та інтернет-ресурси на користь російських, що сприяє поширенню ворожої пропаганди, а також русифікації населення окупованих територій та його асиміляції з населенням країни-окупанта.

В інших же випадках інформаційне пособництво державі-агресору, як уявляється, має здебільшого допоміжний (субсидіарний) характер, оскільки зводиться або до етапу реалізації відповідного рішення, або ж становить собою його підтримку. Так, наприклад, особа, обійнявши відповідну посаду та розпочавши реалізацію рішення держави-агресора щодо паспортизації населення окупованих територій або проведення виборів чи референдуму на цих територіях, з метою популяризації таких рішень поширює проросійський агітаційний контент через свої акаунти у соцмережах чи в утворених Telegram-каналах з відкритим необмеженим доступом. В аналогічний спосіб може здійснюватися й інформаційний супровід збирання коштів або надання гуманітарної та волонтерської допомоги збройним формуванням РФ, коли розміщуються відповідні пости про допомогу в соцмережах та здійснюється поширення цього контенту через інтернет-ресурси. Вочевидь, що подібна діяльність переважно є формою саме підтримки рішень держави-агресора, оскільки особа, яка займається поширенням вище вказаної інформації, може взагалі не мати безпосереднього відношення до збору коштів, обмежуючись популяризацією відповідних заходів, у тому числі у форматі проросійської агітації¹.

¹ Нетеса Н. В. Проблемні питання визначення форм пособництва державі-агресору в інформаційній сфері. *Посилення спроможностей СБУ України та взаємодія зі складовими сектору безпеки і оборони: матеріали міжвідомч. наук.-практ. конференції* (м. Київ, 27 вересня 2024 р.). Київ : НА СБУ, 2024. у 2-х ч. Ч. 1, С. 159–160.

Отже, інформаційна підтримка рішень держави-агресора так чи інакше пов'язана з різними проявами циркуляції інформації з протиправним контентом – від її збирання до поширення, окремі з яких є подібними до інших передбачених КК форм кримінально караних інформаційних діянь. Констатуючи таку ситуацію, Р. О. Мовчан доходить висновку про те, що норма про пособництво державі-агресору у формі підтримки рішень перебуває у конкуренції принаймні з трьома іншими кримінально-правовими нормами, а саме: 1) ч. 6 ст. 111¹ КК, де встановлена кримінальна відповідальність за організацію та проведення заходів політичного характеру, а також здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, що карається позбавленням волі на строк від 10 до 12 років; 2) ч. 1 ст. 111¹ КК, за якою кримінально караними визнаються публічні заклики до підтримки рішень та дій указаних в ній суб'єктів та співпраці з ними, за які передбачено позбавлення права обіймати певні посади або займатися певною діяльністю на строк від 10 до 15 років; 3) ч. 1 ст. 436² КК, за якою можуть кваліфікуватися дії осіб, які здійснюють виправдовування, визнання правомірною, заперечення збройної агресії РФ проти України (найсуворішим видом покарання за які є позбавлення волі на строк до трьох років), а також ч. 2 ст. 436² КК, за якою кваліфікується виготовлення та поширення матеріалів з відповідним змістом (карається позбавленням волі на строк до п'яти років), які, на переконання науковця, можуть розцінюватися як окремі форми підтримки дій держави-агресора¹.

Розглядаючи пособництво державі-агресору в системі окреслених суміжних кримінально протиправних діянь, вважаємо, що при їх розмежуванні насамперед треба виходити з правильного визначення ступеня реалізації діяння щодо підтримки чи реалізації рішень та дій указаних у ній суб'єктів. У цьому аспекті слід наголосити, що фактично ч. 1 ст. 111¹ КК передбачає екстраусічений до стадії готування до кримінального правопорушення склад, за якого ще не починає ви-

¹ Мовчан Р. О. Восенні новели Кримінального кодексу України: правотворчі та правозастосовні проблеми: монографія. Київ: Норма права, 2022. С. 82.

конуватися об'єктивна сторона основного діяння у вигляд підтримки чи реалізації рішень, що недостатньо для констатації того, що особа надає саме допомогу державі-агресору. Тоді як ст. 111² КК передбачає або закінчений злочин із формальним складом (у разі дійсної підтримки чи реалізації відповідних рішень держави-агресора) або ж склад, що є усіченим до стадії замаху, якщо особа вчинила хоча б частину дій, спрямованих на підтримку чи реалізацію таких рішень або дій. І дійсно, закріплене в ч. 1 ст. 111¹ КК публічне заперечення збройної агресії не обов'язково прямо сприяє такій агресії, на відміну від надання допомоги державі-агресору, так само як і публічні заклики – це ще не виконання того діяння, до якого закликає правопорушник інших осіб. Наприклад, особа може вчиняти публічні заклики не з ідеологічних мотивів, а з корисливих, і тоді їй взагалі байдуже, чи вчинять інші особи те діяння, до якого вона закликає, і чи будуть реалізовані рішення та дії держави-агресора.

Щодо ч. 1 ст. 436² КК то, на наш погляд, тут конкуренція майже не виникає, адже, окрім вже висловленого, норма не передбачає факту взаємодії з ворогом взагалі, це, як правило, висловлення власної антиукраїнської позиції, переконань, думок, які за змістом повторюють головні наративи російської пропаганди. Звісно, що суспільна небезпечність таких діянь не стає від цього меншою, більше того, такі інформаційні дії здатні розхитати українське суспільство, що є бажаним результатом для ворога, але це не змінює сутності діяння і не перетворює його на пособництво державі-агресору. Виготовлення ж та поширення матеріалів відповідного змісту (ч. 2 ст. 436² КК), безумовно, вже є матеріалізованою формою руху інформації і могло б становити прояв підтримки, якби супроводжувалося підтвердженням факту реалізації чи підтримки у такий спосіб рішень чи дій держави-агресора. За інших умов такі діяння не можуть підпадати під ознаки ст. 111² КК.

І, нарешті, найбільше складнощів із розмежуванням виникає саме у випадку конкуренції ст. 111² КК з ч. 6 ст. 111¹ КК. Тут, дійсно, вказівка в законі на здійснення інформаційної діяльності у співпраці з державою-агресором (що, як уже зазначалося, вбачається взагалі зайвим), так само як і широке визначення самої інформаційної ді-

яльності у п. 3 примітки до ст. 111¹ КК, створює додаткові умови для ускладнення розмежування цього злочину із пособництвом державі-агресору, враховуючи те, що покарання за обидва кримінальні правопорушення є абсолютно ідентичними – позбавлення волі на строк від 10 до 12 років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк від 10 до 15 років та з конфіскацією майна або без такої. За нині чинних редакцій ч. 6 ст. 111¹ КК та ст. 111² КК в аспекті, що є предметом нашого дослідження, якщо виходити саме з буквального тлумачення законодавчих положень, єдиною очевидною розмежувальною їх ознакою є лише вказівка у ст. 111² КК на те, що суб'єктом цього кримінального правопорушення не може бути громадянин держави-агресора. Зрозуміло, що цього явно не достатньо для розмежування розглянутих кримінальних правопорушень, адже у переважній більшості випадків ці кримінальні правопорушення вчиняються саме громадянами України. Парадоксальність цієї ситуації зумовлена тим, що, як ми вже зазначали, норма про колабораційну діяльність, відповідальність за яку передбачена ч. 6 ст. 111¹ КК, не обмежує коло її суб'єктів громадянами України, що суперечить сутності колабораціонізму як такому і є прикладом грубої помилки законодавця, яка вимагає якнайшвидшого її виправлення. Але поки ця законодавча вада не усунена, шлях до подолання конкуренції зазначених норм, на наш погляд, лежить у площині правильного розуміння інформаційної діяльності саме як професійної, ознаки якої були наведені нами у попередньому підрозділі 1.3.2., та недопущення зведення її до простих форм оперування інформацією. Тоді як в контексті ст. 111² КК інформаційна активність на реалізацію чи підтримку рішень або дій держави-агресора допускає більш прості форми інформаційних діянь, які виконують субсидіарну роль у реалізації стратегічних завдань держави-агресора.

На завершення характеристики пособництва державі-агресору в інформаційній сфері зазначимо, що аналізований склад кримінального правопорушення, так само як і колабораційна діяльність, передбачає лише прямий умисел, на користь чого, серед іншого, свідчить і вказівка на спеціальну мету – завдання шкоди Україні.

Остання іноді використовується для розмежування суміжних складів кримінальних правопорушень, що, на наше переконання, у переважній більшості випадків є штучним, адже ця ознака, незважаючи на відсутність прямої вказівки на неї в нормах про колабораційну діяльність, властива їм за умовчанням через те, що співпраця з державою-агресором, подібно до державної зради, за своєю природою не може бути на користь країни, яка зазнала збройної агресії. Проте безпосереднє зазначення такої мети в диспозиції ст. 111² КК може бути розцінене як не дуже вдала спроба законодавця обмежити об'єктивну сторону пособництва державі-агресору лише найбільш небезпечними для національної безпеки України його формами, які обґрунтовують доцільність застосування достатньо суворого покарання, розуміючи, що рішення та дії держави-агресора можуть становити різний рівень суспільної небезпечності, в тому числі такий, що не завжди завдає шкоди саме державі Україна.

1.4. Інформаційні кримінально-протиправні діяння, що посягають на обороноздатність України (ст. 114² КК України)

1.4.1. Загальні положення

У правовій державі закон, у тому числі про кримінальну відповідальність, повинен бути спрямований на захист прав і свобод людини, її честі та гідності тощо. Він має відповідати природі людини, її цінностям, тобто бути соціально обумовленим¹.

24 лютого 2022 року РФ розгорнула повномасштабну збройну агресію проти України. Указом Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року № 64/2022 в Україні введено воєнний стан, який серед іншого передбачає також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів

¹ Пащенко О. О. Соціальна обумовленість закону про кримінальну відповідальність: загальні питання. Проблеми законності. 2008. Вип. 96. С. 121–129.

юридичних осіб із зазначенням строку дії цих обмежень (ст. 1 Закону України «Про правовий режим воєнного стану»)¹. Враховуючи небезпечність інформаційної експансії ворога, в умовах гібридної війни гостро постало питання обмеження поширення не лише інформації, яка становить державну чи іншу таємницю, а й так званої чутливої в умовах війни іншої інформації, насамперед військового характеру.

Відповідно до пояснювальної записки до проекту Закону про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому розповсюдженню інформації про направлення, переміщення міжнародної військової допомоги в Україну, рух, переміщення або розміщення Збройних Сил України чи інших військових формувань України, вчинене в умовах воєнного або надзвичайного стану (реєстр. № 7189 від 22.03.2022 р.), низка громадян України, іноді несвідомо та необмірковано, надають допомогу ворогу шляхом розповсюдження інформації зазначеного змісту, не реагуючи при цьому на численні заклики Збройних Сил України припинити таку неприпустиму в умовах продовження збройної агресії та ведення бойових дій діяльність. Така діяльність є формою пособництва державі-агресору, яке як явище підриває національну безпеку України та становить безпосередню загрозу державному суверенітету, територіальній цілісності, конституційного ладу та іншим національним інтересам України, а отже, має тягти за собою встановлену законом відповідальність².

¹ Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text> (дата звернення: 15.11.2024).

² Проект Закону про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому розповсюдженню інформації про направлення, переміщення міжнародної військової допомоги в Україну, рух, переміщення або розміщення Збройних Сил України чи інших військових формувань України, вчинене в умовах воєнного або надзвичайного стану (реєстр. № 7189 від 22.03.2022). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=7189&conv=9> (дата звернення: 15.11.2024).

З огляду на це Законом України № 2160-IX від 24.03.2022 р.¹ внесено зміни до КК та криміналізовано 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 (ст. 114²).

Одразу зазначимо, що незважаючи на нетривалий час існування в КК статті 114², вона вже неодноразово піддавалася спробам її вдосконалення з боку самого законодавця. Підтвердженням цьому слугує та кількість законопроектів, що зареєстрована у Верховній Раді України, а саме: «Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації» (реєстр. № 7236 від 31.03.2022 р.², прийнято Закон України № 2178-IX від 01.04.2022 р.³); «Про внесення змін до статті 114-2 Кримінального кодексу України (щодо удосконалення відповідальності за несанкціоноване поширення інформації в умовах воєнного або надзвичайного стану)» (реєстр. № 7455 від

¹ Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню 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, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24.03.2022 № 2160-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#Text> (дата звернення: 15.11.2024).

² Проект Закону про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації (реєстр. № 7236 від 31.03.2022). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/39337> (дата звернення: 15.11.2024).

³ Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 01.04.2022 № 2178-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2178-IX#Text> (дата звернення: 15.11.2024).

10.06.2022 р.)¹; «Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення положень про кримінальну відповідальність за несанкціоноване поширення інформації про вогневе ураження об'єктів на території України» (реєстр. № 8218 від 23.11.2022 р.)²; «Про внесення змін до Кримінального кодексу України щодо посилення кримінальної відповідальності за 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» (реєстр. № 9519 від 24.07.2023 р.)³ тощо.

Не ставлячи за мету надання вичерпного аналізу складу вказаного кримінального правопорушення, адже цьому питанню достатньо багато уваги приділено в наукових джерелах (зокрема, у публікаціях О. О. Дудорова, Р. О. Мовчана, Ю. А. Пономаренка, М. І. Хавронюка, Н. М. Ярмиш та ін.), у межах цього монографічного дослідження зосередимо увагу на окремих проблемних аспектах, що викликають труднощі правозастосування цієї норми. Так, за даними реєстру судових рішень за ст. 114² КК з моменту її прийняття по

¹ Проект Закону про внесення змін до статті 114-2 Кримінального кодексу України (щодо удосконалення відповідальності за несанкціоноване поширення інформації в умовах воєнного або надзвичайного стану) (реєстр. № 7455 від 10.06.2022). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/39765> (дата звернення: 15.11.2024).

² Проект Закону про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення положень про кримінальну відповідальність за несанкціоноване поширення інформації про вогневе ураження об'єктів на території України (реєстр. № 8218 від 23.11.2022). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/40869> (дата звернення: 15.11.2024).

³ Проект Закону про внесення змін до Кримінального кодексу України щодо посилення кримінальної відповідальності за 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 (реєстр. № 9519 від 24.07.2023). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/42345> (дата звернення: 15.11.2024).

16 листопада 2024 року у провадженні слідчих перебувало більш ніж 660 кримінальних проваджень, з яких розглянуто судами 170, розглядається 244, закрито 47, інші знаходяться в провадженні¹. Наведені статистичні дані свідчать про достатню кількість кримінальних проваджень за ст. 114² КК, вже сформовану певну слідчу та судову практику, що потребує якомога скорішого розв'язання наявних проблем кваліфікації кримінальних правопорушень зазначеної категорії як шляхом вироблення єдиної правової позиції щодо її застосування, так і шляхом законодавчого вдосконалення самої норми.

1.4.2. Незаконне поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну (ч. 1 ст. 114² КК України)

Кримінальне правопорушення, передбачене ч. 1 ст. 114² КК, є інформаційним діянням, основу якого становлять дії у формі «поширення інформації» про певні об'єкти. Саме тому вбачається доцільним розпочати кримінально-правовий аналіз цієї норми зі з'ясування наукових підходів до розуміння того, що таке «поширення інформації».

Так, на думку Ю. А. Пономаренка, поширення інформації охоплює будь-які діяння у формі лише активної поведінки, внаслідок яких виникає реальна можливість доступу до інформації хоча б однієї особи, яка раніше не мала права на такий доступ. При цьому поширення інформації може набувати як вербальної форми, так і фізичної (енергетичної). Остання передбачає створення можливості ознайомлення з інформацією, проявами якої є: а) надання доступу до матеріального носія інформації (ознайомлення зі змістом документа (паперовим чи електронним), відкриття доступу до інформації у соціальних мережах, месенджерах тощо); б) тиражування (виготовлен-

¹ Кримінальні правопорушення за ст. 114-2 КК станом на 16.11.2024 р.: витяг з Єдиного реєстру досудових розслідувань № 11292438 від 16.11.2024. *Єдиний реєстр досудових розслідувань*: оф. вебсайт. URL: <https://erdr.gp.gov.ua/erdr/erdr.web.client.UserReportList.cls> (дата звернення: 16.11.2024).

ня копій) матеріального носія інформації (виготовлення копій носія інформації, розповсюдження таких копій серед сторонніх осіб, копіювання інформації в соціальних мережах, месенджерах)¹.

Аналогічну наукову позицію мають М. І. Хавронюк² та Р. О. Мовчан³, які під поширенням інформації розуміють її розголос, опублікування, розміщення в ЗМІ чи соціальній мережі, передачу хоча б одній іншій особі – усно, через месенджер, телефоном тощо. Вони вважають, що поширення не обов'язково має бути публічним. Поширенням є як пост, так і перепост, як твіт, так і ретвіт.

Наведені підходи загалом визнані усталеними у теорії кримінального права. Однак із появою значної кількості норм, які встановлюють кримінальну відповідальність за інформаційні діяння, особливо в умовах війни, у науковій спільноті виникли нові погляди на зміст терміна «поширення». Зокрема, Н. В. Нетеса висловлює думку, що поняття «поширення» обов'язково передбачає широке охоплення аудиторії, а отже, має іманентну ознаку публічності. На її думку, для позначення інших форм дій з інформацією, які не передбачають такої ознаки, існують інші терміни, як-от: надання доступу, передача, заперечення тощо⁴. Цей підхід видається достатньо обґрунтованим.

¹ Пономаренко Ю. А. Кримінально-правове реагування на актуальний виклик інформаційній безпеці в умовах воєнного стану (спроба наукового коментаря до ст. 114-2 ККУ). *Кримінально-правова охорона інформаційної безпеки*: матеріали VI міжнар. наук.-практ. конференції (Харків, 12 травня 2022 р.). Харків: Право, С. 126.

² Хавронюк М. І. Поширення інформації про військову допомогу та дії військових України: кримінальна відповідальність. Аналіз статті 114-2 ККУ із серії науково-практичних коментарів Миколи Хавронюка про зміни до Кримінального кодексу, прийняті під час воєнного стану. *Центр політико-правових реформ*: вебсайт. URL: <https://pravo.org.ua/blogs/poshyrennya-informatsiyi-pro-vijskovu-dopomogu-ta-diyi-vijskovyh-ukrayiny-kryminalna-vidpovidalnist/> (дата звернення: 15.11.2024).

³ Мовчан Р. О. Аналіз кримінально-правової новели про несанкціоноване поширення військово значущої інформації (ст. 114-2 Кримінального кодексу України). *Юридичний науковий електронний журнал*. 2022. № 4. С. 326–330.

⁴ Нетеса Н. В. Глорифікація агресора в контексті деяких форм кримінально караних інформаційних діянь: до питання співвідношення. Інформаційна агресія в сучасному світі: правовий аналіз та протидія : матеріали всеукр. наук.-практ. кругл. столу (м. Харків, 21 червня 2024 р.) : електрон. наук. вид. / редкол.: В. С. Батиргарєва та ін. Харків : Майдан, 2024. С. 216.

ним, адже передача інформації від однієї особи до іншої (так звана «побутова») навряд чи за своїм енергетичним змістом, масштабами та впливом може бути прирівняна до поширення¹, яке має значно більший інформаційний і соціальний резонанс. Таке розмежування розглядуваних термінів дозволяє чіткіше окреслити різні види дій з інформацією, оскільки передача інформації за наявності до того підстав може бути формою інформаційного діяння у складі інших кримінальних правопорушень, наприклад, ст. 111 КК (державна зрада) чи ч. 7 ст. 111¹ КК (колабораційна діяльність).

Для обґрунтування наведеної точки зору доцільним убачається дослідити насамперед етимологію слова «поширення». Так, у Великому тлумачному словнику сучасної української мови термін «поширення» розкривається як дія за значенням поширити, поширитися; як те, що часто трапляється, є широко відомим, популярним. Відповідно поширення інформації трактується як розповсюдження, обнародування інформації, її реалізація у встановленому законом порядку². З огляду на це передавання інформації, так само як і її поширення є процесами, пов'язаними з передачею знань, ідей, даних чи повідомлень. При цьому передавання передбачає передачу інформації від одного джерела до іншого, тоді як поширення охоплює масштабнішу взаємодію, за якої інформація розповсюджується від одного джерела до багатьох. Водночас передавання можна розглядати як перший етап процесу поширення: спочатку інформація передається від одного суб'єкта до іншого, а вже потім поширюється різними каналами – через соціальні мережі, електронну пошту, телефонні дзвінки чи особисті зустрічі. Цю відмінність підкреслює й Н. М. Ярмиш, яка взагалі вважає, що сама передача інформації конкретному адресату – це самостійна, незалежна від поширення дія³.

¹ Федосєєв В. В. Проблемні аспекти тлумачення та застосування норми про кримінальну відповідальність за незаконне поширення інформації про направлення, переміщення зброї, озброєння, та бойових припасів в Україну (ч. 1 ст. 114-2 КК України). *Питання боротьби зі злочинністю*. 2024. Вип. 47. С. 179.

² Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. Київ: Перун, 2005. С. 1098.

³ Ярмиш Н. Проблемні аспекти застосування ч. 3 ст. 114-2 Кримінального кодексу України. *Законодавчі аспекти протидії особливо небезпечним злочинам*

Викладене свідчить, що в ст. 114² КК поняття «поширення інформації» має застосовуватися в обмежувальному значенні, за якого передавання інформації не повинно охоплюватися поширенням інформації з огляду на таке.

Відповідно до положень ст. 34 Основного Закону України кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя¹. Згідно зі ст. 64 Конституції України в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень, передбачені ст. 34 Конституції. Законом, який встановлює обмеження щодо використання інформації, є Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI². Але ж слід зауважити, що цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес. Йдеться про публічну інформацію, до якої відноситься відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних

в Україні: матеріали міжнародного науково-практичного круглого столу (Київ, 14–15 березня 2024). Київ: Алерта, 2024. С. 173.

¹ Конституція України: Закон від 28.06.1996 № 254к/96-ВР. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80?find=1&text=%D1%81%D0%B2%D0%BE%D0%B1%D0%BE%D0%B4#w1_16 (дата звернення: 15.11.2024).

² Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>. (дата звернення: 15.11.2024).

повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом (ст. 1). Наведені нормативно-правові положення підтверджують, що зазначеним Законом регулюється порядок поширення та обмеження використання лише публічної інформації в публічному просторі.

Що стосується поширення інформації представниками засобів масової інформації, то спробою врегулювання порядку здійснення такої діяльності було прийняття наказу Головнокомандувача Збройних Сил України «Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану» від 03.03.2022 р. № 73¹¹. Це було зроблено з метою забезпечення об'єктивного висвітлення подій, пов'язаних з широкомасштабною збройною агресією РФ проти України, та інформування населення та світової спільноти про воєнні злочини РФ, а також задля попередження витoku інформації з обмеженим доступом, запобігання поширенню представниками медіа (у тому числі іноземними) та публічними особами, до думки яких прислуховується громадськість (лідери думок, блогери тощо), відомостей, розголошення яких може нашкодити національній безпеці України у випадку обізнаності противника про дії та плани Збройних Сил України та інших складових сил оборони.

Водночас, незважаючи на наявність окремих нормативно-правових актів, що регламентують діяльність із поширення інформації в умовах воєнного стану, тим не менше доводиться констатувати прогальність чинного законодавства у цій сфері. Відсутність чіткого визначення терміна «поширення інформації» та застосування у правозастосовній практиці розширювального його тлумачення

¹¹ Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками засобів масової інформації на час дії правового режиму воєнного стану: наказ Головнокомандувача Збройних Сил України від 03.03.2022 № 73. *ЛИГА:ЗАКОН*: оф. вебсайт. URL: https://ips.ligazakon.net/document/view/mus36785?an=&ed=2023_02_27&dtm= (дата звернення: 15.11.2024).

породжує низку питань, в тому числі щодо можливості притягнення до кримінальної відповідальності осіб за здійснення ними своєї професійної діяльності. Йдеться насамперед про журналістів, правоохоронців, перших осіб держави, які в рамках виконання своїх посадових обов'язків в месенджерах або в інший спосіб приймають або передають інформацію про направлення, переміщення зброї, озброєння та бойових припасів в Україну, у тому числі про їх переміщення територією України від однієї особи до іншої. Зрозуміло, що така передача інформації відбувається задовго до прийняття офіційного рішення про розміщення або заборони розміщення такої інформації у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України, Головним управлінням розвідки Міністерства оборони України чи Службою безпеки України або в офіційних джерелах країн-партнерів. Такі випадки, на наш погляд, не повинні розглядатися у контексті кримінально протиправного у розумінні ст. 114² КК поширення інформації, адже є складовою здійснення суто професійної діяльності такими особами¹.

При цьому вважаємо за потрібне звернути увагу на те, що поширення саме чутливої інформації не охоплюється, але має охоплюватися аналізованою нормою, з огляду на її значущість для національної безпеки й оборони країни та небезпечність поширення в умовах воєнного стану. До такої чутливої в умовах війни інформації, заборона поширення якої має підпадати під дію ст. 114² КК, на наше переконання, слід відносити принаймні наступне: *інформацію про діяльність об'єктів критичної інфраструктури та державної власності, що мають стратегічне значення для економіки і безпеки держави*, в умовах воєнного або надзвичайного стану (що, до речі, пропонувалося у проекті Закону про внесення змін до статті 114² Кримінального кодексу України (щодо удосконалення відповідальності за несанкціоноване поширення інформації в умовах воєнного або над-

¹ Федосєєв В. В. Проблемні аспекти тлумачення та застосування норми про кримінальну відповідальність за незаконне поширення інформації про направлення, переміщення зброї, озброєння, та бойових припасів в Україну (ч. 1 ст. 114-2 КК України). *Питання боротьби зі злочинністю*. 2024. Вип. 47. С. 181.

звичайного стану), реєстр. № 7455 від 10.06.2022 р.¹), про *захист* таких об'єктів та можливості їх ідентифікації на місцевості, якщо така інформація не розміщувалася у відкритому доступі уповноваженими державними органами; інформацію про *вогневе ураження* державою-агресором або іншими незаконними збройними формуваннями об'єктів критичної інфраструктури або будівель чи споруд, що забезпечують діяльність органів державної влади, органів місцевого самоврядування, державних, комунальних підприємств, установ чи організацій на території України (відповідні доповнення до ст. 114² КК пропонувалися у проєкті Закону про внесення змін до статті 114² Кримінального кодексу України щодо удосконалення положень про кримінальну відповідальність за несанкціоноване поширення інформації про вогневе ураження об'єктів на території України (реєстр. № 8218 від 23.11.2022 р.²); інформацію про *реалізацію вітчизняних проєктів* з розроблення (модернізації) новітнього озброєння і військової техніки, стан виробничих потужностей підприємств, планів їх модернізації та розвитку, темпи (графіки) виробництва готової продукції та залучення підприємств-співвиконавців, відомості щодо відповідальних спеціалістів/розробників інженерно-технічного складу підприємств у сфері безпеки та оборони; інформацію *про місця збору та шляхи евакуації цивільного населення* в умовах воєнного або надзвичайного стану³.

¹ Проєкт Закону про внесення змін до статті 114-2 Кримінального кодексу України (щодо удосконалення відповідальності за несанкціоноване поширення інформації в умовах воєнного або надзвичайного стану) (реєстр. № 7455 від 10.06.2022). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/39765> (дата звернення: 15.11.2024).

² Проєкт Закону про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення положень про кримінальну відповідальність за несанкціоноване поширення інформації про вогневе ураження об'єктів на території України (реєстр. № 8218 від 23.11.2022). *Верховна Рада України. Законопроекти*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/40869> (дата звернення: 15.11.2024).

³ Федосєєв В. В. Проблемні аспекти тлумачення та застосування норми про кримінальну відповідальність за незаконне поширення інформації про направлення, переміщення зброї, озброєння, та бойових припасів в Україну (ч. 1 ст. 114-2 КК України). Питання боротьби зі злочинністю. 2024. Вип. 47. С. 181.

Безумовно, визнаючи доцільною заборону в умовах воєнного стану поширення вказаної інформації, вважаємо за потрібне наголосити на такому.

Наказом Служби безпеки України «Про затвердження Зводу відомостей, що становлять державну таємницю» від 23.12.2020 № 383, зареєстрованого в Міністерстві юстиції України від 14 січня 2021 р. за № 52/35674¹, визначено відомості, що становлять державну таємницю у сферах оборони, економіки, науки і техніки, зовнішніх відносин й державної безпеки та охорони правопорядку тощо. При цьому віднесення відповідної інформації до державної таємниці є виключною компетенцією державних експертів Міністерства оборони або Міністерства з питань стратегічних галузей промисловості України, до сфери компетенції яких відноситься регулювання обігу такої інформації.

Так, наприклад, відомості про належність суб'єктів господарювання до підприємств оборонно-промислового комплексу, які потребують проведення дублювання виробництва товарів оборонного призначення, та визначених відповідним переліком щодо України чи окремого підприємства (п. 1.4.17 Зводу), а також відомості про будівництво підприємств оборонно-промислового комплексу, які розкривають їх дислокацію, призначення, виробничу потужність щодо випуску озброєння (військової техніки, спеціальних комплектувальних виробів до них) за окремими показниками в цілому щодо України або за сукупністю всіх показників у цілому щодо окремого підприємства (п. 2.2.7 Зводу), належать до компетенції Мінстратегпрому².

Відомості за окремими показниками щодо: тактико-технічних характеристик, складу, алгоритмів функціонування, результатів підконтрольної (лідерної) експлуатації окремого складного зразка (системи, комплексу або їх складових) або окремого зраз-

¹ Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Служби безпеки України від 23.12.2020 № 383. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/z0052-21> (дата звернення: 15.11.2024).

² Там само.

ка (системи, комплексу або їх складових) озброєння, військової техніки або боєприпасу, які перебувають в експлуатації (на зберіганні) у військах, витік яких створює загрозу національним інтересам і безпеці (п. 1.9.8 Зводу), є виключною компетенцією Міноборони¹.

Водночас, як свідчить аналіз наведеного документа, на сьогодні більшість видів чутливої інформації не становить державної таємниці, що робить неможливим притягнення особи до кримінальної відповідальності за несанкціоноване публічне розголошення вказаної інформації відповідно до нині чинних норм КК. Саме тому найбільш раціональним шляхом розв'язання ситуації є не внесення доповнень до норми, передбаченої ст. 114² КК, а шляхом внесення змін до регуляторного законодавства, насамперед до ЗВДТ з тим, щоб розширити перелік інформації, яку необхідно визнавати державною таємницею на час дії воєнного стану чи особливого періоду у встановленому законом порядку. Це дозволить кваліфікувати дії винної особи за ст. 328 КК (Розголошення державної таємниці) чи ст. 422 КК (Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості).

Проте на законодавчому рівні неврегульованими залишаються й деякі інші питання відповідальності за вчинення суспільно небезпечних діянь у сфері обігу інформації. Так, досі відсутня кримінальна відповідальність за публічне несанкціоноване поширення відомостей, що становлять державну таємницю, вчинене на шкоду суверенітету, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України, якщо такі дії вчиняє не та особа, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків (що дозволяє притягнути особу до кримінальної відповідальності за ст. 328 чи ст. 422 КК), а, наприклад, якщо такі відомості поширює блогер чи інший інфлюенсер. Так само необхідно констатувати й непередбаченість кримінальної відповідальності за незаконне

¹ Там само.

зберігання такої інформації з метою її подальшої передачі іноземній державі, іноземній організації або їх представникам, а також за передачу відомостей, що становлять державну таємницю, іноземній злочинній організації, а так само за зберігання таких відомостей з метою передачі¹.

1.4.3. Незаконне поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань (ч. 2 ст. 114² КК України)

Ще однією формою кримінально караних інформаційних діянь, предметом яких є військово значуща інформація, є поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань (ч. 2 ст. 114² КК). З огляду на те, що судження з приводу розуміння терміна «поширення», що характеризує об'єктивну сторону цього кримінального правопорушення, викладені у попередньому тексті, тут розглянемо лише ті аспекти, які, на наш погляд, мають значення для вирішення неоднозначних питань притягнення до кримінальної відповідальності за вчинення аналізованого суспільно небезпечного діяння. Вбачається, що одним із таких аспектів, що заслуговує на увагу, є врахування статусу та особливостей території, на якій поширюється така інформація, – чи то контрольована Україною прифронтна зона або деокуповані території, чи то тимчасово окуповані РФ території України, чи то навіть контрольовані Україною території РФ.

Так, слід відмітити, що, наприклад, на деокупованих територіях вчинення таких діянь нерідко сприймається представниками сил

¹ Федосєєв В. В. Проблемні аспекти тлумачення та застосування норми про кримінальну відповідальність за незаконне поширення інформації про направлення, переміщення зброї, озброєння, та бойових припасів в Україну (ч. 1 ст. 114-2 КК України). *Питання боротьби зі злочинністю*. 2024. Вип. 47. С. 182.

безпеки та оборони України¹, а в результаті й іншими правозастосувачами, як колабораційна діяльність, що здебільшого зумовлено невинуватою стигматизацію населення цих територій як колаборантів. Такий підхід, на наше переконання, не може бути підтриманий через те, що не враховує специфічну природу колабораціонізму як такого, що на відміну від інших можливих форм взаємодії з агресором, є можливим лише в умовах окупації, які якраз і визначають сутність цього суспільно небезпечного явища. Саме тому, залежно від обставин вчинення відповідних діянь особами, які не мають постійних зв'язків із тимчасово окупованою територією, необхідно кваліфікувати не як колабораційну діяльність (зокрема за ч. 7 ст. 111¹ КК), а за ст. 114² КК або за наявності підстав за іншими статтями, наприклад, 111, 111² КК тощо.

Дійсно, колабораційна діяльність у формі надання незаконним збройним чи військовим формуванням, створеним на тимчасово окупованих територіях, допомоги у веденні бойових дій проти Збройних Сил України та інших військових формувань, утворених відповідно до законів України, добровольчих формувань, що були утворені або самоорганізувалися для захисту незалежності, суверенітету та територіальної цілісності України (ч. 7 ст. 111¹ КК), якщо така допомога має інформаційний характер, є дуже подібною до несанкціонованого поширення указаної у ч. 2 ст. 114² КК інформації. Підсилює цю подібність вказівка в диспозиції ч. 7 ст. 111¹ КК на те, що ця допомога надається визначеним у законі суб'єктам у веденні бойових дій проти України, визначення яких міститься у ст. 1 Закону України «Про оборону України», де вказано, що бойові дії – це форма застосування з'єднань, військових час-

¹ *Примітка:* Під силами безпеки розуміються правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України, а сили оборони складають Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави (див.: п.п. 17, 18 Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII).

тин, підрозділів (інших сил і засобів) Збройних Сил України, інших складових сил оборони, а також поліції особливого призначення Національної поліції України для вирішення бойових (спеціальних) завдань в операціях або самостійно під час відсічі збройної агресії проти України або ліквідації (нейтралізації) збройного конфлікту, виконання інших завдань із застосуванням будь-яких видів зброї (озброєння)¹. Так само для повнішого розкриття змісту терміносполучення «бойові дії» доцільно звернутися й до ст. 6 Закону України «Про статус ветеранів війни, гарантії їх соціального захисту», в якій під участю у бойових діях розуміється здійснення заходів із забезпечення національної безпеки і оборони, захисту безпеки населення та інтересів держави, відсічі і стримування збройної агресії РФ, забезпечення їх здійснення та перебування безпосередньо в районах та у період здійснення зазначених заходів, а також виконання бойового (службового) завдання із захисту незалежності, суверенітету та територіальної цілісності України в умовах безпосереднього зіткнення та вогневого контакту з військовими формуваннями інших держав і незаконними збройними формуваннями². З наведених законодавчих приписів можна зробити висновок, що надання допомоги ворогу охоплює дуже широке коло суспільно небезпечних дій – як фізичних (зокрема, блокування органів військового управління, об'єднань, з'єднань, військових частин, шляхів сполучення, обладнання, споруд, руху військового транспорту тощо), так й інформаційних, спрямованих на передачу, поширення та інші незаконні дії з так званою військово значущою інформацією на користь ворога та всупереч інтересам України. Але, ще раз повторимося, що кваліфікація таких діянь як колабораційної діяльності є можливою лише у разі вчинення їх на тимчасово окупованій

¹ Про оборону України: Закон України від 06.12.1991 р. № 1932-ХІІ. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/1932-12#Text> (дата звернення: 15.11.2024).

² Про статус ветеранів війни, гарантії їх соціального захисту: Закон України від 22.10.1993 р. № 3551-ХІІ. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/3551-12#Text> (дата звернення: 15.11.2024).

території, що хоча й прямо не зазначено в законі, але безпосередньо впливає з його змісту.

Іншою ситуацією є незаконне поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань на контрольованих Україною територіях РФ. 12 серпня 2024 року Головнокомандувач Збройних Сил України Олександр Сирський на засіданні Ставки Верховного головнокомандувача України вперше підтвердив участь Збройних сил України в бойових діях у Курській області¹, а вже 15 серпня 2024 року він повідомив, що для дотримання правопорядку та забезпечення першочергових потреб населення на підконтрольних територіях створено військову комендатуру².

За таких умов постає питання щодо можливості України відповідно до положень ст. 64 Конвенції про захист цивільного населення під час війни від 12 серпня 1949 р.³ забезпечити на контрольованій Україною території країна-агресора виконання норм міжнародного гуманітарного права. За загальним правилом, на цій території повинно діяти чинне кримінальне законодавство РФ. В той же час, у разі якщо це законодавство становить загрозу безпеці України або є перешкодою виконання цієї Конвенції, Україна має право скасувати чи призупинити його.

На сьогодні на території держави-агресора, що знаходиться під контролем України, відсутні будь-які місцеві органи влади та органи судової системи, що унеможливує здійснення правосуддя на цій території за законодавством РФ. Одночасно з цим, є ймовірність незаконного поширення інформації про розміщення Збройних Сил

¹ Зеленський і Сирський вперше офіційно підтвердили наступ у Курській області. Новинарня: вебсайт. URL: <https://novynarnia.com/2024/08/12/zelenskyj-i-syrskijj-vpershe-oficijjno-pidtvverdylu-nastup-u-kurskij-oblasti/> (дата звернення: 15.11.2024).

² Україна створила військову комендатуру в Курській області, її очолив генерал Москальов. РБК Україна. РБК-Україна: вебсайт. URL: <https://www.rbc.ua/rus/news/ukrayina-stvorila-viyskovu-komendaturu-kurskiy-1723724275.html> (дата звернення: 15.11.2024).

³ Конвенція про захист цивільного населення під час війни (Женева, 12.08.1949 р.). Верховна Рада України. Законодавство України: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_154#Text (дата звернення: 15.11.2024).

України чи інших утворених відповідно до законів України військових формувань на таких територіях, що становить загрозу безпеці ЗСУ й Україні в цілому.

Так, переважна більшість інформації про ситуацію в Курській області РФ надходить від російських джерел, а саме проросійських військорів і блогерів, які активно публікують дані про бої на Курщині. Крім того, час від часу у відкритих джерелах з'являється інформація, яка додатково пояснює події в Курській області, що, врешті-решт, дає розуміння про події на місцях. Українська сторона ефективно зберігає режим інформаційної тиші, не розголошуючи дані про свої дії, оскільки це може створювати небезпеку для захисників із Сил оборони. Також один із найавторитетніших порталів, який регулярно фіксує події на карті бойових дій, Deepstate відмовився уточнювати актуальну інформацію, оскільки це може загрожувати безпеці українських військових. Натомість портал вирішив надавати дані з певним відставанням у часі¹.

Постає логічне запитання: чи містить ознаки кримінального правопорушення, передбаченого ч. 2 ст. 114² КК, незаконне поширення інформації про розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань на території держави-агресора, що знаходиться під контролем України? Адже положення про кримінальну відповідальність, які ухвалюються Україною, можуть набирати чинності лише після того, як їх опубліковано та доведено до відома населення Курської області їхньою рідною мовою. До того ж, ці положення не повинні мати зворотної сили (ст. 65 Конвенції).

Для вирішення питання щодо того, яке законодавство слід застосовувати на цих територіях – РФ чи України, яке наразі перебуває на стадії жвавого обговорення на загальнодержавному рівні, доцільним вбачається звернутися насамперед до принципів чинності кримінального закону у просторі та за колом осіб. Так, якщо йдеться про громадян України та осіб без громадянства, що постійно прожи-

¹ Курський прорив: хронологія подій і карта бойових дій. *Факти*: вебсайт. URL: <https://fakty.com.ua/ua/svit/20240825-kurskyj-proryv-hronologiya-podij-ta-karta-bojovyh-dij/amp/> (дата звернення: 15.11.2024).

вають в Україні, у разі поширення ними зазначеної вище інформації, то тут істотних складнощів не виникає, адже спрацьовує принцип громадянства, відповідно до якого ці особи несуть відповідальність за КК незалежно від того, на території якої держави вчиняється кримінальне правопорушення.

Що стосується іноземців та осіб без громадянства, які не проживають постійно в Україні, то у разі вчинення ними кримінального правопорушення за межами України, за загальним правилом, застосовується або універсальний принцип дії закону у просторі, коли ці особи несуть відповідальність, яка передбачена міжнародними договорами, або ж реальний принцип, який передбачає, що такі особи несуть відповідальність у випадку вчинення тяжких та особливо тяжких злочинів проти прав і свобод громадян, а також проти інтересів України. На жаль, перший з указаних принципів у випадку поширення інформації про розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань на території держави-агресора не спрацьовує, оскільки на сьогоднішній день немає міжнародних договорів, які б передбачали можливість притягнення таких осіб до відповідальності. Що ж стосується застосування реального принципу, то незважаючи на те, що злочин, передбачений статтею 114² КК, належить до злочинів проти інтересів держави, але водночас він не належить до категорії тяжких та особливо тяжких, що так само виключає відповідальність іноземців та осіб без громадянства у разі вчинення даного кримінального правопорушення. Фактично це означає, що у разі вчинення аналізованого кримінального правопорушення негромадянами України на територіях держави-агресора, що наразі перебувають під контролем України, кримінальне законодавство України застосовуватися у такому вигляді не може¹.

¹ Федосєєв В. В. Щодо деяких актуальних питань кримінальної відповідальності за незаконне поширення інформації про розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ч. 2 ст. 114-2 КК України). *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки* : матеріали Всеукраїнської наук.-практ. конференції (м. Київ, 27 вересня 2024 р.) / [редкол.: Вербеньський М. Г., Опришко І. В., Лісниченко Л. В. та ін.]. Вінниця : ТВОРИ, 2024. С. 190.

Проте очевидно, що на цих територіях такі діяння можуть бути вчинені як мешканцями цих територій, так і особами, що є іноземцями та особами без громадянства, які не є їх місцевими мешканцями. Це свідчить про виправданість диференційованого підходу до розв'язання означеної ситуації. Так, якщо говорити про іноземців та осіб без громадянства, які не є мешканцями указаних територій, то вони, як було зазначено вище, відповідно до положень ст. 8 КК, взагалі не несуть відповідальності. У випадку ж, коли йдеться про іноземців та осіб без громадянства, які є мешканцями підконтрольних Україні територій держави-агресора, то вирішення питання їх відповідальності залежить наразі від визначення правового режиму цих територій, тобто гіпотетично у разі вирішення цього питання на законодавчому рівні виникне можливість застосування територіального принципу. Наразі за ст. 7 КК цей принцип стосується лише тих випадків, коли кримінальне правопорушення вчиняється саме на території України. Щодо території, яка стала підконтрольною Україні у зв'язку з відомими подіями, чинність КК на сьогодні не поширюється.

Також слід звернути увагу, що ще однією умовою застосування ч. 2 ст. 114² КК є наявність особливої умови. Так, поширення інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, за можливості їх ідентифікації на місцевості, якщо така інформація не розміщувалася у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України або іншими уповноваженими державними органами, можливе *лише в умовах воєнного або надзвичайного стану*. Згідно з ч. 1 ст. 2 Закону України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII правовою основою введення воєнного стану є Конституція України, цей Закон та указ Президента України про введення воєнного стану в Україні або в окремих її місцевостях, затверджений Верховною Радою України¹. Відповідно до Указу Президента України «Про введення воєнного стану в Україні» від 24.02.2022

¹ Про правовий режим воєнного стану: Закон України від 12.05.2015 р. № 389-VIII. Верховна Рада України. Законодавство України: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text> (дата звернення: 15.11.2024).

№ 64/2022 (зі змінами), в Україні у зв'язку з військовою агресією Російської Федерації проти України, на підставі пропозиції Ради національної безпеки і оборони України, відповідно до п. 20 ч. 1 ст. 106 Конституції України, Закону України «Про правовий режим воєнного стану» введено воєнний стан з 24 лютого 2022 року¹. Зрозуміло, що на територію держави-агресора, що знаходиться під контролем України, вказаний режим свою дію не поширює. Проте, на наш погляд, ознаку наявності воєнного або надзвичайного стану на момент вчинення злочину необхідно розуміти не як таку, що свідчить про прив'язку його вчинення до тієї території, на якій вчиняється кримінальне правопорушення, а як ознаку, яка визначає суспільну небезпечність діяння у відповідний проміжок часу. Тобто, доки в самій Україні буде існувати воєнний або надзвичайний стан, то діяння, пов'язане з поширенням інформації про переміщення, рух або розташування Збройних Сил України чи інших утворених відповідно до законів України військових формувань, буде суспільно небезпечним. А це означає відсутність потреби визнавати умовою відповідальності за ч. 2 ст. 114² КК запровадження на підконтрольних Україні територіях держави-агресора цього стану. Ці питання, звісно, потребують якомога скорішого вирішення на законодавчому рівні.

Наприкінці розглянемо деякі проблемні аспекти застосування ч. 3 ст. 114² КК, де встановлено кримінальну відповідальність за дії, *передбачені частиною першою або другою, вчинені з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням, або якщо вони спричинили тяжкі наслідки, за відсутності ознак державної зради або шпигунства*. Насамперед предметом нашої уваги є вчинення указаних в частинах 1 та 2 ст. 114² КК дій з метою надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням. Не викликає сумнівів, що поширення

¹ Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 р. № 64/2022. *Верховна Рада України. Законодавство України*: офіс вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/64/2022#Text> (дата звернення: 15.11.2024).

військово значущої інформації є нічим іншим, як формою надання допомоги ворогу, яка до того ж може становити склад державної зради (ст. 111 КК) у формі «надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України», вчинення якої в умовах воєнного стану є **обтяжуючою кримінальну відповідальність** ознакою, передбаченою ч. 2 цієї статті.

Як справедливо наголошує Н. В. Нетеса, кримінальна відповідальність за поширення так званої військово значущої інформації (якщо слідувати змісту пояснювальної записки до законопроекту про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому розповсюдженню інформації про направлення, переміщення міжнародної військової допомоги в Україну, рух, переміщення або розміщення Збройних Сил України чи інших військових формувань України, вчинене в умовах воєнного або надзвичайного стану (реєстр. № 7189 від 22.03.2022 р.) мала б наставати лише за необдумане вчинення таких дій. Однак така розмежувальна ознака повністю втрачає свій сенс у контексті ч. 3 ст. 114² КК, де серед іншого вказана мета надання такої інформації державі, що здійснює збройну агресію проти України, або її представникам, або іншим незаконним збройним формуванням, за відсутності ознак державної зради або шпигунства. Виходить, що розмежувати склади аналізованих кримінальних правопорушень практично неможливо. Не вирішує цієї проблеми й уже згадана вище вказівка у ч. 3 ст. 114² КК на відсутність ознак державної зради або шпигунства, адже за змістом цієї статті можна зробити висновок, що це застереження стосується лише характеру поширюваної інформації, яка не має містити державної таємниці¹¹. Так само не полегшує ситуацію й вказівка у ст. 111 КК на вчинення державної

¹¹ Нетеса Н. В. Поширення військово значущої інформації як форма надання інформаційної допомоги ворогу: проблемні аспекти розмежування суміжних складів злочинів. *Формування механізму притягнення до відповідальності представників держави-агресора в світлі ратифікації Україною Римського статуту Міжнародного кримінального суду та поправок до нього: матеріали міжнар. наук.-практ. круглого столу* (Київ, 7 листопада 2024 р.). Київ, 2024. С. 70.

зради на шкоду суверенітету, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України, оскільки в умовах воєнного стану будь-яка взаємодія з ворогом фактично становить таку шкоду.

Таким чином, наявний правовий підхід не забезпечує належного розмежування між поняттями, створюючи правову невизначеність у застосуванні ст. 114² КК. Як результат, маємо неодноманітну слідчу та судову практику, коли абсолютно ідентичні діяння, що полягають у поширенні громадянами України інформації військового характеру кваліфікуються або за ч. 2 ст. 111 КК (державна зрада), або ч. 3 ст. 114² КК, або за ч. 7 ст. 111¹ КК у формі надання інформаційної допомоги у веденні бойових дій.

Наведена ситуація є неприпустимою і породжує потребу у розв'язанні колізії зазначених норм КК, у вирішенні якої, на жаль, не спрацьовують правила її подолання у разі конкуренції загальної та спеціальної норми. Вочевидь, що за цих обставин більш виправданим буде застосування усталеного в теорії кримінального права правила про дію темпоральних норм, яке, до того ж, знайшло своє нормативне закріплення у п. 2) ч. 3 ст. 66 Закону України «Про правотворчу діяльність» (який набув чинності, але ще не введений в дію), де вказано, що у разі виявлення колізії між нормативно-правовими актами рівної юридичної сили пріоритет у застосуванні мають норми, що містяться у нормативно-правових актах, що вступили в дію пізніше¹¹. У даному разі пізнішим за часом прийняття є закон, яким встановлено кримінальну відповідальність у ст. 114² КК, яка з'явилася в КК 27 березня 2022 р. у зв'язку з набранням чинності Законом України № 2160-IX від 24.03.2022 р.

Наведені питання свідчать про необхідність внесення відповідних змін не лише до ст. 114² КК та інших статей КК, а й насамперед до регуляторного законодавства з тим, щоб забезпечити на законодавчому рівні врегулювання відповідних суспільних відносин в сфері безпеки й оборони України. Уявляється, що найоптимальнішим

¹¹ Про правотворчу діяльність: Закон України від 24.08.2023 р. № 3354-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/3354-20#Text/> (дата звернення: 15.11.2024).

способом реалізації такої мети може стати розроблення відповідного закону, в якому, серед іншого, доцільно визначити види інформації, поширення якої (так само як і передача якої) може бути обмежене в інтересах національної безпеки України. Так само необхідним є вироблення єдиного підходу до розуміння поширення інформації, яке не має піддаватися розширювальному тлумаченню, щоб не допустити невинуватої підміни понять, що характеризують різні форми інформаційних діянь (передусім передача інформації чи її розголошення). На наше переконання, поширенню інформації іманентно властива ознака публічності, тобто адресованості широкій аудиторії, що впливає з етимології цього слова як такого, що означає робити щось широко відомим. Це дозволить відмежовувати суспільно небезпечне поширення інформації від так званої «побутової» передачі інформації від однієї особи до іншої, яка за своїм енергетичним змістом не може прирівнюватися до поширення. Крім того, на сьогодні відчувається гостра потреба у виробленні єдиної правової позиції щодо правозастосування норми про 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.

Також вважаємо за необхідне розширити перелік суб'єктів поширення інформації про які завдає шкоди Україні в умовах збройної агресії РФ. Мова йде про встановлення відповідальності також і за поширення інформації про сили оборони України, до яких відповідно до пункту 18 Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII окрім Збройних Сил України, а також інших утворених відповідно до законів України військових формувань, входять також правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави.

Висновки до розділу I

1. Основним безпосереднім об'єктом злочину, передбаченого ч. 2 ст. 109 КК, є суспільні відносини з приводу охорони конституційного ладу та державної влади. Предметом цих відносин виступають такі загальнонаціональні цінності, як конституційний лад та державна влада, їх суб'єктами є фізичні, юридичні особи та суспільство загалом, соціальний зв'язок між цими суб'єктами має форму статички – всі вони мають утримуватися від дій, спрямованих на насильницьку зміну чи повалення конституційного ладу, а також на захоплення державної влади.

2. Додатковим обов'язковим об'єктом злочину, передбаченого ч. 2 ст. 109 КК, є суспільні відносини, що забезпечують інформаційну безпеку. Такий висновок слідує із сутності діянь, що утворюють його об'єктивну сторону, оскільки і заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади (1), і розповсюдження матеріалів із відповідними закликами (2) обов'язково спричиняють негативні зміни в інформаційному просторі.

3. Об'єктивну сторону злочину, передбаченого ч. 2 ст. 109 КК, становлять лише публічні заклики до насильницької зміни конституційного ладу або до захоплення державної влади. При цьому характер насильства, до якого закликає суб'єкт злочину, може бути як фізичним, так і психічним (або взагалі без конкретизації його виду).

4. Мета є іманентною діянням, відповідальність за які передбачено у ч. 2 ст. 109, ч. 1 ст. 110 КК. Вчиняти публічні заклики та поширювати матеріали із такими закликами неможливо без прагнення на досягнення того, що утворює їх зміст. Наявність прямого умислу в цих випадках обов'язково свідчить і про наявність спеціальної мети. Бажаючи вчиняти відповідні суспільно небезпечні діяння суб'єкт злочину обов'язково уявляє собі результат такої поведінки – у адресатів закликів має сформуватися прагнення поводити себе у чітко визначений спосіб.

5. Державна зрада і шпигунство належать до злочинів, що мають високий ступінь суспільної небезпечності. Значну небезпеку ці діяння набувають у часи вирішальних випробувань для існування України як незалежної держави. На сьогодні це воєнний стан, в якому перебуває Україна з 24 лютого 2022 р.

6. Зміни, що відбулися у кримінальному законодавстві України після 24 лютого 2022 р. потребували нового тлумачення змісту норми ст. 111 КК. Зроблено висновок, що в умовах воєнного стану зрадливість у формі «надання допомоги» стає різновидом суміжної з нею форми «перехід на бік ворога». Крім того, обсяг діянь, що охоплювалися формою «надання допомоги», значно зменшився, оскільки більшість з них було переміщено до нових самостійних норм (ст.ст. 111¹, 111², 114² КК).

7. Встановлено, що «перехід на бік ворога» і «надання допомоги», навіть якщо вони здійснюються з використанням інформації, не можуть загалом визнаватися інформаційними кримінальними правопорушеннями, оскільки є діяннями фізичними, спрямованими на зміну зовнішньої, фізичної сфери предметів матеріального світу. На відміну від цих діянь, шпигунство є інформаційним діянням, а, отже, вже за цією властивістю не є суміжним з іншими діяннями, зазначеними в диспозиції норми ст. 111 КК.

8. Розгляд предмета шпигунства, яким є державна таємниця, дозволив встановити, що крім основного об'єкта цього злочину, яким є основи зовнішньої безпеки України, такому діянню притаманна ще одна обов'язкова ознака, а саме додатковий обов'язковий об'єкт, яким є основи інформаційної безпеки. Зазначене дає можливим підтримати пропозиції щодо можливості виділення шпигунства в самостійну норму КК, за якою суб'єктами такого діяння будуть громадяни України, іноземці або особи без громадянства.

9. Колабораційна діяльність в інформаційній сфері являє собою різні форми усвідомленої добровільної інформаційної взаємодії громадян України з ворогом, змістом яких є будь-які прояви циркуляції інформації на шкоду національній безпеці України. При цьому колабораціонізм в інформаційній сфері як родове поняття охоплює різні види – ідеологічний, культурний, освітній, кібернетичний, інфор-

маційний колабораціонізм у тісному сенсі слова, які відрізняються метою здійснення, засобами, сферою застосування, наслідками, але у реальній дійсності нерідко набувають гібридних форм.

10. Кримінально-правовими засобами реагування на явище інформаційного колабораціонізму є нормативні положення частин 1, 3 та 6 ст. 111¹ КК. Водночас окремі їх елементи містяться й в інших положеннях ст. 111¹ КК, зокрема у ч. 5 (публічні заклики до проведення незаконних виборів та референдумів на окупованій території) та ч. 7 (надання вказаним у ній адресатам допомоги (у т. ч. інформаційної) у веденні бойових дій проти ЗСУ та інших законних військових формувань України). Однак тут інформаційний колабораціонізм має субсидіарний характер стосовно інших його форм – політичного й воєнного, що означає спрямованість цих проявів колабораційної діяльності не на інформаційну, а на інші складові національної безпеки.

11. Здійснення інформаційної діяльності як форма інформаційного колабораціонізму (ч. 6 ст. 111¹ КК) не може зводитися до простих форм інформаційних діянь і являє собою специфічну професійну діяльність спеціальних суб'єктів (зокрема, суб'єктів у сфері медіа, блогерів), яка здійснюється систематично та цілеспрямовано і полягає, зокрема, в інформаційній взаємодії з органами влади, юридичними й фізичними особами, створенні доступу до публічної інформації, впорядкуванні інформаційних ресурсів, формуванні інформаційно-комунікаційної інфраструктури та засобів зв'язку, а також засобів інформаційної безпеки.

12. Колізія норм про колабораційну діяльність із нормами статей 111, 111² та 436² КК виникає передусім через те, що законодавець не відбив у тексті закону сутність колабораційної діяльності – те, що це явище можливе лише на окупованій території і завжди передбачає добровільну та ініціативну співпрацю з ворогом саме громадян України. З огляду на це *de lege ferenda* пропонується уніфікувати підхід у всіх частинах ст. 111¹ КК шляхом вказівки на вчинення таких діянь саме громадянином України на тимчасово окупованій території, адже саме умови окупації визначають специфіку колабораційної діяльності.

13. У чистому вигляді інформаційні дії становлять склад посабництва державі-агресору (ст. 111² КК) тоді, коли допомога полягає у наданні певної інформації, яка необхідна державі-агресору для реалізації її відповідних рішень (наприклад, про нейтралізацію патріотично налаштованих громадян України, про русифікацію населення тощо). В інших випадках активність правопорушників в інформаційному просторі має здебільшого допоміжний характер, становлячи або етап реалізації певного рішення, або являючи собою його інформаційну підтримку (наприклад, популяризація рішення держави-агресора шляхом поширення проросійського контенту).

14. Дослідження ознак кримінального правопорушення, передбаченого ст. 114² КК, та практики її застосування зумовило необхідність внесення відповідних змін не лише до неї та інших статей КК, а насамперед до регуляторного законодавства в сфері безпеки й оборони України. Зроблено висновок, що найоптимальнішим способом реалізації такої мети може стати розроблення відповідного закону, в якому, серед іншого, доцільно визначити види інформації, поширення якої (так само як і передача якої) може бути обмежене в інтересах національної безпеки України.

15. Запорукою ефективного застосування ст. 114² КК є вироблення єдиного підходу до розуміння поширення інформації, яке не має піддаватися розширювальному тлумаченню, щоб не допустити невинуватої підміни понять, що характеризують різні форми інформаційних діянь (передусім передача інформації чи її розголошення).

16. Існує необхідність у розширенні в ст. 114² КК переліку суб'єктів, поширення інформації про які завдає шкоди Україні в умовах збройної агресії РФ, а саме про сили оборони України, до яких входять також правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави.

Розділ II

ІНШІ КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА ІНШОЇ ІНФОРМАЦІЇ, ЩО ЗАБЕЗПЕЧУЄ ОБОРОНОЗДАТНІСТЬ ДЕРЖАВИ

Вступні положення

У КК закріплена відповідальність і за інші (окрім тих, що були розглянуті в попередніх розділах цієї монографії) кримінальні правопорушення у сфері охорони державної таємниці та іншої інформації, що забезпечує обороноздатність держави.

Серед таких правопорушень:

- **стаття 328 КК** «Розголошення державної таємниці»;
- **стаття 329 КК** «Втрата документів, що містять державну таємницю»;
- **стаття 330 КК** «Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни»;
- **стаття 422 КК** «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості».

Родовими об'єктами зазначених правопорушень виступають суспільні відносини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації (правопорушення за статтями 328, 329 та 330 КК) та суспільні відносини у сфері встановленого порядку несення військової служби (стаття 422 КК). Основними ж їх об'єктами є інформаційна безпека – суспільні відносини у сфері охорони державної таєм-

ниці й іншої інформації, що забезпечує обороноздатність держави, зокрема:

- за статтями 328 та 329 КК – суспільні відносини з охорони державної таємниці в різних сферах діяльності держави;
- за статтею 330 КК – суспільні відносини з охорони відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни;
- за статтею 422 КК – суспільні відносини з охорони державної таємниці у військовій сфері.

Відмітною рисою усіх зазначених норм є їх бланкетний характер, що обумовлює необхідність звернення до норм інших галузей законодавства при встановленні ознак відповідних правопорушень.

У науковій літературі проблеми кримінальної відповідальності за зазначені кримінальні правопорушення висвітлювалися у працях таких учених, як П. П. Андрушко, Ю. В. Безсусідня, М. І. Бажанов, Т. Ю. Вислоцька, О. С. Володавська, О. П. Горпинюк, Л. Ф. Дадерко, А. О. Данилевський, Л. М. Кривоченко, М. Й. Коржанський, П. С. Матишевський, М. І. Мельник, В. І. Олійник, О. С. Самойлова, О. Г. Семенов, В. В. Сергійчук, О. О. Тихомиров, О. К. Тугарова, Д. С. Усов, М. І. Фіалка, М. І. Хавронюк, С. О. Харитонов та ін. Разом із тим слід відмітити низку дискусійних та недостатньо досліджених питань щодо розуміння та застосування цих норм, що потребує подальших наукових розвідок.

2.1. Кримінальні правопорушення у сфері охорони державної таємниці (статті 328, 329, 422 КК України)

2.1.1. Розголошення державної таємниці (ст. 328 КК України)

У ст. 328 КК за ч. 1 встановлено відповідальність за розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням

службових обов'язків, за відсутності ознак державної зради або шпигунства; а за ч. 2 цієї статті – за те саме діяння, якщо воно спричинило тяжкі наслідки¹.

Предметом цього кримінального правопорушення є відомості, що становлять державну таємницю, поняття, межі, та порядок запровадження якої визначаються Законом України «Про державну таємницю» від 21.01.1994 р. № 3855-ХІІ (далі також Закон № 3855-ХІІ)².

Як впливає із системного тлумачення норм статей 328 та 422 КК, не належить до предмета злочину за ст. 328 КК такий різновид державної таємниці, як відомості військового характеру, оскільки вони виступають предметом кримінального правопорушення за ст. 422 КК.

Об'єктивна сторона розглядуваного злочину виражається в діянні – розголошенні таємних відомостей. Розголошувати, згідно з тлумачним словником, означає піддавати розголосу, обнародувати, робити широко відомим³. Розголошення може бути вчинене як шляхом дії, так і бездіяльності. Прикладами розголошення у виді дії можуть бути поширення відповідних відомостей у приватній розмові або публічній промові, у листуванні, у публікації в медіа, соціальних мережах, в інші способи ознайомленні з цими відомостями осіб, які не мають на це права. Розголошення у виді бездіяльності може відбуватися шляхом недотримання особою правил збереження, обертання, перевезення документів або матеріалів із секретними відомостями, що обумовлювало можливість ознайомлення з цими відомостями сторонніх осіб⁴.

¹ Згідно зі ст. 12 КК правопорушення за ч. 1 ст. 328 КК є нетяжким злочином, а за ч. 2 – тяжким злочином.

² *Примітка.* Характеристика державної таємниці як предмета кримінального правопорушення була здійснена в підрозділі 1.2. розділу І цієї монографії.

³ Розголошувати. *Словник української мови. Академічний тлумачний словник:* вебсайт. URL: <https://sum.in.ua/s/rozgholoshuvaty> (дата звернення: 05.09.2024).

⁴ Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. *Кримінальне право України. Особлива частина:* підручник / за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., переробл. і допов. Харків: Право, 2020. Розд. XV. С. 501.

Разом із тим, як вбачається, у конструкції «розголошення у виді бездіяльності» закладено певне протиріччя. Дієслово «розголошувати» є перехідним (тобто таким, що означає дію, спрямовану безпосередньо на якийсь предмет)¹ і належить до числа дієслів в активному стані², коли суб'єкт виконує відповідну дію. Таким чином, поведінка особи, яка розголошує інформацію, має бути активною, цілеспрямованою. У зв'язку з цим віддієслівний іменник «розголошення» не підходить для окреслення пасивної поведінки щодо поширення відповідної інформації.

Як випливає з аналізу судової практики, у більшості випадків при розголошенні особа умисно здійснює певні активні дії, спрямовані на передачу чи оприлюднення інформації для сторонніх осіб.

Розголошення державної таємниці у виді активних дій може мати місце при безпосередньому наданні відповідних відомостей на ознайомлення³, їх скеруванні⁴, переданні на опрацювання⁵ тощо. Так, наприклад, за умовами справи № 295/11759/19 винний під час

¹ Перехідні і неперехідні дієслова. Зворотні дієслова. Офіційний сайт української мови: вебсайт. URL: http://ukrainskamova.com/publ/chinnij_pravopis/morfologija_i_pravopis/perekhidni_i_neperekhidni_dieslova/6-1-0-117 (дата звернення: 05.09.2024).

² Стан дієслова. Зворотні дієслова. Офіційний сайт української мови: вебсайт. URL: http://ukrainskamova.com/publ/chinnij_pravopis/morfologija_i_pravopis/stan_dieslova_zvrotni_dieslova/6-1-0-118 (дата звернення: 05.09.2024).

³ Вирок Шевченківського районного суду м. Чернівці від 08.09.2022 р. (справа № 727/7323/224; провадження № 1-кп/727/401/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/106173384> (дата звернення: 05.09.2024); вирок Франківського районного суду м. Львова Чернівці від 28.03.2022 р. (справа № 465/1065/22; провадження № 1-кп/465/979/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/103783440> (дата звернення: 05.09.2024).

⁴ Вирок Печерського районного суду м. Києва від 13.12.2022 р. (справа № 757/25481/22-к; провадження № 1-кп-1738/23). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/109190562> (дата звернення: 05.09.2024).

⁵ Вирок Печерського районного суду м. Києва від 04.10.2021 р. (справа № 757/31668/21-к; провадження № 1-кп-863/21). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/102328395> (дата звернення: 05.09.2024).

особистої зустрічі із зацікавленою особою передав їй копію судового рішення, в якій містилися відомості про проведення стосовно неї оперативно-розшукових заходів¹. Окрім того, таке діяння може полягати й у фотографуванні відповідних документів та їх наступному використанні. Для прикладу, у справі № 760/15232/19 особа здійснила фотографування документів, що були їй довірені як слухачу військового навчального закладу, та які містили відомості, що становлять державну таємницю, а згодом скопіювала та зберігала їх на власному комп'ютері, з якого у подальшому було спрямовано декілька файлів із зображеннями документів на невстановлену електронну скриньку².

Натомість розголошення у виді бездіяльності трапляється рідше й такої формі більш властива необережна форма вини. Так, у справі № 569/19931/21 особа вчинила розголошення шляхом недотримання вимог режиму секретності (що відповідає суспільно небезпечній формі бездіяльності). Так, зокрема, встановлено, що обвинувачений залишив на власному робочому ноутбучі, доступ до якого не обмежувався, файл із інформацією про запасні пункти управління та інші військові об'єкти. Як випливає із обставин справи, у подальшому така інформація стала відомою особі, яка здійснювала комп'ютерне налаштування інтернету. Відповідного допуску та доступу до відомостей, що містять державну таємницю, на той час у неї не було³. Отже, така бездіяльність засудженого зумовила настання шкідливого наслідку у виді ознайомлення із державною таємницею сторонніми особами.

¹ Вирок Корольовського районного суду м. Житомира від 03.09.2019 р. (справа № 295/11759/19; провадження № 1-кп/296/663/19). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/84072625> (дата звернення: 05.09.2024).

² Вирок Солом'янського районного суду м. Києва від 22.07.2019 р. (справа № 760/15232/19; провадження № 1-кп/760/1918/19). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/83425983> (дата звернення: 05.09.2024).

³ Вирок Рівненського міського суду Рівненської області від 02.02.2022 р. (справа № 569/19931/21; провадження № 1-кп/569/765/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/103667402> (дата звернення: 05.09.2024).

Аналогічна ситуація мала місце у справі № 761/17067/22, за обставинами якої, особа, незважаючи на взяті на себе зобов'язання, недбало ставлячись до виконання своїх посадових обов'язків, шляхом бездіяльності та невжиття належних заходів щодо збереження секретної інформації, порушуючи правила зберігання матеріальних носіїв секретної інформації, допустила розголошення відомостей, що становлять державну таємницю, протиправно створивши умови, за яких стороння особа, яка не має допуску та доступу до державної таємниці, ознайомила з вмістом секретних документів та скопіювала їх¹.

Зазначені кейси наочно ілюструють, що за своїм характером поняття розголошення не є релевантним для діяння шляхом бездіяльності, адже при розголошенні в пасивний спосіб особа безпосередньо не поширює інформацію, а лише створює умови для цього. Тож більш доречним для такої поведінки було б використання інших конструкцій наприклад, спричинення витоку відомостей.

Таким чином, у диспозиції цієї норми доречно було б передбачити дві альтернативні форми діяння:

- 1) розголошення відомостей;
- 2) спричинення витоку таких відомостей.

При цьому, оскільки суспільна небезпечність активної та пасивної поведінки в цьому випадку є різною (що в тому числі обумовлюється й різними формами вини, які їм властиві), відображення двох зазначених форм поведінок у диспозиції норми ч. 1 ст. 328 КК дозволить більшою мірою диференціювати кримінальну відповідальність за цей злочин та, у свою чергу, призначати судам більш справедливе покарання за його вчинення².

¹ Вирок Шевченківського районного суду м. Києва від 26.10.2022 р. (справа № 761/17067/22; провадження № 1-кп/761/2908/2022). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/107391773> (дата звернення: 05.09.2024).

² Куковинець Д. О., Євтєєва Д. П. До проблеми формулювання діяння в ст. 328 КК України «розголошення державної таємниці». *Українська кримінальна юстиція у пост/воєнній парадигмі*: матеріали Х (XXIII) Львівського форуму кримінальної юстиції (м. Львів, 19–20 верес. 2024 р.). Львів: ЛьвДУВС, 2024. С. 105, 106.

При розголошенні державної таємниці суб'єкт порушує вимоги нормативних актів, що регламентують порядок поведіння з державною таємницею. Зокрема, Законом України «Про державну таємницю» встановлюється спеціальний порядок допуску й доступу до державної таємниці й певні обов'язки її охорони. Серед таких обов'язків, наприклад: не допускати розголошення будь-яким способом державної таємниці, виконувати вимоги режиму секретності та ін. (ст. 28 зазначеного Закону). При цьому, якщо такі вимоги були дотримані, але стороннім особам стали відомі відповідні відомості, кримінальна відповідальність наставати для суб'єкта не має.

Окрім того, як впливає з аналізу практики, обґрунтовуючи розголошення особою державної таємниці, суди найчастіше посиляються на порушення обвинуваченими положень Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18.12.2013 р. № 939 (далі – Порядок № 939)¹, відомчих нормативно-правових актів (наприклад, Інструкції з технології порядку приймання, обробки, зберігання, перевезення та доставки відправлень спеціального зв'язку, затвердженої Державним комітетом зв'язку та інформатизації України від 02.07.1999 р. № 21²; Інструкції з перевезення спеціальних вантажів на залізничному транспорті України, затвердженої наказом Міністерства транспорту України від

¹ Вирок Кам'янець-Подільського міськрайонного суду Хмельницької області від 21 травня 2021 року (справа № 676/1683/19). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/97086919> (дата звернення: 05.09.2024); Вирок Шевченківського районного суду м. Києва від 26 жовтня 2022 року (справа № 761/17067/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/107391773> (дата звернення: 05.09.2024); Вирок Печерського районного суду м. Києва від 13 грудня 2022 року (справа № 757/25481/22-к). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/109190562> (дата звернення: 05.09.2024).

² Вирок Вінницького міського суду Вінницької області від 18 вересня 2015 року (справа № 127/19700/15-к). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/50803207> (дата звернення: 05.09.2024).

19.02.2002 р. № 1т¹ тощо), а також локальних документів (зокрема, наказів², розпоряджень³, посадових інструкцій⁴), якими надається допуск та доступ до державної таємниці.

Таке діяння, як розголошення, передбачає наявність особи, яка розголошує відповідні відомості, та сторонньої особи (або сторонніх осіб). При цьому під сторонніми особами слід розуміти осіб, яким ці відомості не повинні бути відомими⁵. До кола таких осіб, як зазначає Л. Ф. Дадерко, належать всі громадяни, які не мають допуску до такого роду відомостей, а також громадяни, які мали загальний допуск, однак такі відомості не були їм доступні по службі чи роботі. Тож критерієм визначення особи як сторонньої виступає доступ

¹ Вирок Шепетівського міськрайонного суду Хмельницької області від 18 травня 2021 року (справа № 688/1435/21). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/97087291> (дата звернення: 05.09.2024).

² Вирок Київського районного суду м. Полтави від 16 червня 2015 року (справа № 524/4162/15-к). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/45136913> (дата звернення: 05.09.2024); Вирок Київського районного суду м. Полтави від 15 липня 2015 року (справа № 544/969/15-к). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/46777240> (дата звернення: 05.09.2024).

³ Вирок Луцького міськрайонного суду Волинської області від 15 січня 2018 року (справа № 161/15576/17). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/71589136> (дата звернення: 05.09.2024).

⁴ Вирок Печерського районного суду м. Кисва від 04 жовтня 2021 року (справа № 757/31668/21-к). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/102328395> (дата звернення: 05.09.2024); Вирок Рівненського міського суду Рівненської області від 02 лютого 2022 року (справа № 569/19931/21). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/103667402> (дата звернення: 05.09.2024); Вирок Заводського районного суду м. Дніпродзержинська від 11 лютого 2022 року (справа № 208/4254/19). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/103116629> (дата звернення: 05.09.2024).

⁵ Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. *Кримінальне право України. Особлива частина*: підручник / за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., переробл. і допов. Харків: Право, 2020. Розд. XV. С. 500.

до державної таємниці¹. При цьому кількість сторонніх осіб, яким стала відома державна таємниця, для кваліфікації значення не має, однак може враховуватися судом при призначенні покарання.

Кримінальне правопорушення за ч. 1 має формальний склад. Щодо моменту його закінчення в науковій літературі висловлюються різні думки, серед яких можливо виділити *первинний, вторинний та третинний моменти*. Зокрема, таким моментом дослідниками пропонується вважати:

- момент, коли хоча б одна стороння особа мала можливість ознайомлення зі змістом документа² (позначимо його як *первинний*); як приклад такого моменту можливо навести розміщення цієї інформації у відкритому доступі в мережі Інтернет до першого ознайомлення з нею сторонніми особами;
- момент, коли відомості стали відомі хоча б одній сторонній особі³ (його доречно назвати *вторинним*);
- момент, коли відповідні відомості були сприйняті сторонньою особою в обсязі, який свідчить про перехід цієї інформації у власність такої особи (якщо ж стороння особа не сприйняла відповідну інформацію (внаслідок незнання мови, термінології, певного фізичного стану та ін.), суб'єкт, що здійснив розголошення, несе відповідальність за неза-

¹ Дадерко Л. Ф. Кримінальна відповідальність за розголошення державної таємниці. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юриспруденція. 2013. Вип. 6-2. Т. 2. С. 83. URL: <https://vestnik-pravo.mgu.od.ua/archive/juspradenc6-2-2/21.pdf>.

² Данилевський А. О. Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. *Кримінальне право (Особлива частина)*: підручник / за ред. О. О. Дудорова, Є. О. Письменського. Т. 2. Луганськ: Елтон-2, 2012. Гл. 16. С. 270.

³ Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ: Дакор, 2018. С. 1017; Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. *Кримінальне право України. Особлива частина*: підручник / за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., переробл. і допов. Харків: Право, 2020. Розд. XV. С. 501.

кінчений злочин)¹ – такий момент можливо визначити як *третинний*.

На нашу думку, у цій дискусії слід підтримати саме вторинний момент як момент закінчення досліджуваного злочину, на користь чого можливо навести такі аргументи.

За первинного моменту витоку відповідної інформації (як обставини, що визначає високий ступінь суспільної небезпечності діяння) ще не відбувається. Окрім того, в моменті, коли ще жодна особа не ознайомила з відомостями, які складають державну таємницю, якщо його не визнати моментом закінчення кримінального правопорушення за ч. 1 ст. 328 КК, залишатиметься простір для добровільної відмови суб'єкта, що виступає як стимулюючим чинником для останнього, так і може економити засоби кримінальної репресії.

Щодо третинного моменту (який, на наш погляд, слід пов'язувати з переходом інформації не у власність, а у відання сторонньої особи, що свідчить про можливість особи її відтворювати та поширювати далі), то його установлення обумовлює значні труднощі, може вимагати проведення додаткових експертиз та інших процесуальних дій. Більше того, якщо розголошення відбувається публічно (наприклад, через публічні промови або в мережі Інтернет), то така інформація стає відомою широкому колу осіб, яких неможливо установити, а тому й неможливим буде установлення переходу відповідної інформації в їх відання.

Тож визнання моментом закінчення цього злочину саме вторинного моменту, за якого відомості стають відомими хоча б одній особі, є найбільш раціональним, викликатиме менше процесуальних труднощів та забезпечуватиме як додержання прав та інтересів особи, так процесуальну здійсненність кримінального переслідування².

¹ Дадерко Л. Ф. Кримінальна відповідальність за розголошення державної таємниці. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юриспруденція. 2013. Вип. 6-2. Т. 2. С. 84. URL: <https://vestnik-pravo.mgu.od.ua/archive/juspradenc6-2-2/21.pdf>

² Євтуєва Д. П. Щодо моменту закінчення розголошення державної таємниці. *Захист прав людини в українській моделі перехідного правосуддя*: матеріали наук.-практ. кругл. столу (м. Харків, 14 черв. 2024 р.). Харків: Право, 2024. С. 166.

За ч. 2 злочин має матеріальний склад, адже передбачає настання тяжких наслідків, що є оціночним поняттям. Як слушно відмічає В. І. Олійник, питання наявності тяжких наслідків має вирішуватися залежно від сукупності обставин, що характеризують ступінь секретності інформації, її якості й кількості, тих суб'єктів, до кого вона потрапила, чи була вона фактично використана на шкоду інтересам України, правам громадян тощо¹.

У науковій літературі до тяжких наслідків пропонується відносити випадки: 1) розголошення відомостей, що мають особливо важливе значення; 2) доведення інформації, що становить предмет цього кримінального правопорушення, до відома іноземної розвідки²; 3) піддання розголосу відомостей, що вказує на їх зв'язок із: а) організацією охорони певних об'єктів, систем зв'язку, напрямів науководослідних чи конструкторських робіт, що було пов'язано із заподіянням державі значної матеріальної шкоди; б) особами, які здійснюють оперативно-розшукову діяльність, їхніх близьких родичів; осіб, які на конфіденційній основі залучаються, плануються до залучення чи залучалися раніше до співпраці з правоохоронними органами з метою виконання завдань оперативно-розшукової чи розвідувальної діяльності³; 4) спричинення вимушеної зміни відповідними державними органами змісту стратегічних та оперативних планів; 5) провокування дипломатичних ускладнень⁴; 6) зриву державних заходів;

¹ Олійник В. І. Кримінально-правове, кримінологічне та кримінально-виконавче забезпечення охорони державної таємниці в Україні. Україні : дис. ... д-ра юрид. наук. Київ, 2023. С. 289–290. URL: <https://maup.com.ua/assets/files/dis/olijnik/olijnik-disertaciya.pdf>.

² Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. *Кримінальне право України. Особлива частина*: підручник / за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., переробл. і допов. Харків: Право, 2020. Розд. XV. С. 501.

³ Усов Д. С. Кримінально-правова характеристика розголошення державної таємниці (ст. 328 КК України): дис. ... канд. юрид. наук. Харків, 2014. С. 99.

⁴ Сергійчук В. В. Тяжкі наслідки як кваліфікуюча ознака злочинного розголошення державної таємниці. *Кримінально-правове регулювання та забезпечення його ефективності*: матер. Міжнар. наук.-практ. конф. (Харків, 18–19 жовтня 2018 р.). Харків: Право, 2018. С. 538, 539.

7) виникнення потреби передислокації режимного об'єкту Збройних Сил України; 8) викриття законспірованої агентурної розвідувальної мережі тощо¹. Окрім того, як зауважує Т. А. Шевчук, тяжкі наслідки можуть виражатися й у вчиненні діяння, похідного від розголошення державної таємниці, як-от: диверсія як пошкодження чи зруйнування об'єкта оборонного (склад озброєння) чи народногосподарського (електростанція) значення; або ж початок агресивних воєнних дій (розв'язування агресивної війни чи воєнного конфлікту) за конкретним напрямом на визначених ділянках території, що стало можливим через розголошення відомостей про дислокацію військ, характер оснащення підрозділів Збройних Сил України, стан їх боеготовності тощо².

Судова практика з цього приводу виходить із того, що під тяжкими наслідками в контексті ч. 2 ст. 328 КК слід розуміти різноманітні утруднення в діяльності органів досудового розслідування. Так, у вироку Рівненського міського суду Рівненської області від 06.06.2017 р. (справа № 569/5912/17) постановлено, що розголошення засудженим (на момент вчинення кримінального правопорушення співробітником одного з відділів Управління Служби безпеки України (далі – СБУ) державної таємниці завдало шкоду національній безпеці України у сфері державної безпеки та охорони правопорядку. Зокрема, така шкода втілилася у вжитті об'єктами контррозвідувальної справи дій щодо приховування своєї протиправної діяльності, що, як наслідок, ускладнило її подальше документування СБУ. Окрім того, констатовано, що витік цих відомостей може створити значні перешкоди для виконання СБУ завдань контррозвідувальної та оперативно-розшукової діяльності, і навіть може унеможливити її здійснення стосовно відповідних об'єктів оперативної зацікавленості,

¹ Довженко В. Окремі питання кримінально-правової характеристики розголошення державної таємниці. *Новітні кримінально-правові дослідження – 2021* : Альманах наукових праць / за ред. проф. Є. Л. Стрельцова, проф. О. В. Козаченка, PhD О. М. Мусиченко. Миколаїв : МПН НУ «ОЮА», 2021. С. 177.

² Кримінальне право України (у питаннях та відповідях) : навч. посіб. / [О. М. Литвинов, Ю. В. Орлов, В. П. Смелянов та ін.] ; за заг. ред. д-ра юрид. наук, проф. Ю. В. Орлова ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2023. С. 430.

що призведе до необхідності припинення контррозвідувальних та оперативно-розшукових заходів, або, у разі необхідності їх подальшого проведення, – зміни форм, методів, тактики, підходів у ході їх проведення із застосуванням більш складних та коштовних шляхів реалізації цих заходів¹. В іншій справі – у вирокі Солом'янського районного суду м. Києва від 13.06.2017 р. (справа № 760/9476/17-к) до тяжких наслідків було віднесено позбавлення органу досудового розслідування можливості об'єктивного збирання доказів із метою встановлення обставин, що мають значення для кримінального провадження, шляхом проведення негласних слідчих дій відносно конкретних осіб, що, своєю чергою, не дозволило належним чином виконати завдання кримінального провадження².

Суб'єктивна сторона злочину виражається лише в ознаці вини, за формою якої розголошення державної таємниці може вчинятися суб'єктом умисно (із прямим або непрямим умислом) або з необережності (самовпевненості або недбалості). При цьому особа має усвідомлювати, що розголошує саме таємну інформацію – державну таємницю. Ставлення до тяжких наслідків, передбачених ч. 2, може бути лише необережним. Мотив та мета обов'язковими ознаками складу розглядуваного правопорушення не виступають.

Суб'єктом злочину за ст. 328 КК є особа, якій таємні відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, а саме: службова особа (публічного права) або інша особа, робота якої пов'язана з такими відомостями по службі (наприклад, шифрувальник, секретар). При цьому суб'єкт має або мав допуск до державної таємниці (у ст. 22 Закону України «Про державну таємницю» передбачено три форми такого допуску залежно від ступеня секретності інформації) та взяв на себе письмове зобов'язання щодо збереження (нерозголошення) секретної інформації, довіре-

¹ Вирок Рівненського міського суду Рівненської області від 06 червня 2017 року (справа № 569/5912/17). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/67083607> (дата звернення: 05.09.2024).

² Вирок Солом'янського районного суду м. Києва від 13 червня 2017 року (справа № 760/9476/17-к). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/67113994> (дата звернення: 05.09.2024).

ної чи такої, що стала відомою у зв'язку з виконанням службових обов'язків¹.

Окрім того, у частині розголошення відомостей *невійськового* характеру, що становлять державну таємницю, за цією статтею підлягають відповідальності й військовослужбовці (з огляду на їх службове становище), а також прирівняні до них особи, яким певна інформація була довірена або стала відома у зв'язку з проходженням служби й виконанням покладених на них обов'язків. У разі ж розголошення зазначеними особами відомостей *військового* характеру, що є державною таємницею, відповідальність має наставати за ст. 422 КК.

Негативною ознакою цього кримінального правопорушення є відсутність ознак державної зради або шпигунства. Таким чином, на практиці виникає проблема в розмежуванні зазначених кримінальних правопорушень. Розмежувальними ознаками в цьому аспекті можуть бути такі:

- державна зрада або шпигунство є умисно спрямованими на спричинення шкоди основам зовнішньої безпеки України, а кримінальне правопорушення за ст. 328 КК не має такої спрямованості;
- адресат передачі відомостей: при державній зраді або шпигунстві – це іноземна держава, іноземна організація або їх представники, а при кримінальному правопорушенні за ст. 328 КК коло адресатів не обмежене. При цьому, на думку Л. Ф. Дадерка, суб'єкт не усвідомлює й не може усвідомлювати істинний характер адресата у випадку його належності до іноземної держави чи організації та не має наміру ознайомити з такими відомостями іноземну державу, іноземну організацію чи їх представників²;

¹ Дадерко Л. Ф. Кримінальна відповідальність за розголошення державної таємниці. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юриспруденція. 2013. Вип. 6-2. Т. 2. С. 84. URL: <https://vestnik-pravo.mgu.od.ua/archive/juspradenc6-2-2/21.pdf>

² Дадерко Л. Ф. Кримінальна відповідальність за розголошення державної таємниці. *Науковий вісник Міжнародного гуманітарного університету*. Серія: Юри-

- суб'єкт кримінального правопорушення за цими злочинами є спеціальним, однак відповідна спеціальна ознака є різною: за статтями 111 та 114 КК це особа, що є громадянином України або ж іноземцем чи особою без громадянства, а у ст. 328 КК – це особа, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків.

2.1.2. Втрата документів, що містять державну таємницю (ст. 329 КК України)

У ст. 329 КК за ч. 1 передбачено відповідальність за втрату документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації або предметами; а за ч. 2 цієї статті – за те саме діяння, якщо воно спричинило тяжкі наслідки¹.

Предметом цього кримінального правопорушення є:

- документи, що містять державну таємницю;
- інші матеріальні носії секретної інформації, що містять державну таємницю (флеш-накопичувачі, лазерні диски тощо);
- предмети, відомості про які становлять державну таємницю.

Таким чином, до предмета цього правопорушення належить широке коло речей, що містять або становлять державну таємницю, поняття якої було розкрито в підрозділі 1.2. розділу I цього монографічного дослідження.

Документи, що містять державну таємницю. Документом, відповідно до Закону України «Про інформацію» від 02.10.1992 р. № 2657-ХІІ, є матеріальний носій, що містить інформацію, основни-

спруденція. 2013. Вип. 6-2. Т. 2. С. 84. URL: <https://vestnik-pravo.mgu.od.ua/archive/juspradenc6-2-2/21.pdf>

¹ *Примітка.* Згідно зі ст. 12 КК правопорушення за ч. 1 та ч. 2 ст. 328 КК є не тяжкими злочинами.

ми функціями якого є її збереження та передавання у часі та просторі (ст. 1). Виходячи з відсутності вказівки в диспозиції цієї норми на офіційність документів, можливо дійти висновку, що документами, що містять державну таємницю, можуть бути як офіційні документи (у розумінні примітки до ст. 358 КК), так і неофіційні документи. Прикладами документів можуть бути накази, розпорядження, дисертації, наукові висновки, звіти, схеми, карти, фотографії та ін.

Інші матеріальні носії секретної інформації, що містять державну таємницю. У Законі України «Про державну таємницю» матеріальні носії секретної інформації визначені як матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо (ст. 1). До таких носіїв, що містять державну таємницю, відносять форми зберігання таємної інформації, не передбачені законодавством (наприклад, не зареєстровані у встановленому порядку блокноти з нотатками, кресленнями тощо з виписками з відповідних документів тощо)¹.

Предметами, відомості про які становлять державну таємницю, можуть бути різновиди зброї, техніки, обладнання, матеріали, препарати (хімічні, медичні тощо) та ін.

Об'єктивна сторона цього кримінального правопорушення виражається в таких ознаках:

- діянні (дії або бездіяльності) – порушенні встановленого законом порядку поводження із документами та іншими матеріальними носіями секретної інформації, що містять державну таємницю, або предметами, відомості про які становлять державну таємницю;
- наслідках – втраті документів / інших матеріальних носіїв / предметів;

¹ Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ: Дакор, 2018. С. 1019; Данилевський А. О. Злочини у сфері охорони державної таємниці, недоторканості державних кордонів, забезпечення призову та мобілізації. *Кримінальне право (Особлива частина)*: підручник / за ред. О. О. Дудорова, Є. О. Письменського. Т. 2. Луганськ: Елтон-2, 2012. Гл. 16. С. 272.

– необхідному причинному зв'язку між діяннями та наслідками.

Важливе значення для кваліфікації цього злочину має встановлення конкретних визначених у законодавчому акті правил, які винний порушує. У літературі зазначається, що відповідне порушення правил може полягати в недотриманні:

- режиму секретності при роботі з відповідними документами чи предметами: неправильна організація обліку таємних предметів, відсутність необхідної охорони приміщень, де зберігаються таємні документи; недотримання умов транспортування таких документів (предметів), робота з таємними документами в умовах, що не гарантують їх збереження;
- правил таємного діловодства: передача таємних документів на ознайомлення; здійснення такої передачі без належного оформлення; несанкціоноване виготовлення копій таємних документів і т. ін.¹

Разом із тим слід підкреслити, що в диспозиції норми ст. 329 КК безпосередньо вказано на те, що порядок поводження з відповідними документами або предметами, що порушується винним, має бути визначено саме на рівні закону, однак вивчення положень основного закону в цій площині, а саме «Про державну таємницю», надає змогу виявити відсутність у ньому конкретизованих правил такого порядку. Серед норм, що все ж указують на такий порядок загальним чином, можна навести, наприклад:

- ст. 28, в якій встановлено обов'язки громадянина щодо збереження державної таємниці (приміром, обов'язок виконувати громадянами вимоги режиму секретності; обов'язок громадян додержуватися інших вимог законодавства про державну таємницю);
- ст. 21, яка визначає основні завдання режимно-секретних органів, зокрема:
 - а) своєчасне розроблення та реалізація разом з іншими структурними підрозділами державних органів, органів

¹ Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ: Дакор, 2018. С. 1020.

- місцевого самоврядування, підприємств, установ і організацій заходів, що забезпечують охорону державної таємниці;
- в) запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;
 - д) забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин;
 - е) організація та ведення секретного діловодства.

Таким чином, ураховуючи занадто узагальнений характер положень Закону України «Про державну таємницю», що визначають порядок поводження з відповідними документами / предметами, вбачається, що кваліфікація дій особи, якій інкримінується вчинення злочину за ст. 329 КК, обов'язково потребує посилань на конкретні правила, закріплені в підзаконних нормативних актах.

Як видається з аналізу судової практики, таким підзаконним нормативним актом, що регламентує певні правила *поводження із зазначеними в диспозиції цієї норми документами, матеріальними носіями або предметами й на порушення приписів якого, відповідно, посилаються* в більшості випадків судді, є вищезгаданий Порядок № 939. Так, вироком Звенигородського районного суду Черкаської області від 21.03.2019 р. (справа № 694/309/19) особу було засуджено за ч. 1 ст. 329 КК з огляду на те, що вона на порушення п. 364 цього Порядку не долучила довірений їй документ із переліком об'єктів місцевого значення, що підлягають охороні в умовах надзвичайного стану й особливого періоду, до номенклатурної справи і зберігала його в невстановленому місці¹. *В іншій*

¹ Вирок Звенигородського районного суду Черкаської області від 21 березня 2019 року (справа № 694/309/19). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/80671604> (дата звернення: 05.09.2024).

справі, згідно з вироком Жовтневого районного суду м. Запоріжжя від 23.09.2021 р. (справа № 331/1316/15-к), особу визнано винною у вчиненні кримінального правопорушення, передбаченого ч. 1 ст. 329 КК, зважаючи на те, що вона спочатку самостійно отримала та транспортувала примірники відповідних ухвал слідчого судді (що мають гриф секретності «таємно») на порушення вимог ст. 28 Закону України «Про державну таємницю», пунктів 317, 318 Порядку № 939, а згодом усупереч пунктам 116, 318 Порядку не повернула наявну в неї таємну документацію до режимно-секретного органу й залишила її в портфелі в автомобілі, що призвело до її фактичної втрати¹.

Окрім зазначеного Порядку № 939, правила поводження із документами, іншими матеріальними носіями секретної інформації, що містять державну таємницю, а також предметами, відомості про які становлять державну таємницю, також регламентується в таких постановках Кабінету Міністрів України: «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 16.02.1998 р. № 180; «Про затвердження положень з питань державної таємниці та внесення змін до деяких постанов Кабінету Міністрів України» від 29.11.2001 р. № 1601; «Про затвердження Порядку державної реєстрації та обліку секретних науково-дослідних, дослідно-конструкторських робіт і дисертацій» від 24.03.2022 р. № 271) та ін.

Отже, правозастосувач при кваліфікації діяння, яке підпадає під ознаки ст. 329 КК, має вдаватися до поширювального тлумачення відповідної норми, розширюючи наявне в ній поняття «закон» до поняття «законодавство», що охоплює як закони, так і підзаконні нормативно-правові акти. Водночас, ураховуючи необхідність додержання в законодавстві та правозастосуванні принципу правової визначеності, на чому неодноразово звертав увагу у своїх рішеннях

¹ Вирок Жовтневого районного суду м. Запоріжжя від 23 вересня 2021 року (справа № 331/1316/15-к). Єдиний державний реєстр судових рішень: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/99812205> (дата звернення: 05.09.2024).

Конституційний Суд України¹, в аспекті пропозиції *de lege ferenda* можливо запропонувати в диспозиції норми ч. 1 ст. 329 КК змінити поняття «закон» на поняття «законодавство»².

Під втрагою в контексті ст. 329 КК слід розуміти вихід документа / предмета з володіння особи поза її волею (тимчасовий або безповоротний)³.

Кримінальне правопорушення за ч. 1 має матеріальний склад та вважається закінченим із моменту втрати документів / інших матеріальних носіїв / предметів, за якої була створена реальна можливість ознайомлення з ними третіх осіб. Таким чином, для визнання цього злочину закінченим мають значення два фактори: 1) факт втрати документа або предмета; 2) наявність реальної можливості ознайомитися з документом / предметом третіх осіб. Відсутність такої можливості (наприклад, якщо документи були знищені) виключає склад зазначеного кримінального правопорушення⁴. З цього питання думки в літературі співпадають.

¹ Рішення Конституційного Суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) абзацу восьмого пункту 5 частини першої статті 11 Закону України «Про міліцію» від 29 червня 2010 року № 17-рп/2010. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/v017p710-10> (дата звернення: 09.09.2024).

² Євтєєва Д. П., Куковинець Д. О. Щодо проблеми кваліфікації злочину «втрата документів, що містять державну таємницю» (ст. 329 КК України). *Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки*: матеріали всеукр. наук.-практ. конф. (м. Київ, 27 верес. 2024 р.). Вінниця: ТВОРИ, 2024. С. 164.

³ Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. *Кримінальне право України. Особлива частина*: підручник / за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., переробл. і допов. Харків: Право, 2020. Розд. XV. С. 502; Олійник В. І. Кримінально-правове, кримінологічне та кримінально-виконавче забезпечення охорони державної таємниці в Україні. *Україні: дис. ... д-ра юрид. наук*. Київ, 2023. С. 290. URL: <https://maup.com.ua/assets/files/dis/olijnik/olijnik-disertaciya.pdf> (дата звернення: 09.09.2024).

⁴ Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. С. 502; *Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка*. 10-те вид., переробл. та допов. Київ: Дакор,

Якщо порушення порядку із вказаними документами або пред-
метами не спричинило їх втрати або якщо втрата не була наслідком
саме порушення встановленого законом порядку (приміром, при
викраденні документів), склад кримінального правопорушення за
ст. 329 КК в таких випадках буде відсутнім¹.

За ч. 2 зазначене правопорушення вважається закінченим із мо-
менту настання тяжких наслідків, які за змістом можуть співпадати
з тяжкими наслідками за ст. 328 КК.

За суб'єктивною стороною злочин може бути вчинено зі зміша-
ною або необережною формою вини: щодо діяння у виді порушення
правил можливі умисел або необережність, а щодо наслідків у виді
втрати документів / предметів – лише необережність². При цьому
мотив та мета не є обов'язковими ознаками складу цього правопо-
рушення.

Суб'єктом розглядуваного злочину може бути особа, якій ці до-
кументи / матеріальні носії / предмети були довірені, а саме: служ-
бова особа (публічного права) або інша особа, робота якої пов'язана
з такими документами / матеріальними носіями / предметами.

Однією з наукових та практичних проблем є відмежування кри-
мінальних правопорушень за ст. 328 КК та ст. 329 КК. Серед розмеж-
увальних ознак можливо виділити такі:

- предмет кримінального правопорушення (за ст. 328 КК –
лише відомості (вужчий), за ст. 329 КК – документи, інші ма-
теріальні носії, предмети);

2018. С. 1020; Данилевський А. О. Злочини у сфері охорони державної таємниці,
недоторканності державних кордонів, забезпечення призову та мобілізації. *Кримі-
нальне право (Особлива частина): підручник* / за ред. О. О. Дудорова, Є. О. Пись-
менського. Т. 2. Луганськ: Елтон-2, 2012. Гл. 16. С. 272.

¹ Науково-практичний коментар Кримінального кодексу України / за ред.
М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ: Дакор, 2018.
С. 1020.

² Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони
державної таємниці, недоторканності державних кордонів, забезпечення призову та
мобілізації. С. 503; Науково-практичний коментар Кримінального кодексу України /
за ред. М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ: Дакор,
2018. С. 1020.

- конструкція складу (за ч. 1 ст. 328 КК – формальний, за ч. 1 ст. 329 КК – матеріальний);
- критерій волі особи. Якщо документи вибули з володіння особи за її волею – кваліфікація має наставати за ст. 328 КК, якщо поза волею – за ст. 329 КК.

2.1.3. Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422 КК України)

У ст. 422 КК передбачено відповідальність за:

- розголошення відомостей військового характеру, що становлять державну таємницю, за відсутності ознак державної зради (ч. 1);
- втрату документів або матеріалів, що містять відомості військового характеру, які становлять державну таємницю, предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановлених правил поведіння із зазначеними документами, матеріалами або предметами (ч. 2);
- діяння, передбачені частинами першою або другою цієї статті, якщо вони спричинили тяжкі наслідки (ч. 3)¹.

Таким чином, за ч. 1 норма ст. 422 КК є спеціальною щодо норми ст. 328 КК, а за ч. 2 – щодо норми ст. 329 КК. При цьому специфікою правопорушення за ст. 422 КК є:

- а) предмет злочину – відомості військового характеру;
- б) суб'єкти – військовослужбовці.

Стосовно *предмета злочину*, то відомості військового характеру, що містять державну таємницю, визначені у Зводі відомостей, що становлять державну таємницю, затвердженому наказом Служби безпеки України від 23.12.2020 р. № 383. До них, наприклад, на-

¹ *Примітка.* Згідно зі ст. 12 КК правопорушення за ч. 1 та ч. 2 ст. 422 КК є нетяжкими злочинами, а за ч. 3 – тяжким злочином.

лежать відомості у сфері оборони, зокрема, відомості про стратегічне розгортання військ (сил), відомості про зміст стратегічних (оперативних) планів застосування Збройних Сил (військ або сил), відомості про систему бойової, мобілізаційної готовності, рівень готовності (здатності) військ (сил) до виконання завдань за призначенням та ін.

Щодо кола осіб, які можуть бути суб'єктами злочину за ст. 422 КК, то до нього (відповідно до загальної вказівки в ч. 2 ст. 401 КК стосовно суб'єктів кримінальних правопорушень за розділом XIX КК) можуть входити: військовослужбовці Збройних Сил України, Служби безпеки України, Державної прикордонної служби України, Національної гвардії України та інших військових формувань, утворених відповідно до законів України, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, а також інші особи, визначені законом.

Стосовно тяжких наслідків, які можуть настати в результаті вчинення такого суспільно небезпечного діяння, то, як показує судова практика, ними можуть визнаватися зниження обороноздатності держави, а також інші тяжкі наслідки, зокрема, у вигляді:

- 1) розкриття факту володіння Україною інформацією, отриманою за результатами розвідувальної діяльності розвідувального органу Міністерства оборони України про бойові спроможності підрозділів збройних сил російської федерації, що, в свою чергу, ускладнило б ведення розвідувальної діяльності та призвело б до зниження обороноздатності держави;
- 2) надання можливості заінтересованій стороні протидіяти розвідувальному органу Міністерства оборони України в отриманні розвідувальної інформації у визначених законодавством сферах, встановити джерела отримання такої інформації та вжити заходів щодо загострення міжнародних відносин України з іншими державами, що призведе до зниження обороноздатності держави;
- 3) надання збройним силам російської федерації та іншим незаконним збройним формуванням можливості провести перегрупування сил і засобів для їх бойового застосування на

інших оперативних напрямках, що призвело б до невиконання бойових завдань угрупованням військ (сил) Збройних Сил України тощо¹.

Інші наукові та практичні проблеми, що виникають стосовно кримінальних правопорушень за цією статтею, фактично збігаються з проблемами, стосовними кримінальних правопорушень за ст. 328 та 329 КК, які були розглянуті вище.

2.2. Кримінальні правопорушення у сфері охорони іншої інформації, що забезпечує обороноздатність держави (стаття 330 КК України)

У ст. 330 КК за ч. 1 передбачено відповідальність за передачу або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службу інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства. За ч. 2 цієї статті встановлено відповідальність за ті самі дії, вчинені з корисливих мотивів, або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб².

Предметом зазначеного кримінального правопорушення є службова інформація, зібрана у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни³.

¹ Вирок Галицького районного суду м. Львова від 30 серпня 2022 року (справа № 461/3937/22; провадження № 1-кп/461/556/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/106028306> (дата звернення: 05.09.2024).

² *Примітка*. Згідно зі ст. 12 КК правопорушення за ч. 1 ст. 330 КК є нетяжким злочином, а за ч. 2 – тяжким злочином.

³ Базелюк В. В. Відомості, що становлять службу інформацію, як предмет кримінального правопорушення, передбаченого ст. 330 КК України. *ПРОКІІВ*:

Відповідно до ст. 9 Закону України «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI до службової може належати інформація:

- 1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;
- 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці¹. Проте, як вбачається з диспозиції норми ст. 330 КК, предмет цього кримінального правопорушення є не вся службова інформація, а лише передбачена п. 2 ч. 1 ст. 9 Закону, тобто зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 р. № 2135-XII не дає визначення поняття «інформації, зібраної в процесі оперативно-розшукової діяльності», а розкриває лише зміст терміну «оперативно-розшукова діяльність», під якою мається на увазі система гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів².

Згідно із Законом України «Про контррозвідувальну діяльність» від 26.12.2002 р. № 374-IV контррозвідувальна діяльність є спеціальним видом діяльності у сфері забезпечення державної безпеки,

І всеукр. наук.-практ. конф. з міжнар. участю (м. Київ, 26 берез. 2024 р.). Київ: б/в, 2024. С. 437. URL: <https://ndirom.org/wp-content/uploads/2024/06/tezy.pdf>.

¹ Про доступ до публічної інформації : Закон України від 13 січня 2011 року № 2939-VI. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#n40> (дата звернення: 09.09.2024).

² Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 року № 2135-XII. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text> (дата звернення: 09.09.2024).

яка здійснюється із використанням системи контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України¹.

Слід зазначити, що основним способом здійснення контррозвідувального захисту є проведення оперативно-розшукових заходів, перелік яких встановлений Законом України «Про оперативно-розшукову діяльність». Лише за допомогою проведення оперативно-розшукових заходів досягаються поставлені цілі, через які спеціально уповноважений державний орган здійснює контррозвідувальний захист².

Стосовно інформації у сфері оборони країни, відповідно до Закону України «Про оборону України» від 06.12.1991 р. № 1932-ХІІ оборона України являє собою систему політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту³.

Отже, предметом кримінального правопорушення, передбаченого ст. 330 КК, є як зафіксована, так і не зафіксована на матеріальних носіях службова інформація, але не вся, а лише окремі види такої інформації, зібрані в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони. При цьому важливо,

¹ Про контррозвідувальну діяльність : Закон України від 26 грудня 2002 року № 374-IV. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/374-15#Text> (дата звернення: 09.09.2024)

² Павленко В. П. Поняття та особливості контррозвідувального захисту державного суверенітету, конституційного ладу і територіальної цілісності держави України. *Юридичний науковий електронний журнал*. 2021. № 7. С. 35. URL: http://lsej.org.ua/7_2021/9.pdf.

³ Про оборону України: Закон України від 6 грудня 1991 року № 1932-ХІІ. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/1932-12#Text> (дата звернення: 09.09.2024)

щоб уся ця інформація не була віднесена до державної таємниці, оскільки остання є предметом кримінально-правової охорони інших норм КК.¹

Об'єктивна сторона цього кримінального правопорушення виражається у двох формах: 1) передачі відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контрольно-розвідувальної діяльності, у сфері оборони країни, іноземним підприємствам, установам, організаціям або їх представникам; 2) збиранні таких відомостей із метою передачі іноземним підприємствам, установам, організаціям або їх представникам².

Першою формою вираження об'єктивної сторони кримінального правопорушення, передбаченого ст. 330 КК, є *передача відомостей*, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контрольно-розвідувальної діяльності, у сфері оборони країни. Передача має місце у випадках, коли особа володіє ними і повідомляє (передає, вручає) їх іноземним підприємствам, установам, організаціям або їх представникам. Способи передачі можуть бути різними (усна, письмова, безпосереднє ознайомлення з будь-якими матеріалами, передача через Інтернет, по телефону, з використанням тайників, кур'єрів та ін.). Не має також значення передаються першоджерела, їх копії чи лише відомості про них. Тому як передача предмета кримінального правопорушення в буквальному розумінні цього слова, так і створення умов для ознайомлення з ним представника іноземного підприємства, установи, організації, підпадають під поняття «передача»³.

¹ Базелюк В. В. Відомості, що становлять службову інформацію, як предмет кримінального правопорушення, передбаченого ст. 330 КК України. *ПРОКІІВ: І всеукр. наук.-практ. конф. з міжнар. участю* (м. Київ, 26 берез. 2024 р.). Київ: б/в, 2024. С. 437. URL: <https://ndirom.org/wp-content/uploads/2024/06/tezy.pdf>.

² Базелюк В. В. Об'єктивна сторона передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контрольно-розвідувальної діяльності, у сфері оборони країни (ст. 330 КК України). *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. № 85. Ч. 3. С. 238.

³ Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. С. 504.

Другою формою вираження об'єктивної сторони кримінального правопорушення, передбаченого ст. 330 КК, є *збирання відомостей*, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни. Розгляду поняття «збирання відомостей» як ознаки об'єктивної сторони складів різних кримінальних правопорушень присвячено багато досліджень. Так, В. О. Навроцький під збиранням відомостей розуміє отримання інформації будь-яким способом: викрадення, підслуховування, фотографування, кіно- або відео зйомка, використання технічних пристроїв, зосередження інформації або матеріалів, які перебувають у різних джерелах¹. Є. Л. Стрельцов вказує, що незаконне збирання – це діяння, спрямоване на добування будь-яким способом певної інформації². О. Е. Радутний, розглядаючи склад кримінального правопорушення, передбаченого ст. 231 КК, виділив різновиди кримінально протиправного збирання відомостей, що становлять комерційну таємницю, які можуть мати прояв у таких діях: викрадення, шахрайство, привласнення, вимагання, підкуп, зловживання службовим становищем, незаконне перехоплення, фіксування, розшук, спостереження тощо³. Безумовно, розглядаючи збирання інформації як ознаку об'єктивної сторони кримінальних правопорушень, передбачених статтями 114, 231 КК, можна погодитись із вищевикладеними точками зору вчених, що основною характеристикою дій при збиранні відомостей, які становлять державну та комерційну таємницю, є їх незаконність. Проте збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, має свої особливості. Перш за все це пов'язано з тим, що суб'єкт кримінального правопорушення, передбаченого ст. 330 КК, не повинен долати перешкод при отриманні інформації, оскільки вказані

¹ Навроцький В. О. Господарські злочини. Лекції для студентів юридичних факультетів. Львів, 1997. С. 31.

² Стрельцов Є. Л. Господарські злочини: Глава VI Кримінального кодексу України з науково-практичним коментарем. Одеса: АстроПринт, 1998. С. 51.

³ Радутний О. Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) : автореф. дис... канд. юрид. наук: 12.00.08. Харків, 2002. С. 14, 15.

відомості були довірені або стали відомі йому у зв'язку з виконанням службових обов'язків. Таким чином, особі нема необхідності розпитувати, підкупати чи шантажувати інших осіб, які мають доступ до конфіденційної інформації, підслуховувати розмови про такі відомості, використовувати спеціальні технічні засоби тощо. Тому під збиранням відомостей, що становлять предмет досліджуваного злочину, слід розуміти активні дії щодо розшуку, зосередження (зведення, узагальнення) та фіксування (зображення, фотографування, копіювання, запам'ятовування) інформації¹.

Особливістю передачі та збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, є те, що вона стає надбанням тільки іноземних підприємств, установ, організацій чи їх представників, а не будь-якої зацікавленої особи. Під іноземною організацією розуміється будь-яка державна чи недержавна установа, підприємство, об'єднання, орган іншої країни, у тому числі політична партія, релігійна організація, комерційне підприємство, а також міждержавна чи міжнародна організація, у тому числі неофіційна, нелегітимна чи злочинна. Іноземною організацією є також військова, політична, економічна, фінансова, прикордонна чи інша розвідки². Представник іноземної організації – це особа, яка уповноважена виражати інтереси тієї чи іншої іноземної держави (іноземної організації) та діє від її імені або представляє її за спеціальним повноваженням, у тому числі таємним (не офіційним). Проте, як вірно підмітила О. С. Самойлова, поняття іноземної організації охоплює іноземні підприємства і установи. Тому в диспозиції норми ст. 330 КК було б доречно зазначити як адресата передачі інформації тільки іноземні держави, організації та їх представників³.

¹ Самойлова О. С. Особливості об'єктивної сторони злочину, передбаченого ст. 330 КК України. Вісник Харківського національного університету внутрішніх справ. 2006. № 34. С. 139, 140.

² Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року / За ред. М. І. Мельника, М. І. Хавронюка. Київ, 2001. С. 155.

³ Самойлова О. С. Особливості об'єктивної сторони злочину, передбаченого ст. 330 КК України. С. 140, 141.

Як зауважила О. С. Самойлова, закон залишає відкритим питання про зберігання відомостей, що становлять предмет досліджуваного кримінального правопорушення. На її думку, ця прогалина у законодавстві має бути усунута шляхом внесення змін до чинної редакції ст. 330 КК з метою доповнення її таким альтернативним діянням об'єктивної сторони складу кримінального правопорушення, як зберігання відомостей, під яким слід розуміти будь-які умисні дії, пов'язані з незаконним перебуванням зазначеної інформації у володінні винної особи. При цьому умислом суб'єкта кримінального правопорушення повинно охоплюватись те, що такі відомості були зібрані та зберігалися з метою передачі іноземним підприємствам, установам, організаціям або їх представникам¹.

У ч. 1 ст. 330 КК настання суспільно небезпечних наслідків не передбачене, а, отже, не є обов'язковою ознакою об'єктивної сторони відповідного складу кримінального правопорушення. Кримінальне правопорушення, закріплене ст. 330 КК, вважається закінченим або з моменту передачі, або з моменту збирання відомостей з метою їх передачі². У формі передачі відомостей воно вважається закінченим із моменту створення реальної можливості ознайомлення іноземним підприємством, установою, організацією або їх представником з відомостями, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

Разом із тим у ч. 2 ст. 330 КК передбачено злочин із матеріальним складом – однією з ознак, що обтяжують відповідальність за його вчинення, є тяжкі наслідки для інтересів держави. Як і в нормах за ч. 2 ст. 328, ч. 2 ст. 329 та ч. 3 ст. 422 КК, де закріплені тяжкі наслідки, розглядуване поняття є оціночним, водночас, на відміну від останніх, у ч. 2 ст. 330 КК воно є вужчим, адже передбачає заподіяння шкоди лише інтересам держави.

¹ Там само. С. 142.

² Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. С. 504.

Спосіб, засоби, місце, час і обстановка вчинення є факультативними ознаками об'єктивної сторони цього кримінального правопорушення – застосування того або іншого способу передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, використання окремих засобів, а також інші умови (час, місце, обстановка), законодавець залишає за межами кримінального правопорушення за ч. 1 ст. 330 КК, тому на кваліфікацію вони не впливатимуть¹. Указані ознаки являють собою сукупність конкретних умов, за яких здійснюється кримінально протиправне діяння, розвивається об'єктивна сторона й настає кримінально протиправний результат. Ці ознаки існують об'єктивно, незалежно від волі злочинця, хоч в окремих випадках вони можуть бути свідомо ним використані або частково сформовані².

Слід відмітити, що відомості визнаються такими, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, тільки в тому разі, якщо інформація має певну цінність для її власника, а розголошення такої інформації може заподіяти шкоди або створити загрозу заподіяння шкоди державі чи суспільству. Тому, якщо така інформація стає відома іноземним підприємствам, установам, організаціям або їх представникам, спричиняється шкода або створюється реальна загроза спричинення шкоди інтересам держави, суспільства чи особи. Таким чином, в будь-якому разі в результаті вчинення цього кримінального правопорушення порушується стан захищеності, безпеки суспільних відносин, поставлених під охорону закону про кримінальну відповідальність, порушуються безпечні умови їх функціонування³.

¹ Самойлова О. С. Особливості об'єктивної сторони злочину, передбаченого ст. 330 КК України. С. 141.

² Базелюк В. В. Об'єктивна сторона передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330 КК України). *Науковий вісник Ужгородського національного університету. Серія Право*. 2024. № 85. Ч. 3. С. 239.

³ Самойлова О. С. Особливості об'єктивної сторони злочину, передбаченого ст. 330 КК України. С. 141.

Суб'єктивна сторона кримінального правопорушення, передбаченого ст. 330 КК, виражається у вині у формі прямого умислу. Суб'єкт усвідомлює конфіденційність інформації, а також те, що вона є власністю держави, і бажає її передати або збирати для передачі саме іноземним підприємствам, установам, організаціям або їх представникам. Це усвідомлення обумовлено тим, що особи, які працюють з такою інформацією, підлягають обов'язковому ознайомленню під розписку про конфіденційність інформації та встановлені правила щодо користування нею, наприклад заборону виносити за межі службового приміщення документи з такою інформацією, розмножувати їх технічними засобами, які не обладнані спеціальними пристроями охорони, тощо¹.

Окрім того, обов'язковою ознакою суб'єктивної сторони розглядуваного складу кримінального правопорушення є спеціальна мета – передача відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, саме іноземним підприємствам, установам, організаціям або їх представникам (це можуть бути як державні, так і недержавні підприємства, установи, організації – комерційні, наукові тощо). При цьому для кваліфікації є важливим аспект, що передача або збирання такої службової інформації не повинні містити ознак державної зради чи шпигунства, тобто умисел не повинен бути спрямованим на спричинення шкоди основам національної безпеки, а також не повинно бути мети підризу або ослаблення держави².

Суб'єктом кримінального правопорушення, передбаченого ст. 330 КК, є особа, якій відомості, що становлять службову ін-

¹ Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. С. 504.

² Базелюк В. Суб'єкт передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330 КК України). *Правовий дискурс* : матер. IV Всеукр. наук.-практ. конф. (м. Черкаси, 10 жовтня 2024 р.). Київ: 7БЦС, 2024. С. 170. URL: <http://repositc.nuczu.edu.ua/bitstream/123456789/22091/1/Правовий%20курс%2010.10.2024.pdf>.

формацію, були довірені або стали відомі у зв'язку з виконанням службових обов'язків¹. До таких осіб належать: 1) особи, які мають досвід роботи та безпосереднє відношення до цих справ, згідно зі списками, погодженими з канцелярією, а до документів – згідно з вказівками, викладеними у резолюціях керівників організацій (структурних підрозділів); 2) представники інших організацій, які мають дозвіл керівників організацій (структурних підрозділів), у володінні та розпорядженні яких перебувають ці документи, за наявності письмового запиту організацій, в яких вони працюють, із зазначенням характеру завдання, що виконується; 3) громадяни України, яким видаються документи та видання з грифом «Для службового користування» у масових бібліотеках, при наявності письмового клопотання керівників організацій, в яких працюють ці громадяни, із зазначенням теми роботи; 4) особи, які внаслідок свого службового положення наділені правом вимагати від підприємств, установ і організацій незалежно від форм власності і об'єднань громадян надання будь-яких відомостей; 5) особи, до компетенції яких входить розробка та введення в дію переліків конфіденційної інформації, зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни; 6) особи, які проставляють гриф обмеження доступу «Для службового користування»; 7) особи, які забезпечують ведення обліку, зберігання, розмноження та використання документів з грифом «Для службового користування»; 8) особи, які тиражують, друкують і розсилають документи з грифом «Для службового користування»; 9) особи, які після закінчення діловодного року переглядають документи з грифом «Для службового користування»; 10) особи, які працюють в масових бібліотеках, бібліотеках закритого типу та в державних архівних фондах, в яких зберігаються видання з грифом «Для службового користування»².

¹ Орловський Р. С., Ус О. В. Кримінальні правопорушення у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. С. 505.

² Володавська О. С. Суб'єкт злочину, передбаченого ст. 330 Кримінального кодексу України. *Форум права*. 2010. № 4. С. 154.

При цьому такими суб'єктами можуть бути не лише громадяни України, а й іноземці та особи без громадянства¹.

Як вбачається із матеріалів судової практики, суб'єктами цього кримінального правопорушення визнають працівників контррозвідки (вирок Печерського районного суду м. Києва від 12.10.2015 р. (справа № 757/35881/15-к)², військовослужбовців (вирок Корольовського районного суду м. Житомира від 25.04.2022 р. (справа № 296/1922/22))³ і навіть викладачів (вирок Дзержинського районного суду м. Харкова від 22.04.2019 р. (справа № 638/5564/19)⁴ тощо.

¹ Базелюк В. Суб'єкт передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330 КК України). С. 170.

² Вирок Печерського районного суду м. Києва від 12 жовтня 2015 року (справа № 757/35881/15-к). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/52901355> (дата звернення: 05.09.2024).

³ Вирок Корольовського районного суду м. Житомира від 25 квітня 2022 року (справа № 296/1922/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/104068632> (дата звернення: 05.09.2024).

⁴ Вирок Дзержинського районного суду м. Харкова від 22 квітня 2019 року (справа № 638/5564/19). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/81322388> (дата звернення: 05.09.2024).

Висновки до розділу II

1. Об'єктивна сторона злочину за ст. 328 КК (розголошення державної таємниці) виражається в діянні, яке фактично може бути вчинено як шляхом дії, так і бездіяльності. Однак віддієслівний іменник «розголошення», що походить від перехідного дієслова в активному стані, не підходить для окреслення пасивної поведінки щодо поширення відповідної інформації. У зв'язку з цим у диспозиції цієї норми доречно було б передбачити дві альтернативні форми діяння: 1) розголошення відомостей; 2) спричинення витоку таких відомостей. При цьому, оскільки суспільна небезпечність активної та пасивної поведінки в цьому випадку є різною (що в тому числі обумовлюється й різними формами вини, які їм властиві, зокрема, активній – умисна вина, а пасивній – необережна), відображення двох зазначених форм поведінок у диспозиції норми ч. 1 ст. 328 КК дозволить більшою мірою диференціювати кримінальну відповідальність за цей злочин та, у свою чергу, призначати судам більш справедливе покарання за його вчинення.

2. Кримінальне правопорушення за ч. 1 ст. 328 КК має формальний склад. Щодо моменту його закінчення серед поглядів, висловлених у науковій літературі, виділені такі моменти, як первинний (коли хоча б одна стороння особа мала можливість ознайомлення зі змістом документа), вторинний (коли відомості стали відомі хоча б одній сторонній особі) та третинний (коли відповідні відомості були сприйняті сторонньою особою в обов'язі, який свідчить про перехід цієї інформації у власність такої особи). У цій дискусії визнання моментом закінчення цього злочину саме вторинного моменту, за якого відомості стають відомими хоча б одній особі, слід визнати найбільш раціональним, адже це викликатиме менше процесуальних труднощів та забезпечуватиме як додержання прав та інтересів особи, так процесуальну здійсненність кримінального переслідування.

3. Важливе значення для кваліфікації злочину за ст. 329 КК (втрата документів, що містять державну таємницю) має встановлення конкретних визначених у законодавчому акті правил, які винний

порушує. При цьому в диспозиції норми ст. 329 КК безпосередньо вказано на те, що порядок поводження з відповідними документами або предметами, що порушується винним, має бути визначено саме на рівні закону, однак в основному законі в цій площині (Законі «Про державну таємницю») відсутні конкретизовані правила такого порядку. Ураховуючи занадто узагальнений характер положень цього Закону, кваліфікація дій особи, якій інкримінується вчинення злочину за ст. 329 КК, обов'язково потребує посилань на конкретні правила, закріплені в підзаконних нормативних актах.

Отже, правозастосувач при кваліфікації діяння, яке підпадає під ознаки ст. 329 КК, має вдаватися до поширювального тлумачення відповідної норми, розширюючи наявне в ній поняття «закон» до поняття «законодавство», що охоплює як закони, так і підзаконні нормативно-правові акти. Водночас, ураховуючи необхідність додержання в законодавстві та правозастосуванні принципу правової визначеності, в аспекті пропозиції *de lege ferenda* можливо запропонувати в диспозиції норми ч. 1 ст. 329 КК змінити поняття «закон» на поняття «законодавство».

Розділ III

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Вступні положення

Процеси всеохоплюючої інформатизації, що виступають основою для формування глобального інформаційного простору, створюють підґрунтя до зміни парадигми суспільного життя – формування інформаційного суспільства. Поряд з бурхливим розвитком технологій констатуємо, однак, наявність численних небезпечних викликів, як перед державами, так і світовою спільнотою в цілому. Належне реагування на такі виклики полягає, зокрема, в удосконаленні кримінально-правових основ боротьби з кіберзлочинністю та необхідність гарантування інформаційної безпеки, тобто захищеності життєво важливих інтересів людини, суспільства та держави від потенційних або реальних загроз інформаційного простору, пов'язаних з використанням інформаційних технологій. Норми розділу XVI Особливої частини КК, безсумнівно, лежать в основі правових засобів боротьби з кіберзлочинністю, а також становлять собою «ядро» кримінально-правової охорони «технологічної» складової інформаційної безпеки.

За своєю суттю кримінальні правопорушення, передбачені розділом XVI Особливої частини КК, характеризуються як найбільш небезпечні посягання на суспільні відносини у сфері належного використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Серед цих кримінальних правопорушень:

- **стаття 361 КК** «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»;
- **стаття 361¹ КК** «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;
- **стаття 361² КК** «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»;
- **стаття 362 КК** «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»;
- **стаття 363 КК** «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»;
- **стаття 363¹ КК** «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку».

У науковій літературі проблеми кримінальної відповідальності за зазначені кримінальні правопорушення висвітлювалися у працях таких учених, як Д. С. Азаров, П. П. Андрушко, Ю. А. Бельський, В. М. Бутузов, В. О. Голубев, С. В. Дрьомов, М. В. Карчевський, О. О. Кирбят'єв, М. О. Кравцова, Т. В. Міхайліна, А. А. Музика, С. О. Орлов, М. В. Плугатир, М. В. Рудик, Н. А. Савінова та інші. Водночас, стрімкий розвиток

комп'ютерної техніки та сфери її використання, поширення практики проявів кримінальних правопорушень в сфері використання інформаційних технологій, роблять актуальним дослідження означеної проблематики.

У цьому розділі праці, перш за все, наведено та узагальнено статистичні дані й актуальну судову практику щодо кримінальних правопорушень, передбачених розділом XVI Особливої частини КК. Надалі увагу приділено висвітленню теоретичних питань родового об'єкта зазначеної групи кримінальних правопорушень, а також здійснено аналіз ознак елементів складів кримінальних правопорушень, передбачених ст.ст. 361–363¹ КК. Крім цього, запропоновано ознайомитись з напрацюваннями щодо окреслення перспективних напрямків кримінально-правового регулювання у контексті розвитку інформаційних технологій. Йдеться, зокрема, про шляхи подолання проблеми примітивізації протидії «комп'ютерним» кримінальним правопорушенням, а також про наявні проблеми протидії тим кримінальним правопорушенням, що вчиняються щодо віртуальних активів або з використанням штучного інтелекту. Насамкінець, підкреслюється особливе значення гармонізації національного законодавства з положеннями норм міжнародного права для протидії кримінально-протиправним діянням транскордонного характеру у сфері використання інформаційних технологій.

3.1. Кримінальні правопорушення в сфері використання інформаційних технологій (ст.ст. 361–363¹ КК України)

Науково-технічний прогрес змінює суспільні відносини. Впровадження нових технологій у всі сфери життя неминуче призводить до розширення інформаційних потоків та збільшення потреби в інформації. Сучасна людина потребує значних обсягів інформації для ефективної діяльності.

Зміна кількісних характеристик інформаційних процесів створює певне протиріччя, яке прийнято називати «інформаційний вибух»: з одного боку, для ефективної та результативної діяльності необхідний зростаючий обсяг інформації, а з другого – фізичні можливості людини щодо збереження, передачі та обробки інформації обмежені. Подолання цього протиріччя пов'язане з процесом, який має назву «інформатизація».

Відповідно до Закону України «Про Національну програму інформатизації» від 01.12.2022 р. № 2807-ІХ, який набув чинності 1 березня 2023 року, інформатизація представляє собою «сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, технологічних та виробничих процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій»¹. Варто зазначити, що названий закон визнав таким, що втратив чинність попередній нормативний документ з аналогічною назвою – Закон України «Про Національну програму інформатизації» від 04.02.1998 р. № 74/98-ВР². Визначення, яке містив закон, що втратив чинність, на нашу думку, було більш коректним, в ньому йшлося не про абстрактний «розвиток інформаційного суспільства», а про «задоволення інформаційних потреб громадян та суспільства». Зрештою, будемо розглядати попереднє визначення інформатизації як уточнення чинного: інформатизація представляє собою сукупність направлених на розвиток інформаційного суспільства та впровадження інформаційних технологій суспільних процесів, соціальна значимість яких визначається тим, наскільки вони забезпечують задоволення інформаційних потреб громадян та суспільства.

З інформатизацією тісно пов'язаний процес комп'ютеризації: розвиток та впровадження в різні сфери життя і діяльності людини технічної бази, що забезпечує оперативну роботу з інформацією.

¹ Про Національну програму інформатизації: Закон України від 01.12.2022 р. № 2807-ІХ. *Відомості Верховної Ради*. 2023. № 51. Ст. 127.

² Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР. *Відомості Верховної Ради України*. 1998. № 27–28. Ст. 181.

Комп'ютерна техніка стала важливою умовою існування та розвитку суспільства, оскільки саме вона дозволяє зберігати, обробляти та передавати обсяги інформації, достатні для ефективної діяльності в сучасних умовах. Отже, комп'ютеризація як реакція людства на ситуацію «інформаційного вибуху» є технічною основою сучасного етапу інформатизації. Розвиток комп'ютерної техніки характеризується стрімким зростанням показників швидкості роботи та збільшенням обсягу інформації, яку здатні обробляти комп'ютери. Завдяки успіхам технологій ці процеси супроводжуються зниженням співвідношення ціни та продуктивності ЕОМ, що спричиняє, без перебільшення, вибухове зростання сфери використання комп'ютерної техніки.

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

Якісна зміна «комп'ютерної»¹ злочинності пов'язана з розвитком мережевих комп'ютерних технологій. Станом на квітень 2024 року в усьому світі налічувалося 5,44 мільярда користувачів Інтернету, що становило 67,1% світового населення. З них 5,07 мільярда або 62,6% були користувачами соціальних мереж². У сучасному світі глобалізація комунікацій зумовила глобальний характер кіберзлочинності.

¹ Надалі на сторінках цієї праці пояснимо, чому поняття «комп'ютерні» кримінальні правопорушення нами вживається у лапках. Зараз же зазначимо, що під ним ми розуміємо кримінальні правопорушення, передбачені Розділом XVI КК.

² Petrosyan A. Worldwide digital population 2024. *Statista*: website. URL: <https://www.statista.com/statistics/617136/digital-population-worldwide/> (дата звернення: 30.08.2024).

Завдяки швидкому розвитку Інтернету та соціальних мереж кіберзлочинність перестала бути локальною проблемою і перетворилася на глобальну загрозу. Якщо у 2022 році світова вартість кіберзлочинності оцінювалася приблизно в 8,4 трильйона доларів США, то до 2026 року річні витрати на кіберзлочинність у всьому світі за наявними оцінками можуть перевищити 20 трильйонів, тобто, порівняно з 2022 роком, збільшитися майже на 150%¹.

Український законодавець приділяє значну увагу цій проблемі: чинний КК (у порівнянні з попередніми кодексами) вперше передбачив самостійний розділ про ці кримінальні правопорушення – розділ XVI Особливої частини «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Положення цього розділу неодноразово змінювалися та доповнювалися.

3.1.1. Статистичні дані та дослідження судової практики

Дані офіційної статистики² 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).

¹ Petrosyan A. Annual cost of cybercrime worldwide 2018-2029. *Statista*: website. URL: <https://www.statista.com/statistics/1280009/cost-cybercrime-worldwide/> (дата звернення: 30.08.2024).

² 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. В. (2024). Протидія злочинності в Україні: інфографіка (2013–2024): інтерактивний довідник. URL: <https://karchevskiy.com/i-dovidnyk/> (дата звернення: 30.08.2024). Цей ресурс інтегрує статистичні звіти форми 1 та 2 Офісу Генерального прокурора України та форми 6 та 7 Державної судової адміністрації України.

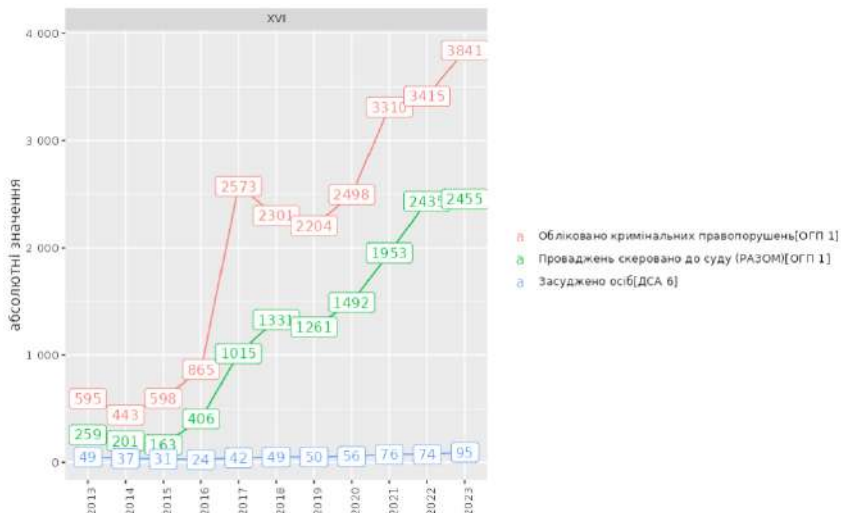


Рис. 1. Розподіл основних показників протидії кримінальним правопорушенням, передбаченим Розділом XVI Особливої частини КК

Розподіл кількості облікованих проваджень та кількості засуджених осіб (Таблиця 1) свідчить, що найбільш поширеним «комп'ютерним» кримінальним правопорушенням є передбачене ст. 361 КК. З цим кримінальним правопорушенням пов'язано більше половини (54%) облікованих проваджень. Більше половини (53,3%) засуджених за кримінальні правопорушення, передбачені Розділом XVI, вчинили несанкціоноване втручання в роботу... (ст. 361 КК). Другими за поширеністю є несанкціоновані дії, вчинені особою, яка має право доступу до комп'ютерної інформації (ст. 362 КК), – 38,1% проваджень та 20,1% відповідно засуджених. Статистично значимими та майже рівними є показники, що характеризують незаконні дії з шкідливими програмними або технічними засобами (ст. 361¹ КК) та незаконні збут або розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361² КК), – відповідно на 3,9% та 3,5% проваджень за незаконні дії, передбачені цими статтями, припадає 12,9% та 12,5% засуджених.

Таблиця 1.

Розподіл облікованих проваджень та кількості засуджених осіб за статтями Розділу XVI КК. Період часу: 2013–2023 рік

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	8619 (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	22 643	583

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% випадків). Позбавлення волі призначалося кожному п'ятому засудженому (21% засуджених). Порівняння цих показників із практикою призначення покарань у означений період за всі кримінальні правопорушення також свідчить, що до «комп'ютерних» злочинців судді ставилися більш поблажливо. Так, за період 2013–2023 рр. серед засуджених за всі кримінальні правопорушення, передбачені розділом XVI Особливої частини КК, штраф було призначено 39%, а позбавлення волі – 36% від усіх засуджених. Тож до осіб, які вчинили «комп'ютерні» кримінальні правопорушення, судді застосовували в цілому менш суворі засоби кримінально-правового реагування.

Для подальшого аналізу судової практики нами було сформовано запит до Єдиного державного реєстру судових рішень за наступними

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. На підставі такого запиту було отримано добірку з 244 судових рішень.

Серед отриманих судових рішень достатньо значною є частина виправдувальних рішень (11, що становить 4,5% від їх загальної кількості). Відповідно до статистичної звітності Державної судової адміністрації середня частка виправданих серед осіб, вирок (постанови) щодо яких набрали чинності, складає 0,2%, тож значення цього показника у отриманій добірці судових рішень істотно відрізняється від загальних тенденцій. Дослідження змісту таких судових рішень дозволяє зробити висновок 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 недостатню якість формулювання обвинувачення: «...суд вважає формулювання вказаного обвинувачення неконкретним та таким, що позбавляє обвинуваченого можливості розуміти його суть і відповідно захищатися від нього»¹. Фіксували недостатню якість доказової бази: «отримання доказів на підставі інформації, отриманої з недопустимого доказу, тягне за собою їхню безумовну недопустимість»². Та, зрештою, як правило, доходили висновку про те, що «стороною обвинувачення не доведено належними та достатніми доказами вчинення обвинуваченим кримінального правопорушення»³.

¹ Вирок Кіровоградського районного суду м. Кіровограда від 20.07.2022. Справа № 404/2447/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/105322891> (дата звернення: 30.08.2024).

² Вирок Бучацького районного суду Тернопільської області від 28.06.2023. Справа № 595/671/21. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/111824835> (дата звернення: 30.08.2024).

³ Вирок Жовтневого районного суду м. Запоріжжя від 27.10.2023. Справа № 331/814/21. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/115096847> (дата звернення: 30.08.2024).

Нааявність такого незначного за кількістю, але важливого для аналізу сегмента судових рішень у досліджуваній добірці висвітлює кілька важливих моментів. З одного боку, ефективність кримінально-правової протидії «комп'ютерним» правопорушенням потребує не тільки якісного законодавства та кваліфікованих суб'єктів його застосування. А з іншого – 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, сьогодні це достатньо стала практика. Сьогодні ми досліджуємо нові можливості штучного інтелекту. Маємо впевненість, що за кілька років судова практика буде реагувати на випадки несанкціонованого втручання у роботу комп'ютерних мереж з використанням згенерованих системами штучного інтелекту шкідливих програмних засобів або давати оцінку використанню індивідуалізованих дипфейків для вчинення шахрайства, що охоплює десятки тисяч потерпілих. Назвемо цю особливість кримінально-правової протидії досліджуваним посяганням так: високий рівень залежності ефективності від актуалізації професійних компетенцій працівників правоохоронних та судових органів.

Водночас, переважну більшість отриманої добірки судових рішень складають обвинувальні вироки (232; 95,1%). Розподіл судових рішень, пов'язаних з визнанням особи винною у вчиненні «комп'ютерних» кримінальних правопорушень, за кримінально-правовою кваліфікацією вчиненого є наступним (Табл. 2). Найчастіше зустрічається несанкціоноване втручання... (ст. 361 КК) (100 засуджених осіб; 43,1%). Несанкціоновані дії з комп'ютерною інформацією, вчинені особами, які мають право доступу до неї (ст. 362 КК), є другим за поширенням серед досліджуваних кримінальних правопорушень (67 засуджених осіб; 28,9%). Майже кожне п'яте засудження за кримінальні правопорушення в сфері використання

інформаційних технологій пов'язане із незаконним збутом або розповсюдженням комп'ютерної інформації з обмеженим доступом (ст. 361² КК) (45 осіб; 19,4%). 8,2% засуджених (19 осіб) вчинили незаконні дії з шкідливим програмним або технічним забезпеченням (ст. 361¹ КК). Кримінальні правопорушення, передбачені ст.ст. 363 та 363¹ КК, майже не представлені у судовій практиці.

Таблиця 2.
Розподіл досліджених судових рішень
за статтями Розділу XVI КК

Стаття КК	Загальна кількість осіб, щодо яких прийнято судові рішення	Засуджено осіб. Кількість та частка серед засуджених відповідно до всіх досліджених судових рішень	Виправдано осіб. Кількість та частка серед всіх осіб, щодо яких прийнято рішення за певною статтею Розділу XVI
361	104	100 (43,1%)	3 (2,9%)
361 ¹	21	19 (8,2%)	2 (9,5%)
361 ²	46	45 (19,4%)	1 (2,2%)
362	72	67 (28,9%)	5 (6,9%)
363	0	0	0
363 ¹	1	1 (0,4%)	0
Разом	244	232 (95,1%)	11 (4,5%)

Тут варто зазначити, що отримана нами добірка характеризується таким розподілом за кримінально-правовою кваліфікацією, який є достатньо близьким до аналогічного розподілу генеральної добірки, тобто розподілу серед всіх судових рішень, пов'язаних із засудженням осіб за вчинення кримінальних правопорушень, передбачених Розділом XVI КК (див. Рис. 2, Табл. 4).

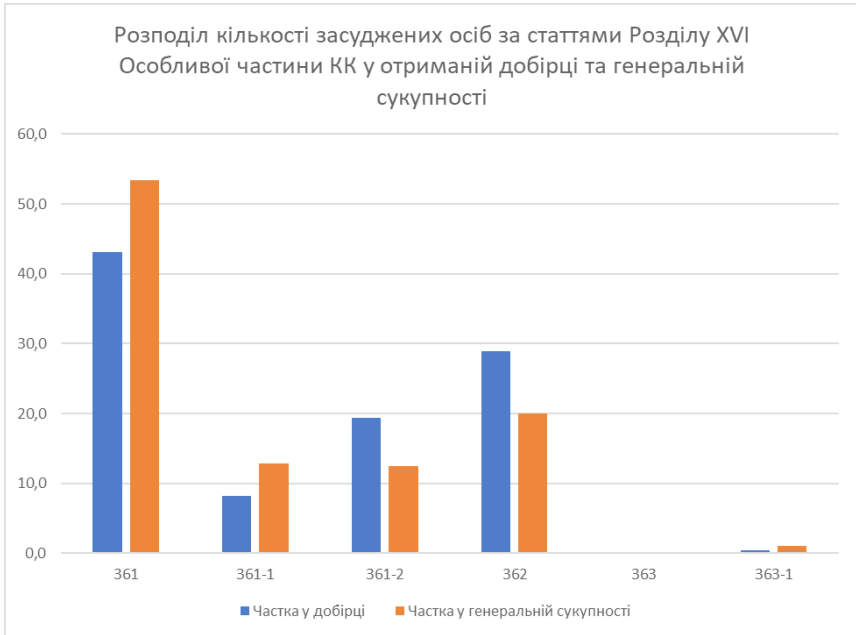


Рис. 2. Графічне представлення репрезентативності добірки судових рішень

Таблиця 4.
Розподіл кількості засуджених за статтями КК у досліджуваній добірці судових рішень та генеральній сукупності

Стаття КК	Засуджено осіб відповідно до рішень, включених у добірку		Засуджено осіб відповідно до даних ДСА	
	Кількість	Частка	Кількість	Частка
361	100	43,1	311	53,3
361 ¹	19	8,2	75	12,9
361 ²	45	19,4	73	12,5

Стаття КК	Засуджено осіб відповідно до рішень, включених у добірку		Засуджено осіб відповідно до даних ДСА	
	Кількість	Частка	Кількість	Частка
362	67	28,9	117	20,1
363	0	0,0	1	0,2
363 ¹	1	0,4	6	1,0
Разом	232	100,0	583	100,0

Отже, нами було отримано репрезентативну добірку судових рішень. Її дослідження дозволить охарактеризувати тенденції правозастосовного рівня кримінально-правового регулювання в сфері використання інформаційних технологій.

Найбільшу кількість осіб (100; 43,1%) засуджено за вчинення несанкціонованого втручання (ст. 361 КК). Дослідження змісту судових рішень дозволяє виділити в цій групі 5 категорій залежно від специфіки вчинюваних дій (Табл. 5).

Таблиця 5.

Розподіл засуджених за несанкціоноване втручання (ст. 361 КК) за особливостями протиправної поведінки

Категорія кримінального правопорушення	Засуджено осіб
Транзакція	50 (50%)
Отримання авторизаційних даних та (або) їх використання	20 (20%)
Внесення даних до реєстрів	11 (11%)
Отримання послуг без оплати або з порушенням порядку	10 (10%)
Інше	9 (9%)

Половина випадків засудження за статтею 361 КК (50%) пов'язана із учиненням несанкціонованих транзакцій з використанням

автоматизованих систем банківського обслуговування. Власне транзакція отримувала кримінально-правову оцінку, як крадіжка або шахрайство¹. Як несанкціоноване втручання розглядалося отримання доступу до автоматизованої системи банку від чужого імені та спотворення інформації про рух безготівкових коштів² або отримання несанкціонованого доступу та виток інформації про поточний стан банківського рахунку потерпілої особи³ тощо.

Дії кожної п'ятої особи (20% від усіх засуджених за несанкціоноване втручання) полягали у отриманні авторизаційних даних або їх використанні. Авторизаційні (автентифікаційні, облікові) дані, як правило, представляють собою набір інформації, що використовується для встановлення особи та надання доступу до певних ресурсів або систем. До таких даних належать логіни, паролі, PIN-коди, сертифікати, токени та інші засоби аутентифікації. Наприклад, вироком Заводського районного суду м. Дніпродзержинська по справі № 208/544/22⁴ було засуджено особу, яка вчинила несанкціоноване втручання в роботу комп'ютерної мережі, з метою отримання та збору інформації про облікові записи користувачів ТОВ «Меґого» для їх подальшого продажу. За допомогою шкідливого програмного засобу винна особа здійснила несанкціоноване втручання в роботу Інтернет-платформи «MEGOGO», внаслідок чого отримала персональні дані облікових записів користувачів загальною кількістю

¹ Цю проблему ми раніше досліджували. Див.: Карчевський М. В., Дудоров О. О. Проблеми кримінально-правової кваліфікації злочинів проти власності, вчинюваних із використанням платіжних карток або їх реквізитів. *Кримінальне судочинство. Судова практика у кримінальних справах*. 2014. № 1. С. 97-123.

² Вирок Ужгородського міськрайонного суду Закарпатської області від 12.01.2022. Справа № 308/13958/21. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/102793110> (дата звернення: 30.08.2024).

³ Вирок Хмельницького міськрайонного суду Хмельницької області від 03.02.2022. Справа № 686/29494/21. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/103041659> (дата звернення: 30.08.2024).

⁴ Вирок Заводського районного суду м. Дніпродзержинська від 08.02.2022. Справа № 208/544/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/103569489> (дата звернення: 30.08.2024).

22120 записів (адреси електронних скриньок, номера мобільних телефонів, паролі, які застосовуються при користуванні веб-сайтом «MEGOGO» та необхідні для авторизації користувачьких облікових записів). Мали місце випадки засудження за отримання авторизаційних даних для доступу до соціальних мереж¹, отримання доступу до корпоративних баз даних з використанням чужих авторизаційних даних², отримання доступу до акаунту у банківській установі³ тощо.

До категорії «внесення даних до реєстрів» (11%) ми віднесли випадки засудження осіб, які отримували несанкціонований доступ до певних державних реєстрів та вносили до них неправдиву інформацію. Як правило, це дії медичних працівників, які використовували облікові дані їхніх колег (відповідальних за ведення реєстру) для внесення неправдивих даних щодо проведення щеплень від коронавірусної інфекції⁴. Судова практика зустрічалася з подібними діями й відносно Єдиного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань⁵.

До категорії «отримання послуг без оплати або з порушенням порядку» (10%) ми віднесли випадки отримання шляхом несанкціонованого втручання безкоштовного доступу до програм телевізійного мовлення⁶, порушення порядку надання послуг міжнародного

¹ Вирок Франківського районного суду м. Львова від 07.10.2022. Справа № 465/7/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/106651859> (дата звернення: 30.08.2024).

² Вирок Мукачівського міськрайонного суду Закарпатської області від 24.10.2022. Справа № 303/5070/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/106895634> (дата звернення: 30.08.2024).

³ Вирок Жовтневого районного суду м. Дніпропетровська від 30.01.2023. Справа № 201/525/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/108944441> (дата звернення: 30.08.2024).

⁴ Вирок Амур-Нижньодніпровського районного суду м. Дніпропетровська від 04.07.2022. Справа № 199/3089/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/105054174> (дата звернення: 30.08.2024).

⁵ Вирок Дарницького районного суду м. Києва від 30.08.2023. Справа № 753/13244/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/113148566> (дата звернення: 30.08.2024).

⁶ Вирок Конотопського міськрайонного суду Сумської області від 14.11.2023. Справа № 577/5902/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/114884775> (дата звернення: 30.08.2024).

телефонного зв'язку¹, зміни показань електронних лічильників для ухилення від сплати за спожиту електроенергію².

Досліджувана добірка містить 19 судових рішень (8,2%), пов'язаних із засудженням за незаконні дії з шкідливими програмними або технічними засобами. Розподіл за формами об'єктивної сторони представлено у Табл. 6.

Таблиця 6.

Розподіл засуджених за незаконні дії з шкідливими програмними або технічними засобами (ст. 361¹ КК) за особливостями протиправної поведінки

Категорія кримінального правопорушення	Кількість засуджених
Розповсюдження	7 (36,84%)
Збут	5 (26,32%)
Створення	7 (36,84%)

Як правило, розповсюдженням суди визнають випадки надання доступу до шкідливого програмного забезпечення необмеженому колу осіб через певні сайти³ або соціальні медіа⁴. Збутом подібних засобів визнається їх передача певним особам⁵ або встановлення на

¹ Вирок Дніпровського районного суду м. Києва від 22.07.2022. Справа № 755/19568/21. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/105379051> (дата звернення: 30.08.2024).

² У цьому випадку обвинувачених було визнано невинуватими і виправдано за відсутністю в їх діях складу кримінального правопорушення. Водночас, подібні дії є достатньо поширеними тому наводимо посилання на це судове рішення. Вирок Першотравневого районного суду м. Чернівців від 26.03.2024. Справа № 725/964/17. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/117900544> (дата звернення: 30.08.2024).

³ Вирок Подільського районного суду м. Києва від 30.01.2023. Справа № 758/6085/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/108659542> (дата звернення: 30.08.2024).

⁴ Вирок Шевченківського районного суду м. Києва від 06.02.2023. Справа № 761/14407/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/108812895> (дата звернення: 30.08.2024).

⁵ Вирок Уманського міськрайонного суду Черкаської області від 14.01.2022. Справа № 705/4795/20. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/102617850> (дата звернення: 30.08.2024).

комп'ютерну техніку¹. До створення шкідливих засобів відносять як випадки розробки нових програм так і модифікацію існуючих².

45 вироків (19,4%) у досліджуваній добірці судових рішень пов'язано із незаконним збутом або розповсюдженням комп'ютерної інформації з обмеженим доступом (ст. 361² КК). Предметом таких посягань ставали персональні дані³, відомості відомчих АС⁴, авторизаційні дані⁵ тощо. Слід зазначити і те, що чіткого відмежування понять «розповсюдження» та «збут» у даній групі судових рішень не спостерігається.

Частка судових рішень, пов'язаних з кримінально-правовою кваліфікацією дій осіб, які мають доступ до інформації, складає 28,9%. Розподіл за формами об'єктивної сторони представлено у Табл. 7.

Таблиця 7.

**Розподіл засуджених за незаконні дії осіб,
які мають право доступу до комп'ютерної інформації (ст. 362 КК)
за особливостями протиправної поведінки**

Категорія кримінального правопорушення	Кількість засуджених
Копіювання, яке призвело до витоку	14 (20,9%)
Зміна	53 (79,1%)

Переважна частина судових рішень даної категорії (79,1%) стосується випадків незаконної зміни комп'ютерної інформації особами,

¹ Вирок Подільського районного суду м. Києва від 16.02.2024. Справа № 758/707/24. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/117032221> (дата звернення: 30.08.2024).

² Вирок Коломийського міськрайонного суду Івано-Франківської області від 26.05.2022. Справа № 346/391/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/104474011> (дата звернення: 30.08.2024).

³ Вирок Соснівського районного суду м. Черкаси від 31.05.2023. Справа № 712/3621/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/111223492> (дата звернення: 30.08.2024).

⁴ Вирок Десянянського районного суду м. Києва від 15.06.2023. Справа № 754/7392/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/111560514> (дата звернення: 30.08.2024).

⁵ Вирок Ленінського районного суду м. Запоріжжя від 25.10.2023. Справа № 334/8910/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/114468126> (дата звернення: 30.08.2024).

які мають правомірний доступ до неї. Це такі випадки, як внесення до відомчих АС відповідальними особами неправдивих даних щодо щеплення від коронавірусної інфекції¹, внесення до АС банківських установ неправдивих відомостей щодо ідентифікації осіб², внесення неправдивих даних до державних реєстрів³ або АС правоохоронних органів⁴ тощо. Як копіювання, що призвело до витоку (20,1%), переважно кваліфікувалися випадки пошуку за відомчими АС певних даних з подальшим повідомленням результатів⁵.

Нарешті, досліджувана добірка має лише одне судове рішення, пов'язане з кримінально-правовою оцінкою дій винної особи за ст. 363¹ КК, як масового розповсюдження повідомлень електрозв'язку, здійсненого без попередньої згоди адресатів, що призвело до припинення роботи автоматизованих систем⁶. Аналізу цього рішення приділимо увагу в подальшому.

Таким чином, представлені у судовій практиці «комп'ютерні» кримінальні правопорушення можна поділити на три групи: високої поширеності (64%), середньої поширеності (25%) та низької поширеності (11%). До кримінальних правопорушень високої поширеності відносяться: зміна даних, здійснена особами, які мають право доступу до комп'ютерної інформації (23%); несанкціоновані

¹ Вирок Рожнятівського районного суду Івано-Франківської області від 25.03.2022. Справа № 350/286/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/103755525> (дата звернення: 30.08.2024).

² Вирок Петропавлівського районного суду Дніпропетровської області від 03.05.2022. Справа № 188/857/21. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/104161922> (дата звернення: 30.08.2024).

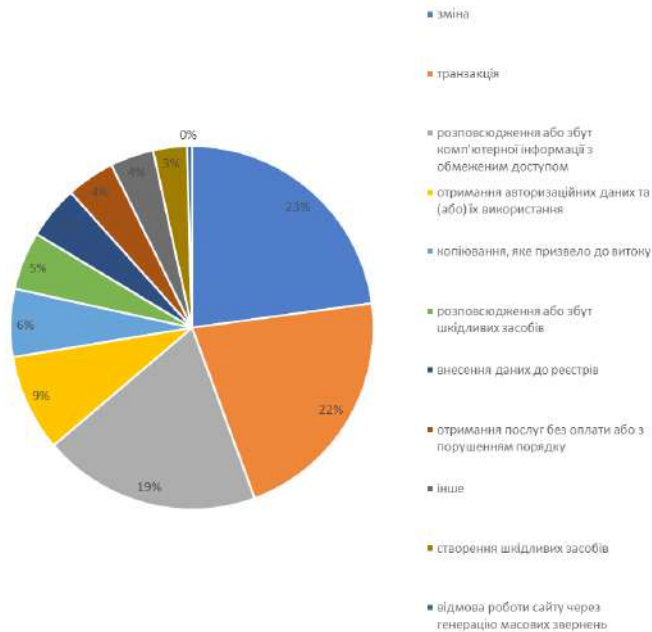
³ Вирок Печерського районного суду м. Києва від 16.11.2022. Справа № 367/1769/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/107561352> (дата звернення: 30.08.2024).

⁴ Вирок Білгород-Дністровського міськрайонного суду Одеської області від 07.10.2022. Справа № 495/7521/22. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/107157492> (дата звернення: 30.08.2024).

⁵ Вирок Автозаводського районного суду м. Кременчука від 11.05.2023. Справа № 524/179/21. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/110852146> (дата звернення: 30.08.2024).

⁶ Вирок Малиновського районного суду м. Одеси від 27.10.2023. Справа № 521/21945/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/114483840> (дата звернення: 30.08.2024).

транза
кримі
ня абс
«Комп
ширен
даних
доступ
реєстр
ливих
корист
ляє від



ня ін-
ржен-
(19%).
ої по-
ційних
право
них до
шкід-
рі ви-
дозво-
ністю.

Рис. 3. Види «комп'ютерних» кримінальних правопорушень, представлених у судовій практиці

На окрему увагу заслуговує розподіл форм реалізації кримінальної відповідальності у отриманій добірці судових рішень (Табл. 8). Призначено реальні покарання у 43,5% випадків, звільнено від покарання – у 56,5% випадків.

Більшість осіб, визнаних винними у вчиненні несанкціонованого втручання (ст. 361 КК) (68%), та незаконних дій особи, яка має право доступу до інформації (ст. 362 КК) (62,7%), звільнено від покарання. Реальне покарання призначене більшості осіб, які вчинили незаконні дії з шкідливими засобами (ст. 361¹ КК) (68,4%), та розповсюдження комп'ютерної інформації з обмеженим доступом (ст. 361² КК) (66,7%).

Таблиця 8.

**Співвідношення випадків призначення реального покарання
та звільнення від покарання**

Стаття КК	Призначено реальне покарання. Кількість та частка серед осіб, засуджених за певною статтею КК	Звільнено від покарання. Кількість та частка серед осіб, засуджених за певною статтею КК
361	32 (32%)	68 (68%)
361 ¹	13 (68,4%)	6 (31,6%)
361 ²	30 (66,7%)	15 (33,3%)
362	25 (37,3%)	44 (62,7%)
363	0	0
363 ¹	1 (100%)	0 (0%)
Разом	101 (43,5%)	131 (56,5)

У разі призначення реального покарання, судді, як правило, застосовують штраф (Табл. 9). У таких випадках практично завжди штраф застосовується до осіб, які вчинили кримінальні правопорушення, передбачені статтями 361¹ та 361² КК.

Таблиця 9.

Види застосованих покарань

Стаття КК	Виправні роботи	Громадські роботи	Обмеження волі	Позбавлення волі	Службові обмеження для військово-службовців	Штраф	Частка покарань у вигляді штрафу	Разом
361	-	-	2	5	-	25	78,1%	32

361 ¹	-	-	-	-	-	13	100,0%	13
361 ²	-	1	-	-	-	29	96,7%	30
362	3	-	1	2	1	18	72,0%	25
363 ¹	-	-	-	-	-	1	100,0%	1
Разом	3	1	3	7	1	86	85,1%	101

51,9% досліджених судових рішень містять відомості про укладення та затвердження угоди про визнання винуватості. У переважній більшості такі угоди укладаються особами, які вчинили кримінальні правопорушення, передбачені ст.ст. 361¹ КК (78,9%) та 361² КК (68,9%).

Таблиця 10.
Укладання угод про визнання винуватості

Стаття КК	Укладено угоду про визнання винуватості	
	Ні	Так
361	63 (63%)	37 (37%)
361 ¹	4 (21,1%)	15 (78,9%)
361 ²	14 (31,1%)	31 (68,9%)
362	31 (45,6%)	37 (54,4%)
363 ¹	(0%)	1 (100%)
Разом	112 (48,1%)	121 (51,9%)

Таким чином, за особливостями використання засобів кримінально-правового реагування випадки засудження за кримінальні правопорушення, передбачені Розділом XVI Особливої частини КК, можуть бути поділені на дві групи: перша характеризується переважним використанням реальних покарань (67–69%) у вигляді штрафів та укладанням угод (69–79%) про визнання винуватості (ст.ст. 361¹, 361² КК – 64 випадки, що становить 27,6% від обвинувальних вироків); другій властиве більш широке використання звільнення від покарання (63–68%) та менше використання угод

(37–54%) про визнання винуватості (ст.ст. 361, 362 КК – 167 випадків, що становить 72% від обвинувальних вироків).

Дослідження статистичних даних з необхідністю потребує важливого уточнення. Не можна не відзначити, що предметом такого аналізу стали тільки зареєстровані «комп'ютерні» кримінальні правопорушення. Проблема латентності «комп'ютерних» кримінальних правопорушень, реального масштабу та фактичної поширеності посягань на кібербезпеку в Україні потребує самостійного аналізу. Враховуючи зазначене уточнюємо, що проведений нами аналіз даних офіційної статистики та змісту судових рішень дає достатньо повне уявлення про діяльність правоохоронних та судових органів щодо протидії злочинності в сфері використання інформаційних технологій. Саме в межах цієї діяльності відбувається застосування досліджуваних нами норм законодавства про кримінальну відповідальність. Тож переходимо до аналізу змісту ознак складів кримінальних правопорушень, передбачених статтями Розділу XVI Особливої частини КК.

3.1.2. Родовий об'єкт кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Назва Розділу XVI Особливої частини КК дозволяє зазначити, що родовим об'єктом передбачених ним кримінальних правопорушень є частина інформаційних відносин, які можна визначити як *інформаційні відносини, засобом забезпечення яких є ЕОМ, системи, комп'ютерні мережі та мережі електрозв'язку*. Інакше кажучи, кримінальні правопорушення, що передбачені цим розділом, посягають на певну частину інформаційних відносин – інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів. У кримінальному законі наведено чотири види таких засобів: електронно-обчислювальна машина (комп'ютер), автоматизована система, комп'ютерна мережа та мережа електрозв'язку.

Відповідно визначення міжнародної організації стандартизації, імплементація якого здійснена у ДСТУ ISO/IEC 2382:2017, ЕОМ (комп'ютер) являє собою функціональний блок, який може виконувати значні обчислення, включаючи численні арифметичні та логічні операції, без втручання людини¹.

Поняття «автоматизована система» система визначалося у ранніх редакціях Закону України «Про захист інформації в інформаційно-комунікаційних системах». У першій редакції цей Закон (від 5 липня 1994 р.) мав назву «Про захист інформації в автоматизованих системах» та містив таке визначення: «автоматизована система – система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення». 1 січня 2006 року набрала чинності нова редакція цього Закону. Було змінено назву даного нормативного документу, замість поняття «автоматизована система» було використано поняття «інформаційна (автоматизована) система». Відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах» інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів².

Водночас, дотепер є чинним стандарт ДСТУ 2226-93. «Автоматизовані системи. Терміни та визначення» від 01 липня 1994 р., який містить визначення поняття «автоматизована система». Нею визнається організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність. Такі системи відрізняються від електронно-обчислювальних машин (комп'ютерів) наявністю периферійних пристроїв, які забезпечують автомати-

¹ ДСТУ ISO/IEC 2382:2017. Інформаційні технології. Словник термінів (ISO/IEC 2382:2015, IDT). [Чинний від 2019-01-01]. Вид. офіц. Технічний комітет стандартизації «Інформаційні технології», 2017. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=75076 (дата звернення: 30.10.2024).

² Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

зацію певного виду діяльності людини¹. Наприклад, банківський автомат представляє собою конструкцію з електронно-обчислювальної машини, засобу ідентифікації користувача, сховища для банкнот та механізму їх видачі. Такий пристрій є автоматизованою системою.

Комп'ютерна мережа – мережа вузлів обробки даних, які з'єднані між собою з метою передачі даних. Дане визначення також міститься у словникові ISO SO/IEC 2382:2015 Information technology – Vocabulary, на основі якого розроблено ДСТУ ISO/IEC 2382:2017².

Поняття «мережа електрозв'язку» визначається на основі змісту Закону України «Про електронні комунікації». Цим нормативним документом «електронна комунікаційна мережа» визначається як «комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг». У свою чергу, «електронна комунікаційна послуга» полягає в «прийманні та/або передачі інформації через електронні комунікаційні мережі, крім послуг з редакційним контролем, змісту інформації, що передається за допомогою електронних комунікаційних мереж і послуг». Нарешті «електронна комунікація» та тотожні відповідно до згаданого Закону поняття «телекомунікація» й «електрозв'язок» представляють собою «передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій».

Залежно від цих засобів інформаційні відносини, які є родовим об'єктом досліджуваних кримінальних правопорушень, може бути поділено на чотири види:

- інформаційні відносини, засобом забезпечення яких є комп'ютери;

¹ ДСТУ 2226:1993. Автоматизовані системи. Терміни та визначення [Чинний від 1994-07-01]. Вид. офіц. Київ, 1994. С. 2.

² ДСТУ ISO/IEC 2382:2017. Інформаційні технології. Словник термінів (ISO/IEC 2382:2015, IDT). [Чинний від 2019-01-01]. Вид. офіц. Технічний комітет стандартизації «Інформаційні технології», 2017. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=75076 (дата звернення: 30.10.2024).

- інформаційні відносини, засобом забезпечення яких є комп'ютерні системи;
- інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі;
- інформаційні відносини, засобом забезпечення яких є мережі електров'язку.

Перший вид цих інформаційних відносин – це найпростіша форма застосування комп'ютерної техніки для роботи з інформацією. Суб'єкти таких відносин використовують комп'ютерну техніку для виконання здебільшого нескладних операцій: підготування документів, проведення інженерних розрахунків, організація та робота з базами даних. Зазначимо, що під ЕОМ розуміють не тільки комп'ютери в їх «класичному», можна сказати, звичному вигляді, тобто «системний блок – монітор – клавіатура – принтер», але й інше устаткування, яке містить процесор і може виконувати розрахунки без участі людини. Йдеться про бортові комп'ютери транспортних засобів¹, електронні лічильники електроенергії, інші технології, які зараз прийнято об'єднувати поняттям «інтернет речей».

Використання комп'ютерних систем належить до більш складних інформаційних відносин й становить другий вид останніх. Автоматизовані системи використовують для виконання широкого кола завдань: управління підприємством, технологічного підготування виробництва, контролю й випробування промислової продукції, управління службами життєзабезпечення підприємства тощо.

Третій вид інформаційних відносин, які утворюють досліджуваний родовий об'єкт, пов'язаний з використанням комп'ютерних мереж, що бувають двох видів: локальні, які об'єднують комп'ютери в межах однієї організації, і глобальні, що забезпечують зв'язок між різними організаціями, юридичними та фізичними особами. Найвідомішою й найпоширенішою глобальною комп'ютерною мережею є Інтернет, що застосовують в основному для таких видів роботи з ін-

¹ Карчевський М. В., Савченко А. В. Особливості кримінально-правової кваліфікації несанкціонованого втручання в роботу вбудованих комп'ютерних систем. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 30. С. 256.

формацією: електронна пошта; передавання файлів; віддалений доступ – можливість підключатися до віддаленого комп'ютера й працювати з ним в інтерактивному режимі.

Інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку (четвертий вид), полягають у наданні й отриманні послуг електричного зв'язку, тобто у використанні мереж електрозв'язку для передачі або приймання інформації. Що ж до визначення змісту цих суспільних відносин, то певний інтерес становить питання їх відмежування від інформаційних відносин, засобом забезпечення яких є комп'ютерні мережі. Аналіз чинного законодавства у сфері телекомунікації дає змогу стверджувати, що наявність у законі про кримінальну відповідальність одночасно з терміном «мережа електрозв'язку» іншого – «комп'ютерна мережа» – фактично означає, що під мережею електрозв'язку маються на увазі всі телекомунікаційні мережі, крім комп'ютерних (мережі міського, міжміського та міжнародного телефонного зв'язку, рухомого (мобільного) зв'язку, проводового радіомовлення, ефірного телерадіомовлення тощо). Отже, під інформаційними відносинами, засобом забезпечення яких виступають мережі електрозв'язку, треба розуміти суспільні відносини у сфері використання телекомунікаційних мереж, за винятком комп'ютерних мереж.

Із визначенням родового об'єкта кримінальних правопорушень у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку пов'язана ще одна проблема – проблема найменування кримінальних правопорушень, які посягають на цей об'єкт.

Слід зазначити, що оскільки КК не оперує, для прикладу, такими поняттями як «комп'ютерне кримінальне правопорушення» або «кібернетичне кримінальне правопорушення» (кіберзлочин), то невирішеним залишається питання віднесення в межах цього нормативно-правового акту тих чи інших суспільно небезпечних діянь саме до таких, що відповідають виключно ознакам «комп'ютерних» кримінальних правопорушень (у розумінні їх родового об'єкта, передбаченого розділом XVI Особливої частини КК) або ознакам кіберзлочинів у широкому розумінні.

Помітно, що в літературі дедалі частіше розглядувані кримінальні правопорушення йменуються «комп'ютерними» кримінальними правопорушеннями. При цьому дослідниками по-різному визначається обсяг цього поняття. Досить поширеним є віднесення до комп'ютерних всіх суспільно небезпечних посягань, за яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом¹ або кримінальні правопорушення, пов'язані з втручанням у роботу комп'ютерів або використовують комп'ютери як необхідні технічні засоби² Згідно з таким розумінням «комп'ютерним» кримінальним правопорушенням може визнаватися будь-яке – розкрадання, шпигунство, незаконне збирання відомостей, які становлять комерційну таємницю, і т. ін., якщо воно вчиняється з використанням комп'ютера. Так, наприклад, постійно зростає потужність та кількість дистанційних кібервтручань, багато з яких мають явно шпигунське спрямування, в тому числі й щодо інформації, яка становить державну таємницю (ст. 114 КК). Зокрема, зафіксовано випадки використання державою-агресором шкідливого програмного забезпечення, яке здатне робити скріншоти, викрадати файли, записувати звук з мікрофону тощо³. Слід зазначити, що кібершпигунство може здійснюватись як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютерні мережі⁴. З наведеного обґрунтованим видається припущення, що описані різновиди вчинення кібершпигунства доречно називати кібернетичними (інформаційно-комунікаційними, передусім) технологіями. Останні у поєднанні з фактичним способом дії особи

¹ Див.: Азаров Д. С. Порухення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації. *Право України*. 2000. № 12. С. 72; Біленчук П. Д., Бут В. В., Гавловський В. Д. та ін. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. С. 65.

² Голубев В. О. Правові проблеми захисту інформаційних технологій. *Вісн. Запоріж. юрид. ін-ту*. 1997. № 2. С. 39, 40; Лісовий В. «Комп'ютерні» злочини: питання кваліфікації. *Право України*. 2002. № 2. С. 87.

³ Білан І. А. Особливості застосування шкідливого програмного забезпечення спецслужбами країни-агресора. *Інформація і право*. 2023. № 2. С. 145.

⁴ Діордіца І. В. Поняття та зміст кібершпигунства. *Наук. пр. Нац. ун-ту «Одес. юрид. акад.»*. Одеса: Гельветика, 2020. Т. 26. С. 51.

мають бути покладені в основу досягнення кінцевої кримінально протиправної мети, тобто надання, у випадку шпигунства, відповідних відомостей іноземній державі іноземній організації або їх представникам. Для прикладу, ч. 3 ст. 130 Кримінального кодексу Республіки Польща встановлює кримінальну відповідальність для особи, яка для того, щоб надати іноземному розвіднику відомості, що можуть нанести шкоду Польській Республіці, збираючи, зберігає їх, входить в інформаційну систему з метою їх отримання або повідомляє про готовність діяти на користь іноземної розвідки проти Польської Республіки. Тобто, по суті, у Польщі криміналізоване кібершпигунство у розділі, який має назву «Злочини проти Польської Республіки»¹. Тож, видається, що крізь призму наведеного прикладу, розуміння «комп'ютерних» кримінальних правопорушень, як виключно таких, що технологічно вчиняються із використанням комп'ютерів, є неправильним, бо не дозволяє відбити їх сутність, специфіку та відрізнити від інших, у яких комп'ютер є лише знаряддям, засобом або предметом. Крім того, його використання в науковому контексті може призвести лише до плутанини через відсутність чітких меж дослідження.

Водночас саме таке розуміння поняття «*cybercrime*» можна достатньо часто зустріти в американській науковій літературі. Сюзан Бреннер² вважає, що існує три категорії «кіберзлочинів»: 1) посягання, у яких комп'ютер є метою злочину; 2) посягання, у яких комп'ютер використовується як засіб вчинення злочину; 3) посягання, у яких комп'ютер відіграє незначну роль у вчиненні злочину.

В якості прикладу «кіберзлочинів»(!) третього виду дослідниця наводить такий випадок. *Melanie McGuire* була засуджена за вбивство чоловіка. Вона використала снадійне, здійснила кілька пострілів у потерпілого, труп розчленувала та приховала у водоймищі.

¹ Kodeks karny : Ustawa of 06.06.1997 Nr 88 poz. 553 : od 1 lipca 2024 r. *Kancelaria Sejmu*: strona internetowa. URL: <http://surl.li/ucuvna> (data dostępu: 30.10.2024).

² Brenner S. W. *Cybercrime: Criminal Threats from Cyberspace* / ed. by F. Y. Bailey, S. Chermak. Santa Barbara: Praeger, 2010. P. 39–48. URL: <https://doi.org/10.5040/9798400636554> (дата звернення: 30.08.2024).

У комп'ютері засудженої були знайдені сліди пошуку за темами «снодійне», «отрута», «незаконне придбання зброї», а також листування засудженої та її керівника («romantic emails»).

Поняття кіберзлочину ставало предметом наукових розвідок багатьох сучасних українських дослідників кримінального права. Слід відмітити напрацювання О. І. Денькович, яка узагальнила висловлені позиції інших вітчизняних науковців стосовно критеріїв віднесення кримінального правопорушення до кіберзлочину. Відповідно до такого узагальнення кіберзлочинами визнаються: 1) кримінальні правопорушення (дотримуючись чинної термінології КК), передбачені розділом XVI Особливої частини КК; 2) кримінальні правопорушення, предметом яких є комп'ютерна інформація; 3) кримінальні правопорушення, в яких комп'ютер є або предметом кримінального правопорушення, або знаряддям, або способом його вчинення; 4) кримінальне правопорушення, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення¹. Деякі із зазначених визначень кіберзлочинів, як помітно, є подібними до тих, що надані американськими дослідниками.

Не можна залишити поза увагою і законодавче визначення кіберзлочину, що надано поза КК. Відповідно до п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. кіберзлочином (комп'ютерним злочином) є «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України»². Варто констатувати, що наразі таке визначення не враховує положення чинного КК в аспекті поділу кримінальних правопорушень на кримінальні проступки та злочини, проте, як видається, воно відображає осно-

¹ Кіберзлочинність та електронні докази = cyber crime and digital evidence: навч. посіб. / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан ; за ред. О. Д. Денькович, Габріеле Шмельцер. Львів: Львів. нац. ун-т ім. Івана Франка, 2022. С. 19, 20.

² Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

вні характеристики розглядуваного поняття. Йдеться про те, що, *по-перше*, було здійснено ототожнення кіберзлочину та комп'ютерного злочину, а, *по-друге*, визначено його специфіку (вчинення діяння у кіберпросторі та/або з його використанням). А тому основним завданням вбачається, враховуючи розмаїтість процесів у кіберпросторі та особливостей їх протікання, виокремлення безпосередньо кіберзлочинів (у вузькому розумінні, як «комп'ютерних»), так і суспільно небезпечних винних діянь, які посягають на абсолютно різні об'єкти кримінально-правової охорони, але використовують кіберпростір, як предмет, знаряддя чи засіб їх вчинення (кіберзлочини у широкому розумінні)¹. Так, згідно з абз. 9 п. 3 Стратегії кібербезпеки України, затвердженої Указом Президента України № 447/2021 від 26.08.2021 р., набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо².

Тому з метою адекватного розуміння та застосування всього обсягу поняття «кіберзлочин» щодо тлумачення певних діянь, передбачених нормами Особливої частини КК, як кримінальних правопорушень безпосередньо у сфері «кібер» (т. зв. «комп'ютерних») та кіберзлочинів у широкому розумінні необхідно розмежувати ці поняття, які в Законі вживаються як синоніми. Так, зазначається, що комп'ютерним злочином є протиправне втручання в роботу кіберне-

¹ Федюк В. В. Поняття кіберзлочину та його застосування в нормах закону про кримінальну відповідальність. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання*: матеріали III Всеукр. наук.-практ. конф. (Київ, 23 листоп. 2023 р.) / упоряд.: М. В. Дубняк, С. О. Дорогих. Київ: ПП «Фенікс», 2023. С. 116.

² Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № 447/2021. *Офіс Президента України*: оф. вебсайт. URL: <https://www.president.gov.ua/documents/4472021-40013> (дата звернення: 30.08.2024).

тичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо). Натомість, кіберзлочином є злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин в кіберпросторі. Під кіберпростором слід розуміти штучне електронне середовище існування інформаційних об'єктів у цифровій формі або простір, представлений інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну та знищення) інформації, представленої у вигляді електронних комп'ютерних даних¹.

Особливістю кіберзлочину виступає те, що він пов'язаний із використанням саме кібернетичних технологій у межах як однієї комп'ютерної системи (чи мережі) або декількох таких систем (мереж), так і в межах інформаційної (автоматизованої), інформаційно-комунікаційної чи електронної комунікаційної систем. Формами кримінально-протиправного використання кібернетичних технологій у межах комп'ютерних систем (мереж) можуть бути, приміром, несанкціоноване отримання доступу до керування комп'ютерною мережею та її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві шляхом дезорганізації управлінської діяльності підприємства), а також створення та використання з кримінально-протиправною метою однієї комп'ютерної мережі (або поєднання декількох) проти інших таких мереж (наприклад, створення мережі заражених комп'ютерів для здійснення атак на веб-сайти тощо).

¹ Словник термінів з кібербезпеки / за заг. ред. О. В. Копана, Є. Д. Скулиша. Київ: АванпостПрим, 2012. С. 85, 86.

Тож, з точки зору національного кримінально-правового дискурсу міркування щодо ототожнення «комп'ютерних» кримінальних правопорушень та кіберзлочинів (у їх законодавчому розумінні), а також запропоновані американською кримінально-правовою доктриною (багато в чому підтриманою й українськими дослідниками) підходи до визначення перших виглядають дуже спірними. Певною мірою, це можна пояснити тим, що, як відомо, у 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 доречно в межах зарубіжної правової доктрини кримінального права визначення «комп'ютерних» кримінальних правопорушень має обмежене поле для використання на національному рівні. Таке визначення може бути використано в межах кримінологічних, криміналістичних або кримінально-процесуальних досліджень.

У національному кримінально-правовому дискурсі використання такого поняття слід обмежити аби уникати плутанини, або, як ми це робимо з початку цього Розділу, використовувати поняття «комп'ютерні» кримінальні правопорушення в лапках.

Більш доречним для позначення посягань, передбачених Розділом XVI Особливої частини КК, видається використання поняття «кримінальні правопорушення у сфері використання інформаційних технологій».

Послідовним, відповідним системі законодавства про кримінальну відповідальність буде визначення, яке ґрунтується на найважливішій ознаці кримінальних правопорушень – їх об'єкті. Класифікація за родовим об'єктом – це системоутворюючий чинник сукупності норм Особливої частини КК. Тому визначення запропонованого поняття має конструюватися на основі специфічних ознак родового об'єкта. Таким чином, у подальшому *під кримінальними правопорушеннями в сфері використання інформаційних технологій*

(«комп'ютерними» кримінальними правопорушеннями) ми будемо розуміти суспільно небезпечні, протиправні, кримінально карані, вчинені суб'єктом кримінального правопорушення винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку (ст.ст. 361–363¹ КК).

3.1.3. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно- комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України)

Безпосередній об'єкт кримінального правопорушення, передбаченого ст. 361 КК, складається з суспільних відносин власності на комп'ютерну інформацію та відносин надання й отримання послуг електрозв'язку.

Право власності на комп'ютерну інформацію являє собою сукупність права та можливості особи володіти інформацією, змінювати, використовувати її для задоволення своєї інформаційної потреби, давати можливість іншим особам використовувати інформацію. Механізм заподіяння шкоди суспільним відносинам власності на комп'ютерну інформацію полягає в створенні небезпеки, порушенні, позбавленні або обмеженні реалізації власником інформації повноважень володіння, розпоряджання, користування нею. Такі суспільні відносини регулюються складним комплексом правових норм. Загальні положення визначаються Законом України «Про інформацію» та, залежно від змісту інформації, конкретизуються у Цивільному кодексі, законах України «Про захист персональних даних», «Про цифровий контент та цифрові послуги», «Про медіа», «Про науково-технічну інформацію», «Про захист інформації в інформаційно-комунікаційних системах» тощо.

Зауважимо також, що редакція статті дає підстави стверджувати, що крім права власності на комп'ютерну інформацію, вона охороняє й суспільні відносини надання та отримання послуг електрозв'язку. До цих суспільних відносин можна вжити термін «альтернативний безпосередній об'єкт кримінального правопорушення». Специфіка чинної редакції ст. 361 КК полягає в тому, що вона забезпечує охорону від злочинних посягань двох різних видів суспільних відносин: власності на комп'ютерну інформацію та надання послуг електрозв'язку. Отже, ст. 361 *охороняє, крім відносин власності на комп'ютерну інформацію, суспільні відносини надання послуг електрозв'язку*. Зміст цих відносин полягає в тому, що оператори й провайдери телекомунікацій забезпечують їхнім споживачам можливість передавання та приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду за допомогою радіо, дротових, оптичних або інших електромагнітних систем¹.

У науці представлені й інші точки зору щодо об'єкта несанкціонованого втручання. Д. С. Азаров вважає, що «основним об'єктом цього злочину є суспільні відносини, пов'язані з інформаційною діяльністю щодо комп'ютерної інформації чи обміном інформацією в мережах електрозв'язку, яким було завдано або створено загрозу завдання шкоди. Він також зазначає, що додатковим об'єктом є суспільні відносини власності щодо інформації, оскільки інформація завжди перебуває у чийсь власності»². С. О. Орлов визначає об'єкт втручання, як суспільні відносини щодо обробки інформації в комп'ютерних системах та мережах, а також забезпечення їх нормальної роботи³. Подібні положення містяться й у дослідженні

¹ Докладніше див.: *Карчевський М. В.* Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 116.

² Азаров Д. С. Про розмежування злочинів, передбачених статтями 361 і 362 Кримінального кодексу України. *Кримінальне право України*. 2006. № 3. С. 34.; Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. С. 62.

³ Орлов С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах. : дис. ... канд. юрид. наук. Харків, 2004. С. 184.

М. В. Рудика¹. Хоча предметом названих досліджень були попередні редакції ст. 361 КК, висловлені пропозиції потребують аналізу.

Визначення об'єктом несанкціонованого втручання не відносин з приводу власності на інформацію, а відносин з приводу обробки інформації не враховує сутність досліджуваного посягання. Небезпечність втручання полягає не в порушенні обробки інформації чи роботи обладнання, а в цінності інформації, яка є предметом посягання. Наприклад, незаконне втручання з метою знищення цінної наукової інформації становить значно більшу суспільну небезпеку, ніж знищення незначної інформації, яка не впливає на діяльність власника. Визначення об'єкта як власності на інформацію дозволяє враховувати це, визначення об'єкта як відносин щодо обробки інформації – ні. Ситуація подібна до визнання основним об'єктом крадіжки з проникненням відносин недоторканості житла.

Предметом кримінального правопорушення, передбаченого ч.ч. 1, 2 та 4 ст. 361 КК є інформаційні (автоматизовані) системи, електронні комунікаційні системи, інформаційно-комунікаційні системи та електронні комунікаційні мережі. Предмет кримінального правопорушення, передбаченого ч. 3 ст. 361 КК, – інформація. Предметом правопорушення, передбаченого ч.5 ст. 361 КК, можуть бути як названі технічні засоби роботи з інформацією, так й інформація.

Технічні засоби обробки інформації як предмет несанкціонованого втручання. Законом України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-ІХ від 24.03.2022 р. істотно змінено ст. 361 КК. Криміналізовано несанкціоноване втручання без настання наслідків у вигляді втрати, витоку подробиці інформації тощо (ч. 1 ст. 361). Законодавче визначення несанкціонованого втручання (ст. 361 КК) та незаконних дій з шкідливими пристроями (ст. 361¹ КК) сформульоване з використанням іншого переліку технічних засобів опрацювання інформації ніж той,

¹ Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом: дис. ... канд. юрид. наук. Харків, 2007. С. 89.

що використовується у назві Розділу XVI, ст.ст. 361², 362, 363 та 363¹ КК (Табл. 11).

Таблиця 11.
Переліки технічних засобів обробки інформації,
що використовуються у Розділі XVI Особливої частини КК

Перелік технічних засобів обробки інформації, що використовується у назві Розділу XVI, ст.ст. 361 ² , 362, 363 та 363 ¹ КК	Перелік технічних засобів обробки інформації, що використовується у ст.ст. 361, 361 ¹ КК
<ul style="list-style-type: none"> • електронно-обчислювальна машина (комп'ютер) • автоматизована система • комп'ютерна мережа • мережа електрозв'язку 	<ul style="list-style-type: none"> • інформаційна (автоматизована) система • електронна комунікаційна система • інформаційно-комунікаційна система • електронна комунікаційна мережа

Поняття «електронна комунікаційна мережа» є тотожним до розглянутого раніше поняття «мережа електрозв'язку». Така електронна мережа є предметом несанкціонованого втручання у випадку незаконного підключення до мереж кабельного телебачення, створення перешкод під час користування мережами радіозв'язку, мобільного зв'язку тощо.

Решта видів технічних засобів, перелічених у диспозиції ст. 361 КК, визначаються Законом України «Про захист інформації в інформаційно-комунікаційних системах». Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб. Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Чинне законодавче рішення з необхідністю породжує питання співвідношення понять, що використовуються у назві Розділу XVI та ст.ст. 361, 361¹ КК. По-перше, співвідношення понять «електронно-обчислювальна машина» (ЕОМ), «автоматизована система» (АС) та «інформаційна (автоматизована) система». Раніше ми наводили визначення ЕОМ та АС, які містяться у державних стандартах. Відповідно до визначення, яке міститься у Законі «Про захист інформації в інформаційно-комунікаційних системах» поняття «інформаційна (автоматизована) система» охоплює як ЕОМ так і АС. Отже, відповідно до чинної редакції ст. 361 КК несанкціонованим втручанням в роботу інформаційної (автоматизованої) системи слід вважати як порушення роботи окремих комп'ютерів (ЕОМ), так і систем, призначених для автоматизації певних видів діяльності людини, наприклад, банкоматів (АС).

Наступне питання полягає у тому, як співвідносяться поняття «комп'ютерна мережа», що використовується у назві Розділу XVI, та поняття «електронна комунікаційна система» й «інформаційно-комунікаційна система», що використовуються у ст.ст. 361 та 361¹ КК.

Електронними комунікаційними системами є маршрутизатори, комутатори, антени, передавачі тощо. До прикладів інформаційно-комунікаційних систем можна віднести інтегровані системи управління підприємством, хмарні обчислювальні платформи або системи відеоконференцій. Перші та другі попри певні схожі риси виконують різні функції. Електронні комунікаційні системи забезпечують інфраструктуру для зв'язку між користувачами або пристроями. Можна сказати, що вони відповідають за фізичну передачу сигналів, таких як радіохвилі, оптичні сигнали в оптоволоконних кабелях тощо. Інформаційно-комунікаційні системи охоплюють ширший спектр функцій. Вони включають в себе не лише передачу інформації, але й її зберігання, обробку, управління та представлення користувачам.

Іншими словами, електронні комунікаційні системи забезпечують передачу інформації, можуть бути частиною більш складних систем, але самі по собі вони не обробляють і не аналізують дані. Натомість інформаційно-комунікаційні системи інтегрують як можливість передачі даних, так і їхньої обробки.

Таким чином, можна стверджувати, що поняття «комп'ютерна мережа», використане у назві Розділу XVI Особливої частини КК, охоплює поняття «електронна комунікаційна система» та «інформаційно-комунікаційна система».

Інформація як предмет несанкціонованого втручання. З огляду на диспозицію одним з видів предметів досліджуваного кримінального правопорушення є інформація, аналіз об'єкта та відповідних форм об'єктивної сторони (ч. 3 ст. 361 КК) дає підстави стверджувати, що до предметів належить *комп'ютерна інформація та інформація, що передається каналами електрозв'язку.*

Комп'ютерна інформація. Об'єкт і предмет будь-якого кримінального правопорушення є взаємозалежними, взаємозумовленими. Тому аналізуючи ознаки предмета несанкціонованого втручання, треба виходити з викладеної вище характеристики змісту безпосереднього об'єкта як відносин власності на інформацію. Загальновизнаним у кримінальному праві є погляд, що предмет кримінального правопорушення характеризується сукупністю трьох ознак: фізичної, економічної та юридичної. Визначаючи інформацію предметом, треба проаналізувати її ознаки.

Фізична ознака. Специфіка комп'ютерної інформації як предмета правопорушення полягає в неможливості її віднесення ні до матеріальних, ні до нематеріальних предметів. Інформація як нематеріальний предмет включається в систему суспільних відносин за допомогою матеріального носія. Інакше кажучи, фізична ознака комп'ютерної інформації як предмета правопорушення полягає в її носії, котрий зазвичай розуміється як предмет, річ, властивості якої використовують для передачі, зберігання та обробки інформації. Носіями комп'ютерної інформації є оптичні та жорсткі диски, flash-носії, SD-карти, сигнали в мережах передавання даних тощо.

Фізична ознака комп'ютерної інформації є предметом наукової дискусії. Так, С. В. Дрьомов вважає, що комп'ютерна інформація

є річчю нематеріального світу¹. О. Мазуренко та Н. Розенфельд пропонують вважати комп'ютерну інформацію не матеріальним, а віртуальним предметом, оскільки вона не має зовнішнього представлення, але може набувати його завдяки використанню спеціальних засобів, таких як комп'ютерні системи, які надають їй форму, придатну для сприйняття та обробки². Така позиція викликає певні зауваження.

По-перше, вона не узгоджується із загальноновизнаними визначеннями понять «ідеальне» та «матеріальне». «Ідеальне» позначає нематеріальну природу образів дійсності, які виникають у людській свідомості, тоді як «матеріальне» представляє об'єктивну дійсність, незалежну від волі та свідомості людей. Предмет посягань у сфері використання комп'ютерної техніки існує незалежно від свідомості винної особи, тобто є матеріальним. Знищення, перекручення або блокування комп'ютерної інформації відбувається в об'єктивній реальності, а не у свідомості правопорушника або потерпілої особи. По-друге, якщо комп'ютерна інформація була б нематеріальним або віртуальним предметом, то відповідні слідчі дії мали б також бути нематеріальними і відбуватися лише у свідомості, що очевидно позбавлено сенсу.

Інформація як предмет кримінального правопорушення має *економічну ознаку*, ціну, яка зрештою визначається її змістом і заінтересованістю споживача в її одержанні. Цінність інформації буває різною: інформація може бути цінною по суті, оскільки є результатом тривалої роботи значної кількості осіб, а може бути цінною за призначенням, адже її наявність є потрібною умовою для вирішення певного завдання.

Юридична ознака комп'ютерної інформації полягає в тому, що вона має бути чужою для винного й мати свого власника.

Отже, з огляду на викладене комп'ютерну інформацію як предмет кримінального правопорушення видається можливим визначити

¹ Дрьомов С. Комп'ютерна інформація як предмет злочину, передбаченого ст. 362 Кримінального кодексу України. *Підприємництво, господарство і право*. 2005. № 4. С. 132.

² Мазуренко О., Розенфельд Н. Комп'ютерна інформація, як предмет злочинів, передбачених Розділом XVI КК України. *Право України*. 2004. № 6. С. 82.

в такий спосіб: *відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника й ціну*¹.

Інформація, що передається каналами електрозв'язку. Співвідношення категорій «інформація, що передається мережами електрозв'язку» та «комп'ютерна інформація», яка теж належить до предметів незаконного втручання, можна визначити так: якщо комп'ютерна інформація – це відомості, подані у формі, яка дає змогу опрацювати їх за допомогою комп'ютерної техніки, то інформацією, що передається мережами електрозв'язку, є *відомості, подані у формі, що дає змогу їх приймати або передавати засобами електрозв'язку.* Інформація в цих мережах передається за допомогою сигналів, які є матеріальними носіями передавання інформації.

Об'єктивна сторона. Диспозиція ст. 361 КК дає можливість наступним чином визначити ознаки об'єктивної сторони передбачених нею складів кримінальних правопорушень. За конструкцією об'єктивної сторони складу несанкціонованого втручання, передбачені частиною 1 та 2 ст. 361 КК є формальними. Діяння полягає у несанкціонованому втручанні в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем або електронних комунікаційних мереж. Частина 3, 4 та 5 ст. 361 КК передбачають матеріальні склади, аналогічне ч.1 ст. 361 КК діяння та різні види наслідків. Частина 3 ст. 361 КК передбачає відповідальність за несанкціоноване втручання, якщо воно призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Частина 4 – за несанкціоноване втручання, яке заподіяло значну шкоду чи створило небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків. Частина 5 – за

¹ Докладніше див.: Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 119–123.

несанкціоноване, яке призвело до наслідків, передбачених частиною 3 або 4, вчинене під час дії військового часу (Табл. 12).

Таблиця 12.

**Ознаки об'єктивної сторони несанкціонованого втручання
(ст. 361 КК)**

Частина ст. 361 КК	Діяння	Причинний зв'язок	Наслідки	Інші ознаки
ч.1	Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	-	-	-
ч. 2	Несанкціоноване втручання	-	-	-
ч. 3	Несанкціоноване втручання	+	<ul style="list-style-type: none"> • виток інформації • втрата інформації • підробка інформації • блокування інформації • спотворення процесу обробки інформації • порушення встановленого порядку маршрутизації інформації 	-

ч. 4	Несанкціоноване втручання	+	<ul style="list-style-type: none"> • значна шкода • небезпека тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків 	
ч. 5	Несанкціоноване втручання	+	<ul style="list-style-type: none"> • виток інформації • втрата інформації • підробка інформації • блокування інформації • спотворення процесу обробки інформації • порушення встановленого порядку маршрутизації інформації • значна шкода • небезпека тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків 	час дії воєнного стану

Відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах» несанкціоновані дії щодо інформації в системі являють собою «дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства». Своєю чергою, порядок доступу до інформації в системі визначається як «умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації». Відповідно до ст. 4 даного Закону порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації¹.

Таким чином, *несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем або електронних комунікаційних мереж* можна визначити, як будь-яку зміну режиму їх роботи, вчинену з порушенням установленого відповідно до законодавства порядку доступу до інформації, що заподіює шкоду суспільним відносинам власності на комп'ютерну інформацію або відносинам в сфері надання послуг електрозв'язку.

Варто зазначити, що у науці представлено аргументи на користь більш вузького тлумачення несанкціонованого втручання. Так, В. М. Бутузов вважає, що воно може проявлятися в несанкціонованому доступі, котрий розуміється як доступ до інформації, пов'язаний з подоланням програмних, технічних чи організаційних заходів захисту, або в несанкціонованому впливі на інформацію, що здійснюється з порушенням методів і процедур автоматизованого опрацювання інформації². А. А. Музика та Д. С. Азаров зазначали, що «фізичний вплив безпосередньо на ЕОМ, автоматизовані систе-

¹ Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

² Бутузов В. М., Остапеч С. Л., Шеломенцев В. П. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: науково-практичний коментар. Київ: МВС України, 2005. С. 15–17.

ми, комп'ютерні мережі та мережі електрозв'язку чи відповідні носії інформації не охоплюється складом злочину, передбаченого ст. 361 КК. Такі діяння, вчинені з метою заволодіння інформацією, знищення, пошкодження, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку маршрутизації інформації, за наявності підстав можуть кваліфікуватися за ст. 360 КК або як відповідний злочин проти власності»¹. Тут слід відмітити, що ст. 361 КК не містить указівки на те, що несанкціоноване втручання обов'язково має супроводжуватися подоланням засобів захисту інформації, не обмежує спосіб вчинення діяння, не містить указівки на те, що діяння не може бути вчинене шляхом безпосереднього фізичного впливу на засоби комп'ютерної техніки або телекомунікації.

Витік інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Витік є порушенням такого повноваження власника комп'ютерної інформації, як право розпорядження.

Втрата комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, що дає змогу опрацювати її за допомогою комп'ютерної техніки.

Підробка комп'ютерної інформації, як видається, являє собою порушення такого повноваження власника, як користування, адже через підробку він повністю або частково втрачає можливість реалізувати свою інформаційну потребу. З огляду на це можна так визначити підробку комп'ютерної інформації: зміна без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особою, яка має право власності на таку інформацію.

Блокування комп'ютерної інформації також є специфічною формою порушення повноваження користування інформацією. Відпо-

¹ Музика А. А., Азаров Д. С. Законодавство України про відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. Київ: Паливода А. В., 2005. С. 26–29.

відно до Закону «Про захист інформації в інформаційно-комунікаційних системах» блокування інформації в системі – «дії, внаслідок яких унеможливується доступ до інформації в системі». Воно являє собою ситуацію, коли комп'ютерна інформація не знищена, не підроблена, але можливість використовувати її відсутня. Можна сформулювати таке визначення: блокування комп'ютерної інформації – відсутність у власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.

Прикладом несанкціонованого втручання, що призвело до блокування інформації, можуть слугувати так звані розподілені атаки відмови від обслуговування (DDoS-атаки, Distributed Denial of Service attacks), які полягають у надсиланні дуже великої кількості запитів на один або кілька серверів, що викликає їх перевантаження та призводить до того, що інформаційний ресурс, доступ до якого забезпечується сервером, стає недоступним.

Спотворення процесу обробки комп'ютерної інформації – отримання під час операцій з комп'ютерною інформацією, які здійснювалися за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми.

Порушення встановленого порядку маршрутизації комп'ютерної інформації матиме місце, коли комп'ютерна інформація, що передається за допомогою комп'ютерної мережі конкретному абонентові (абонентам), ним не отримується або доступ до певних мережевих ресурсів здійснюється з порушенням встановленого порядку.

Як зазначалося раніше, предметом досліджуваного кримінального правопорушення є не тільки комп'ютерна інформація, але й інформація, що передається мережами електрозв'язку. Вказані у ч. 3 ст. 361 КК наслідки мають специфіку для даного виду інформації.

Так, *витік інформації, що передається мережею електрозв'язку*, є результатом несанкціонованого втручання в роботу мережі електрозв'язку, унаслідок якого інформація, що передається мере-

жею, стає відомою чи доступною фізичним та/або юридичним особам, які не мають права доступу до неї.

Утрата інформації, що передається мережами електрозв'язку, – це порушення електрозв'язку у вигляді неотримання абонентом мережі інформації, якому вона надсилається.

Підробкою інформації буде такий вплив на носій інформації, що передається мережею електрозв'язку, у результаті якого абонент отримує відомості, які не збігаються з тими, що було йому надіслано.

Блокування інформації, що передається каналами зв'язку, є результатом несанкціонованого втручання в роботу мережі електрозв'язку у вигляді неможливості або значного ускладнення протягом певного часу отримувати чи надсилати інформацію за допомогою цієї мережі.

Порушення порядку маршрутизації інформації в мережі електрозв'язку, як звичайно, матиме місце, коли інформація, що передається за допомогою мережі конкретному абонентові (абонентам), ним не отримується, а також у випадках отримання інформації, що передається в мережі, на кінцеве обладнання, яке не є складовою цієї мережі. Це може бути незаконне підключення телефонних апаратів до мереж телефонного зв'язку, а також незаконне підключення телевізійних приймачів до мереж кабельного телебачення. Існують і більш складні види порушення порядку маршрутизації, які пов'язані, зокрема, з маршрутизацією вхідного міжнародного трафіку на телефонні мережі загального користування.

Під *спотворенням процесу обробки інформації*, що передається каналами електрозв'язку, потрібно розуміти отримання під час роботи технічного засобу зв'язку результатів, що не відповідають його характеристиці. Зазначимо, що підроблення та спотворення процесу обробки інформації в мережі електрозв'язку можуть характеризуватися спільним суспільно небезпечним результатом (заподіянням об'єкту однакової шкоди), проте різним є механізм її заподіяння: підроблення вчиняється через вплив на носій інформації, а спотворення процесу оброблення – через вплив на технічний засіб зв'язку.

Значною шкодою, відповідно до примітки до ст. 361 КК, вважається така, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян. Зазвичай ця шкода полягає в заподіянні позитивних матеріальних збитків. У такому разі її потрібно оцінювати з огляду на витрати власника щодо придбання (створення) інформації, яка є предметом посягання. Але щодо значної шкоди як обставини, що обтяжує відповідальність та впливає на кваліфікацію кримінального правопорушення у сфері використання інформаційних технологій, зауважимо, що іноді вона може виражатися і в упущеній вигоді. Це можна пояснити тим, що на сучасному етапі будь-яка діяльність як потрібний елемент містить інформаційне забезпечення. Ефективність діяльності багато в чому залежить від кількості та якості вхідної інформації, позаяк перекручення або знищення інформації, що має порівняно невелику ціну, здатне завдати значних матеріальних збитків у вигляді упущеної вигоди. Саме тому видається правильним, крім втрати або зменшення обсягу інформації, якою володіє потерпілий, у розмір матеріальних збитків від «комп'ютерного» кримінального правопорушення вносити також і упущену вигоду, яка може полягати в укладанні невігідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Створення небезпеки тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків. Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні «комп'ютерного» кримінального правопорушення можуть виражатися і в нематеріальних видах шкоди, що зумовлено використанням інформаційних систем для контролю над складними технологічними процесами, об'єктами та керування ними. Це така шкода, як порушення нормальної роботи підприємств, зупинення або порушення складних технологічних процесів, погіршення обороноздатності держави, підриг авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю та здоров'ю громадян, порушення безпеки руху транспорту тощо.

Причинний зв'язок як обов'язкова ознака об'єктивної сторони несанкціонованого втручання полягає в тому, що діяння (несанкціоноване втручання) спричиняє настання наслідків: воно передуює настанню зазначених суспільно небезпечних наслідків, містить у собі реальну можливість наслідків і в конкретному випадку є необхідною умовою, без якої б наслідки не настали.

Суб'єктивна сторона несанкціонованого втручання, передбаченого ч. 1 ст. 361 КК, полягає в усвідомленні винною особою несанкціонованого характеру своїх дій та бажанні вчиняти такі дії.

Суб'єктивна сторона несанкціонованого втручання, передбаченого ч. 3 ст. 361 КК полягає в тому, що особа: а) усвідомлювала суспільну небезпеку втручання, тобто фактичні та соціальні ознаки діяння, його несанкціонованість; б) передбачала наслідки у вигляді витоку, втрати, підроблення, блокування інформації, спотворення процесу обробки інформації або порушення порядку її маршрутизації; в) бажала або свідомо припускала настання цих наслідків.

Тобто суб'єктивна сторона аналізованого складу може виражатись у вигляді як прямого, так і непрямого умислу¹.

Суб'єктивна сторона несанкціонованого втручання, яке заподіяло значну шкоду або тяжкі наслідки (ч.ч. 4, 5 ст. 361 КК), характеризується змішаною формою вини. Психічне ставлення особи до діяння, несанкціонованого втручання, виражається в умислі, а до наслідків може бути як умисним, так і необережним. Зауважимо, що в деяких випадках умисне заподіяння шкоди в результаті кримінального правопорушення у сфері використання інформаційних технологій може фактично являти собою інший склад кримінального правопорушення. Скажімо, цілком очевидно, що знищення певної надзвичайно важливої для обороноздатності країни комп'ютерної інформації для ослаблення держави не буде вважатися несанкціонованим втручанням, яке заподіяло тяжкі наслідки, а є нічим іншим, як диверсією (ст. 113 КК).

Суб'єкт несанкціонованого втручання загальний; ним є фізична осудна особа, яка досягла 16-річного віку.

¹ З цього питання див. також: Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. С. 190.

3.1.4. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361¹ КК України)

Безпосередній об'єкт кримінального правопорушення, передбаченого ст. 361¹ КК, складають суспільні відносини власності на комп'ютерну інформацію та відносини надання й отримання послуг електрозв'язку. Специфіка механізму заподіяння шкоди цим суспільним відносинам полягає в тому, що створення, розповсюдження або збут шкідливих програмних чи технічних засобів створює реальну загрозу порушення суспільних відносин власності на інформацію або відносин надання послуг електрозв'язку.

До *предметів* відносяться призначені для несанкціонованого втручання шкідливі програмні засоби та шкідливі технічні засоби.

Ознака «шкідливі» вказує на здатність програмних та технічних засобів завдавати шкоди інформаційним відносинам, які забезпечуються комп'ютерною технікою або мережами електрозв'язку, або створювати загрозу такої шкоди. Ознака «призначені для несанкціонованого втручання» підкреслює їхнє спеціальне призначення – несанкціоноване втручання в роботу комп'ютерної техніки чи мереж. На відміну від інших комп'ютерних програм і обладнання, шкідливі засоби спеціально розробляються для порушення роботи інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем або електронних комунікаційних мереж.

Отже, під шкідливими програмними засобами, призначеними для несанкціонованого втручання в роботу інформаційних, електронних, інформаційно-комунікаційних систем або електронних комунікаційних мереж, слід розуміти програмне забезпечення, спеціально створене для такого втручання, яке призводить або може призвести до шкоди інформаційним відносинам.

Технічні засоби, призначені для несанкціонованого втручання в роботу інформаційних, електронних, інформаційно-комунікаційних систем або електронних комунікаційних мереж, включають різ-

номанітні пристрої та обладнання, розроблені для того, щоб порушувати роботу комп'ютерної техніки або мереж, що спричиняє або може спричинити шкоду інформаційним відносинам.

Прикладом кримінальної відповідальності за незаконні дії з подібними пристроями може слугувати вирок Ленінського районного суду м. Кіровограда в справі № 1-133/10 від 10.06.2010 р.¹, яким засуджено особу, котра здійснила збут технічного пристрою «Portable mobile signale jammer». Засуджений продавав пристрій, який заглушував сигнал стільникового або мобільного зв'язку. При його використанні блокуються будь-які дзвінки мобільного зв'язку. Ураховуючи функції вказаного пристрою – переривання та блокування розмов (інформації) у межах електрозв'язку, а також його здатність впливати на процес передавання сигналу (інформації) та відсутність можливості його застосування за будь-яким іншим призначенням, він обґрунтовано був визнаний таким, що призначений для несанкціонованого втручання в роботу мереж електрозв'язку.

Кримінальне правопорушення, передбачене ч. 1 ст. 361¹ КК, вважається закінченим з моменту вчинення одного з альтернативних дійнь, зазначених у диспозиції. Досліджувана норма передбачає такі форми об'єктивної сторони:

- 1) створення шкідливих програмних або технічних засобів з метою використання, розповсюдження або збуту;
- 2) розповсюдження шкідливих програмних або технічних засобів;
- 3) збут шкідливих програмних або технічних засобів.

Створення шкідливих програмних або технічних засобів являє собою результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу. Зазначимо, що створення буде кримінально караним тільки за наявності відповідної ознаки суб'єктивної сторони – мети використання, розповсюдження або збуту.

¹ Вирок Ленінського районного суду м. Кіровограда від 10.06.2010. Справа № 1-133/10. Єдиний державний реєстр судових рішень: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/12030191> (дата звернення: 30.08.2024).

Розповсюдження шкідливих програмних – це платне або безплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а також їх «закладання» в програмне забезпечення або розповсюдження за допомогою комп'ютерних мереж чи поширення шляхом самовідтворення¹.

Розповсюдження шкідливих технічних засобів аналогічне простому розповсюдженню матеріальних предметів. Однак і це діяння має певну специфіку. Крім простого передавання таких засобів можливим є їх встановлення в обладнання, яке продається або передається на іншій основі, наприклад здається в оренду. Отже, розповсюдження шкідливих технічних засобів можна визначити таким чином: платне або безплатне передавання шкідливого технічного засобу, а також його установа в інформаційні, електронні комунікаційні, інформаційно-комунікаційні системи.

Треба зазначити ще одну особливість розповсюдження шкідливих програмних і технічних засобів. Воно може здійснюватися як за згодою особи, якій ці засоби надаються, так і без неї. У низці випадків згода особи на одержання шкідливого програмного або технічного засобу може виключати суспільну небезпечність, а отже, караність діяння. До таких випадків слід віднести придбання шкідливих програм або технічних засобів для перевірки систем інформаційної безпеки, створення антивірусних програм, а також із метою проведення досліджень. Водночас кримінальна відповідальність не виключається, якщо названі засоби купуються для вчинення кримінальних або інших правопорушень. Відсутність в особи, яка розповсюджує шкідливі програмні та технічні засоби за згодою особи, що їх купує, відомостей про мету їх подальшого використання не виключає суспільної небезпечності, а отже, кримінальної протиправності розповсюдження.

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний із відчуженням предмета. Тобто якщо при розповсюдженні предмет залишається в особи

¹ Шинкаренко І. Р., Голубев В. О., Карчевський М. В., Хараберюш І. Ф. Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія: монографія. Донецьк : РВВ ЛДУВС, 2007. 266 с.

(шкідливе програмне забезпечення продовжує знаходитися на мережевому ресурсі, з якого розповсюджується, повертається шкідливий програмний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває. Отже, під збутом шкідливих програмних або технічних засобів слід розуміти їх оплатне або безоплатне відчуження. Типовим прикладом збуту шкідливих програм є продаж дисків з записаними на них шкідливими програмами.

Розмежування форм об'єктивної сторони даного кримінального правопорушення досліджувала Т. В. Михайліна. Дослідниця обґрунтовувала такі положення. Розповсюдження шкідливих програмних засобів – це «передача фізичного носія зі шкідливими програмними засобами виключно в безоплатний спосіб або передача (чи пропозиція) шкідливих програм для ЕОМ через автоматизовані системи чи комп'ютерні мережі в оплатний чи безоплатний спосіб». Розповсюдження шкідливих технічних засобів – «їх фізичне відчуження виключно в безоплатний спосіб». Збут шкідливих програмних засобів – «форма передачі або реалізації шкідливих програмних засобів, внаслідок якої вони передаються у володіння або розпорядження інших осіб виключно на платній основі... Під час збуту відбувається незаконне відчуження шкідливих програмних засобів виключно на фізичному носії»¹. Як можна зрозуміти, збут шкідливих технічних засобів являє собою їх фізичне відчуження виключно на платній основі. Спроба автора відійти від запропонованої вище класифікації розповсюдження та збуту на підставі відчуження предмета видається не зовсім вдалою. Дослідниця змішує у своїх визначеннях принципово різні характеристики дій щодо шкідливих програмних і технічних засобів. Навряд чи можна вважати послідовним таке положення: якщо передача дисків є платною – має місце збут, розповсюдженням буде тільки безоплатна передача дисків з шкідливим програмним забезпеченням, а також надання платного

¹ Михайліна Т. В. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут: автореф. дис. ... канд. юрид. наук. Київ, 2011. С. 13, 14.

або безоплатного доступу до них, наприклад, через Інтернет. Принципова різниця збуту та розповсюдження навіть на лінгвістичному рівні у тому, що при збуті предмет не залишається в особі, яка його здійснює. При розповсюдженні ж це має місце та взагалі робить його можливим.

Оскільки кримінальне правопорушення, передбачене ст. 361¹ КК, характеризується формальним складом, зміст його *суб'єктивної сторони* визначається лише психічним ставленням до діяння і полягає в усвідомленні суспільної небезпечності та протиправності створення, розповсюдження або збуту шкідливих програмних і технічних засобів та бажанні вчинення таких дій. Отже, у цій формі умисел може бути тільки прямим, а його специфіка полягає в тому, що свідомістю особи обов'язково охоплюється розуміння того, що створювані або розповсюджені засоби спеціально призначені для несанкціонованого втручання.

Обов'язковою ознакою суб'єктивної сторони є усвідомлення особою особливостей і призначення технічних і програмних засобів, які вона поширює. Якщо особа не усвідомлює властивості цих засобів, вона не підлягає кримінальній відповідальності за їх поширення. Яскравим прикладом є ситуація, коли шкідливі програми розповсюджуються під виглядом звичайного програмного забезпечення. У такому випадку особа створює програму з прихованими шкідливими функціями і пропонує її для загального доступу в мережі, при цьому організовуючи поширення програми за винагороду. В результаті, кримінальна відповідальність буде виключена для тих, хто скопіював та розповсюдив цю програму через відсутність у них усвідомлення ознак предмета. Якщо ж особа помиляється, вважаючи програмні або технічні засоби шкідливими, коли насправді це не так, вона може підлягати відповідальності за замах на розповсюдження шкідливих засобів.

Усвідомлення дій, як важливий елемент суб'єктивної сторони розповсюдження або збуту шкідливих програм, полягає в розумінні особою того, що її дії можуть призвести до використання шкідливих засобів іншими людьми.

Суб'єкт незаконних дій з шкідливими програмними або технічними засобами загальний, ним є фізична, осудна особа, яка досягла 16-річного віку.

3.1.5. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361² КК України)

Безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 361² КК, виступають суспільні відносини власності на комп'ютерну інформацію з обмеженим доступом.

Предметом кримінального правопорушення є інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства. Тобто інформація, що є предметом кримінального правопорушення, передбаченого ст. 361² КК, характеризується такими ознаками:

- 1) вона відноситься до інформації з обмеженим доступом;
- 2) зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;
- 3) створена відповідно до чинного законодавства;
- 4) захищена відповідно до чинного законодавства.

До *інформації з обмеженим доступом* згідно зі ст. 21 Закону України «Про інформацію» відноситься конфіденційна, таємна та службова інформація¹. До таємної та службової інформації належать відомості, що становлять державну та іншу *передбачену* законом та-

¹ Про інформацію: Закон України від 02.10.1992 р. № 2657-ХІІ. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

ємницю. Саме на рівні закону встановлюється порядок віднесення інформації до таких видів, а також порядок доступу до неї.

Наприклад, державна таємниця – вид таємної інформації, яка охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України та які віднесено законом до державної таємниці й поставлено під охорону з боку держави. Віднесення інформації до державної таємниці та порядок її використання визначаються Законом України «Про державну таємницю». Перелік відомостей, що становлять державну таємницю, затверджується наказом голови Служби безпеки України.

До таємної інформації, крім державної, відноситься також інша передбачена законом таємниця, розголошення якої завдає шкоди особі, суспільству, державі. Такою може бути, наприклад, таємниця страхування (Закон України «Про страхування»), таємниця усиновлення (Сімейний кодекс), таємниця наради суддів (Кримінальний процесуальний кодекс) тощо.

Конфіденційною інформація є інформація про фізичну особу, а також інформація, доступ до якої обмежено *фізичною або юридичною особою*, крім суб'єктів владних повноважень. Громадяни та юридичні особи, котрі володіють інформацією професійного, ділового, комерційного та іншого характеру, придбаною на власні кошти або такою, що є предметом їх професійного, ділового, комерційного та іншого інтересу, самостійно визначають її належність до конфіденційної. Наприклад, на підставі ч. 1 ст. 36 Господарського кодексу України відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, але розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею.

Перелік відомостей, що складають комерційну таємницю підприємства, порядок роботи з ними й організація їх охорони визначаються наказом керівника, зміст якого не повинен суперечити положенням чинного законодавства. Підставою для прийняття такого наказу служить згадана норма Господарського кодексу, у якій зазна-

чається: «Склад і обсяг відомостей, що складають комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону»¹. Перелік відомостей, які не можуть складати комерційну таємницю, міститься в Постанові Кабінету Міністрів України № 611 від 09.08.1993 р. «Про перелік відомостей, які не складають комерційну таємницю»².

Використання терміна «інформація, яка зберігається (або оброблюється (ст. 362 КК – додано автором)) в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або на носіях такої інформації» є не зовсім вдалим, оскільки він громіздкий, а за змістом повністю відповідає більш вдалому термінові «комп'ютерна інформація». Крім того, напевно чи можна визнати доцільним розмежування термінів «інформація, що оброблюється...» (ст. 362 КК) та «інформація, що зберігається...» (ст. 361² КК), оскільки оброблення інформації в ЕОМ, системі чи комп'ютерній мережі обов'язково передбачає її зберігання, а зберігання передбачає оброблення. У цьому питанні можна погодитися з Д. С. Азаровим, який зазначає, що закон має визначати форму подання інформації, а не спосіб або засоби її оброблення чи зберігання³. Таким чином, друга виділена нами ознака інформації як предмета кримінального правопорушення, передбаченого ст. 361² КК, полягає в тому, що вона є комп'ютерною, тобто подана у формі, що дозволяє її оброблення або зберігання з використанням комп'ютерної техніки.

Інформація, що є предметом, *створена відповідно до чинного законодавства*, тобто розповсюдження або збут інформації, створеної з порушенням законодавства, не є кримінальним правопорушенням, передбаченим ст. 361² КК.

¹ Господарський кодекс України: Закон України від 16.01.2003 № 436-IV. *Відомості Верховної Ради України*. 2003. № 18. № 19-20, № 21-22. Ст. 144.

² Про перелік відомостей, які не складають комерційну таємницю: Постанова Кабінету Міністрів України № 611 від 09.08.1993 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/611-93-%D0%BF#Text> (дата звернення 30.08.2024 р.).

³ Азаров Д. С. Нові зміни до розділу XVI Особливої частини Кримінального кодексу України – нові проблеми. *Юридичний вісник України*. 2005. № 6. С. 29.

Нарешті, предметом розгляданого правопорушення є тільки інформація, яка «захищена відповідно до чинного законодавства». Наприклад, відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» власник системи, у якій оброблюється інформація, що є власністю держави, або інформація з обмеженим доступом, вимогу щодо захисту якої встановлено законом, зобов'язаний утворювати службу захисту інформації¹ (ч. 2 ст. 9 Закону). Крім того, така інформація повинна оброблятися із застосуванням «комплексної системи захисту інформації з підтвердженою відповідністю» (ч. 2 ст. 8 Закону). У цьому випадку захищену подібним чином інформацію можна відносити до предметів посягання, передбаченого ст. 361² КК. Склад указанного кримінального правопорушення буде мати місце тоді, коли незаконно розповсюджується або збувається інформація, що зберігається з застосуванням комплексної системи захисту. Ця система являє собою сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації.

Зауважимо, що деякі дослідники вважають предметом кримінального правопорушення, передбаченого ст. 361² КК, тільки ту інформацію, яка відповідно до закону підлягає обов'язковому захисту. Керуючись цим, доходять висновку про те, що предметом може бути тільки інформація, що становить державну таємницю, конфіденційна інформація, що є власністю держави, банківська таємниця, а також таємниця телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікації². Таке бачення видається необґрунтовано звуженим. У диспозиції ст. 361² КК ідеться про інформацію, «захищену відповідно до чинного законодавства», а не про інформацію, «вимога щодо захисту якої міститься в законодавстві». Це означає, що до «інформації, захищеної відповідно до чинного законодавства», слід відносити як ту, що під-

¹ Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

² Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. С. 104.

лягає обов'язковому захисту, так і ту, захист якої може здійснюватися відповідно до закону.

Українське законодавство в питанні створення систем захисту інформації містить не тільки імперативні, але й диспозитивні приписи. Наприклад, ч. 2 ст. 21 Закону України «Про інформацію» наділяє громадян та юридичних осіб правом самостійно визначати режим доступу до неї, включаючи належність її до категорії конфіденційної¹. Достатньо цікавим у цьому плані є регулювання права на захист від незаконного використання комерційної таємниці. Так, відповідно до ст. 162 Господарського кодексу України однією з умов наявності такого права є вживання належних заходів до охорони її конфіденційності. Отже, до предметів досліджуваного правопорушення слід відносити комп'ютерну інформацію з обмеженим доступом, яка створена відповідно до закону та захищена специфічними засобами, використання яких відповідає законодавству.

За конструкцією *об'єктивної сторони* правопорушення, передбачене ст. 361² КК, є формальним. Воно вважається закінченим із моменту вчинення несанкціонованого збуту або несанкціонованого розповсюдження комп'ютерної інформації з обмеженим доступом.

Збут або розповсюдження інформації буде несанкціонованим, якщо вчиняється без дозволу власника цієї інформації.

Розповсюдження комп'ютерної інформації з обмеженим доступом являє собою оплатне або безоплатне надання копій цієї інформації або доступу до неї невизначеному колу осіб. Одним із прикладів подібного діяння є незаконне розповсюдження персональних даних. Під *збутом комп'ютерної інформації з обмеженим доступом* необхідно розуміти її оплатне або безоплатне відчуження.

Суб'єктивна сторона цього правопорушення характеризується виною у формі прямого умислу: особа усвідомлює суспільну небезпечність і протиправність збуту або розповсюдження комп'ютерної інформації з обмеженим доступом та бажає вчиняти такі дії. Особа усвідомлює, що комп'ютерна інформація, яку вона збуває або розпо-

¹ Про інформацію: Закон України від 2.10.1992 № 2657-ХІІ. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

всюджує, є інформацією з обмеженим доступом; усвідомлює, що не має права або дозволу власника інформації на вчинення подібних дій.

Суб'єкт – загальний. Якщо збут або розповсюдження інформації з обмеженим доступом вчиняє особа, якій інформацію було довірено у зв'язку з виконанням службових або професійних обов'язків, вчинене, за наявності відповідних ознак суб'єктивної сторони, необхідно кваліфікувати за ст. 232 або ст. 328 КК.

3.1.6. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України)

Безпосереднім об'єктом кримінального правопорушення є суспільні відносини власності на комп'ютерну інформацію. *Предметом* відповідно до диспозиції є інформація, яка опрацьовується в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації. Як уже зазначалося, термін, що вживається для характеристики предмета, є не зовсім вдалим: він громіздкий, а за змістом не відрізняється від більш вдалого – «комп'ютерна інформація».

Об'єктивна сторона розгляданого кримінального правопорушення характеризується наявністю декількох форм:

- несанкціонована зміна комп'ютерної інформації;
- несанкціоноване знищення комп'ютерної інформації;
- несанкціоноване блокування комп'ютерної інформації;
- несанкціоноване перехоплення комп'ютерної інформації, що призвело до її витоку;
- несанкціоноване копіювання комп'ютерної інформації, що призвело до її витоку.

Несанкціонована зміна комп'ютерної інформації являє собою порушення права власності на інформацію шляхом перекручення без відома власника змісту відомостей, відображених на носії, що робить інформацію цілком або частково непридатною для задоволення інформаційної потреби особи, яка має право власності на таку інформацію.

Несанкціоноване знищення комп'ютерної інформації має місце тоді, коли вона перестає існувати у формі, яка дозволяє її опрацювати за допомогою комп'ютерної техніки.

Несанкціоноване блокування комп'ютерної інформації – позбавлення власника можливості використовувати інформацію для задоволення інформаційної потреби за умови, що її не втрачено та не підроблено.

Якщо три перші форми являють собою прості, звичайні правопорушення з матеріальним складом і вважаються закінченими з моменту настання зазначених наслідків, то структура двох останніх – несанкціонованого перехоплення та копіювання – ускладнена наявністю похідного наслідку – витоку інформації, якому передують такі види порушення права власності на комп'ютерну інформацію, як несанкціоноване копіювання або перехоплення.

Оскільки *витік інформації* відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» є результатом дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що *не мають права доступу до неї*¹, можна зробити висновок, що предметом несанкціонованого перехоплення або копіювання є тільки комп'ютерна інформація з обмеженим доступом.

Копіювання комп'ютерної інформації представляє собою відтворення даних зі збереженням вихідної інформації. Тож несанкціоноване копіювання можна визначити як відтворення, з перевищенням наданих власником прав доступу, комп'ютерної інформації з обмеженим доступом зі збереженням вихідної ін-

¹ Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

формації. Наприклад, особа має право лише на ознайомлення та внесення змін до певної бази даних, а вона без дозволу власника створює її копію. Погодимось з С. В. Дрьомовим у тому, що для констатації факту копіювання однією з визначальних обставин, що підлягають установленню, є тотожність змісту цієї інформації зі змістом отриманої¹.

Перехоплення являє собою специфічний вид копіювання. Для перехоплення, як зазначає С. В. Дрьомов, характерним є те, що предмет (інформація) циркулює в мережі, відповідно під несанкціонованим перехопленням інформації слід розуміти дії, спрямовані на привласнення або затримування інформації під час її маршрутування в комп'ютерній мережі². На нашу думку, більш правильно вважати перехоплення певним видом копіювання. Відповідно до Конвенції про кіберзлочинність, прийнятої в рамках Ради Європи 23 листопада 2001 року (ратифікована Україною у вересні 2005 року), *несанкціонованим перехопленням* є навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, не призначених для публічного користування, які проводяться з комп'ютерної системи, усередині її або на неї, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить у собі такі комп'ютерні дані³. Отже, несанкціоноване перехоплення: 1) вчиняється за допомогою специфічних технічних засобів; 2) полягає в отриманні копії інформації під час її передавання від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем чи комп'ютерних мереж; 3) вчиняє особа, яка не має

¹ Дрьомов С. Сутність копіювання як форми несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації. *Підприємництво, господарство і право*. 2005. № 9. С. 147.

² Дрьомов С. Кримінально-правова характеристика перехоплення комп'ютерної інформації як форми об'єктивної сторони злочину, передбаченого статтею 362 КК України. *Юридичний журнал*. 2006. № 6. С. 56.

³ Конвенція про кіберзлочинність: міжнародний документ від 23.11.2001 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 30.10.2024 р.).

права на отримання інформації з обмеженим доступом, що є його предметом.

Таким чином, *несанкціоноване перехоплення* – це отримання, з перевищенням наданих власником прав, копії інформації з обмеженим доступом за допомогою специфічних технічних засобів під час передавання цієї інформації від одного комп'ютера до іншого, або від периферійних приладів до комп'ютера, або шляхом обробки електромагнітних випромінювань під час роботи ЕОМ, автоматизованих систем чи комп'ютерних мереж, у яких опрацьовується така інформація.

Наприклад, під час роботи електронно-обчислювальної машини сигнали, які формують зображення на дисплеї, можуть за допомогою спеціального обладнання отримуватися на певній відстані від працюючого комп'ютера. Тож особа шляхом перехоплення отримуватиме ту комп'ютерну інформацію, яка відображається на дисплеї.

Суб'єктивна сторона характеризується виною у формі прямого або непрямого умислу: особа усвідомлює суспільну небезпечність і протиправність своїх дій і бажає або свідомо допускає настання наслідків. При цьому особа має усвідомлювати, що вчиняє такі дії, які є перевищенням повноважень, наданих власником інформації. Слід погодитися з С. Дрьомовим, який до змісту інтелектуального моменту умислу при несанкціонованих діях з інформацією, яка обробляється в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, відносить також усвідомлення властивостей спеціального суб'єкта, які є конститутивними ознаками цього складу кримінального правопорушення¹.

Суб'єкт кримінального правопорушення, передбаченого ст. 362 КК, спеціальний – особа, яка має право доступу до комп'ютерної інформації. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації.

¹ Дрьомов С. Умисел при вчиненні несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації (ст. 362 КК України). *Підприємництво, господарство і право*. 2005. № 7. С. 116.

Достатньо цікавий приклад кримінального правопорушення, що розглядається, описується у вирокі Косівського районного суду Івано-Франківської області в справі № 1-56/2007 від 7.06.2007 р.¹ щодо обвинувачення Б. у вчиненні злочинів, передбачених ст.ст. 364, 366 та 362 КК. Так, Б., працював з на посаді бухгалтера по реалізації філії енергетичної компанії та був *особою, яка має доступ до програми, призначеної для комп'ютерної обробки інформації* по розрахунках з юридичними особами.

Приватне підприємство «Ф.» згідно договору на постачання сплатило за використану електроенергію 38 2671,45 грн. В цей час, Б. зловживаючи своїм службовим становищем, діючи умисно, в інтересах третіх осіб, а саме приватних підприємців Т., Р., Л., В., Д незаконно занижив показник спожитої електроенергії ПП «Ф.» та коштів фактично сплачених за неї в сумі 76 008,07 грн., які безпідставно у програмі розрахунків з юридичними споживачами, розніс вказаним приватним підприємцям, що споживали електроенергію, але не здійснювали оплати за неї. Внаслідок цих умисних дій енергетичній компанії заподіяно тяжкі наслідки в сумі 76 008,07 грн.

Суд правильно кваліфікував дії Б., що виразились у зловживанні службовим становищем, тобто умисному, в інтересах третіх осіб використанні свого службового становища в супереч інтересам служби, що заподіяло тяжкі наслідки як злочин, передбачений ч. 2 ст. 364 КК. Крім цього, правильною є й оцінка дій підсудного за ст. 366, як службового підроблення, та ст. 362, як *несанкціонованої зміни комп'ютерної інформації, вчиненої особою, яка має доступ до неї*. Зазначимо, що в даному випадку вчинене Б. службове підроблення обов'язково потребувало додаткової кваліфікації за ст. 362, оскільки спосіб у який вчинено службове підроблення представляє собою самостійний злочин (ст. 362), який не охоплюється диспозицією відповідної норми про злочин в сфері службової діяльності.

¹ Вирок Косівського районного суду Івано-Франківської області від 07.06.2007. Справа № 1-56/2007. Єдиний державний реєстр судових рішень: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/2372954> (дата звернення: 30.08.2024).

3.1.7. Порухення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України)

Безпосередній об'єкт кримінального правопорушення, передбаченого цією статтею, складають суспільні відносини, у межах яких забезпечується безпека використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також дотримання порядку та правил захисту комп'ютерної інформації.

Правила експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку являють собою вимоги, які ставить власник ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Вони, як правило, містяться в окремих підзаконних актах (наказах, розпорядженнях), що видаються власником комп'ютерної техніки або мережі електрозв'язку. Наприклад, правила експлуатації засобів обчислювальної техніки регламентуються Положенням про роботу із засобами обчислювальної техніки та інформаційно-телекомунікаційною мережею Міністерства розвитку економіки, торгівлі та сільського господарства України, затвердженим наказом Міністерства розвитку економіки, торгівлі та сільського господарства України № 1800 від 15.09.2020 р. Відповідно до положень даного відомчого нормативного акту користувачам заборонено розкривати корпуси засобів обчислювальної техніки, вносити зміни до конфігурації або самостійно їх ремонтувати; під'єднання засобу обчислювальної техніки користувача до телекомунікаційної мережі, установлення, оновлення та вилучення програмного забезпечення здійснюють відповідні спеціалісти й т. ін.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» захист інформації в систе-

мі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі¹. Регламентація цієї діяльності здійснюється за допомогою визначення порядку та правил захисту комп'ютерної інформації. Видається, що *порядок захисту інформації* – це визначені нормативно-правовими актами вимоги щодо створення системи захисту інформації та організації її роботи. *Правила захисту інформації*, у свою чергу, являють собою вимоги щодо використання системи захисту інформації певного інформаційного ресурсу. Тобто, якщо систему захисту певного інформаційного ресурсу не створено, то й неможливо порушити правила захисту цього ресурсу. Той факт, що систему захисту не створено, може бути визнаний, за наявності відповідних нормативно-правових положень, порушенням порядку захисту інформації.

На певну увагу заслуговують питання нормативного регулювання захисту комп'ютерної інформації: після прийняття відповідних законів, їх положення конкретизуються указами Президента, постановами Кабінету Міністрів, нормативними документами міністерств і відомств. Базовим нормативним документом у сфері захисту комп'ютерної інформації є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». У цьому законі формулюється, можна сказати, головний принцип регулювання питань захисту комп'ютерної інформації національним законодавством: *відповідальність за захист інформації покладається на власника системи (у якій вона обробляється), при цьому в тих випадках коли в системі обробляється інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вона повинна оброблятися в системі з застосуванням комплексної системи захисту інформації з підтвердженою відповідністю*. Тобто спеціальні вимоги встановлюються лише до захисту державної інформації або інформації, захист якої спеціально передбачено в законі. Решта нормативних актів у сфері інформаційної безпеки конкретизує це положення.

¹ Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

Так, правові та організаційні засади технічного захисту інформації органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України й інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій устанавлюються Указом Президента України «Про Положення про технічний захист інформації в Україні» № 1229/99¹ від 27.09.1999 р.

Державна політика технічного захисту інформації формується згідно із законодавством і реалізується Державною службою спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку України) у взаємодії з органами, щодо яких здійснюється технічний захист інформації. Саме Держспецзв'язку проводить сертифікацію засобів технічного захисту інформації. Правові основи організації та діяльності цього державного органу визначаються Законом України «Про Державну службу спеціального зв'язку та захисту інформації України».

Постанови Кабінету Міністрів України встановлюють чіткі вимоги щодо інформаційної безпеки в органах державної влади. Так, відповідні постанови уряду як обов'язкову складову державних автоматизованих інформаційних систем передбачають систему захисту інформації²; на органи державної влади покладається вимога щодо забезпечення захисту інформаційного наповнення їх веб-порталів³ тощо.

¹ Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99. Верховна Рада України. Законодавство України: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/1229/99#Text> (дата звернення: 30.08.2024).

² Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»: Постанова Кабінету Міністрів України № 208 від 24.02.2003 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/208-2003-%D0%BF#Text> (дата звернення: 30.08.2024); Деякі питання єдиної державної інформаційної системи у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Постанова Кабінету Міністрів України № 627 від 22.07.2020 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/627-2020-%D0%BF#Text> (дата звернення: 30.08.2024).

³ Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: Постанова Кабінету Міністрів України № 3 від 04.01.2002 р. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text> (дата звернення: 30.08.2024).

У свою чергу, нормативні документи міністерств і відомств закріплюють конкретні організаційні та інженерно-технічні заходи безпеки щодо їх інформаційних ресурсів. До організаційних заходів відноситься, установа інструкцій щодо використання відомчих мереж, періодичне створення комісій з перевірки дотримання вимог інформаційної безпеки, обмеження доступу до приміщень, у яких розташоване обладнання, що забезпечує роботу мережі, тощо. До технічних заходів, передбачених відомчими нормативними документами, можна віднести обов'язкове включення до відомчих комп'ютерних мереж засобів технічного захисту інформації, встановлення вимог до обладнання та програмного забезпечення.

Спеціальних вимог щодо захисту комп'ютерної інформації, яка не є власністю держави, крім положення Закону України «Про захист інформації в автоматизованих системах», що захист інформації покладається на власника системи, національне законодавство не встановлює. Тому порушення правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, у яких обробляється недержавна інформація, стосовно якої законодавство не встановлює спеціальних вимог щодо забезпечення її захисту, а також порушення порядку чи правил захисту такої інформації, якщо воно заподіяло істотну шкоду, буде вважатися кримінальним правопорушенням, передбаченим ст. 363 КК, лише тоді, коли власником інформації або власником засобу автоматизованого опрацювання інформації у формі наказу, розпорядження або іншого офіційного документа закріплено відповідні правила експлуатації, порядок і правила захисту інформації.

Склад правопорушення, передбаченого цією статтею, матеріальний, його *об'єктивна сторона* характеризується такими ознаками:

- 1) діяння – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту комп'ютерної інформації;
- 2) суспільно небезпечні наслідки – значна шкода;
- 3) причинний зв'язок між діянням і суспільно небезпечними наслідками.

Аналіз диспозиції дозволяє зробити висновок про те, що діяння може виявлятися в трьох альтернативних формах:

- порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
- порушення порядку захисту комп'ютерної інформації;
- порушення правил захисту комп'ютерної інформації.

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – недотримання вимог, що ставляться власником ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Таке порушення може полягати, наприклад, у спробі користувача самостійно встановлювати нове програмне або апаратне забезпечення, підключенні комп'ютерної техніки до електромережі без фільтрів, порушенні порядку включення або відключення засобів комп'ютерної техніки тощо.

Порушення порядку захисту комп'ютерної інформації – недотримання визначених нормативними актами вимог щодо створення системи захисту інформації та організації її роботи. Прикладом такого діяння може бути використання комп'ютерної техніки для роботи з таємною інформацією за відсутності сертифікованої належним чином системи захисту.

Порушення правил захисту комп'ютерної інформації – недотримання вимог щодо використання системи захисту інформації певного інформаційного ресурсу. Це може бути, наприклад, неналежне зберігання паролів для доступу до інформації.

Оскільки аналізований склад є матеріальним, він буде вважатися закінченим від моменту настання суспільно небезпечних наслідків – значної шкоди. За змістом закону під значною в цій нормі слід розуміти будь-яку шкоду, заподіяну порушенням нормативів інформаційної безпеки. При цьому в тих випадках, коли вона полягає в заподіянні матеріальних збитків, значною слід уважати таку шкоду, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Суб'єктивна сторона характеризується тим, що діяння може бути вчинено як умисно, так і з необережності, а стосовно наслідків можлива тільки необережність. Якщо настання наслідків охоплюється умислом винної особи, то склад правопорушення, передбаченого ст. 363 КК, відсутній. У таких випадках дії винної особи, за наявності відповідних ознак, необхідно кваліфікувати як умисне пошкодження майна (ст. 194 КК), або як пособництво в несанкціонованому втручанні в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 5 ст. 27, ст. 361 КК), або як несанкціоновані дії з комп'ютерною інформацією, вчинені особою, що має доступ до неї (ст. 362 КК).

Суб'єкт кримінального правопорушення, передбаченого ст. 363 КК, спеціальний – особа, яка відповідає за експлуатацію електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації чи засобу її автоматизованого опрацювання та закріпленими на підставі цього наказу функціональними обов'язками.

3.1.8. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363¹ КК України)

Безпосередній об'єкт перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363¹ КК) складають суспільні відносини щодо забезпечення безвідмовного функціонування комп'ютерної техніки та мереж електрозв'язку як технічних засобів забезпечення відносин власності на інформацію.

Предметом цього кримінального правопорушення є повідомлення електрозв'язку – відомості, подані у вигляді, що дозволяє їх пере-

давати за допомогою комп'ютерних мереж або мереж електрозв'язку. Слід зазначити, що стосовно предмету даного кримінального правопорушення у науці висловлені й інші позиції. До нього пропонується відносити «програмні та технічні засоби ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»¹ або комп'ютерну інформацію та інформацію в мережах електрозв'язку². При цьому повідомлення електрозв'язку називається «матеріальним утворенням, за допомоги якого при реалізації об'єктивної сторони цього посягання чиниться вплив на предмет злочину (інформацію)»³.

Оскільки склад, передбачений статтею 363¹ КК, є *матеріальним*, до ознак його *об'єктивної сторони* належать: 1) діяння – масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів; 2) суспільно небезпечні наслідки – порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) причинний зв'язок між діянням та наслідками.

Діяння як ознака об'єктивної сторони цього складу полягає в розповсюдженні повідомлень електрозв'язку, тобто надісланні певним адресатам копій цих повідомлень, яке, по-перше, є масовим і, по-друге, здійснюється без попередньої згоди адресатів.

Розповсюдження слід уважати *масовим* тоді, коли одне або кілька повідомлень отримує більше, ніж один адресат, адже в диспозиції аналізованої статті йдеться про множинність повідомлень електрозв'язку та їх адресатів. Зазначимо, що поняття «масове» в цій нормі використовується як оцінне, тобто встановлення того, чи було певне розповсюдження повідомлень електрозв'язку масовим, залежить від аналізу багатьох обставин конкретного розповсюджен-

¹ Бутузов В. М., Остапеч С. Л., Шеломенцев В. П. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: науково-практичний коментар. Київ: МВС України, 2005. С. 39.

² Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. С. 146.

³ Там само.

ня (кількість повідомлень або копій повідомлень, їх розмір; кількість адресатів; час, який було використано для розповсюдження; технічні характеристики обладнання, що використовувалося для розповсюдження тощо).

Відсутність попередньої згоди адресатів полягає в тому, що адресат ні в якій формі (письмово, усно, шляхом використання електронної пошти або в інший спосіб) не давав згоди на надсилання йому повідомлень, які є предметом правопорушення.

Порушення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку являє собою таку зміну режиму роботи комп'ютерної техніки або мережі електрозв'язку, яка створює загрозу для їх функціонування, тобто погіршення роботи повністю або частково, тимчасове створення перешкод для використання за призначенням.

Припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку полягає в тимчасовому або остаточному припиненні функціонування комп'ютерної техніки або мереж електрозв'язку, невиконанні ними завдань щодо зберігання, опрацювання, пересилання чи отримання комп'ютерної інформації або інформації, що передається мережами електрозв'язку.

Слід погодитися з висновками В. М. Бутузова, С. Л. Остапця та В. П. Шеломенцева про те, що загальною ознакою як порушення, так і припинення роботи ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку є збереження названими технічними засобами фізичної цілісності, тому випадки фізичного знищення чи пошкодження обладнання слід кваліфікувати, як умисне пошкодження чужого майна (ст. 194 КК) або умисне пошкодження ліній зв'язку (ст. 360 КК)¹.

Суб'єктивна сторона характеризується виною у формі прямого умислу стосовно діяння й умисним або необережним ставленням

¹ Бутузов В. М., Остапек С. Л., Шеломенцев В. П. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: науково-практичний коментар. Київ: МВС України, 2005. С. 40, 41.

до наслідків. Особа усвідомлює, що вчиняє масове розповсюдження повідомлень електрозв'язку, і бажає вчинити такі дії, а також вона бажає або свідомо допускає порушення чи припинення роботи комп'ютерної техніки чи мереж електрозв'язку або легковажно розраховує на ненастання таких наслідків.

Суб'єкт цього кримінального правопорушення загальний.

Серед досліджених нами судових рішень лише одне стосувалося ст. 363¹ КК. Вироком Малиновського районного суду м. Одеси по справі № 521/21945/23 від 27.10.2023 р.¹ особу було визнано винним у вчиненні кримінального правопорушення, передбаченого ст. 363¹ КК. Дана особа, використовуючи апаратні та програмні засоби здійснила «надсилання масових запитів» до веб-ресурсу, який належав потерпілій особі. Внаслідок цих дій відбулося перенавантаження онлайн системи взаємодії підприємства потерпілої особи зі споживачами, що призвело до припинення роботи веб-ресурсу. З нашої точки зору, надсилання повідомлень електрозв'язку та надсилання запитів до веб-ресурсу представляють собою різні процеси. Ураховуючи це, більш правильним було б розглядати цю ситуацію, як несанкціоноване втручання у роботу інформаційно-комунікаційної системи, яке призвело до блокування комп'ютерної інформації. Проте, у цьому випадку було укладено угоду про визнання винуватості, що порушує цілу низку проблем, які перебувають поза межами предмету нашого дослідження.

3.2. Перспективи кримінально-правового регулювання в контексті розвитку інформаційних технологій

Проведений аналіз даних офіційної статистики, судової практики та змісту ознак правопорушень у сфері використання інформаційних технологій дозволяє перейти до розгляду перспектив кримінально-правового регулювання в означеній сфері.

¹ Вирок Малиновського районного суду м. Одеси від 27.10.2023. Справа № 521/21945/23. *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reestr.court.gov.ua/Review/114483840> (дата звернення: 30.08.2024).

В першу чергу потребує обговорення питання ефективності протидії «комп'ютерним» кримінальним правопорушенням. Війна РФ проти України висуває підвищені вимоги до правового регулювання. Більш ніж значна частина агресії відбувається у інформаційному просторі. Кримінальне право, як *ultima ratio*, фокусується на найбільш небезпечних посяганнях. Воно використовує найбільш суворі засоби реагування на винних осіб та, відповідно, потребує значних соціальних ресурсів для реалізації.

Водночас, як такий, що є менше середнього можна визначити рівень інтенсивності кримінально-правового впливу на осіб, які вчинили «комп'ютерні» кримінальні правопорушення. Щодо осіб, визнаних винними у вчиненні цих правопорушень рідше, ніж в середньому застосовуються реальні покарання. У тих випадках, коли реальне покарання призначається, частіше, ніж в середньому, використовуються менш суворі покарання (штрафи). Все це відбувається в умовах подальшого розширення сфери застосування інформаційних технологій та, відповідно, збільшення уразливості суспільних відносин від посягань у вигляді «зламів» інформаційних систем, так званих атак, відмов від обслуговування тощо. Іншими словами, розширення сфери застосування інформаційних технологій дозволяє прогнозувати збільшення небезпечності «комп'ютерних» кримінальних правопорушень, що вчиняються. В свою чергу, судова практика не демонструє відповідної динаміки.

Такі тенденції можуть свідчити про те, що у поле зору кримінальної юстиції потрапляють переважно найпростіші та найменш небезпечні форми відповідних кримінальних правопорушень. Цю проблему ми називаємо примітивізацією правозастосовчого рівня кримінально-правового регулювання¹. Вона не є новою. За результатами дослідження судової практики по Розділу XVI Особливої частини КК ще у 2012 році було зроблено такий висновок: практика національних судів містить рішення, у яких застосування кримінальної відповідальності до осіб, які вчиняли комп'ютерні злочини,

¹ Карчевський М. В. Протидія злочинності в умовах війни: аналіз статистичних даних (2013–2023). *Наук. вісн. Львів. держ. ун-ту внутр. справ. Сер. юрид.* 2024. № 2. С. 84. URL: <https://doi.org/10.32782/2311-8040/2024-2-12> (дата звернення: 30.10.2024).

було пов'язане з посяганнями, які дійсно є суспільно небезпечними (43,71%); разом із тим, більш ніж половина судових рішень досліджуваної категорії (56,29%) пов'язані з кваліфікацією таких діянь, віднесення яких до суспільно небезпечних є досить спірним¹.

Розглянемо під аналогічним кутом зору проведене нами дослідження актуальної судової практики. Як зазначалося раніше, 22% судових рішень пов'язані зі здійсненням несанкціонованих транзакцій. У таких випадках несанкціоноване втручання інкримінується додатково до крадіжки або шахрайства. Не потребує аргументації теза про те, що суспільна небезпечність таких «комп'ютерних» кримінальних правопорушень є опосередкованою та в першу чергу залежить від характеристики предмета відповідного посягання на власність.

23% досліджених судових рішень пов'язані зі зміною даних, що вчиняється особою, яка має право доступу до них. Вважаємо, що і ця група судових рішень характеризується опосередкованою суспільною небезпечністю. Незаконні зміни інформації у службових автоматизованих системах потребують кримінально-правового реагування не самі по собі, а лише тоді, коли такі зміни заподіюють шкоду тим відносинам для інтенсифікації яких використовується автоматизована система. Якщо працівник банківської установи вносить до АС неправдиві дані про емісію платіжної картки, безпека його дій визначається не порушенням правил, а створенням умов для подальшого шахрайства. Такі міркування підтверджуються і тим, що серед 53 досліджених судових рішень даної категорії, 21 (40%) містить дані про кваліфікацію за сукупністю. Крім зміни комп'ютерної інформації (ст. 362 КК) дії, наприклад, працівників банків кваліфікувалися як шахрайство (ст. 190 КК), медичних працівників, що вносили неправдиві дані про щеплення, як підкуп працівника установи (ст. 354 КК) тощо.

Нарешті 19% досліджених судових рішень стосуються розповсюдження або збуту комп'ютерної інформації з обмеженим доступом (19%).

¹ Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 221.

Актуалізуємо наведені раніше міркування про відмежування даного кримінального правопорушення від суміжних¹. Розгляд цього кримінального правопорушення у контексті наявних у КК заборон, пов'язаних з інформацією з обмеженим доступом порушує питання криміналізації окремої криміналізації незаконного збуту або розповсюдження комп'ютерної інформації з обмеженим доступом. Як свідчить проведений аналіз, відповідальність за кримінальне правопорушення, передбачене ст. 361² КК може наставати в таких випадках:

- 1) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає державну таємницю, здійснює особа, якій ці відомості довірені не були й це не пов'язане з передачею її іноземній державі, іноземній організації або їх представникам;
- 2) коли розповсюдження або збут комп'ютерної інформації, зміст якої складають:
 - відомості про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби;
 - лікарська таємниця;
 - комерційна, банківська таємниця, професійна таємниця на ринках капіталу та організованих товарних ринках;
 - відомості про заходи безпеки щодо особи, взятої під захист;
 - дані оперативно-розшукової діяльності досудового слідства чи дізнання,
 - здійснює особа, якій ці відомості довірені не були, тобто вона не мала спеціальних зобов'язань щодо збереження їх в таємниці;
- 3) коли розповсюдження або збут комп'ютерної інформації, зміст якої складає лікарську, комерційну, банківську таємницю, професійну таємницю на ринках капіталу та організова-

¹ Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. С. 200, 201.

- них товарних ринках здійснює особа, якій вони були довірені, але наслідків, зазначених у ст.ст. 145 чи 232 КК не настало;
- 4) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складає таємницю усиновлення (ст. 168 КК) або приватного життя (ст. 182 КК), але до умислу суб'єкта не включається усвідомлення та бажання чи свідоме допущення заподіяння шкоди конкретній особі або чітко визначеній групі осіб, тобто відсутні ознаки складу кримінального правопорушення проти конституційних прав та свобод;
 - 5) коли здійснюється розповсюдження або збут комп'ютерної інформації, зміст якої складають відомості з обмеженим доступом інших видів.

Щоб не перевантажувати запропоновану схему, «за дужки» ми винесли такі ознаки комп'ютерної інформації, предмета кримінального правопорушення, передбаченого ст. 361² КК, як «створена та захищена відповідно до чинного законодавства». Однак видається, що і без цього запропонований перелік випадків, коли можливим є застосування ст. 361² КК, яскраво демонструє очевидну надлишковість кримінально-правової заборони, передбаченої досліджуваною нормою. Дійсно, крім випадків шпигунства, не можна погодитися з тим, що слід уважати кримінально-протиправним діянням розповсюдження відомостей, які складають певну таємницю, вчинене особою, якій вони не були довірені. Ситуація з відповідальністю за порушення лікарської, комерційної або банківської таємниці є ще більш наочною. Чи обґрунтовано вважати певні дії кримінальним правопорушенням, коли наслідки, що зумовлюють кримінальну відповідальність за них, не настали? Єдиним аргументом, який може бути використаний для обґрунтування доцільності такої відповідальності, можна вважати лише те, що кримінальна відповідальність продиктована формою цих відомостей, тим, що вони є комп'ютерною інформацією. Однак, крім того, що він спірний, цього аргументу явно недостатньо для обґрунтування кримінальної відповідальності за подібні дії. *Форма інформації ні в якому разі не може обґрунтовувати підвищену суспільну небезпечність її розповсюдження або збуту.*

Означені критичні положення можуть бути у повній мірі застосовані до судових рішень, які ми досліджували. Достатньо спірною є суспільна небезпечність передачі стороннім особам даних з службових АС, за умови відсутності ознак інших кримінальних правопорушень. До того ж, якщо, наприклад, база даних існує тільки у паперовому вигляді, підстави кримінальної відповідальності відсутні.

Таким чином, три найбільші групи досліджених судових рішень, що в сумі складають 64% від всієї добірки, характеризуються спірною суспільною небезпечністю. Саме це, на нашу думку, є індикатором проблеми ефективності кримінально-правової протидії «комп'ютерним» кримінальним правопорушенням: *в умовах стрімкої інформатизації більше половини судових рішень стосуються випадків зі спірною суспільною небезпечністю.*

У цьому контексті не можна не звернути уваги на Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24.03.2022 р. № 2149-IX. Закон передбачав зміни до Розділу XVI Особливої частини КК. Зокрема здійснено самостійну криміналізацію несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ч. 1 ст. 361 КК). Дії, які раніше вважалися основним складом кримінального правопорушення, передбаченого ч. 1 ст. 361 КК, стали складом з особливо обтяжуючими відповідальність обставинами (ч. 3 ст. 361 КК) і отримали більш суворої санкції. В умовах встановлених тенденцій примітивізації протидії «комп'ютерним» кримінальним правопорушенням, названі зміни законодавства про кримінальну відповідальність мають негативний потенціал. Вони можуть стати причиною появи у сфері дії кримінальної юстиції ще більшої кількості діянь, які, з одного боку, характеризуються спірною суспільною небезпечністю та не потребують заходів кримінально-правового впливу. А з другого – ми не маємо права ігнорувати такі кримінально-протиправні діяння (на кшталт несанкціонованого втручання в роботу інформаційних та інших подібного роду систем та мереж відповідно до ч. 1 ст. 361 КК,

що не спричинило певних суспільно небезпечних наслідків). Таке твердження базується на розумінні суспільної небезпечності, закладеному у ч. 2 ст. 11 КК. З тлумачення даної норми доходимо висновку, що суспільною небезпечністю характеризуються діяння, як такі, що реально заподіюють шкоду охоронюваному законом суспільним відносинам, так і ті, що можуть її заподіяти (шкоду потенційну). А тому формальні склади «комп'ютерних» кримінальних правопорушень теж обґрунтовано мають право на існування в світлі їх суспільної небезпечності, ба більше, деякі з них передбачені у міжнародних договорах (до цього ще повернемося на сторінках цієї роботи).

Значно важливішим в контексті наукового дискурсу з'ясувати, а що саме є визначальним для розуміння певного кримінального правопорушення як «комп'ютерного». Припускаємо, що це родовий об'єкт означеної групи кримінальних правопорушень (передбачених розділом XVI Особливої частини КК), і заподіяння йому реальної чи потенційної шкоди. Як зазначалося нами раніше, таким родовим об'єктом виступають інформаційні відносини, засобами забезпечення нормального функціонування яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку. Подібну позицію обстоює й В. І. Борисов, стверджуючи, що родовим об'єктом кримінальних правопорушень, відповідальність за які визначена у розділі XVI Особливої частини КК, варто визнавати суспільні відносини у сфері належного використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку¹. Щоправда, низка науковців, серед яких М. І. Панов та О. Е. Радутний зазначає, що родовим об'єктом кримінальних правопорушень, визначених у аналізованому розділі КК, є інформаційна безпека у сфері використання електронно-обчислювальних машин (комп'ютерів), їх систем чи

¹ Борисов В. І. Щодо родового об'єкта кримінальних правопорушень, передбачених розділом XVI Особливої частини КК України. *Інформаційна агресія в сучасному світі: правовий аналіз та протидія*: матеріали всеукр. наук-практ. кругл. столу (Харків, 21 черв. 2024 р.) : електрон. наук. вид. / редкол.: В. С. Батиргареева та ін. Харків: Майдан, 2024. С. 123.

комп'ютерних мереж та мереж електровз'язку¹. Зупинимось на цьому детальніше.

Проблема визначення змісту інформаційної безпеки була предметом дослідження багатьох вчених із різних галузей правничої науки². Помітне домінування широкого підходу до її визначення. Як квінтесенцію широкого розуміння інформаційної безпеки, наведемо твердження О. О. Золотар. Дослідниця пише, що інформаційна безпека – це стан і процес захищеності людини від інформаційних загроз і викликів, що забезпечує можливість людини як біологічного організму і соціальної істоти функціонувати, розвиватись, задовольняти свої потреби і досягати бажаних для себе результатів в інформаційному суспільстві³.

Стосовно кримінально-правового розуміння інформаційної безпеки А. В. Ландіна на підставі аналізу наукового доробку вчених-криміналістів з цього питання справедливо помічає, що на сьогодні в кримінально-правовому дискурсі поняття «інформаційна безпека» переважно використовується в надто вузькому значенні: як захищеність від витоку відомостей, що містять державну таємницю. Швидше за все, це пов'язано з тим, що у КК термін «інформаційна безпека» вживається лише у ч. 1 ст. 111 КК «Державна зрада» і розуміється як витік інформації, що становить державну таємницю⁴. Однак, все ж таки у контексті норм розділу XVI Особливої частини КК нами підтримується точка зору В. І. Борисова, який вважає інформаційну безпеку відповідно до змісту певних діянь, зазначених у нормах

¹ Панов М. І., Радутний О. Е. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж і мереж електровз'язку. *Кримінальне право України: Особлива частина: підручник* / за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., перероб. і допов. Харків: Право, 2020. С. 550.

² Наприклад, виокремлюють, щонайменше, вісім підходів до розуміння інформаційної безпеки (див. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. *Інформаційна безпека України в умовах євроінтеграції: навч. посіб.* Київ: КНТ, 2006. С. 33).

³ Золотар О. О. Поняття та зміст категорії «інформаційна безпека людини». *Інформація і право*. 2021. № 1 (36). С. 77.

⁴ Ландіна А. В. Інформаційна безпека як об'єкт злочину. *Правова держава*. 2016. Вип. 27. С. 357.

цього розділу КК, предмета посягання та шкоди, що спричиняється використанню електронно-інформаційним технологіям, додатковим обов'язковим об'єктом.¹ Лише додамо, що вирішальним судженням на обґрунтування саме такого бачення інформаційної безпеки як родового об'єкта «комп'ютерних» кримінальних правопорушень є зміщення акцентів концепції «інформаційна безпека – стан захищеності» в значно вужче її розуміння. Йдеться про опосередкованість розуміння інформаційної безпеки, здебільшого, крізь призму суспільних відносин із безпечного використання електронно-інформаційних технологій для створення, передачі, зберігання, обробки та відображення інформації за допомогою комп'ютерів, систем, комп'ютерних мереж і мереж електровз'язку.

В контексті примітивізації протидії «комп'ютерним» кримінальним правопорушенням на окрему увагу заслуговує і таке питання: як можна пояснити, що відповідно до даних Офісу Генерального прокурора, починаючи з 2017 до 2023 року кількість обвинувальних матеріалів, надісланих до суду за Розділом XVI Особливої частини КК, зростає від 1015 до 2455, а відповідно до даних Державної судової адміністрації кількість осіб, засуджених за «комп'ютерні» кримінальні правопорушення, у той самий період змінилася від 42 до 95 (рис. 1). Виявлена аномалія даних безсумнівно потребує самостійного дослідження, проте найбільш обґрунтовано видається така гіпотеза: розбіжність даних зумовлена особливостями статистичного обліку. У випадку сукупності кримінальних правопорушень Державна судова адміністрація України (ДСА) обліковує судові рішення за найтяжчим обвинуваченням. У подібних випадках Офіс Генерального прокурора обліковує всі обвинувальні матеріали. Ураховуючи зазначене, поясненням аномалії даних може бути припущення про те, що звинувачення в незаконних діях з інформаційними технологіями у переважній більшості супроводжуються звинуваченнями в більш тяжких кримінальних правопорушеннях (шахрайство, вимагання тощо). Тому в статистичних звітах Офісу Генерального

¹ Борисов В. І. Вибрані твори. Кн. 2 / уклад.: М. В. Шепітько, О. О. Пашенко, Д. П. Євгєєва,; відп. за вип. М. В. Шепітько. Харків: Право, 2023. С. 460.

прокурора відповідні обвинувальні матеріали фіксуються, а в звітах ДСА – ні. Така гіпотеза потребує подальшої перевірки, але якщо вона підтвердиться, цілком слушним буде провокаційне, але лише на перший погляд, питання: «Може, настав час замислитися, чи існують насправді «комп'ютерні» кримінальні правопорушення?». 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, ці питання потребують самостійного дослідження, однак їх актуальність є значною, особливо в контексті проблеми ефективного використання соціальних ресурсів для протидії злочинності.

Розв'язання означеної проблеми головним чином визначає перспективні напрями розвитку кримінально-правового регулювання в сфері використання інформаційних технологій.

По-перше, одним з чинників примітивізації протидії «комп'ютерним» кримінальним правопорушенням є відсутність у їх законодавчих визначеннях чітких критеріїв суспільної небезпечності. Через це до сфери впливу кримінальної юстиції потрапляють не тільки діяння, які дійсно є суспільно небезпечними, але й ті, які такими не є (проведене дослідження судової практики дозволяє стверджувати, що більше половини судових рішень відповідної категорії (64%) пов'язані з кваліфікацією таких діянь, віднесення яких до суспільно небезпечних є досить спірним). Тож обґрунтованим, на нашу думку, буде встановлення кримінальної відповідальності не просто за несанкціонований доступ або, наприклад, за знищення інформації, а за такий (доступ), що є суспільно небезпечним: заподіяв істотну шкоди або обґрунтовано реальну можливість її заподіяння (потенційна шкода) тим суспільним відносинам, в межах яких використовуються інформаційні технології, за умови, що вчинене особою кримінально-протиправне діяння посягає на суспільні відносини, які включені до родового та (у певних випадках) обов'язкового додаткового об'єктів.

По-друге, норми Розділу XVI Особливої частини КК містять терміни, які неоднаково визначаються як на рівні законодавства, так і на рівні наукового тлумачення. Невиправданим видається формулювання кримінально-правових заборон на основі двох майже схожих переліків засобів технічної обробки інформації (автоматизована система, електронно-обчислювальна машина, інформаційна система тощо). Такий підхід не тільки створює небезпеку «технологічної залежності» законодавства, але й ускладнює його використання. Замість складних та неоднозначних переліків технічних засобів в подальшому є сенс використовувати більш широке поняття. Таким може бути поняття «комп'ютерна система», що визначається у ратифікованій Україною Конвенції про кіберзлочинність¹.

По-третє, заборона, передбачена ст. 361² КК є очевидно надлишковою. Вона передбачає відповідальність за діяння, які не можна визнавати суспільно небезпечними в контексті інших норм щодо відповідальності за незаконні дії з інформацією з обмеженим доступом. Основна проблема кримінально-правової охорони відносин інформаційної безпеки в сфері забезпечення доступу до інформації полягає у надмірній кількості кримінально-правових заборон у даній сфері. Предметом значної кількості кримінальних правопорушень, передбачених чинним КК, є інформація з обмеженим доступом, об'єктивна сторона таких посягань полягає у різноманітних формах порушення обмеженого доступу до такої інформації. До таких кримінальних правопорушень можна віднести: державну зраду (ст. 111 КК); шпигунство (ст. 114 КК); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132 КК); незаконне розголошення лікарської таємниці (ст. 145 КК); порушення таємниці голосування (ст. 159 КК); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163

¹ Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. *Верховна Рада України. Законодавство України*: офісний вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2824-15#Text> (дата звернення 30.08.2024 р.).

КК); розголошення таємниці усиновлення (удочеріння) (ст. 168 КК); порушення недоторканності приватного життя (ст. 182 КК); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК); розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках (ст. 232 КК); незаконне використання інсайдерської інформації (ст. 233 КК); розголошення державної таємниці (ст. 328 КК); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361² КК) тощо.

Існування такої кількості окремих норм для різних видів інформації з обмеженим доступом є невиправданим і таким, що потребує оптимізації. Способом розв'язання даної проблеми може бути заміна наявних у КК спеціальних заборон однією спеціальною. Або використання тих чи інших норм КК у цьому випадку доцільно визначати не за видом інформації з обмеженим доступом, а за спричиненою або потенційною шкодою. У контексті «комп'ютерних» кримінальних правопорушень (розділ XVI Особливої частини КК), передусім, така шкода завдається (або потенційно може бути завдана) родовому (у певних випадках – й обов'язковому додатковому) об'єктам даної групи кримінальних правопорушень.

Цікавим, оригінальним і, без сумніву, перспективним варіантом хоча б часткового розв'язання проблеми примітивізації протидії «комп'ютерним» кримінальним правопорушенням є підготовлений Робочою групою з питань розвитку кримінального права під керівництвом проф. Ю. В. Бауліна проєкт КК (далі – проєкт) (станом на 01.08.2024 р.)¹. Свою основну увагу приділимо розділу 7.7 проєкту «Кримінальні правопорушення проти безпеки інформаційних систем». На нашу думку, пропоновані у цьому розділі проєкту норми виступають наразі неофіційною (з метою наукового пошуку) альтер-

¹ Текст проєкту нового Кримінального кодексу України: контрольний текст (станом на 01.08.2024). *Робоча група з питань розвитку кримінального права*: веб-сайт. URL: <https://newcriminalcode.org.ua/criminal-code> (дата звернення: 30.10.2024).

нативою нормам нині чинного розділу XVI Особливої частини КК. Розділ 7.7 проекту складається з шести статей, з яких одна розкриває терміни, вжиті в цьому Розділі, ще одна наводить ознаки, що підвищують тяжкість злочину (саме злочину, оскільки у нормах даного розділу проекту проступки відсутні), а також міститься чотири види злочинів.

Як помітно, родовим об'єктом пропонованої групи злочинів, розробники вважають «безпеку інформаційних систем». Робоча група визначила родове поняття інформаційної системи через перерахування цих систем, безпека яких охороняється цим розділом від несанкціонованих діянь: інформаційна (автоматизована), електронна комунікаційна, інформаційно-комунікаційна системи, а також електронна комунікаційна мережа¹. Вважаємо, що застосування такого підходу вже є кращим, аніж чинна редакція відповідного розділу КК, оскільки, по-перше, помітно «приведення до спільного знаменника» абсолютно різнорідних понять, таких як «комп'ютер», «автоматизована система», «електронно-комунікаційна мережа» та «мережа електрозв'язку», хоча змістовно це все ще не відповідає терміну «комп'ютерна система», вжитому у Конвенції про кіберзлочинність. По-друге, виглядає цілком обґрунтованим відмова у проекті (порівняно з попередніми редакціями того ж проекту) від формалізації інформаційної безпеки як родового об'єкта злочинів, що передбачені даним розділом проекту. Зокрема, як зазначає М. А. Рубашенко, розділ 7.7 проекту де-факто передбачає відповідальність лише за посягання на інформаційну безпеку в першому (вузькому, технічному) аспекті її розуміння. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. (ратифікована Україною) фактично всі, вказані в розділі 7.7. проекту, діяння), щоправда, в більш узагальненому форматі, відносить до кіберзлочинів I групи – правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Саме такий вузький зміст інформаційної безпеки закла-

¹ Проект нового Кримінального кодексу України: передумови розробки, концептуальні засади, основні положення: монографія / П. П. Андрушко, О. С. Бакумов, Ю. В. Баулін та ін.; за заг. ред. Ю. В. Бауліна, М. І. Хавронюка. Київ: ВАІТЕ, 2024. С. 322.

дається і в міжнародних стандартах ISO/IEC сімейства 27000, присвяченим різноманітним питанням забезпечення інформаційної безпеки. Згідно ISO/IEC 27000:2014 (E), під інформаційною безпекою розуміється збереження конфіденційності, цілісності та можливості застосування інформації. А отже, підсумовує автор, не варто надавати «інформаційній безпеці» в матеріальному кримінальному праві такого ж обмеженого (вузького) трактування, що охоплює лише один із її аспектів¹.

Побічний аналіз інших положень проекту дозволив виявити ще одну прогресивну відмінність останнього порівняно з чинним КК. Вона полягає в тому, що норми проекту надали формальну (поки що, звісно, неофіційну) можливість провести розмежування, що є кіберзлочинами у вузькому розумінні, тобто «комп'ютерними» кримінальними правопорушеннями, чи кіберзлочинами у широкому розумінні (за аналогією з вище згаданими прикладами крадіжки чи шахрайства, вчинені способом отримання доступу до інформаційної системи банку або норми, що встановлює відповідальність за розголошення таємниці усиновлення, як правопорушення проти доступу до інформації). Таке розмежування базується на тому, що кіберзлочинами у широкому розумінні згідно з нормами проекту доцільно вважати більшість тих, в яких є вказівка на спосіб вчинення («із використанням інформаційної системи»). Так, наприклад, використання інформаційної системи є ознакою, яка підвищує тяжкість злочину проти режиму таємниці інформації, що належить державі (ст. 9.2.1 проекту). Не заглиблюючись до розгляду кожного з таких перспективних видів кримінальних правопорушень, в яких формалізований даний спосіб, а також «винісши за дужки» їх родові об'єкти, відмітимо, що таким чином значно зменшиться кількість випадків кваліфікації діянь за сукупністю із «чисто» «комп'ютерними» кримінальними правопорушеннями, підкресливши особливі специфічні риси останніх.

До перспективних напрямів розвитку кримінально-правового регулювання в сфері використання інформаційних технологій слід

¹ Рубашенко М. А. Кримінальні правопорушення проти інформаційної безпеки: нотатки на берегах Проекту нового КК. *Наук. вісн. НДІ проблем досудового розслідування*. 2023. № 2. С. 11.

віднести й забезпечення готовності соціуму до злочинного використання новітніх технологій. Йдеться, в першу чергу, про віртуальні активи та штучний інтелект.

Готовність до використання *віртуальних активів* для вчинення кримінальних правопорушень. Головний аспект у даному питанні – незавершеність правового регулювання використання віртуальних активів на національному рівні (прийнято відповідний закон, але він набере чинності після внесення змін до Податкового кодексу). За умови, що «розмітку» правового поля не завершено, відбувається фактичне використання віртуальних активів для вчинення кримінальних правопорушень. Тільки за даними станом на листопад 2021 р. зафіксовано таку кількість кримінальних правопорушень, що кваліфіковано за статтями розділу XVI Особливої частини КК, предметами яких виступали віртуальні активи: за ст. 361 КК – 2; за ст. 361¹ КК – 12; за ст. 361² КК – 1¹.

Існує певний вакуум щодо визначеності дій правоохоронців у випадку вилучення віртуальних активів, визначення їх вартості в національній валюті, збереження після вилучення тощо. Організаційно-технічне забезпечення вказаних процесів за нашою оцінкою є недостатнім. Тому факти злочинного використання криптовалюти з великою вірогідністю не отримують належного реагування. Наприклад, вилучення криптовалюти доцільно організовувати як транзакцію на електронний гаманець, що контролюється правоохоронним органом. Водночас порядок створення таких гаманців, документування цього процесу поки не отримали нормативного регулювання.

Істотні зміни «комп'ютерної» злочинності пов'язують з розповсюдженням технологій *штучного інтелекту* (далі – ШІ)². Обґрун-

¹ Власенко С. О. Кримінологічні аспекти використання криптовалюти під час вчинення кримінальних правопорушень. *Юридичний науковий електронний журнал*. 2021. № 11. С. 561.

² Див.: Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. Харків. 2023. Вип. 46. С. 21–31.

тованим є прогноз їх широкого використання для злочинних цілей¹. Сучасна міжнародна дискусія щодо правового регулювання соціалізації ШІ характеризується більшою увагою до практичних та прикладних проблем. Правове регулювання використання технологій ШІ розглядається одночасно як засіб мінімізації ризиків та засіб стимулювання позитивних економічних трансформацій.

Існує потреба правового регулювання використання систем ШІ в Україні. В першу чергу, для обмеження сфери нормативного впливу та структурування національного юридичного та технічного дискурсів, необхідне нормативне визначення систем штучного інтелекту. Далі, наслідуючи європейський підхід, доцільним буде здійснення класифікації систем штучного інтелекту за ступенем ризику, формулювання для кожного виду пропорційних можливим небезпекам нормативних вимог до розробки та використання. Регулювання використання систем ШІ національними правоохоронними органами має відбуватися у спосіб формулювання спеціальних норм до загальних правил, які названі вище. Водночас, використання технологій ШІ національними правоохоронними органами без чітких та зрозумілих законодавчих положень про можливі обмеження приватності громадян, створює реальну небезпеку визнання діяльності правоохоронців незаконною навіть за формальною ознакою (не «відповідно до закону»)². Обов'язковому і першочерговому врахуванню під час впровадження практик ШІ підлягає Регламент (UE) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, який встановлює гармонізовані правила щодо ШІ³. Серед положень Ре-

¹ Artificial Intelligence in the Context of Crime and Criminal Justice: report for the Korean Institute of Criminology / B. Dupont, Y. Stevens, H. Westermann, M. Joyce. Canada : Université de Montréal, 2019. P. 33–37. URL: https://www.researchgate.net/publication/337402608_Artificial_Intelligence_in_the_Context_of_Crime_and_Criminal_Justice (дата звернення: 04.05.2024).

² Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. *Питання боротьби зі злочинністю*. Харків. 2023. Вип. 46. С. 29.

³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No 168/2013, (EU) 2018/858,

гласменту – класифікація систем ШІ відповідно до ризику, який вони можуть створити, і способи використання таких систем.

Нарешті, одним із найважливіших питань у сфері законодавчого забезпечення протидії кримінальним правопорушенням у сфері використання інформаційних технологій є гармонізація національного законодавства з положеннями норм міжнародного права. Розвиток сучасних систем телекомунікації та комп'ютерних мереж призвів до такої ситуації, коли протидія цим злочинам не може бути достатньо ефективною, якщо вона здійснюється в межах однієї країни¹. Так званий кіберпростір не має державних кордонів. Наприклад, особа, котра вчиняє несанкціонований доступ до комп'ютерної інформації, необов'язково має перебувати в тій країні, де фізично розташований носій цієї інформації. Автор комп'ютерного вірусу може розмістити його на популярному сайті в мережі Інтернет, що призведе до його розповсюдження у великій кількості країн. Усе це вимагає узгодження національних кримінальних законодавств та створення єдиного правового простору для забезпечення ефективного захисту від злочинних посягань, пов'язаних з використанням комп'ютерної техніки.

Не можна не помітити, що розробка згаданого вже Проєкту КК (в контексті кримінальних правопорушень проти безпеки інформаційних систем) в аспекті підготовки до формальної гармонізації на рівні чинного КК, справляє позитивне враження. По-перше, для прикладу, у розділі 7.7 Проєкту гармонізовано більшість термінології відповідно до Конвенції про кіберзлочинність (вжито термін «комп'ютерні дані» у ст.ст. 7.7.4 та 7.7.5 Проєкту тощо). По-друге, ознаки незаконного доступу до інформаційної системи, що полягає в діяннях особи щодо незаконного отримання доступу до інформаційної системи або її частини (ст. 7.7.3) та незаконного перехоплен-

(EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *EUR-lex*: of. website. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 (дата звернення 30.10.2024 р.).

¹ Орлов Ю. Ю. Реалізація вимог міжнародної Конвенції про кіберзлочинність у законодавстві України. *Наук. вісн. Нац. акад. внутр. справ*. 2011. № 6. С. 3–9.

ня комп'ютерних даних (під час їх виходу з інформаційної системи, надходження до інформаційної системи або під час операції з ними всередині інформаційної системи) (ст. 7.7.4) Робоча група сформулювала, зокрема, з урахуванням вимог Директиви 2013/40/ЄС щодо атак на інформаційні системи¹. По-третє, досліджуючи Конвенцію про кіберзлочинність, маємо також зауважити, що національне кримінальне законодавство прямо не передбачає відповідальності за такі дії, як: 1) навмисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст.ст. 2–5 Конвенції; 2) володіння пристроями, включаючи комп'ютерні програми, створені або адаптовані насамперед з метою вчинення будь-якого зі злочинів, перелічених у ст.ст. 2–5 Конвенції, або комп'ютерними паролями, кодами доступу або подібними даними, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст.ст. 2–5 Конвенції, з наміром використання зазначених предметів для вчинення будь-якого зі злочинів, перерахованих у ст.ст. 2–5².

Натомість відмітимо, що ст. 7.7.6 проєкту вже пропонує відповідальність за незаконні дії зі шкідливим програмним чи технічним

¹ Проєкт нового Кримінального кодексу України: передумови розробки, концептуальні засади, основні положення: монографія / П. П. Андрушко, О. С. Бакумов, Ю. В. Баулін та ін. ; за заг. ред. Ю. В. Бауліна, М. І. Хавронюка. Київ: ВАІТЕ, 2024. С. 323.

Детальніше про перспективи врахування положень зазначеної Директиви у чинному КК України та відповідності положень останнього цій Директиві див.: Пономаренко Ю. А. Директива Європейського парламенту і Ради № 2013/40/EU і національне кримінальне право України. *Національна безпека України в умовах інформатизації глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання*: матеріали VII Міжнар. наук.-практ. конф. (Харків, 11 трав. 2023 р.). Харків: Право, 2023. С. 35–41.

² Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки: монографія: електрон. наук. вид. / за заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька. Харків: Право, 2023. 152 с.

засобом або шкідливими даними (даними доступу), надаючи визначення зазначених предметів кримінально-протиправних діянь, так і перелік діянь щодо них.

Проведене нами дослідження дозволяє зазначити: 1) у цілому національне законодавство відповідає ратифікованим міжнародним нормативно-правовим актам; 2) є підстави казати про окремі випадки надлишкової ратифікації, яка зобов'язує на рівні національного законодавства визнавати кримінальними правопорушеннями діяння, які характеризуються спірною суспільною небезпечністю; 3) подальша робота щодо вдосконалення чинного законодавства потребує, зокрема, внесення нових застережень до Закону України «Про ратифікацію Конвенції про кіберзлочинність». Внесення таких застережень дозволить забезпечити виконання принципу міжнародно-правової необхідності та допустимості криміналізації при внесенні змін до КК.

Висновки до розділу III

1. Дослідження показало, що «комп'ютерні» кримінальні правопорушення доцільно 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.

2. Аналіз судової практики дозволив виявити серед кримінальних правопорушень в сфері використання інформаційних технологій дві основні групи за специфікою використовуваних засобів кримінально-правового реагування. Перша група характеризується переважним використанням реальних покарань (67–69%) у вигляді штрафів та частим укладанням угод про визнання винуватості (69–79%). Ця група охоплює правопорушення, передбачені статтями 361¹ та 361² КК, 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, і становить 72% від загальної кількості обвинувальних вироків.

3. У контексті перспектив кримінально-правового регулювання у сфері інформаційних технологій в фокусі уваги постає проблема

примітивізації протидії «комп'ютерним» кримінальним правопорушенням. Аналіз судової практики показав, що у поле зору кримінальної юстиції переважно потрапляють найпростіші та найменш небезпечні форми «комп'ютерних» кримінальних правопорушень, які часто є лише допоміжними засобами для вчинення інших суспільно небезпечних діянь, наприклад, 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 кримінальних правопорушень, зосередившись на боротьбі з менш небезпечними проявами злочинності. 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 і забезпечення кібербезпеки.

4. Розв'язання проблеми примітивізації протидії «комп'ютерним» кримінальним правопорушенням визначає кілька перспективних напрямів вдосконалення законодавства:

- встановлення чітких критеріїв суспільної небезпечності та врахування ознак обов'язкового додаткового об'єкта. Для цього необхідно:
 - а) конкретизувати законодавчі визначення «комп'ютерних» кримінальних правопорушень, передбачити вказівки на заподіяння істотної шкоди (або в процесі правозастосування окремих норм обґрунтовувати реальну можливість її заподіяння) суспільним відносинам, в межах яких використовують інформаційні технології (родовому об'єкту «комп'ютерних» кримінальних правопорушень);
 - б) при кваліфікації кримінального правопорушення як «комп'ютерного» (передбаченого розділом XVI Особливої частини КК) слід враховувати, що певні діяння мають свій обов'язковий додатковий об'єкт – інформаційну безпеку (у її розумінні як збереження конфіденційності, цілісності та можливості застосування інформації). Наведені положення дозволять уникнути криміналізації діянь,

які або не становлять реальної чи потенційної загрози, зосередившись на більш небезпечних правопорушеннях, або таких, об'єкти яких не відповідають родовому та обов'язковому додатковому об'єктам «комп'ютерних»;

- вдосконалення змісту правових норм. Варто спростити норми розділу XVI Особливої частини КК шляхом заміни складних переліків технічних засобів більш узагальненим поняттям «комп'ютерна система». Це зменшить технологічну залежність законодавства та спростить його застосування;
- перегляд та оптимізація норм щодо інформації з обмеженим доступом. Доцільно передбачити одну загальну норму, яка регламентувала б відповідальність за порушення обмеженого доступу до інформації, незалежно від її виду. Суворість покарання має визначатися заподіяною (або потенційною) шкодою, а не видом інформації.

5. Положення проекту КК (розділ 7.7. «Кримінальні правопорушення проти безпеки інформаційних систем») визнаємо такими, що, більшою мірою, спрямовані на подолання проблеми примітивізації «комп'ютерних» кримінальних правопорушень, та здатні в перспективі забезпечити більш уніфікований та зрозумілий підхід до кримінально-правової охорони інформаційної безпеки.

6. Існує проблема недостатньої готовності до протидії злочинному використанню віртуальних активів. Правове регулювання їх обігу незавершене. Хоча прийнято відповідний закон, його набрання чинності залежить від внесення змін до Податкового кодексу України, що створює правовий вакуум. Це ускладнює дії правоохоронців щодо вилучення, оцінки вартості та збереження віртуальних активів, які можуть використовуватися для вчинення кримінальних правопорушень.

7. Злочинне використання технологій штучного інтелекту стає дедалі більш ймовірним, що вимагає відповідних правових і технічних заходів. Для підготовки до цієї загрози необхідно розробити нормативне визначення систем штучного інтелекту, класифікувати їх за ступенем ризику, а також встановити пропорційні нормативні вимоги для кожного виду систем ШІ. Такий підхід дозволить не тіль-

ки мінімізувати ризики, пов'язані з використанням ШІ, але й стимулювати позитивні економічні перетворення, що виникають у процесі його інтеграції у різні сфери суспільного життя.

8. Формування єдиного міжнародного правового простору є критично важливим для ефективної протидії «комп'ютерним» кримінальним правопорушенням, які не обмежуються територіальними кордонами. Кримінальні правопорушення у кіберпросторі, такі як несанкціонований доступ до інформації чи розповсюдження комп'ютерних вірусів, можуть мати глобальний характер, що вимагає узгодження національних законодавств та співпраці на міжнародному рівні. Для України важливо забезпечити гармонізацію національного законодавства (зокрема, як норм чинного КК, так і нинішнього перспективного проекту КК) з міжнародними стандартами, що сприятиме створенню ефективної системи захисту від кіберзагроз.

Розділ IV

ІНФОРМАЦІЙНІ КРИМІНАЛЬНО-ПРОТИПРАВНІ ДІЯННЯ, ЩО ПОСЯГАЮТЬ НА МИР, БЕЗПЕКУ ЛЮДСТВА ТА МІЖНАРОДНИЙ ПРАВОПОРЯДОК

Вступні положення

Злочинами, що посягають на мир безпеку, людства та міжнародний правопорядок (міжнародні злочини) прийнято вважати злочини агресії (ст. 437 КК) та геноциду (ст. 442 КК), воєнні злочини (ст. 438 КК) та проти людяності (ст. 4421 КК). Їх зазвичай визначають «ядром» («core») міжнародних злочинів та «звірствами» («atrocities crimes»)¹. Норми, що містяться у зазначених статтях, розкриваються шляхом звернення до міжнародних конвенцій² та звичаєвого міжнародного гуманітарного права.

Важливу частину цих міжнародних злочинів складають інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок. Інформаційний вплив, спрямований на готування до війни, пришвидшує та робить реальним перехід від мирного співіснування народів та окремих національних, етнічних, расових, релігійних та політичних груп до ворожості, ненависті, збройних конфліктів та стану війни. Це призводить до численних жертв серед цивільного населення, знищення інфра-

¹ International Crimes. Open Society Justice Initiative. URL: <https://www.justiceinitiative.org/publications/international-crimes>

² Гаазькі конвенції 1899 та 1907 рр., Конвенція про запобігання злочину геноциду та покарання за нього 1948 р., Женевські конвенції 1949 р. та додаткові протоколи до них, Гаазька конвенція про захист культурних цінностей у випадку збройного конфлікту 1954 р. та протоколи до неї, Римський статут Міжнародного кримінального суду та ін.

структури, культурних цінностей, жертв серед військових та серйозних гуманітарних та політичних криз континентального та світового масштабу.

До інформаційних кримінально-протиправних посягань на мир, безпеку людства та міжнародний правопорядок можна віднести такі діяння:

- 1) пропаганда війни (ст. 436 КК);
- 2) виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436¹ КК);
- 3) виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436² КК);
- 4) публічні заклики до геноциду (ч. 2 ст. 442 КК);
- 5) незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала (ст. 445 КК);
- 6) окремі види злочину агресії (ст. 437 КК) та воєнних злочинів (ст. 438 КК) за умови їх вчинені з використанням інформації.

Особливістю цих інформаційних дій є використання інформації державою-агресором (суб'єктами, що діють від її імені) для уведення свого населення в оману, підбурювання своїх військовослужбовців до вчинення злочинних дій проти цивільних країни, щодо якої здійснено напад. Особливе місце становить інформація як предмет цих кримінальних правопорушень, що перекручується, приховується, незаконно змінюється, як і використовується для доведення погроз. Передавання такої інформації пришвидшується засобами масової інформацією, через Інтернет, соціальними мережами та іншими каналами зв'язку. На сьогодні інформація все частіше є цифровою, неофіційною та неперевіреною. Таким чином, жертвами від інформаційної (гібридної) війни та застосованого незаконного інформаційного впливу (фактично психічного насильства) стає все більше коло осіб.

У науковій літературі інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок досліджувалися у працях В. Базова, О. Житного,

К. Задой, Р. Лемкіна, В. Миронової, Р. Мовчана, С. Моханчука, О. Наден, Е. Поллманн, В. Поповичук, М. Рубашенка, О. Сенаторової, Ж.-М. Хенкертс та інших.

У цьому розділі монографії здійснено аналіз кримінального законодавства та супутніх нормативно-правових актів, які допомагають розкрити ознаки вищеназваних кримінальних правопорушень, міжнародно-правових актів, законів та звичаїв війни, практики міжнародних та національних судів. Звернено увагу на проблеми та перспективи кваліфікації інформаційних кримінально-протиправних діянь, що посягають на мир, безпеку людства та міжнародний правопорядок. Наведені посилання на рішення Міжнародних трибуналів в Нюрнберзі, щодо Руанди та діяльності Міжнародного кримінального суду (Гаага) стосовно засудження воєнних злочинців.

4.1. Інформаційні кримінально-протиправні діяння, що посягають на мир шляхом поширення пропаганди, виправдовування та глорифікації тоталітарних режимів та їх представників (ст.ст. 436, 436¹, 436² КК України)

Кримінальні правопорушення, що посягають на мир, безпеку людства та міжнародний правопорядок, є одними із найтяжчих злочинів, передбачених Кримінальним кодексом України, оскільки вони загрожують фундаментальним принципам міжнародного права, спричиняють масові страждання та руйнування, підривають стабільність держав і можуть мати катастрофічні наслідки для всього людства. Серед зазначених кримінальних правопорушень є декілька, що становлять загрозу інформаційній безпеці держави. Зокрема, до їх переліку слід віднести: пропаганду війни (ст. 436 КК), виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436¹ КК) та виправдовування, визнання право-

мірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436² КК).

Ці кримінальні правопорушення є особливо небезпечними в сучасних умовах інформаційних війн та гібридних загроз, коли деструктивна інформація може швидко поширюватися через засоби масової інформації та соціальні мережі. Вони спрямовані на підрив національної безпеки, дестабілізацію суспільства та маніпуляцію громадською думкою. Тому удосконалення кримінально-правової протидії цим кримінальним правопорушенням є важливим завданням національного кримінального права.

Пропаганда війни (ст. 436 КК). Пропаганда війни як явище інформаційного простору є невід'ємною частиною всіх сучасних збройних конфліктів. З часів появи засобів масової інформації будь-яка держава, що планує акт агресії або агресивну війну, активно використовує наявні інформаційні ресурси для мілітаризації населення, виправдання необхідності вторгнення на територію іншої країни, демонізації країни-жертви та її збройних сил, глорифікації цілей та учасників майбутньої збройної агресії, маргіналізації антивоєнних настроїв та політичних опонентів у країні. На сьогодні пропаганда війни виступає важливим засобом підготовки до агресії й саме тому справедливо вважається провісником війни.

Водночас пропагандувати війну може не тільки держава. До такої пропаганди часто вдаються деякі радикальні політичні партії, організації й окремі особи з метою підвищення свого політичного рейтингу та приходу до влади. Такі суб'єкти використовують образ певної країни чи нації як ворога та ідею війни з нею для консолідації суспільства навколо своєї персони або організації. У майбутньому, після приходу до влади цих осіб чи організацій, сам акт агресії стає лише справою часу. Таким чином, пропаганда війни виступає ще й інформаційним засобом досягнення політичних цілей.

Міжнародне співтовариство врахувало досвід світових війн та з метою підтримання миру, безпеки людства та міжнародного правопорядку заборонило не тільки розв'язання агресивної війни чи воєнного конфлікту, нападу збройних сил держави на терито-

рію іншої держави, анексію із застосуванням сили, але й пропаганду війни. Так, заборона останньої в прямій чи непрямій формі міститься у багатьох міжнародно-правових документах, зокрема, у Міжнародній конвенції про використання радіомовлення в інтересах миру 1936 р. (ст.ст. 2 та 3)¹, Резолюції Генеральної Асамблеї ООН № 110 «Заходи проти пропаганди та підбурювання до нової війни» 1947 р.², Резолюції Генеральної Асамблеї ООН № 127 (II) «Неправдива або перекручена інформація» 1947 р.³, Конвенції про міжнародне право спростування 1952 р. (преамбула)⁴, Декларації про принципи міжнародного права, що стосуються дружніх відносин і співробітництва між державами 1970 р.⁵, Декларації про право народів на мир 1984 р.⁶ та деяких інших. Так, у Міжнародному пакті про громадянські та політичні права 1966 р.⁷ зазначено, що

¹ Міжнародна конвенція про використання радіомовлення в інтересах миру: Міжнародний документ від 23.09.1936. *PRO. Платформа ефективного регулювання*: вебсайт. URL: <https://regulation.gov.ua/documents/id211299> (дата звернення: 01.10.2024).

² Резолюція Генеральної Асамблеї ООН № 110 «Заходи проти пропаганди та підбурювання до нової війни»: Міжнародний документ від 03.11.1947. *ZakonOnline*: вебсайт. URL: https://zakononline.com.ua/documents/show/140896__140896 (дата звернення: 01.10.2024).

³ Резолюція Генеральної Асамблеї ООН № 127 (II) «Неправдива або перекручена інформація»: Міжнародний документ від 15.11.1947. *Zakon.cc: вебсайт*. URL: https://zakon.cc/law/document/read/995_275 (дата звернення: 01.10.2024)

⁴ Конвенція про міжнародне право спростування: Міжнародний документ від 16.12.1952. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_319#Text (дата звернення: 01.10.2024).

⁵ Декларація про принципи міжнародного права, що стосуються дружніх відносин і співробітництва між державами: Міжнародний документ від 24.10.1970. *ООН*: оф. вебсайт. URL: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата звернення: 01.10.2024).

⁶ Декларація про право народів на мир: Міжнародний документ від 12.11.1984. *ООН*: оф. вебсайт. URL: https://www.un.org/ru/documents/decl_conv/declarations/right_to_peace.shtml (дата звернення: 01.10.2024).

⁷ Міжнародний пакт про громадянські та політичні права: Міжнародний документ від 16.12.1966. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 01.10.2024)

будь-яка пропаганда війни повинна бути заборонена законом (п. 1 ст. 20).

Україна імплементувала міжнародну заборону пропаганди війни в багатьох актах національного законодавства. Відповідно до ч. 1 ст. 28 Закону України від 02.10.1992 р. № 2657-XII «Про інформацію» інформація не може бути використана для закликів до пропаганди війни. До того ж на території України в медіа та на платформах спільного доступу до відео забороняється поширювати заклики до розв'язування або ведення агресивної війни або воєнного конфлікту та інформацію, яка виправдовує чи пропагує такі дії (п. 1 ч. 1 ст. 36 Закону України від 13.12.2022 р. № 2849-IX «Про медіа»). У видавничій справі забороняється випускати у світ, виготовляти та/або розповсюджувати продукцію, що містить матеріали (висловлювання, заклики тощо), зміст яких спрямований на пропаганду війни (ч. 1 ст. 28 Закону України від 05.06.1997 р. № 318/97-ВР «Про видавничу справу»). Окремі заборони на пропаганду війни також містяться у Законах України «Про театри і театральну справу» від 31.05.2005 р. № 2605-IV (ч. 5 ст. 5), «Про охорону дитинства» від 26.04.2001 р. № 2402-III (ч. 1 ст. 30), «Про звернення громадян» від 02.10.1996 р. № 393/96-ВР (ч. 3 ст. 231) тощо. Варто зазначити, що згідно зі ст. 37 Конституції України, забороняється утворення і діяльність політичних партій та громадських організацій, програмні цілі або дії яких спрямовані на пропаганду війни. Зазначена конституційна заборона знайшла своє відображення й у Законах України «Про політичні партії в Україні» від 05.04.2001 р. № 2365-III (ч. 1 ст. 21) та «Про громадські об'єднання» від 22.03.2012 р. № 4572-VI (ч. 1 ст. 4).

Законодавча заборона пропаганди війни в Україні забезпечена й засобами кримінального права. Норма ст. 436 КК передбачає кримінальну відповідальність за публічні заклики до агресивної війни або до розв'язування воєнного конфлікту, а також виготовлення матеріалів із закликами до вчинення таких дій з метою їх розповсюдження або розповсюдження таких матеріалів.

Згідно з даними офіційної кримінально-правової статистики, за останні десять років в Україні обліковано 117 кримінальних право-

порушень за ст. 436 КК¹. З них упродовж 2022 – 2023 рр. обліковано 73 випадки²; засуджено за цей же період – 7 осіб³.

¹ Єдиний звіт про кримінальні правопорушення за січень-грудень 2014 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2015 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2016 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2017 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2018 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2019 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2020 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2021 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-серпень 2024 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>.

² Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>.

³ 2022 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2022; 2023 рік.

Аналіз обвинувальних вироків та наукових публікацій свідчить про наявні теоретичні та прикладні проблеми, що пов'язані із розумінням змісту норми ст. 436 КК та її застосуванням. Їх можна поділити на дві групи: теоретичні, що обумовлені недоліками чинної редакції ст. 436 КК та взагалі доцільністю криміналізації пропаганди війни на національному рівні, та прикладні, які стосуються неправильного тлумачення судами ст. 436 КК та, відповідно, її хибного правозастосування¹.

Проблеми теоретичного рівня.

1. Аналіз положень міжнародного та національного законодавства однозначно засвідчує, що «злочини агресії» (у тому числі й пропаганда війни) існують у двох вимірах: з позиції міжнародного права та внутрішньодержавного кримінального права². Водночас, досліджуючи кримінальне законодавство держав континентальної Європи, М. І. Хавронюк звернув увагу на відсутність у більшості цих країн кримінальної відповідальності за пропаганду війни. Науковець пояснив це тим, що поступово дедалі більше європейських держав визнають юрисдикцію Міжнародного кримінального суду (далі – МКС) і, відповідно, в їх національних кримінальних кодексах зникають положення про відповідальність за міжнародні злочини³. Враховуючи приєднання України до юрисдикції МКС⁴, також вини-

Форма № 7 Звіт про склад засуджених. Судова влада України: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2023.

¹ Це матеріал знайшов відображення у науковій статті (див.: Новикова К. А. Проблеми кримінальної відповідальності за пропаганду війни. Питання боротьби зі злочинністю. редкол.: В. С. Батиргарєєва (голов. ред.) та ін. Харків: Право. 2024. Вип. 47. С. 77-86. URL: <http://pbz.nlu.edu.ua/issue/view/18335>)

² Олійник Х. В. Кримінальна відповідальність за пропаганду, планування, підготовку, розв'язування та ведення агресивної війни: дис. ... докт. філософії 081: Право. Львів, 2022. С. 77.

³ Хавронюк М. І. Кримінальне законодавство України та інших держав континентальної Європи: порівняльний аналіз, проблеми гармонізації: дис. ... д-ра юрид. наук: 12.00.08. Київ, 2007. С. 442.

⁴ Про ратифікацію Римського статуту Міжнародного кримінального суду та поправок до нього: Закон України від 21.08.2024. Верховна Рада України: Законодавство України: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/3909-20#n2> (дата звернення: 01.10.2024)

кає питання доцільності існування кримінальної відповідальності за пропаганду війни на національному рівні.

При вирішенні зазначеного питання слід, по-перше, виходити з того, що пропаганда війни як інформаційно небезпечне явище не тільки посягає на суспільні відносини з охорони миру й мирного співіснування держав і народів, але й має значну суспільну небезпечність для правопорядку всередині країни. Відсутність кримінальної відповідальності за пропаганду війни на національному рівні може призвести до безконтрольного поширення мови міжнародної ворожнечі, що сприятиме підвищенню агресивності й ворожості населення країни щодо певних соціальних груп, верств, національних та інших меншин тощо. Це призведе до соціальних конфліктів в країні та підвищення рівня насильства загалом.

По-друге, Україна має міжнародні зобов'язання щодо протидії пропаганді війни на національному рівні, реалізація яких неможлива без встановлення кримінальної відповідальності за такі дії.

По-третє, криміналізація пропаганди війни на міжнародному рівні є дещо умовною. Пропаганда війни дійсно визнавалася міжнародним злочином проти миру та безпеки людства на рівні спеціалізованих (ad hoc) міжнародних кримінальних трибуналів. Але в Римському статуті МКС такий склад злочину відсутній, про що неодноразово зазначав М. Керні, вказуючи на необхідність доповнення Статуту таким самостійним складом злочину як пряме та публічне підбурювання до агресії або пропаганди війни¹.

З урахуванням вищенаведеного, варто підтримати думку У. З. Коруц щодо хибності практики декриміналізації пропаганди війни, оскільки це створює ризики для уникнення кримінальної відповідальності за такі дії у тому випадку, коли вони не виходять на міжнародний рівень і мають виключно внутрішньодержавний або внутрішньонаціональний характер².

¹ Kearney M. The prohibition of propaganda for war in international law. New York: Oxford University Press, 2007. P. 274.

² Коруц У. З. Заборона пропаганди війни у сучасному міжнародному праві: дис. ... д-ра юрид. наук: 12.00.11. Київ, 2023. С. 88.

2. Деякі дослідники, зокрема, П. В. Пекар, вказують на *невідповідність назви статті 436 КК змісту її диспозиції*, що порівнюючи з іншими кримінально-правовими нормами порушує принцип системності кримінального законодавства¹. Термін «пропаганда війни» дійсно має доволі широке значення, яке не зводиться лише до публічних закликів до агресивної війни або до розв'язування воєнного конфлікту, чи-то виготовлення матеріалів із закликами до вчинення таких дій із метою їх розповсюдження або розповсюдження таких матеріалів. Пропаганда війни як засіб інформаційного впливу включає різноманітні форми підбурювання до застосування збройної сили проти іншої держави або етнічної групи, розпалювання шовіністичних настроїв на підтримку агресії², а також виправдання такої агресії. Це навмисний та цілеспрямований вплив як на окремих осіб та соціальних груп, так і на суспільство загалом із використанням різних каналів поширення інформації.

Публічні заклики – це звернення, що спрямовані на виникнення у частини населення бажання вчинити певні дії. Мета публічних закликів полягає у доведенні до людей певних висловлювань з наміром змінити їх поведінку, схилити до здійснення діяльності чи вчинення дій³. Пропаганда війни не вичерпується лише публічними закликами до агресивної війни чи воєнного конфлікту, які є лише частиною цього явища. Публічні заклики до агресивної війни можна назвати лише однією зі складових системного комплексу дій, спрямованих на формування суспільної думки, а сама пропаганда може мати будь-які інші форми (зокрема, поширення неправдивої інформації; може набувати письмового, усного, електронного виразу тощо)⁴. Крім того, пропаганда є систематичною діяльністю (при-

¹ Пекар П. В. Кримінально-правова характеристика пропаганди війни: автореф. дис. ... канд. юрид. наук: 12.00.08. Київ, 2017. С. 14.

² Шпилик С. Інформаційна війна, пропаганда та PR: такі схожі й такі різні. *Галицький економічний вісник*. 2014. Том 47. № 4. С. 180.

³ Кубальський В. Н. Проблеми кримінальної відповідальності за публічні заклики до вчинення злочинів проти державного суверенітету. *Судова апеляція*. 2018. № 2. С. 67-78.

⁴ Ботнарченко І. А. Актуальні питання кримінальної відповідальності за пропаганду війни в умовах воєнного стану. Проблеми кваліфікації та розслідування кри-

наймні у суб'єкта має бути сформований умисел на повторюваність однаково спрямованих дій), а публічні заклики можуть виступати як одноразова акція¹.

Загалом необхідно погодитися з тим, що назва ст. 436 КК має відповідати диспозиції. У чинній редакції диспозиції норми ст. 436 КК більш коректною буде така її назва: «Публічні заклики до агресивної війни або до розв'язування воєнного конфлікту, виготовлення або розповсюдження матеріалів із такими закликами».

3. Науковці також звертають увагу на *невідповідність диспозиції норми ст. 436 КК термінології міжнародно-правових актів*². Так, у Резолюції 3314 (XXIX) Генеральної асамблеї ООН від 14 грудня 1974 р.³ вживаються терміни «агресія», «акт агресії», «агресивна війна», у Римському статуті МКС⁴ – «акт агресії». Міжнародне гуманітарне право використовує термін «збройний конфлікт». Термін «воєнний конфлікт» не застосовується в міжнародно-правових актах. Його визначення міститься лише на національному рівні у Законі України від 21.06.2018 р. № 2469-VIII «Про національну безпеку України». Відповідно до цього Закону воєнний конфлікт – це форма розв'язання міждержавних або внутрішньодержавних суперечностей із двостороннім застосуванням воєнної сили. Основними видами воєнного конфлікту є війна та збройний конфлікт.

мінальних правопорушень в умовах воєнного стану: матеріали наук.-теорет. конф., м. Київ, 26 трав. 2022 р./ Нац. акад. внутр. справ. Київ, 2022. С. 29. URL: <https://elar.naiu.kiev.ua/server/api/core/bitstreams/f5940194-46fe-4af0-84cf-775451ff2267/content> (дата звернення: 01.10.2024)

¹ Орловська Н. А. Актуальні питання кримінальної відповідальності за пропаганду війни (у світлі законопроекту № 2689). *Держава та регіони. Серія: Право*. 2021. № 4(74). С. 74. URL: http://www.law.stateandregions.zp.ua/archive/4_2021/11.pdf (дата звернення: 01.10.2024)

² Пекар П. В. Кримінально-правова характеристика пропаганди війни: автореф. дис. ... канд. юрид. наук: 12.00.08. Київ, 2017. С. 14.

³ Визначення агресії: Міжнародний документ від 14.12.1974. *ООН*. URL: https://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (дата звернення: 01.10.2024)

⁴ Римський статут Міжнародного кримінального суду: Міжнародний документ від 17.07.1998. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text (дата звернення: 01.10.2024)

Слушною є думка про необхідність відмови від використання терміна «воєнний конфлікт» у ст. 436 КК задля забезпечення єдності термінології та системного підходу до її вживання, а також увідповіднення до норм міжнародного права¹. Крім того, вбачається недоречним і використання терміна «агресивна війна» через його юридичну невизначеність, зумовлену відсутністю розуміння істотних та необхідних ознак цього явища².

Таким чином, в диспозиції норми ст. 436 КК доцільно замінити термін «агресивна війна» на «акт агресії», а термін «воєнний конфлікт» на «збройний конфлікт».

4. Досліджуючи питання караності за пропаганду війни В. П. Пекар доходить до думки про *невідповідність санкції ст. 436 КК ступеню суспільної небезпечності передбаченого нею кримінального правопорушення*. Учений вважає, що висока суспільна небезпечність пропаганди війни, поряд із такими діяннями, як ведення агресивної війни, розв'язування, підготовка, планування тощо, повинна знайти своє відображення в санкції статті. На його думку, максимальна межа покарання у виді трьох років позбавлення волі не відображає підвищеного ступеня суспільної небезпечності, прописаного в різноманітних конвенціях, і має бути збільшена принаймні до п'яти років позбавлення волі при збереженні існуючих альтернативних видів покарання. Такий підхід до збільшення розмірів покарання за пропаганду війни В. П. Пекар обґрунтовує також тим, що за менш суспільно небезпечне діяння, передбачене ст. 436¹ КК («Виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів»), встановлене більш суворе покарання (обмеження волі на строк до п'яти років або позбавлення

¹ Коруч У. З. Заборона пропаганди війни у сучасному міжнародному праві: дис. ... д-ра юрид. наук: 12.00.11. Київ, 2023. С. 325.

² Олійник Х. В. Стан теоретичного дослідження питань кримінальної відповідальності за пропаганду, планування, підготовку, розв'язання та ведення агресивної війни. *Вісник Львівського торговельно-економічного університету. Юридичні науки*. 2019. Вип. 8. С. 121. URL: <https://www.lute.lviv.ua/fileadmin/www.lac.lviv.ua/data/DOI/2616-7611-2019-08-13.pdf> (дата звернення: 01.10.2024)

волі на той самий строк, з конфіскацією майна або без такої), ніж за пропаганду війни¹.

5. Дослідники вказують також на *необхідність закріплення обставин, що обтяжують відповідальність за пропаганду війни у нормі ст. 436 КК*. Зокрема, пропонуються такі обставини, як: вчинення дій, передбачених ч. 1 цієї статті особою, яка є представником влади / службовою особою / службовою особою, яка займає відповідальне становище; повторно; організованою групою; з використанням засобів масової інформації або мереж комунікації². Серед особливо обтяжуючих відповідальність обставин пропонують закріпити вчинення діяння службовою особою, яка займає особливо відповідальне становище³.

На доцільність таких пропозицій вказує й зарубіжний досвід унормування пропаганди війни. Так, кримінальні кодекси інших країн містять такі обтяжуючі кримінальну відповідальність ознаки пропаганди війни: використання засобів масової інформації (ч. 2 ст. 101 КК Азербайджану, ч. 2 ст. 385 КК Вірменії, ч. 2 ст. 405 КК Грузії, ч. 2 ст. 157 КК Казахстану, ч. 2 ст. 396 КК Таджикистану), вчинення злочину службовою особою (ч. 2 ст. 101 КК Азербайджану), вчинення злочину особа-

¹ Пекар П. В. Щодо питання конструювання санкцій за пропаганду війни (ст. 436 КК України). *Верховенство права*. 2017. № 3. URL: <https://sd-vp.info/2017/shhodo-pitannya-konstruuvannya-sanktsij-za-propagandu-vijni-st-436-kk-ukrayini/> (дата звернення: 01.10.2024)

² Ботнарченко І. А. Актуальні питання кримінальної відповідальності за пропаганду війни в умовах воєнного стану. *Проблеми кваліфікації та розслідування кримінальних правопорушень в умовах воєнного стану*: матеріали наук.-теорет. конф., м. Київ, 26 трав. 2022 р./ Нац. акад. внутр. справ. Київ, 2022. С. 29. URL: <https://elar.naiu.kiev.ua/server/api/core/bitstreams/f5940194-46fe-4af0-84cf-775451ff2267/content> (дата звернення: 01.10.2024); Пекар П. В. Щодо питання конструювання санкцій за пропаганду війни (ст. 436 КК України). *Верховенство права*. 2017. № 3. URL: <https://sd-vp.info/2017/shhodo-pitannya-konstruuvannya-sanktsij-za-propagandu-vijni-st-436-kk-ukrayini/> (дата звернення: 01.10.2024)

³ Ботнарченко І. А. Актуальні питання кримінальної відповідальності за пропаганду війни в умовах воєнного стану. *Проблеми кваліфікації та розслідування кримінальних правопорушень в умовах воєнного стану*: матеріали наук.-теорет. конф., м. Київ, 26 трав. 2022 р./ Нац. акад. внутр. справ. Київ, 2022. С. 29. URL: <https://elar.naiu.kiev.ua/server/api/core/bitstreams/f5940194-46fe-4af0-84cf-775451ff2267/content> (дата звернення: 01.10.2024)

ми, які займають вищі державні посади (ч. 2 ст. 385 КК Вірменії, ч. 2 ст. 123 КК Білорусії), особою, яка займає державно-політичну посаду (ч. 2 ст. 405 КК Грузії), особою, яка займає відповідальну державну посаду (ч. 2 ст. 157 КК Казахстану, ч. 2 ст. 140 КК Молдови), особою, яка займає державну посаду (ч. 2 ст. 396 КК Таджикистану)¹.

Прикладні проблеми застосування ст. 436 КК «Пропаганда війни».

1. Основним безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 436 КК, є суспільні відносини у сфері охорони миру та мирного співіснування держав, їх взаємовигідної співпраці, що ґрунтується на принципах міжнародного права, зокрема, незастосування сили, недоторканності кордонів, територіальної цілісності, невтручання у внутрішні справи суверенних держав². На підставі цього С. М. Мохончук справедливо стверджує, що не можуть кваліфікуватися як пропаганда війни публічні заклики продовжувати агресивну війну або воєнний конфлікт, що вже розпочалися³, адже мир між державами та народами вже порушено.

Водночас в Єдиному державному реєстрі судових рішень є *низка вироків за ст. 436 КК, якими засуджено осіб за публічні заклики до продовження РФ війни проти України або розповсюдження матеріалів із такими закликами*⁴. Хоча здебільшого дії засуджених кваліфі-

¹ Кацнір В., Олійник Х. Іноземний досвід регламентації кримінальної відповідальності за пропаганду, планування, підготовку, розв'язування та ведення агресивної війни. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2020. Т. 7. № 1. С. 193. URL: <https://cyberleninka.ru/article/n/inozemniy-dosvid-reglamentatsiyi-kriminalnoyi-vidpovidalnosti-za-propagandu-planuvannya-pidgotovku-rozv-yazuvannya-ta-vedennya/viewer> (дата звернення: 01.10.2024)

² Пропаганда війни: поняття та форми. *WikiLegalAid*, 2022. URL: https://wiki.legalaid.gov.ua/index.php/%D0%9F%D1%80%D0%BE%D0%BF%D0%B0%D0%B3%D0%B0%D0%BD%D0%B4%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B8:%D0%BF%D0%BE%D0%BD%D1%8F%D1%82%D1%82%D1%8F_%D1%82%D0%B0_%D1%84%D0%BE%D1%80%D0%BC%D0%B8 (дата звернення: 01.10.2024)

³ Мохончук С. М. Злочини проти миру та безпеки людства: генезис, еволюція, сучасна регламентація у кримінальному праві та законі. Харків: Право, 2013. С. 274.

⁴ Вирок Вінницького міського суду Вінницької області від 24.01.2024 (справа № 127/15700/23). *Єдиний державний реєстр судових рішень*: оф. вебсайт.

кувалися й за іншими статтями КК, зокрема, за ч. 2 ст. 109 («Публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій»), ч. 1 ст. 110 («Публічні заклики чи розповсюдження матеріалів із закликами до зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України»), ст. 436² («Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників») тощо. Видається, що кваліфікація дій засуджених у вказаних вирокх за ст. 436 КК є доволі спірною, а, отже, така судова практика є помилковою.

У цей же час виникає питання: а чи можна кваліфікувати за ст. 436 КК публічні заклики до вступу певної країни в уже розпочату агресивну війну, якщо така країна не є стороною цього конфлікту? Слід навести таку ситуацію: громадянин України публічно закликає до вступу Туреччини в агресивну війну РФ проти України на стороні держави-агресора. Фактично між Україною та Туреччиною немає

URL: <https://reyestr.court.gov.ua/Review/116618973> (дата звернення: 01.10.2024); Вирок Вінницького міського суду Вінницької області від 31.08.2022 (справа № 127/10958/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/105980081> (дата звернення: 01.10.2024); Вирок Дарницького районного суду м. Києва від 31.10.2022 (справа № 753/5145/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/107195357> (дата звернення: 01.10.2024); Вирок Приморського районного суду м. Одеси від 26.07.2023 (справа № 522/2787/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/112474344> (дата звернення: 01.10.2024); Вирок Хмельницького міськрайонного суду Хмельницької області від 12.09.2023 (справа № 686/18993/23). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/113624865> (дата звернення: 01.10.2024); Вирок Самбірського міськрайонного суду Львівської області від 02.03.2023 (справа № 452/3283/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/109295763> (дата звернення: 01.10.2024); Вирок Стрийського міськрайонного суду Львівської області від 01.11.2022 (справа № 456/3226/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/107130559> (дата звернення: 01.10.2024); Вирок Березнегуватського районного суду Миколаївської області від 27.07.2022 (справа № 383/410/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/105452794> (дата звернення: 01.10.2024).

стану війни. Чи можна у цій ситуації говорити про посягання на мир та мирне співіснування України та Туреччини? Видається, що так. Тому такі заклики слід кваліфікувати за ст. 436 КК незважаючи на те, що агресивна війна вже розпочалася. Це саме стосується й публічних закликів до вступу України в інші розпочаті збройні конфлікти, стороною яких наша країна не є.

2. З досліджених вироків вбачається, що доволі часто *суди взагалі не вдаються до аналізу змісту публічних закликів* до агресивної війни чи розповсюджених матеріалів із такими закликами, а покладаються на висновки лінгвістичної експертизи, або обмежуються тим, що обвинувачений визнав свою вину¹.

Публічні заклики до агресивної війни або до розв'язання воєнного конфлікту передбачають усні або письмові відкриті звернення до невизначеного кола осіб. Такі звернення пропагують ідеї, погляди чи навіть вимоги і розповсюджуються серед значної кількості людей з метою схилити їх до відповідних дій. За своїм характером публічні заклики можуть виступати способом психологічного впливу на людей, агітацією, спрямованою на формування громадської думки². Як наголошує М. А. Рубашенко, «визначальним моментом в оцінці суспільної небезпечності публічних закликів виступає неможливість ознайомлення багатьох осіб із змістом закликів, а можливість того, що вже ознайомлені із закликами особи можуть вчинити дії, до яких вони закликалися»³.

Таким чином, суд, кваліфікуючи дії обвинуваченого за ст. 436 КК, має встановити наявність у його діях публічних закликів до агре-

¹ Вдовенко О., Воробійов Є., Гринишак М. Кримінальна відповідальність за поширення інформації в інтернеті до та після 24 лютого 2022 року. Київ: ГО «Платформа прав людини», 2022. С. 66. URL: <https://www.ppl.org.ua/wp-content/uploads/2023/01/%D0%9D%D0%9D%D0%9B%D0%86%D0%A2%D0%98%D0%A7%D0%9D%D0%98%D0%99-%D0%97%D0%92%D0%86%D0%A2-A4-30-12-22.pdf> (дата звернення: 01.10.2024)

² Кубальський В. Н. Проблеми кримінальної відповідальності за публічні заклики до вчинення злочинів проти державного суверенітету. *Судова апеляція*. 2018. № 2. С. 67–78.

³ Рубашенко М. А. Кримінальна відповідальність за посягання на територіальну цілісність і недоторканність України. Харків: Право, 2016. С. 127–128.

сивної війни або до розв'язування воєнного конфлікту. Але є в Єдиному реєстрі судових рішень вирок, в яких відсутні такі публічні заклики¹. Крім того, існують вирок, в яких інформація, що містить публічні заклики до агресивної війни, є прихованою, що унеможливає перевірку обґрунтованості кваліфікації за пропаганду війни².

Виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436¹ КК).

Чинна редакція ст. 436¹ КК була викладена Законом України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки» від 09.04.2015 р. № 317-VIII, відповідно до якого пропаганда комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів та їхньої символіки визнається наругою над пам'яттю мільйонів жертв комуністичного тоталітарного режиму, націонал-соціалістичного (нацистського) тоталітарного режиму та заборонена законом (ч. 1 ст. 3). До того ж пропаганда та використання символіки комуністичного та нацистського тоталітарних режимів може сприяти розпалюванню національної, расової, релігійної чи ідеологічної ворожнечі, підривати громадський порядок, а також призводити до дестабілізації суспільно-політичної ситуації в країні, посилення соціальної напруги та провокації конфліктів, що становить загрозу для національної безпеки країни. Більше того, пропаганда тоталітарних ідеологій суперечить принципам демократії, прав людини та верховенства права, закріпленим у Конституції України та міжнародних зобов'язаннях держави.

¹ Див. наприклад: Вирок Дарницького районного суду м. Києва від 22.04.2022 (справа № 753/3955/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/104069991> (дата звернення: 01.10.2024)

² Вирок Малиновського районного суду м. Одеси від 04.03.2020 (справа № 521/1945/20). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/88051413> (дата звернення: 01.10.2024); Вирок Прилуцького міськрайонного суду Чернігівської області від 07.09.2022 (справа № 742/1931/22). *Єдиний державний реєстр судових рішень*: оф. вебсайт. URL: <https://reustr.court.gov.ua/Review/106107436> (дата звернення: 01.10.2024)

У міжнародному праві є низка документів, які засуджують комуністичний та нацистський тоталітарні режими, а відтак – їх пропаганду¹. Серед них можна вирізнити такі, як: Декларація Європейського Парламенту щодо проголошення 23 серпня європейським днем пам'яті жертв сталінізму і нацизму від 23.09.2008 р.², Резолюції ПАРЄ (щодо заходів з ліквідації спадку колишніх комуністичних тоталітарних систем від 27.06.1996 р. № 1096³; щодо необхідності міжнародного засудження злочинів тоталітарних комуністичних режимів від 26.01.2006 р. № 1481⁴; щодо боротьби з відродженням нацистської ідеології від 12.04.2006 р. № 1495⁵; щодо ставлення до пам'ятників, які мають суперечливу історичну інтерпретацію у державах-членах Ради Європи від 29.01.2009 р. № 1652⁶), Резолюції

¹ Лаба С. В. Кримінальна відповідальність за пропаганду комуністичного та нацистського тоталітарних режимів: дис. ... канд. юрид. наук: 12.00.08. Львів, 2023. С. 174. URL: https://shron1.chtyvo.org.ua/Laba_Sviatoslav/Kryminalna_vidpovidalnist_za_propahandu_komunistychnoho_ta_natsystyskoho_totalitarnykh_rezhymiv.pdf?PHPSESSID=bmuqvarjs36oqq085ar701duo3 (дата звернення: 01.10.2024)

² Декларація Європейського Парламенту щодо проголошення 23 серпня європейським днем пам'яті жертв сталінізму і нацизму: Міжнародний документ від 23.09.2008. *European Parliament*. URL: https://www.europarl.europa.eu/doceo/document/TA-6-2008-0439_EN.html?redirect (дата звернення: 01.10.2024)

³ Резолюція Парламентської Асамблеї Ради Європи щодо заходів з ліквідації спадку колишніх комуністичних тоталітарних систем № 1096: Міжнародний документ від 27.06.1996. *Parliamentary Assembly. Council of Europe*. URL: <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16507&lang=en#> (дата звернення: 01.10.2024)

⁴ Резолюція Парламентської Асамблеї Ради Європи щодо необхідності міжнародного засудження злочинів тоталітарних комуністичних режимів № 1481: Міжнародний документ від 26.01.2006. *Parliamentary Assembly. Council of Europe*. URL: <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17403&lang=en> (дата звернення: 01.10.2024)

⁵ Резолюція Парламентської Асамблеї Ради Європи щодо боротьби з відродженням нацистської ідеології № 1495: Міжнародний документ від 12.04.2006. *Parliamentary Assembly. Council of Europe*. URL: <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=17427&lang=en> (дата звернення: 01.10.2024)

⁶ Резолюція Парламентської Асамблеї Ради Європи щодо ставлення до пам'ятників, які мають суперечливу історичну інтерпретацію у державах-членах Ради Європи № 1652: Міжнародний документ від 29.01.2009. *Parliamentary Assembly. Council of Europe*. URL: <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17713&lang=en> (дата звернення: 01.10.2024)

Європейського Парламенту (в пам'ять про Голодомор – штучний голод в Україні 1932–1933 років від 23.10.2008 р.)¹; щодо європейської свідомості та тоталітаризму від 02.04.2009 р.². Враховуючи це, а також збройну агресію РФ проти України, яка використовує комуністичну символіку в інформаційній війні, криміналізація виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів є доволі логічним кроком української влади.

За десятирічний строк існування ст. 436¹ КК у різних редакціях та десятирічну практику її застосування відповідно до статистичних даних Офісу Генерального прокурора (з 2014 р. по серпень 2024 р.) було обліковано 1055 кримінальних правопорушень³. Причому біль-

¹ Резолюція Європейського Парламенту в пам'ять про Голодомор – штучний голод в Україні 1932–1933 років: Міжнародний документ від 23.10.2008. *European Parliament*. URL: https://www.europarl.europa.eu/doceo/document/TA-6-2008-0523_EN.html?redirect (дата звернення: 01.10.2024)

² Резолюція Європейського Парламенту щодо європейської та тоталітаризму: Міжнародний документ від 02.04.2009. *European Parliament*. URL: https://www.europarl.europa.eu/doceo/document/TA-6-2009-0213_EN.html (дата звернення: 01.10.2024)

³ Єдиний звіт про кримінальні правопорушення за січень-грудень 2014 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2015 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2016 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2017 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2018 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2019 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2020 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень

шість із них (а саме 600) було зафіксовано у 2022–2023 рр. У період з 2014 по 2023 рр. за цією статтею КК було засуджено 160 осіб України¹, переважна частка яких (141 особа) – у 2022–2023 рр.

Водночас чинна редакція норми вказаної статті не позбавлена низки недоліків концептуального та теоретичного характеру, які потребують законодавчого вирішення для забезпечення ефективного та справедливого застосування Закону про кримінальну відповідальність, а також відповідності його положень принципу правової визначеності (як складової частини принципу верховенства права) та конституційним правам і свободам людини й громадянина.

2021 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-серпень 2024 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogorozsliduvannya-2>.

¹ 2014 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/lkflghkjlh; 2015 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/Sud_statustuka_Zvit_2015; 2016 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/2016_zvit; 2017 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2017; 2018 рік. Форма № 7 «Звіт про склад засуджених». *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2018; 2019 рік. Форма № 7 Звіт про склад засуджених за 2019 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2019; 2020 рік. Форма № 7 Звіт про склад засуджених за 2020 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2020; 2021 рік. Форма № 7 Звіт про склад засуджених за 2021 рік. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvitn1st_21; 2022 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2022; 2023 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2023.

Щодо концептуальних недоліків, то серед них насамперед можна назвати певну суперечність криміналізації виготовлення, поширення комуністичної, нацистської символіки та пропаганди комуністичного й націонал-соціалістичного (нацистського) тоталітарних режимів таким конституційним правам, як право на свободу думки і слова, на вільне вираження своїх поглядів і переконань (ч. 1 ст. 34 Конституції України), вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (ч. 2 ст. 34 Конституції України), а також конституційній забороні на цензуру (ст. 15 Конституції України). Незважаючи на те, що Конституційний Суд України у своєму рішенні у справі за конституційним поданням 46 народних депутатів України щодо відповідності Конституції України (конституційності) Закону України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки» від 16 липня 2019 р. № 9-р/2019 визнав означений закон зі змінами (а, отже, і чинну редакцію ст. 436¹ КК) таким, що відповідає Конституції України (є конституційним). Однак, аргументація, яку використав Конституційний Суд України у мотивувальній частині Рішення, виглядає дещо заполітизованою та сумнівною. Зокрема, суддя Конституційного Суду України Н. К. Шаптала в Окремій думці¹ стосовно згаданого Рішення зазначив, що «Конституційний Суд України, розглядаючи цю справу, зосередив свою увагу лише на дослідженні легітимної мети Закону, і мотивувальна частина Рішення присвячена виключно цьому дослідженню, здійсненому на підставі історичних дописів, зокрема і в засобах масової інформації, без аналізу відповідності положень Закону конкретним конституційним приписам, на які вказував суб'єкт права на конституційне подання. ...Означене дає підстави стверджувати, що Конституційний

¹ Окрема думка судді Конституційного Суду України Шапталі Н. К. стосовно Рішення Конституційного Суду України у справі за конституційним поданням 46 народних депутатів України щодо відповідності Конституції України (конституційності) Закону України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки». *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/nc09d710-19#n2> (дата звернення: 01.10.2024)

Суд України фактично не здійснив повного та всебічного розгляду справи. Крім того, левова частка висновків, які зробив Конституційний Суд України у цій справі, носить оціночний, а здебільшого й політичний характер і ґрунтується не на юридичному аналізі, а виключно на історичному контексті без дослідження таких аспектів легітимної мети Закону, як пропорційність та справедливість засобів її досягнення».

Крім того, досвід зарубіжних країн показує, що аналогічні до ст. 436¹ КК норми кримінальних кодексів європейських держав, вже визнавалися неконституційними, зокрема, через порушення права на свободу вираження поглядів. Так, 19 липня 2011 р. Конституційний суд Польщі у своєму рішенні Ref. о. К 11/10 визнав неконституційними положення КК Польщі щодо кримінальної відповідальності за пропаганду тоталітарної ідеології, у тому числі нацистської та комуністичної, а також вироблення, збут, купівлю чи використання продукції, пов'язаної з нею, у тому числі комуністичної та нацистської символіки. Конституційний суд Угорщини 19 лютого 2013 р. у своєму рішенні № IV/2478/2012 також визнав неконституційними положення про кримінальну відповідальність за поширення чи публічне використання чи демонстрування свастики, знаків СС, знаку схрещених стріл (знак національно-соціалістичної партії схрещених стріл, створеної в 1937 році), серпа та молота, червоної зірки чи будь-яких символів з їхнім використанням¹.

Враховуючи вищезазначене, питання щодо конституційності ст. 436¹ КК досі залишається відкритим.

Другим концептуальним недоліком ст. 436¹ КК є *незначна сутільна небезпечність виготовлення, поширення комуністичної, нацистської символіки та пропаганди комуністичного та націонал-*

¹ Яворський В. Аналіз закону про заборону комуністичних символів. *Права людини в Україні: інформаційний портал Харківської правозахисної групи*. URL: <https://khp.org/1430493970> (дата звернення: 01.10.2024); Спільний проміжний висновок № 823/2015 щодо Закону України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки», ухваленому Венеціанською комісією на 105-му пленарному засіданні (18-19 грудня 2015 р.). URL: <https://www.osce.org/files/f/documents/c/f/216291.pdf> (дата звернення: 01.10.2024)

соціалістичного (нацистського) тоталітарних режимів, яка не досягає рівня необхідного для криміналізації таких діянь. Зокрема, Головне науково-експертне управління апарату Верховної Ради України у своєму висновку на проєкт Закону України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їх символіки» (реєстр. № 2558 від 06.04.2015 р.) від 09.04.2015 р.¹ зазначило, що такі діяння, як «виготовлення, поширення, а також публічне використання символіки комуністичного тоталітарного режиму, у тому числі сувенірної, публічне виконання гімнів СРСР, УРСР (УСРР), інших союзних радянських республік або їх фрагментів на всій території України» не можна розглядати як злочини, оскільки вони самі по собі не становлять суспільної небезпечності, необхідної та достатньої для визнання їх злочинами (ч. 1 ст. 11 КК). Суспільно небезпечними та кримінально караними є самі злочини проти життя людини (наприклад, вбивство, відповідальність за яке передбачена ст. 115 КК), проти людяності (наприклад, злочин геноциду, відповідальність за який передбачена ст. 442 КК) та інші злочини, що були вчинені за часів Радянського Союзу, а не «використання символіки, в тому числі сувенірної, чи виконання гімну радянських республік» (п. 7 зазначеного Висновку).

У цьому контексті, слід також зазначити, що питання доцільності криміналізації символіки тоталітарних режимів багаторазово було предметом розгляду ЄСПЛ і національних судів Європи. Яскравим прикладом є Рішення від 2008 р. у справі «Важнай проти Угорщини» (№ 33629/06), де ЄСПЛ встановив порушення ст. 10 Конвенції та зазначив, що «пропаганда комуністичної ідеології, якою б нестерпною вона не була, не може бути єдиною підставою для обмеження використання символу, особливо багатозначного, за допомогою кримінального покарання. Просте використання напказ або використання символу фізичною особою, зокрема членом

¹ Проєкт Закону про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їх символіки. *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2558&skl=9 (дата звернення: 01.10.2024)

zareestrovanoї politichnoї partії, yakij ne vyjaviv sebe yak lyudyna z totalitarnimi ambicijami, ne moze buty pryrivnyane do nebezpečnoї propahandy»¹.

Щодо інших недоліків складу кримінального правопорушення, передбаченого ст. 436¹ КК, теоретичного характеру, то вони вже достатньо повно та обґрунтовано висвітлені у науковій літературі. Так, фахівець у галузі кримінального права Є. О. Письменський вирізнив наступні хиби кримінально-правового припису, передбаченого вказаною статтею КК:

- 1) *невідповідність назви ст. 436¹ КК її змісту* (склад кримінального правопорушення не охоплює усі форми пропаганди комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів, передбачених п. 2 ч. 1 ст. 1 Закону України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки»);
- 2) *зайвість у конструкції складу кримінального правопорушення такої форми об'єктивної сторони як публічне виконання гімну*, адже воно є проявом публічного використання символіки;
- 3) *обмеженість предмета кримінального правопорушення лише символікою комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів*, зокрема через не визначення предметом цього правопорушення символіки фашистського режиму, який так само вважається тоталітарним;
- 4) *неспіврозмірність покарання, передбаченого ст. 436¹ КК, характеру та ступеню суспільної небезпечності кримінального правопорушення* (встановлені види та розміри покарання не

¹ Бабак М. А., Філей Ю. В. Вітчизняні новели кримінально-правового механізму протидії пропаганді комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів з огляду на деякі конституційні права й основоположні свободи людини і громадянина. *Право і суспільство*. 2018. № 3. Ч. 2. С. 184. URL: http://pravoisuspilstvo.org.ua/archive/2018/3_2018/part_2/31.pdf (дата звернення: 01.10.2024)

дозволяють належним чином індивідуалізувати кримінальну відповідальність та штучно підвищують характер суспільної небезпечності);

- 5) *зайвість такого додаткового виду покарання за виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів як конфіскація майна (відповідно до ч. 2 ст. 59 КК конфіскація майна встановлюється за тяжкі та особливо тяжкі корисливі злочини, а також за злочини проти основ національної безпеки України та громадської безпеки незалежно від ступеня їх тяжкості. Зі свого боку, кримінальне правопорушення, передбачене ст. 436¹ КК таким не є)*¹.

Крім того, Є. О. Письменський у своїй статті описав цілу низку недоліків законодавчої техніки, використаної при конструюванні досліджуваного складу кримінального правопорушення, на яку звернув увагу також професор М. І. Хавронюк, зокрема: *невиправданість використання в диспозиції ч. 1 ст. 436¹ КК єднального сполучника «а також» (замість «або»)*, що «вимагає» від особи вчинення і виготовлення, і поширення, і публічного використання; *некоректність використаного звороту «інших союзних радянських республік або їх фрагментів» (треба було: «або фрагментів гімну»); помилковість використання слова «гімнів» у множині (виходить, що злочином є лише виконання кількох гімнів) та слів «на всій те-*

¹ Письменський Є. О. Кримінально-правова охорона національної та історичної пам'яті: плутаний шлях законодавця. *Вісник Асоціації кримінального права України*. 2015. № 1 (4). С. 267-270. URL: https://www.academia.edu/36941538/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE_%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%B0_%D0%BE%D1%85%D0%BE%D1%80%D0%BE%D0%BD%D0%B0_%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%97_%D1%82%D0%B0_%D1%96%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D1%97_%D0%BF%D0%B0%D0%BC_%D1%8F%D1%82%D1%96_%D0%BF%D0%BB%D1%83%D1%82%D0%B0%D0%BD%D0%B8%D0%B9_%D1%88%D0%BB%D1%8F%D1%85_%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%BE%D0%B4%D0%B0%D0%B2%D1%86%D1%8F (дата звернення: 01.10.2024)

риторії України» (тобто, його виконання на окремих територіях не є кримінальним правопорушенням); *недоречність відсилання в диспозиції ч. 1 ст. 436¹ КК до статей інших законів* (замість цього треба було б сформулювати норму-примітку з визначенням переліку цих законів)¹.

Інші дослідники також вказували на недоліки чинної редакції ст. 436¹ КК та висловлювали цікаві пропозиції щодо удосконалення складу цього кримінального правопорушення. Так, Ю. М. Беклеміщева пропонує передбачити *наявність спеціальної мети кримінального правопорушення в разі вчинення його шляхом виготовлення комуністичної, нацистської символіки, а саме «виготовлення з метою поширення»*². Крім того, дослідниця пропонує в ч. 2 ст. 436¹ КК *замінити обставину, що обтяжує відповідальність за вчинення дій, передбачених ч. 1 ст. 436¹ КК, – «особою, яка є представником влади», на обставину «вчинення дій, передбачених ч. 1 ст. 436¹ КК, службовою особою з використанням влади чи службових повноважень»*³.

¹ Письменський С. О. Кримінально-правова охорона національної та історичної пам'яті: плутаний шлях законодавця. *Вісник Асоціації кримінального права України*. 2015. № 1 (4). С. 269. URL: https://www.academia.edu/36941538/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE_%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%B0_%D0%BE%D1%85%D0%BE%D1%80%D0%BE%D0%BD%D0%B0_%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%97_%D1%82%D0%B0_%D1%96%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D1%97_%D0%BF%D0%B0%D0%BC_%D1%8F%D1%82%D1%96_%D0%BF%D0%BB%D1%83%D1%82%D0%B0%D0%BD%D0%B8%D0%B9_%D1%88%D0%BB%D1%8F%D1%85_%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%BE%D0%B4%D0%B0%D0%B2%D1%86%D1%8F (дата звернення: 01.10.2024).

² Беклеміщева Ю. М. До постановки проблеми визначення предмета злочину, передбаченого ст. 436-1 КК України. *Право та державне управління*. 2019. № 3 (36). Т. 2. С. 16–17. URL: http://pdu-journal.kpu.zp.ua/archive/3_2019/tom_2/4.pdf (дата звернення: 01.10.2024).

³ Беклеміщева Ю. М. Кримінально-правова характеристика виготовлення, поширення комуністичної, нацистської символіки та пропаганди комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів: дис. ... канд. юрид. наук: 12.00.08. Запоріжжя, 2020. С. 210. URL: http://virtuni.education.zp.ua/info_cpu/sites/default/files/Беклеміщева%20дис.pdf (дата звернення: 01.10.2024)

Проаналізувавши судові рішення О. Березніков пропонує *встановити більші м'які види та розміри покарань* за виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів¹. Аналогічну точку зору відстоює й В. Яворський, який пропонує виключити покарання у виді позбавлення волі, замінивши його більш м'якими санкціями, а в найкращому варіанті – встановити адміністративну відповідальність за відповідне правопорушення².

Науковець С. В. Лаба запропонував *розширити межі кримінально-правової заборони злочинної пропаганди, передбачивши відповідальність за публічні заклики до розбудови комуністичного та нацистського тоталітарних режимів або за публічне заперечення чи виправдання злочинів комуністичного чи нацистського тоталітарних режимів, які визнані на державному та (або) міжнародному рівні*³. Зазначена пропозиція також потребує свого обговорення в науковій спільноті.

Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікацію її учасників (ст. 436² КК).

Кримінальне правопорушення, передбачене ст. 436² КК, було криміналізовано на початку повномасштабного вторгнення РФ на територію нашої держави Законом України «Про внесення змін до

¹ Березніков О. В. Проблемні питання застосування статті 436-1 КК України. Новітні кримінально-правові дослідження – 2020: Альманах наукових праць / за ред. професора О. В. Козаченка, О. М. Мусиченко. Миколаїв: Миколаївський інститут права Національного університету «Одеська юридична академія», 2020. С. 171. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/16a2626a-acf5-4caabe18-549f35aaba68/content> (дата звернення: 01.10.2024)

² Яворський В. Аналіз закону про заборону комуністичних символів. *Права людини в Україні: інформаційний портал Харківської правозахисної групи*. URL: <https://khp.org/1430493970> (дата звернення: 01.10.2024)

³ Лаба С. В. Кримінальна відповідальність за пропаганду комуністичного та нацистського тоталітарних режимів: дис. ... канд. юрид. наук: 12.00.08. Львів, 2023. С. 174. URL: https://shron1.chtyvo.org.ua/Laba_Sviatoslav/Kryminalna_vidpovidalnist_za_propahandu_komunistychnoho_ta_natsystyskoho_totalitarnykh_rezhymiv.pdf?PHPSESSID=bmuqvarjs36oqq085ar701duo3 (дата звернення: 01.10.2024)

деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» від 03.03.2022 р. № 2110-IX. У пояснювальній записці до вказаного проєкту Закону України констатовано, що гібридний характер агресії, який здійснюється РФ в інформаційній сфері, несе загрозу державному суверенітету та територіальній цілісності України. Вагомою складовою такої гібридної інформаційної війни проти України були і залишаються прояви ворожої пропаганди, що негативно впливають на суспільну свідомість в Україні¹. Через вищенаведене, перед державою постало завдання оперативно реагувати та ефективно вирішувати ключові виклики, особливо ті, що направлені на виправдання та підтримку злочинних дій країни-агресора. Адже саме вони чинять негативний вплив на всі сфери життєдіяльності держави й суспільства, серйозно гальмують соціальні, економічні та політичні перетворення в країні, підривають її міжнародний імідж і відтермінують перемогу над ворогом.

Одним із важливих кроків кримінально-правової політики в напрямі захисту інформаційної безпеки та інформаційного середовища й було встановлення кримінальної відповідальності за виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників². Слід погодитися, що зазначені діяння є суспільно небезпечними та підривають національну безпеку, сприяють поширенню ворожої пропаганди та розпалюють соціальну напругу в суспільстві.

Згідно зі статистичною інформацією Офісу Генерального прокурора станом на 2022–2023 рр. у державі було обліковано 2636

¹ Проєкт Закону про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції). *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5102&conv=9> (дата звернення: 01.10.2024)

² Абакіна-Пілявська Л. М. Глорифікація як кримінально-правове явище: теорія та практика. *Правові новели*. 2023. № 20. С. 212. URL: http://legalnovels.in.ua/journal/20_2023/20_2023.pdf#page=212 (дата звернення: 01.10.2024).

кримінальних правопорушень, передбачених ст. 436² КК¹. За цей же період за вказаною статтею було засуджено 672 особи².

Аналіз наукових праць та судових рішень вказує на наявність низки теоретичних проблем визначення кримінального правопорушення, передбаченого ст. 436² КК, та покарання за нього, які потребують обговорення та відповідного законодавчого вирішення. Так, науковці Д. П. Євтеєва та А. В. Лапкін вирізняють такі проблеми кримінальної відповідальності за виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікацію її учасників, які виникають у теорії та практиці:

- 1) *складність відмежування одне від одного діянь, передбачених ч. 1 ст. 436² КК* (зокрема, законодавчого тлумачення потребують такі терміни як «виправдовування», «визнання правомірною», «заперечення», «глорифікація»);
- 2) *невизначеність за змістом іншомовного терміна «глорифікація»*, використання якого суперечить законодавчій техніці (цілком справедливим стала б його заміна на всім відомі в українській мові терміни «звеличення» або «схвалення»);
- 3) *надмірно широкий обсяг кримінально-правової заборони у ст. 436² КК* (кримінально караними є діяння, передбачені у ч. 1, 2 та 3 ст. 436² КК, вчинені як публічно, так і в приватній сфері (наприклад, приватні розмови або листування); за ч. 2 ст. 436² КК кримінально караним визначено виготовлення відповідних матеріалів як із метою їх поширення, так і без мети поширення);
- 4) *невизначеність поняття «матеріали» у ч. 2 ст. 436² КК*, що може призвести до занадто широкого тлумачення зазначеної

¹ Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravorogushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravorogushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>.

² 2022 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2022; 2023 рік. Форма № 7 Звіт про склад засуджених. *Судова влада України*: оф. вебсайт. URL: https://court.gov.ua/inshe/sudova_statystyka/zvit_dsau_2023.

норми; із цим пов'язана й конкуренція норм за ч. 1 та ч. 2 в аспекті кваліфікації висловлювання суб'єктивної думки в соціальних мережах та проставлення відмітки «вподобати» на публікації, що виправдовують російську агресію;

- 5) *проблема відмежування вчинення продовжуваного кримінального правопорушення від повторності при кваліфікації кількох діянь, що підпадають під ознаки ч. 1 або ч. 2 ст. 436² КК;*
- 6) *проблема утворення повторності дій особи, якщо вона вчинила правопорушення за ч. 1, а потім за ч. 2 ст. 436² КК (або навпаки);*
- 7) *проблема відмежування кримінальних правопорушень, передбачених ст. 436² КК, від інших кримінальних правопорушень (ст. 111, ч. 1 ст. 111¹, ч. 1 ст. 111², ст.ст. 436, 436¹, 437 КК);*
- 8) *наявність у санкціях ст. 436² КК покарання у виді позбавлення волі за ненасильницькі дії, що створює умови для ухвалення судами вироків із занадто суровими покараннями¹.*

Головне науково-експертне управління апарату Верховної Ради України у своєму висновку на проєкт Закону «Про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції)» (реєстр. № 5102 від 18.02.2021 р.) вказало на *неприйнятність передбачення у санкціях ч.ч. 2 та 3 ст. 436² КК додаткового покарання у виді конфіскації майна*, адже це порушує положення Загальної частини КК².

¹ Євтєєва Д. П., Лапкін А. В. Щодо проблем тлумачення та застосування ст. 436-2 Кримінального кодексу України. *Кримінально-правова охорона безпеки людини, нації, світу: фундаментальність, трансдисциплінарність і ноонауковість забезпечення*: матеріали VIII Міжнар. наук.практ. конф., м. Харків, 17 трав. 2024 р. Харків: Право, 2024. С. 134. URL: https://dspace.nlu.edu.ua/jspui/bitstream/123456789/20090/3/konf_MPO_2024_o.pdf (дата звернення: 01.10.2024).

² Проєкт Закону про внесення змін до деяких законодавчих актів України (щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції). *Верховна Рада України: Законодавство України*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=5102&conv=9>. (дата звернення: 01.10.2024).

Деякі дослідники, зокрема Ю. В. Шинкарьов, О. О. Коваленко, вказують на *необхідність розширення переліку суб'єктів, яких може бути піддано глорифікації*. На їх думку, героїзації, яка становить небезпеку для українського суспільства, можуть піддаватися і цілі квазідержавні об'єднання, воєнізовані злочинні угруповання (як, наприклад, терористичне угруповання «Спарта») та інше, що не наділене характеристиками фізичної особи¹.

Професор Р. О. Мовчан здійснивши ґрунтовний аналіз ст. 436² КК дійшов висновку про те, що, по-перше, у цій статті слід *встановити кримінальну відповідальність виключно за публічне вчинення дій*, передбачених наразі в її ч. 1, а, по-друге, у межах такої оновленої ч. 1 *має бути уніфіковано відповідальність*, з одного боку, за згадані вище публічні дії, а з другого – за передбачене у чинній ч. 2 ст. 436² КК виготовлення або поширення відповідних матеріалів². Крім того, дослідник вказує й на проблему караності кримінального правопорушення, передбаченого ч. 3 ст. 436² КК, через встановлення безальтернативного виду покарання (позбавлення волі на строк від п'яти до восьми років), яке не відповідає характеру та ступеню суспільної небезпеки³. До схожих висновків доходить й М. А. Руба-

¹ Шинкарьов Ю. В., Коваленко О. О. Правова характеристика поняття «глорифікація» як форми об'єктивної сторони складу кримінального правопорушення, передбаченого ст. 436-2 Кримінального кодексу України. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди «ПРАВО»*. 2022. Випуск 36. С. 29. URL: <http://journals.hnpu.edu.ua/index.php/law/article/view/7867/4179> (дата звернення: 01.10.2024).

² Мовчан Р. О. Кримінально-правова новела про виправдовування збройної агресії російської федерації проти України (ст. 436-2 КК України): правозастосовні та правотворчі проблеми. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право*. 2022. Вип. 13 (25). С. 203. URL: <https://visnyk.iful.edu.ua/випуск-журналу-№-1325/мовчан-р-о-кримінально-правова-новела/> (дата звернення: 01.10.2024).

³ Мовчан Р. О. Кримінальна правотворчість воєнного часу: аналіз концептуальних помилок. *Кримінальне право України перед викликами сучасності і майбуття: яким воно є і яким йому бути*: матеріали міжнар. наук. конференції, м. Харків, 21–22 жовт. 2022 р./ редкол.: В. Я. Тацій, Ю. А. Пономаренко, Ю. В. Баулін та ін. Харків: Право, 2022. С. 21. URL: <https://ivpz.kh.ua/wp-content/uploads/2023/02/Кримінальне-право-України-перед-викликами-сучасності-і-майбуття.pdf> (дата звернення: 01.10.2024).

щенко, який, між іншим, пропонує взагалі *пом'якшити санкції всіх частин ст. 436² КК*¹.

Наприкінці вважаємо за необхідне також звернутися й до напрацювань Робочої групи з питань розвитку кримінального права (далі – Робоча група), а саме до тексту проєкту нового КК (далі – проєкт)². Так, аналогічна зі ст. 436² КК стаття під назвою «Виправдовування збройної агресії проти України» (ст. 9.1.12 проєкту) розмішена в розділі 9.1 («Злочини проти національної безпеки»). Слід погодитися з розробниками проєкту, що видовий об'єкт виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (ст. 436² КК) дійсно більше тяжіє саме до суспільних відносин, що забезпечують державний суверенітет, територіальну цілісність, недоторканність та безпеку держави, кримінальна відповідальність за посягання які регламентована розділом I Особливої частини КК («Злочини проти основ національної безпеки України»).

До того ж, варто звернути увагу, що редакція ст. 9.1.12 проєкту передбачає відповідальність за публічне виправдання, заперечення, будь-якої збройної агресії проти України або тимчасової окупації частини її території, так само як і публічне вихвалляла чи звеличувала будь-якої держави-агресора, її органів влади чи осіб, які виконують їхні функції. Порівнюючи чинну редакції ст. 436² КК та запропоновану проєктом аналогічну статтю, можна зробити висновок, що безпосередній об'єкт складу кримінального правопорушення, передбаченого ст. 9.1.12 проєкту, є більш ширшим за такий об'єкт кримінального правопорушення, передбаченого ст. 436² КК. Чинна

¹ Рубашенко М. А. Непублічні виправдовування, визнання правомірною, заперечення агресії/ окупації (ст. 436² КК України) vs. свобода вираження поглядів. *Кримінальне право України перед викликами сучасності і майбуття: яким воно є і яким йому бути*: матеріали міжнар. наук. конференції, м. Харків, 21–22 жовт. 2022 р. / редкол.: В. Я. Тацій, Ю. А. Пономаренко, Ю. В. Баулін та ін. Харків: Право, 2022. С. 71. URL: <https://ivpz.kh.ua/wp-content/uploads/2023/02/Кримінальне-право-України-перед-викликами-сучасності-і-майбуття.pdf> (дата звернення: 01.10.2024).

² Кримінальний кодекс України: контрольний текст проєкту (станом 01.08.2024). URL: <https://newcriminalcode.org.ua/upload/media/2024/08/02/kontrolnyj-tekst-proyektu-kk-stanom-na-01-08-2024.pdf> (дата звернення: 01.10.2024).

редакція ст. 436² КК спрямована на кримінально-правову протидію лише «глюорифікації» збройної агресії Російської Федерації проти України, розпочатої у 2014 р., яка вже у вигляді повномасштабної війни триває по сьогодні.

Загалом же вважаємо, що напрацювання Робочої групи доцільно використовувати під час доопрацювання чинної редакції ст. 436² КК.

4.2. Інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок шляхом планування, розв'язування та ведення агресивної війни (ст. 437 КК України)

Особливо тяжкими злочинами, що посягають на мир, безпеку людства та міжнародний правопорядок (міжнародні злочини), прийнято вважати злочини агресії та геноциду, воєнні злочини та злочини проти людства. До таких злочинів за чинним КК слід віднести: 1) Злочин агресії (ст. 437 КК); 2) Воєнні злочини (ст. 438 КК); 3) Геноцид (ст. 442 КК); 4) Злочини проти людяності (ст. 442¹ КК).

Потрібно зауважити, що норми, які містяться в зазначених статтях, визначені в міжнародних конвенціях: Гаазькі конвенції 1899 та 1907 рр., Конвенція про запобігання злочину геноциду та покарання за нього 1948 р., Женевські конвенції 1949 р. та додаткові протоколи до них, Гаазька конвенція про захист культурних цінностей у випадку збройного конфлікту 1954 р. та протоколи до неї та інші. Особливим правовим джерелом у визначенні цих міжнародних злочинів є Римський статут Міжнародного кримінального суду (далі – Римський статут МКС), оскільки юрисдикція цього суду є визнаною в Україні.

Важливу частину цих міжнародних злочинів складають інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок. Особливістю таких інформаційних дій є використання інформації (відповідні предмети,

зброя, засоби) державою-агресором для введення свого населення в оману, підбурювання своїх військовослужбовців до вчинення злочинних дій проти цивільних осіб країни, щодо якої здійснено напад. Такі інформаційні дії також спрямовуються і на населення ворога, таким чином нейтралізуючи можливу протидію здійсненої агресії та задля сприяння в пошуку співучасників вчиненого нападу на іншу державу (жертву).

Особливе місце становить інформація як предмет цих кримінальних правопорушень, що перекручується, приховується, незаконно змінюється, як і використовується для доведення погроз. Обертання неправдивої інформації з використанням Інтернета, цифрових засобів зв'язку призводить до підбурювання населення однієї держави до нападу, а іншої – до відсутності спротиву та допомоги в такому нападі. Таким чином, жертвами від інформаційної війни та застосованого інформаційного впливу стає все більше коло осіб.

Одними із найбільш тяжких інформаційних кримінально-протиправних діянь є злочин агресії, який пов'язується із використанням інформації під час планування, підготовки та розв'язування війни чи воєнного конфлікту, а також участь у змові, що спрямована на вчинення таких дій. Міжнародна основа для кваліфікації та визначення таких злочинів має важливе значення для встановлення винуватих у вчиненні подальшої агресії та встановлення суб'єктів цього злочину. Також доцільним є й звернення до витоків формування поняття «злочин агресії».

Слід погодитися з О. Базовим, що концепція злочину агресії почала формуватися ще в середньовіччі при вирішенні філософської проблеми «чесної та несправедливої війни» (Гуго Гроцій, Франсіско де Віторія). Сучасне розуміння злочину агресії сталося після Першої світової війни в межах Ліги Націй (Пакт Ліги Націй, Декларація Ліги Націй щодо загарбницьких воєн тощо)¹. У міжвоєнний період цікавим міжнародним актом, що визначав злочин агресії, була Лондонська конвенція від 3 липня 1933 р. (Конвенція про

¹ Базов О. Деякі питання визначення злочину агресії в міжнародному кримінальному праві. Публічне право. 2018. № 1 (29). С. 123–133.

визначення агресії), підписана Румунією, Естонською Республікою, Латвійською Республікою, Польською Республікою, Турецькою Республікою, Персією, СРСР, Афганістаном і Фінляндією. У цьому акті, який певною мірою відповідає сучасним міжнародно-правовим актам, використано таке визначення: «агресором у міжнародному конфлікті, відповідно до чинних домовленостей між сторонами спору, вважається держава, яка першою вчинить будь-яку з наступних дій:

- 1) оголошення війни іншій державі;
- 2) вторгнення її збройних сил з оголошенням війни або без нього на територію іншої держави;
- 3) напад її сухопутних, військово-морських або повітряних сил, з оголошенням війни чи без нього, на територію судна чи літака іншої держави;
- 4) морська блокада берегів або портів іншої держави;
- 5) надання підтримки збройним групам, сформованим на її території, які вторглися на територію іншої держави, або відмова, незважаючи на прохання, держави, що вторглася, вжити на своїй власній території всіх заходів, що від неї залежать, щоб позбавити ці банди будь-якої допомоги чи захисту» (ст. 2)¹.

Європейська мережа контактних пунктів щодо осіб, відповідальних за геноцид, злочини проти людяності та воєнні злочини (*the Genocide Network*) наголошує на тому, що спроби криміналізувати злочин агресії після Першої світової війни провалилися, але після Другої світової війни ця концепція стала актуальною зі створенням Нюрнберзького трибуналу².

Водночас ці концепції працювали в контексті перемоги та «суду переможця». Такий підхід та слабкість міжнародних інституцій унеможливають здійснення правосуддя в конфлікті та війні, що три-

¹ Convention for the Definition of Aggression on 3 July 1933. *Institute for International Law and Justice*: website. URL: <https://www.iilj.org/wp-content/uploads/2016/08/Convention-for-the-Definition-of-Aggression-1933.pdf> (дата звернення: 16.10.2024)

² The crime of aggression in the national laws of EU Member States, Genocide Network Observer States and Ukraine. *Genocide Network Paper*. 2023. 28 p.

ває. Це також пов'язано з відсутністю доступу до місць вчинення таких злочинів, а також до осіб, які провокували та здійснювали таку агресію. Сьогодні подібна ситуація сформувалася в Україні, оскільки російська агресія не зупинена, а загарбницька війна продовжує знищувати українську ідентичність разом із громадянами, цілими містами та селищами, їх інфраструктурою, культурою, історією та мовою.

Визначаючи злочин агресії, чинне національне кримінальне законодавство керується насамперед Статутом ООН. Так, ст. 1 Статуту ООН формулює цілі і принципи: «підтримувати міжнародний мир та безпеку і з цією метою вживати ефективних колективних заходів для запобігання та усунення загрози миру й придушення актів агресії, або інших порушень миру...» (Статут ООН, 1945 р.)¹. У той самий час ч. 4 ст. 2 Статуту ООН передбачає, що «усі Члени ООН *утримуються* в своїх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і якимось іншим чином, несумісним із Цілями ООН». При цьому саме «Рада Безпеки визначає існування будь-якої загрози миру, будь-якого порушення миру або акта агресії та надає рекомендації або вирішує те, які дії варто почати у відповідності зі ст.ст. 41 та 42 для підтримки або відновлення міжнародного миру й безпеки» (ст. 39)². За такою редакцією рішення Ради Безпеки ООН можуть бути заблоковані державою-агресором. У таких випадках унеможливується реалізація цілей Статуту ООН. Статут ООН, який приймався у 1945 р., не передбачав імовірності того, що агресором може бути член Ради Безпеки ООН, як це сталося в ситуації, пов'язаною з російською агресією проти України.

¹ Статут Організації Об'єднаних Націй від 26 червня 1945. *United Nations*: вебсайт. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN Charter_Ukrainian.pdf (дата звернення: 16.10.2024)

² Статут Організації Об'єднаних Націй від 26 червня 1945. *United Nations*: вебсайт. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN Charter_Ukrainian.pdf (дата звернення: 16.10.2024)

Ознаки злочину агресії продовжували визначатися в інших міжнародно-правових актах. Відповідно до Резолюції 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 р. передбачено таке поняття агресії: «застосування збройних сил державою проти суверенітету, територіальної цілісності чи політичної незалежності іншої держави або будь-яким іншим способом, що суперечить Статуту ООН, як викладено в цьому Визначенні» (ст. 1 Додатку до Резолюції). Ця резолюція містить перелік дій, які кваліфікуються як *агресія незалежно від оголошення війни*:

- a) вторгнення або напад збройних сил держави на територію іншої держави або будь-яка військова окупація, якою б тимчасовою вона не була, в результаті такого вторгнення або нападу, або будь-яка із застосуванням сили анексія території іншої держави або його частина;
- b) бомбардування збройними силами держави території іншої держави або застосування будь-якої зброї державою проти території іншої держави;
- c) блокада портів або узбережжя держави збройними силами іншої держави;
- d) напад збройних сил держави на сухопутні, морські чи повітряні сили або морський і повітряний флот іншої держави;
- e) використання збройних сил однієї держави, які знаходяться на території іншої держави за згодою приймаючої держави, *всупереч умовам, передбаченим угодою*, або будь-яке продовження їх присутності на такій території *після припинення дії договору*;
- f) дія держави, що дозволяє, щоб його територія, яку вона *надала в розпорядження іншої держави*, використовувалася цією іншою державою для вчинення акта агресії проти третьої держави; використовувати свою територію, яку вона *надала у розпорядження іншої держави*, цією іншою державою для вчинення акту агресії проти третьої держави;
- g) надсилання державою або від її імені збройних банд, груп, *нерегулярних формувань або найманців, які здійснюють дії*

збройної сили проти іншої держави настільки тяжкі, що порівнюються до перелічених вище дій, або її суттєва участь у них» (3314 Визначення агресії, 1974) (Стаття 3 Додатку до Резолюції). Крім того, перелік таких діянь не є вичерпним (ст. 4 додатку до Резолюції)¹.

Необхідно зазначити, що Римський статут МКС безпосередньо відтворює у своїх нормах наведене визначення агресії (ст. 8bis). Тут варто звернути увагу, що європейська мережа контактних пунктів стосовно осіб, відповідальних за геноцид, злочини проти людяності та воєнні злочини (*the Genocide Network*) наполягає на тому, що «відповідно до визначення ст. 8bis, індивідуальну кримінальну відповідальність за злочин агресії *можуть понести лише члени керівництва держави з урахуванням порогової вимоги щодо типу порушення Статуту ООН*»². На нашу думку, такий підхід до визначення суб'єкта злочину агресії є ключовим, оскільки дозволяє відмежувати злочин агресії від інших міжнародних та воєнних злочинів, злочинів проти людяності та геноциду.

Ще з 2014 р., а особливо після 2022 р., російська агресія набула всіх ознак злочину, зазначених у міжнародних актах, поєднуючи агресивні дії з воєнними та іншими тяжкими злочинами. Е. Полманн з цього приводу зазначає, що військовий напад Росії на Україну відповідає всім необхідним вимогам статті 8bis Римського статуту МКС³. У ст. 437 КК передбачається кримінальна відповідальність за планування, підготовку або *розв'язування агресивної війни* чи воєнного конфлікту, участь у змові, що спрямована на вчинення таких дій, а також за ведення агресивної війни або агресивних воєнних дій. Таке визначення злочину в національному кримінальному законодавстві є відповідником визначенню злочину агресії, сформульова-

¹ Definition of Aggression: General Assembly resolution 3314 (XXIX) on 14 December 1974. URL: <https://ijl.org/wp-content/uploads/2016/08/General-Assembly-Resolution-3314.pdf> (дата звернення: 16.10.2024)

² The crime of aggression in the national laws of EU Member States, Genocide Network Observer States and Ukraine. *Genocide Network Paper*: 2023. 28 p.

³ Pollmann E. The Crime of Aggression and the Case of Ukraine. *American Yearbook of International Law*. 2020. Vol. 1, No. 1. P. 717.

ному в міжнародному кримінальному праві. Водночас особливістю визначення цього злочину за національним законодавством є те, що в ньому прямо не зазначений суб'єкт злочину, що може розвинути судження про можливість притягнення за цей злочин до кримінальної відповідальності будь-якої фізичної, осудної особи, яка досягла віку кримінальної відповідальності (загальний суб'єкт). За цим підходом і формувалася судова практика до прийняття постанови Великої Палати Верховного Суду від 28 лютого 2024 р. у справі № 415/2182/20, відповідно до якої діяння, зазначені у ст. 437 КК, здатні вчиняти особи, які в силу службових повноважень або фактичного суспільного становища спроможні здійснювати ефективний контроль за політичними чи воєнними діями або керувати ними, та/або істотно впливати на політичні, військові, економічні, фінансові, інформаційні та інші процеси у власній державі чи за її межами, та/або керувати конкретними напрямками політичних або воєнних дій. Це судове рішення обґрунтовує правову позицію щодо можливості кримінальної відповідальності за національним кримінальним законодавством лише юридично визнаних відповідальних осіб держави-агресора (лідерів), що керують або впливають на певні процеси у своїй країні або поза її межами (спеціальний суб'єкт). Однак судова практика за ст. 437 КК поки що не підтвердила (за відсутністю справ) такий підхід, що був обґрунтовано обраний Верховним судом.

Цей підхід на сьогодні щодо застосування ст. 437 КК очевидно підтримує Офіс Генерального прокурора. Цікаво, що на його сайті в магістральній справі «24 лютого» серед підозрюваних осіб зазначені міністри оборони та внутрішніх справ, депутати Державної думи, Федеральних зборів, військово командування, сенатори, керівники окремих органів влади, корпорацій та стратегічних підприємств, *розпалювачі війни та пропагандисти Кремля* (включаючи керівників вищих навчальних закладів)¹.

За такого специфічного визначення «злочину агресії» на міжнародному та національному рівнях виникає питання щодо надан-

¹ Список підозрюваних магістральній справі «24 лютого». Офіс Генерального прокурора: оф. вебсайт. URL: <https://gp.gov.ua/detectable> (дата звернення: 16.10.2024).

ня можливих рекомендацій щодо його підсудності та особливостей кваліфікації. Злочин агресії очевидно має перслідуватися міжнародним кримінальним трибуналом (судом). На національному рівні також може здійснюватися досудове розслідування та судовий розгляд таких кримінальних проваджень, оскільки спеціальних суб'єктів-лідерів, які можуть бути притягати до кримінальної відповідальності може бути більше, ніж у міжнародному кримінальному трибуналі (суді), що і підтверджує великий перелік підозрюваних, визначений Офісом Генерального прокурора.

4.3. Інформаційні кримінально-протиправні діяння, що посягають на мир та міжнародний правопорядок у контексті вчинення воєнних злочинів (ст. 438 КК України)

У нормі ст. 438 КК визначені такі суспільно небезпечні діяння:

- 1) жорстоке поводження з військовополоненими або цивільним населенням;
- 2) вигнання цивільного населення для примусових робіт;
- 3) розграбування національних цінностей на окупованій території;
- 4) застосування засобів ведення війни, заборонених міжнародним правом;
- 5) інші порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України;
- 6) віддання наказу про вчинення таких дій.

Зазначені діяння переважно вчиняються шляхом застосування фізичної сили (жорстоке поводження, вигнання, розграбування тощо). Однак їх вчинення можливе й шляхом використання інформації. У такому разі вони набувають ознак інформаційного кримінально-протиправного діяння. Зокрема, до таких належить віддання наказу про вчинення воєнного злочину. Наразі, юридична природа

цих діянь однакова. Всі вони сформовані на підставі визначень, що містяться у Женевських конвенціях (1949 р.), додаткових протоколів до них та інших міжнародних документах. І хоча певні з наведених діянь (наприклад, розграбування національних цінностей на окупованій території) в нормі ст. 438 КК не потребують обов'язкового звернення до міжнародно-правових актів, однак, фактично, розуміння змісту всіх діянь, зазначених у цій статті, неможливе без звернення до документів міжнародного рівня.

Важливим нормативно-правовим актом для встановлення змісту воєнних злочинів є Римський статут МКС, який наразі є головним міжнародно-правовим інструментом притягнення до відповідальності воєнних злочинців. 21 серпня 2024 р. Верховна Рада України прийняла Закон України про ратифікацію Римського статуту МКС та поправок до нього¹. Ратифікувавши Римський статут, Україна стає його повноправною учасницею з усіма правами і обов'язками. 09.10.2024 р. Верховна Рада України приймає Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Римського статуту Міжнародного кримінального суду та поправок до нього»². Тим самим Україною здійснено перший, вкрай значущий крок, з імплементації положень Римського статуту МКС у національний нормативно-правовий простір. Потрібно зазначити, що одним із завдань при імплементації положень Римського статуту МКС до КК є зближення визначень злочину агресії, воєнних злочинів та злочинів проти людяності. Необхідність такого текстуального зближення пов'язана із визнанням юрисдикції Міжнародного кримінального суду і його взаємодією з національними органами, насамперед, по ситуації

¹ Про ратифікацію Римського статуту Міжнародного кримінального суду та поправок до нього: Закон України від 21.08.2024 № 3909-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/3909-20#Text> (дата звернення: 16.10.2024).

² Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Римського статуту Міжнародного кримінального суду та поправок до нього: Закон України від 09.10.2024 № 4012-IX. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/4012-20#Text> (дата звернення: 16.10.2024).

в Україні¹. Так, ст. 437 КК отримала назву «Злочин агресії» на заміну попередньої «Планування, підготовка, розв'язування та ведення агресивної війни», ст. 438 КК – «Воєнні злочини» замість «Порушення законів та звичаїв війни». Слід зазначити, що діяння, зазначені в ст. 438 КК «Воєнні злочини», на сьогодні загалом відповідають Женевським конвенціям та додаткам до них. Це означає, що КК в цій частині певним чином відповідає і Римському статуту МКС, який приймався на основі Женевських конвенцій та додатків до них. Разом з тим, текстуальне відображення воєнних злочинів у ст. 438 КК потребує нагальних змін, оскільки частина діянь, зазначених у диспозиції норми цієї статті, формально може бути застосована без посилення на міжнародно-правові акти. Однак реально правозастосувач звертається до таких актів, оскільки в їх нормах діяння визначені більш конкретизовано, ніж у нормі ст. 438 КК. Тому виглядає доречною пропозиція, що надана Головним юридичним управлінням Апарату Верховної Ради України у зауваженнях до проєкту Закону України про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Римського статуту Міжнародного кримінального суду та поправок до нього (реєстровий № 11484 від 15.08.2024). Запропонована така редакція диспозиції норми ст. 438 КК: «Порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а так само вчинення одного або декількох діянь, передбачених статтею 8 Римського статуту Міжнародного кримінального суду»².

¹ Варто зазначити, що в проголосованому Законі України про ратифікацію Римського статуту Міжнародного кримінального суду та поправок до нього (№ 0285 від 15.08.2024 р.) акцентується увага на невизнанні юрисдикції Міжнародного кримінального суду стосовно воєнних злочинів, що були вчинені громадянами України, протягом 7 років після набрання Римським статутом чинності для України.

² Головне юридичне управління Верховної Ради України. Зауваження до проєкту Закону України про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Римського статуту Міжнародного кримінального суду та поправок до нього (до реєстр. № 11484 від 15.08.2024 (друге читання)). *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/44725> (дата звернення: 16.10.2024).

Дослідження воєнних злочинів за Римським статутом МКС, що, як вже зазначалося, відповідає Женевським конвенціям та додаткам до них, дає можливим побачити, що певна частина з них є інформаційними кримінально-протиправними діяннями. Це викликано тим, що такі воєнні злочини мають вчинятися із використанням інформації, яка приховується, перекручується, незаконно змінюється тощо. На наш погляд, за Римським статутом МКС до таких інформаційних кримінально-протиправних діянь, що посягають на мир та міжнародний правопорядок шляхом вчинення воєнних злочинів, відносяться:

I. Інші серйозні порушення законів і звичаїв, що застосовуються у міжнародних збройних конфліктах:

- 1.1) неналежне використання прапора парламентарера, прапора чи військових знаків розрізнення та форми ворога або Організації Об'єднаних Націй, а також розпізнавальних емблем, встановлених Женевськими конвенціями, наслідком чого є смерть або заподіяння особі серйозних ушкоджень;
- 1.2) заява про те, що пощади не буде;
- 1.3) оголошення скасованими, призупиненими або недопустимими в суді прав і позовів громадян ворожої сторони;
- 1.4) примушення громадян ворожої сторони до участі у воєнних діях проти їхньої власної країни, навіть якщо вони перебували на службі воюючої сторони до початку війни;
- 1.5) набір або вербування дітей віком до п'ятнадцяти років до складу національних збройних сил або використання їх для активної участі в бойових діях;

II. У разі збройного конфлікту неміжнародного характеру, грубі порушення статті 3, спільної для чотирьох Женевських конвенцій від 12 серпня 1949 року, а саме: будь-яке з таких діянь, вчинених стосовно осіб, які не беруть активної участі у бойових діях, у тому числі військовослужбовців, що склали зброю, та осіб, виведених зі строю в результаті хвороби, поранень, тримання під вартою чи з будь-якої іншої причини:

- 2.1) посягання на людську гідність, зокрема образливе і принизливе поводження;

- 2.2) винесення вироків і приведення їх до виконання без попереднього рішення, ухваленого створеним у встановленому порядку судом, який забезпечує дотримання всіх судових гарантій, які загально визнані обов'язковими;

*III. Інші серйозні порушення законів і звичаїв, що застосовують-
ся у збройних конфліктах неміжнародного характеру:*

- 3.1) набір або вербування дітей віком до п'ятнадцятих років до складу збройних сил чи груп або використання їх для активної участі в бойових діях;
- 3.2) віддання розпоряджень про переміщення цивільного населення з причин, пов'язаних з конфліктом, якщо тільки цього не вимагають міркування безпеки відповідного цивільного населення або настійна необхідність військового характеру.

На підтвердження прямого зв'язку Римського статуту МКС з Женевськими конвенціями та додатками до них потрібно зазначити, що в ст. 3 I ЖК, ст. 3 II ЖК, ст. 3 III ЖК, ст. 3 IV ЖК вказано на заборону таких діянь як: наруга над людською гідністю, зокрема образливе та принизливе ставлення; засудження та застосування покарання без попереднього судового рішення, винесеного судом, який створено належним чином і який надає судові гарантії, визнані цивілізованими народами як необхідні. У кожній із цих Женевських конвенцій 1949 р. зазначені серйозні порушення, які напряму пов'язуються із воєнними злочинами в контексті ст. 438 КК України, що, зокрема, можуть полягати й у формі інформаційних кримінально-протиправних діянь:

- 1) *примушування військовополоненого до служби в збройних силах ворожої держави або умисне позбавлення його прав на справедливе та належне судове розслідування, передбачених цією Конвенцією (ст. 130 III ЖК);*
- 2) *примушення особи, що перебуває під захистом, служити в збройних силах ворожої держави, або умисне відбирання в особи, що перебуває під захистом, прав на справедливий і офіційний судовий процес, рекомендований цією Конвенцією, (ст. 146 IV ЖК);*
- 3) *віроломне використання на порушення статті 37 розпізнавальної емблеми Червоного Хреста, Червоного Півмісяця або*

Червоного Лева і Сонця, або інших захисних знаків, визнаних Конвенціями і цим Протоколом (п. f ч. 3 ст. 85 I Додаткового протоколу до ЖК)¹;

- 4) *заборона видавати наказ не залишати нікого в живих, знущання над людською гідністю, погроза вчинити будь-які заборонені діяння; діти, які не досягли п'ятнадцятирічного віку, не підлягають вербуванню у збройні сили або групи, і їм не дозволяється брати участь у воєнних діях (ст. 4 II Додаткового протоколу до ЖК), ...погрози насильством, що мають на меті тероризувати цивільне населення (ст. 13 II Додаткового протоколу до ЖК).*

Також не слід забувати й про порушення звичаїв війни, що закріплені в звичасвому міжнародному гуманітарному праві, вчинення яких пов'язується із серйозністю порушень нормативних положень задуваних міжнародних актів, якщо вони ставлять у небезпеку осіб або об'єкти, що знаходяться під захистом, або порушують важливі соціальні цінності (принципи). Саме остання форма серйозних порушень може бути віднесена, перш за все, до інформаційних кримінально-протиправних діянь². Вважаємо, що до порушень звичаїв війни інформаційного характеру можна віднести такі норми звичасвого МГП:

- 1) Норма 46. Заборона віддавати наказ не залишати нікого в живих, погрожувати цим противнику або вести воєнні дії на цій основі;
- 2) Норма 58. Неналежне використання білого прапора паремир'я заборонено;
- 3) Норма 59. Неналежне використання розпізнавальних емблем, зазначених в Женевських конвенціях, заборонено;

¹ Потрібно звернути увагу, що незаконне використання емблем Червоного Хреста, Червоного Півмісяця, Червоного Кристала, яке за своєю суттю є воєнним злочином, порушенням звичасвого міжнародного гуманітарного права та Женевських конвенцій 1949 р. в Україні охороняється окремими ст.ст. 435, 445 КК України.

² Rule 156. Definition of War Crimes. *International Humanitarian Law Databases*: of website. URL: <https://ihl-databases.icrc.org/en/customary-ihl/rules> (data of access: 16.10.2024).

- 4) Норма 60. Забороняється використовувати емблему та форму ООН, окрім як з дозволу цієї Організації;
- 5) Норма 61. Неналежне викорситання інших міжнародно визнаних емблем заборонено;
- 6) Норма 62. Заборонено використовувати прапори, воєнні емблеми, військові знаки відмінності або форменний одяг проти-лежної сторони;
- 7) Норма 63. Заборонено використовувати прапори, воєнні емблеми, військові знаки відмінності або форменний одяг ней-тральних чи інших держав, що не є сторонами конфлікту;
- 8) Норма 64. Заборонено укладати договір про тимчасове зупи-нення бойових дій з наміром неочікувано здійснити напад на противника, що покладається на цю угоду;
- 9) Норма 65. Заборона вбивати, наносити поранення або брати в полон противника, використовуючи віроломство;
- 10) Норма 69. Парламентери, які користуються своїм привіле-йовним статусом для вчинення дій, які протирчать міжнарод-ному праву та заподіюють шкоду противній стороні, втрача-ють право на недоторканність.
- 11) Норма 136. Діти не мають вербуватися до збройних сил або озброєних угруповань;
- 12) Норма 137. Неможна допускати, щоб діти приймали участь у воєнних діях;
- 13) Норма 138. Люди похилого віку, інваліди та немічні, які по-страждали від збройних конфліктів, мають право на особливу повагу та захист;
- 14) Норма 152. Відповідальність командирів за наказ вчинити во-єнний злочин;
- 15) Норма 153. Відповідальність командирів за неспроможність попередити, зупинити або повідомити про воєнні злочини;
- 16) Норма 154. Виконання наказів вищого керівництва;
- 17) Норма 155. Захист від наказів командира та ін.¹

¹ Customary IHL. *International Humanitarian Law Databases*: of. website. URL: <https://ihl-databases.icrc.org/en/customary-ihl/rules> (data of access: 16.10.2024).

Таким чином, наведений орієнтовний перелік інформаційних кримінально-протиправних діянь, що посягають на мир та міжнародний правопорядок шляхом порушень законів та звичаїв війни, вказує на те, що вони становлять окрему групу діянь як на національному, так і міжнародному рівні. При цьому деякі з них є настільки суспільно небезпечними, що становлять окремі злочини. На рівні чинного законодавства України злочинами визнані: Воєнні злочини (ст. 438 КК) та Незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала (ст. 445 КК).

4.4. Інформаційні кримінально-протиправні діяння, що посягають на міжнародний правопорядок шляхом незаконного використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала (ст. 445 КК України)

З часу прийняття символів Червоного Хреста, Червоного Півмісяця, Червоного Кристала їх застосування регулярно супроводжується труднощами, а вони самі є предметом постійних дискусій. Виходячи з того, що будь-яке використання розглядуваної символіки, несанкціоноване Женевськими конвенціями і додатковими протоколами до них, є зловживанням, держави-учасниці зобов'язалися прийняти кримінально-правові заходи, що дозволяють попереджати і припиняти випадки незаконного використання емблеми як у мирний, так і у воєнний час¹. При цьому доречним буде зауважити, що норми міжнародного права не будуть ефективними без належної їх імплементації у законодавство держав.

¹ Поповичук В. О. Міжнародні стандарти закріплення правопорушень у сфері незаконного використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. 2018. Т. 29 (68). № 2. С. 108–114. С. 108.

Незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала є не тільки окремих видом воєнного злочину, але й загалом є інформаційним кримінально-протиправним діянням. Цей висновок базується не тільки на тому, що символіка Червоного Хреста, Червоного Півмісяця, Червоного Кристала визнається специфічною інформацією, а й тому, що при його вчиненні використовується інформаційний спосіб, пов'язаний із введенням в оману супротивника (ворога) щодо реальності медичних та пов'язаних із цим гуманітарних цілей для досягнення тактичної чи стратегічної переваги на полі бою, під час збройного конфлікту чи війни.

Наголошується, що «Міжнародний Рух Червоного Хреста і Червоного Півмісяця має три емблеми: червоний хрест, червоний півмісяць та червоний кристал. Кожна з них має захисний статус, закріплений міжнародним гуманітарним правом у Першій Женевській Конвенції 1949 р. та Третьому Додатковому Протоколі до Конвенції 2005 р. Емблеми надають захист медичному та духовному персоналу збройних сил та особам і об'єктам, які належать до Міжнародного Руху Червоного Хреста та Червоного Півмісяця. Емблеми не мають жодного культурного, релігійного, або політичного значення»¹. У статуті Товариства Червоного Хреста України конкретизується, що «товариство має виключне право на використання емблеми, прапора, розпізнавальних знаків та найменування Червоного Хреста, передбачених Указом Президента України від 28 жовтня 1992 р. «Про Товариство Червоного Хреста України», Законом України «Про символіку Червоного Хреста, Червоного Півмісяця, Червоного Кристала в Україні» від 8 липня 1999 р., правилами використання національними товариствами емблеми Червоного Хреста і Червоного Півмісяця 1991 р., прийнятими XX Міжнародною конференцією (Відень, 1965 р.) і переглянутими Радою делегатів (Будапешт, 1991 р.), Додатковим протоколом III від 8 грудня 2005 р. (Женева, 2005), пунктом 2 Резолюції 1 XXIX Міжнародної конференції Чер-

¹ Символіка міжнародного руху та захист емблеми. *Товариство Червоного Хреста України*: вебсайт. URL: <https://redcross.org.ua/ihl/emblem-protection/> (дата звернення: 16.10.2024).

воного Хреста та Червоного Півмісяця від 22 червня 2006 р. та Статутом Товариства Червоного Хреста України для цілей, визначених міжнародними конференціями Червоного Хреста і Червоного Півмісяця, відповідно до Женевських конвенцій 1949 р.»¹.

Зрозуміло, що положення, які використовуються національними товариствами Червоного Хреста в різних країнах, сформульовані в міжнародних актах, найбільш важливим серед яких є Женевські конвенції та додаткові протоколи до них. І саме ці конвенції наголошують на необхідності захисту як представників означених організацій, так і їх емблем.

Зокрема, у ст.ст. 38, 44 Конвенції про поліпшення долі поранених і хворих у діючих арміях від 12 серпня 1949 р. (I Женевська конвенція), ст.ст. 24, 25 Конвенції про поліпшення долі поранених, хворих та осіб, які зазнали корабельної аварії, зі складу збройних сил на морі від 12 серпня 1949 р. (II Женевська конвенція) та ст.ст. 21, 22 Конвенції про захист цивільного населення під час війни від 12 серпня 1949 р. (IV Женевська конвенція) визначені певні правила та ситуації використання відмітної емблеми товариств Червоного Хреста.

Першим додатковим протоколом до Женевських конвенцій від 12 серпня 1949 р., що стосується захисту жертв міжнародних збройних конфліктів, від 8 червня 1977 р. було заборонено використовувати не за призначенням розпізнавальну емблему Червоного Хреста, Червоного Півмісяця, Червоного Лева і Сонця або інші емблеми, знаки та сигнали, передбачені Конвенціями або цим Протоколом. Також заборонено навмисно зловживати під час збройних конфліктів іншими міжнародно визнаними захисними емблемами, знаками та сигналами, включаючи прапор перемир'я та захисну емблему культурних цінностей (ст. 38).

Другим додатковим протоколом до Женевських конвенцій від 12 серпня 1949 р., що стосується захисту жертв збройних конфліктів неміжнародного характеру від 8 червня 1977 р. також наголошується, що емблема Червоного Хреста, Червоного Півмісяця або Червоного

¹ Символіка міжнародного руху та захист емблеми. *Товариство Червоного Хреста України*: вебсайт. URL: <https://redcross.org.ua/ihl/emblem-protection/> (дата звернення: 16.10.2024).

Лева і Сонця користується повагою за всіх обставин. Особливо наголошується на тому, що ця емблема не повинна використовуватися не за призначенням (ст. 12). Певні особливості використання таких емлем також згадуються в Третьому додаковому протоколі до Женевських конвенцій від 12 серпня 1949 р, що стосується прийняття додаткової відмітної емблеми від 8 грудня 2005 р. (ст.ст. 1, 2 та ін.).

За звичаєвим міжнародним гуманітарним правом ця норма є досить давньою, визнаною ще в Кодексі Лібера, Брюссельській декларації та Оксфордському керівництві. Вона була кодифікована в Гаазьких положеннях 1899 р. та 1907 р. і в Женевських конвенціях 1906 р., 1929 р. і 1949 р.¹. У звичаях ведення війни також вказується, що заборонено використовувати відмітні емблеми вказані в Женевських конвенціях (норма 59) та інші міжнародно визнані емблеми (норма 61)². Важливим є те, що Римський статут МКС визнає воєнним злочином «неналежне використання прапора парламентаря, прапора чи військових знаків розрізнення та форми ворога або ООН, а також розпізнавальних емблем, встановлених Женевськими конвенціями, наслідком чого є смерть або заподіяння особі серйозних ушкоджень».

Слід акцентувати увагу, що в КК було включено одразу дві норми, які захищають символіку цих організацій:

- 1) незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала та зловживання нею (ст. 435 КК, військове кримінальне правопорушення);
- 2) незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала (ст. 445 КК, кримінальне правопорушення проти миру, безпеки людства та міжнародного правопорядку).

Особливостями викладення норм у ст.ст. 435 та 445 КК є їх відповідність міжнародним актам, формальне дублювання та неконкретизованість певних визначень. Відповідність означених норм поло-

¹ Див. дет.: Хенкертс Ж.-М., Досвальд-Бек Л. Звичаєве міжнародне гуманітарне право. Норми. МКЧХ, 2006. С. 267.

² Там само. С. 267–273.

женням міжнародного права передбачає необхідність звернення до міжнародних норм та звичаїв ведення війни для більш поглибленого розуміння змісту таких інформаційних кримінально-протиправних діянь. Також важливою особливістю стає і те, що ці кримінально-протиправні діяння є інформаційними, коли інформаційний спосіб їх вчинення є домінуючим і робить можливим їх вчинення загалом, що пов'язується з незаконним використанням символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала та введенням в оману їх демонстрацією.

Значається, що правоохоронними органами України, у тому числі Національною поліцією та військовою прокуратурою, жодного кримінального провадження до 2020 р. за ознаками кримінальних правопорушень, передбачених ст.ст. 435 та 445 КК, не зареєстровано¹. Лише у 2020 р. вперше в Україні в Єдиному реєстрі досудових розслідувань було зареєстровано кримінальне правопорушення за ст. 445 КК. У 2022 р. було зареєстровано 1 кримінальне правопорушення за ст. 445 КК, у 2023 р. – 0, у січні – травні 2024 р. – 5².

Досить актуальним є також питання відмежування кримінального правопорушення, передбаченого ст. 445 КК, від суміжних кримінальних правопорушень, особливо передбаченого ст. 435 КК. Назви зазначених кримінальних правопорушень є фактично тотожними. Однак слід звернути увагу, що зазначені норми розміщені в різних

¹ Поповичук В. О. Судова практика незаконного використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала в зарубіжних країнах, проблематика правозастосування та кваліфікації цих кримінальних правопорушень в Україні. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: юридичні науки. 2020. Том 31 (70). № 5. С. 99–105. С. 103.

² Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2>; Єдиний звіт про кримінальні правопорушення за січень-травень 2024 року. *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата звернення: 27.06.2024).

розділах Особливої частини КК: ст. 445 КК – у розділі XX «Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку», а ст. 435 КК – у розділі XIX «Кримінальні правопорушення проти встановленого порядку несення військової служби». Отже, родовим об'єктом кримінального правопорушення, передбаченого ст. 445 КК, є суспільні відносини у сфері забезпечення миру, безпеки людства та міжнародного правопорядку, а ст. 435 КК – суспільні відносини, які складаються при проходженні військовослужбовцями військової служби. Відповідно й різними є їх безпосередні об'єкти. Безпосереднім об'єктом кримінального правопорушення, закріпленого у ст. 445 КК, є міжнародний правопорядок у сфері використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала¹. Безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 435 КК, є суспільні відносини, які забезпечують порядок дотримання законів і звичаїв ведення війни в районі воєнних дій, що включає територію, яка зайнята під час бойових дій військами в межах від переднього краю фронту до розташування тилових підрозділів фронту ведення воєнних дій. Такий порядок вироблено міжнародною спільнотою і відображено в міжнародно-правових актах, ратифікованих у тому числі й Україною².

Предметом таких кримінальних правопорушень визнається інформація у формі символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала, яка захищається міжнародним (передусім згадуваними вище Женевськими конвенціями та додатками до них, а також звичаєвим міжнародним гуманітарним правом) та національним законодавством. Слід додатково наголосити, що відповідно до ст. 1 Закону України «Про символіку Червоного Хреста, Червоного Півмісяця, Червоного Кристала в Україні» від 8 липня 1999 р. сим-

¹ Мохончук С. М. Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку. *Кримінальне право України. Особлива частина*: підручник / за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., переробл. і допов. Харків: Право, 2020. Розд. XXI. С. 744.

² Поповичук В. О. Кримінальна відповідальність за незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала : . дис. ... канд. юрид. наук : 12.00.08. Київ, 2018. С. 76.

воліка Червоного Хреста, Червоного Півмісяця, Червоного Кристала (у тому числі Міжнародного руху Червоного Хреста та Червоного Півмісяця) – це емблеми Червоного Хреста, Червоного Півмісяця, Червоного Кристала (зображення відповідно червоного хреста на білому тлі; червоного півмісяця на білому тлі; червоної рамки у формі квадрата на білому тлі, що стоїть на одній із своїх вершин), назви (слова «Червоний Хрест», «Червоний Півмісяць», «Червоний Кристал») і розпізнавальні сигнали (спеціальні міжнародно визнані допоміжні сигнали (світлові, радіо-, електронні), що використовуються як захисні та розпізнавальні знаки для позначення осіб, рухомого та нерухомого майна відповідно до Женевських Конвенцій про захист жертв війни від 12 серпня 1949 р., Додаткових протоколів до них та цього Закону¹.

Об'єктивна сторона кримінального правопорушення, передбаченого ст. 445 КК, виявляється в порушенні встановленого в міжнародно-правових актах та національному законодавстві режиму використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала. Незаконне використання символіки може полягати у носінні її особами, які не мають на це права, незаконному позначенні транспортних засобів, іншого майна або певних зон і територій на місцевості, використанні майна з незаконно нанесеною символікою тощо².

Відповідно до ст. 15 Закону України «Про символіку Червоного Хреста, Червоного Півмісяця, Червоного Кристала в Україні» забороняється використання емблем Червоного Хреста, Червоного Півмісяця, Червоного Кристала, комбінацій цих емблем; слів «Червоний Хрест», «Червоний Півмісяць», «Червоний Кристал», комбінацій цих слів; розпізнавального знака чи будь-якого іншого знака,

¹ Про символіку Червоного Хреста, Червоного Півмісяця, Червоного Кристала в Україні: Закон України від 8 липня 1999 р. № 862-XIV. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/862-14#Text> (дата звернення: 27.06.2024).

² Киричко В. В. Злочини проти миру, безпеки людства та міжнародного правопорядку. *Кримінальний кодекс України. Науково-практичний коментар*: у 2 т. за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна. 5-те вид., допов. Право, 2013. Розділ XX. С. 1001.

найменування або сигналу, які являють собою імітацію (використання подібних кольорів або зображень) або можуть призвести до змішування, незалежно від мети такого використання, з порушенням положень цього Закону і Правил. Забороняється використання зазначених емблем або слів на вивісках, плакатах, оголошеннях, листівках, або розміщення їх на товарах чи упаковках, або продаж цих товарів чи спроба продажу; спроба введення в обіг товарів, помічених таким чином; або використання зазначених емблем або слів як елемента знака для інших емблем або найменувань, з порушенням положень цього Закону і Правил. Забороняється використання слів «Червоний Хрест», «Червоний Півмісяць», «Червоний Кристал», комбінацій цих слів у найменуваннях підприємств, установ, організацій незалежно від форм власності; зображення емблем Червоного Хреста, Червоного Півмісяця, Червоного Кристала на знаках для товарів і послуг, промислових зразках; використання цих слів або зображень як елемента знака для товарів і послуг, промислових зразків чи найменувань згідно з чинним законодавством України¹.

Водночас об'єктивна сторона кримінального правопорушення, передбаченого ст. 435 КК, включає таку обов'язкову ознаку, як місце вчинення в районі воєнних дій, а також обставини, за яких було вчинено кримінальне правопорушення, – вчинення в умовах особливого періоду (ч. 1 ст. 435 КК) або в умовах воєнного стану (ч. 2 ст. 435 КК). Законодавством не визначено критерії та характеристики, які формулюють поняття «район воєнних дій». Під районом воєнних дій розуміється територія, на якій ведуться воєнні (бойові) дії. Визначення конкретних меж такого району є формально-визначеним поняттям, а його зміст визначається з урахуванням інтенсивності бойових дій, чисельності військ, тощо².

¹ Про символіку Червоного Хреста, Червоного Півмісяця, Червоного Кристала в Україні: Закон України від 8 липня 1999 р. № 862-XIV. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/862-14#Text> (дата звернення: 27.06.2024).

² Поповичук В. О. Кримінальна відповідальність за незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала : . дис. ... канд. юрид. наук : 12.00.08. Київ, 2018. С. 156.

Суб'єктивна сторона кримінальних правопорушень, передбачених ст.ст. 435 та 445 КК передбачає наявність вини у формі прямого умислу. Суб'єкт усвідомлює, що використовує символіку Червоного Хреста, Червоного Півмісяця, Червоного Кристала, не маючи на те права і бажає її використати в немедичних та пов'язаних із цим гуманітарних цілях.

Суб'єктом кримінального правопорушення, передбаченого ст. 445 КК, може бути:

- 1) загальний суб'єкт, яким є фізична осудна особа, якій на момент вчинення кримінального правопорушення виповнилось 16 років;
- 2) спеціальний суб'єкт, яким є особа, яка входить до складу медичного або духовного персоналу організацій Міжнародного руху Червоного Хреста і Червоного Півмісяця, або службова особа підприємства за визначених умов об'єктивної сторони.

До того ж, суб'єкт розглядуваного складу кримінального правопорушення буде службовою особою, оскільки службовими особами визнаються посадові особи іноземних держав, включаючи працівників міжнародної організації чи будь-яких інших осіб, уповноважених такою організацією діяти від її імені. Водночас ст. 445 КК охоплено випадки, коли суб'єкт кримінального правопорушення буде спеціальним, наприклад, при використанні емблеми Червоного Хреста, Червоного Півмісяця, Червоного Кристала для позначення медичного, духовного персоналу іноземних організацій, що входять до Міжнародного руху Червоного Хреста і Червоного Півмісяця, не під час їх перебування в офіційному відрядженні в Україні¹.

Суб'єкт кримінального правопорушення, передбаченого ст. 435 КК, є спеціальним. Ним визнається тільки військовослужбовець Збройних Сил України, Служби безпеки України, Державної прикордонної служби України, Національної гвардії України та інших військових формувань, утворених відповідно до законів України, Державної спеціальної служби транспорту, Державної служби спе-

¹ Поповичук В. О. Кримінальна відповідальність за незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала : . дис. ... канд. юрид. наук : 12.00.08. Київ, 2018. С. 157.

ціального зв'язку та захисту інформації України, а також інші особи, визначені законом (див. ст. 401 КК).

У судовій практиці України були встановлені факти, коли різні особи з корисливих мотивів, імітуючи своє відношення до руху Червоного Хреста (саме представляючись усно, без наявних письмових підтверджень), заволодівали грошовими коштами та майном громадян, підриваючи тим самим авторитет Міжнародного руху Червоного Хреста та Червоного Півмісяця. Так, суб'єкт однією дією посягає на два об'єкти: економічні відносини власності (ст.ст. 185, 190 КК); міжнародний правопорядок у сфері використання символіки Червоного Хреста (ст. 445 КК). Прикладом цього є вироки Чуднівського районного суду Житомирської області від 25 квітня 2013 р.¹, Кролевецького міськрайонного суду Сумської області від 28 травня 2015 р.², Тернопільського міськрайонного суду Тернопільської області від 25 травня 2015 р.³ та Вінницького міського суду Вінницької області від 21 вересня 2017 р.⁴. На нашу думку, така судова практика є такою, що не відображає звичаєве міжнародне гуманітарне права та не знаходиться у зв'язку із порушенням законів та звичаїв війни і такою, що не здатна досягнути на мир, безпеку людства та міжнародний правопорядок. На нашу думку, продемонстровані діяння, де вербально або невербально із застосуванням обману використовуюва-

¹ Вирок Чуднівського районного суду Житомирської області від 25 квітня 2013 року (справа № 625/1747/2012, провадження № 1/294/289/13). Єдиний державний реєстр судових рішень: оф. вебсайт. URL: : <https://reyestr.court.gov.ua/Review/30933399> (дата звернення: 27.06.2024).

² Вирок Кролевецького міськрайонного суду Сумської області від 28 травня 2015 року (судова справа № 579/621/15-к, провадження № 1-кп/579/45/15). Єдиний державний реєстр судових рішень: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/44575828> (дата звернення: 27.06.2024).

³ Вирок Тернопільського міськрайонного суду Тернопільської області від 25 травня 2015 року (справа № 607/7490/15-к). Єдиний державний реєстр судових рішень: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/46129905> (дата звернення: 27.06.2024).

⁴ Вирок Вінницького міського суду Вінницької області від 21 вересня 2017 року (справа № 127/17120/15-к, провадження № 1-кп/127/34/17). Єдиний державний реєстр судових рішень: оф. вебсайт. URL: <https://reyestr.court.gov.ua/Review/69682966> (дата звернення: 27.06.2024).

лися емблеми товариств Червоного Хреста з корисливих мотивів не можуть кваліфікуватися за ст. 445 КК. Натомість, коли використання таких емблем набуває ознак воєнного злочину, пов'язується із порушенням міжнародного правопорядку, що зводиться до порушення звичаїв ведення війни, то таке діяння має бути кримінально-караним.

4.5. Інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок шляхом здійснення публічних закликів до геноциду (ч. 2 ст. 442 КК України)¹

За національним законодавством у структурі норми ст. 442 КК «Геноцид» у ч. 2 визначено суспільно небезпечне діяння, що є різновидом інформаційних кримінально-протиправних діянь: *«публічні заклики до геноциду, а також виготовлення матеріалів із закликами до геноциду з метою їх розповсюдження або розповсюдження таких матеріалів»*². Наведене визначення ґрунтується на положенні ст. III Конвенції про запобігання геноциду та покарання за нього 1948 р., відповідно до якого караним також є *«прямі та публічні заклики до вчинення геноциду»*.

Кваліфікація геноциду потребує розуміння співвідношення цього суспільно небезпечного діяння зі злочином агресії, а також із воєнними злочинами та злочинами проти людяності. Із початком широкомасштабного російського вторгнення питання визнання певних діянь геноцидом стали актуальними в українських реаліях, оскільки

¹ Примітка. Матеріал цього підрозділу ґрунтується на положеннях ст. 442 у редакції до внесення змін Законом України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Римського статуту Міжнародного кримінального суду та поправок до нього» від 09.10.2024 р. № 4012-IX.

² Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. *Верховна Рада України. Законодавство України*: оф. вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 27.06.2024).

публічні заклики з боку ворога до знищення української державності разом із знищенням української ідентичності набули потенціальної загрози.

У Конвенції про запобігання злочину геноциду та покарання за нього 1948 р. визначено, що геноцидом є будь-яке з діянь, вчинене з наміром знищити, повністю або частково, національну, етнічну, расову або релігійну групу як таку:

- а) вбивство членів такої групи;
- б) заподіяння серйозних тілесних ушкоджень або психічного розладу членам такої групи;
- в) умисне створення для такої групи умов життя, розрахованих призвести до її повного або часткового фізичного знищення;
- г) впровадження заходів, спрямованих на запобігання дітонародженню в такій групі;
- д) примусове переміщення дітей такої групи до іншої групи (ст. II).

Фактичними формами геноциду у цій Конвенції встановлено:

- а) геноцид;
- б) змова з метою вчинення геноциду;
- в) *прямі та публічні заклики до вчинення геноциду*;
- г) замах на вчинення геноциду;
- д) співучасть у геноциді (ст. III).

Р. Лемкін, як ідеолог поглядів щодо необхідності рішучої протидії геноциду та введення цього терміна в науковий та практичний обіг у міжнародному праві, вказував, що геноцид не має мети негайного знищення національної групи шляхом масових убивств її членів, а, скоріше, є комплексом спланованих дій, спрямованих на знищення основ такої групи. Ціллю геноциду щодо українців за часів радянської влади Р. Лемкін визначив «релігійний, інтелектуальний і політичний провід», і тому «радянська сокира вдарила з повним розмахом саме по цих групах, вдаючись до відомих знарядь масового вбивства, депортації, примусової праці, заслання і голоду»¹.

¹ Лемкін Р. Радянський геноцид в Україні (стаття 33 мовами) / за ред. Р. Сербин; упоряд. О. Стасюк. Київ: Вид-во Мельник М. Ю., 2020. С. 54.

Комплекс дій, вчинення яких спрямовано на знищення національної, етнічної, расової або релігійної групи, і є метою здійснення геноциду. Прояви знищення таких груп в різні проміжки часу стосувалися геноциду вірмен на території Османської імперії та Турецької республіки (1915–1923), масової загибелі людей в Україні під час Голодомору (1932–1933), геноциду етнічної групи тутсі в Руанді (1994), геноциду боснійських мусульман у Сребрениці (Боснія, 1995).

Розгортання широкомасштабної російської агресії проти України з 2022 р., що супроводжується вчиненням вкрай нелюдських дій проти цивільного населення нашої країни, дає підстави до визнання їх геноцидом в Україні вже в XXI ст. Так, в 2023 р. Президент України Володимир Зеленський на Генеральній Асамблеї ООН назвав масове викрадення та депортацію українських дітей на тимчасово окупованих територіях геноцидом¹. Відповідно до цих дій Міжнародний кримінальний суд за вчинення воєнного злочину видав ордери на арешт Президента РФ Володимира Путіна та уповноваженої з прав дитини Марії Львової-Белової². У 2024 р. на Генеральній асамблеї ОБСЄ дії Росії було визнано геноцидом проти Українського народу³. Також у цьому ж році на засіданні ПАРЕ було визнано геноцидом дії Росії проти української культурної ідентичності⁴.

Важливим і складним у виявленні, розслідуванні та кваліфікації є кримінально-правовий аналіз прямих та публічних закликів до вчинення геноциду, які супроводжують та передують фізичному ге-

¹ Це геноцид: Президент про викрадення Росією українських дітей. *Укрінформ*: вебсайт. URL: <http://www.ukrinform.ua/amp/rubric-politics/3763484-ce-genocid-prezident-pro-vikradenna-rosie-u-ukrainskih-ditej.html> (дата звернення: 27.06.2024).

² Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova. *International Criminal Court*: of website. URL: <https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and> (дата звернення: 27.06.2024).

³ Ivashkiv O. OSCE Parliamentary Assembly adopts resolution recognising Russia's actions as genocide of Ukrainian people. *Ukrainska Pravda*: of website. URL: <https://www.pravda.com.ua/eng/news/2024/06/30/7463294/> (дата звернення: 27.06.2024).

⁴ Pavliuk O., Oliynyk T. PACE adopts three resolutions on Ukraine, mainly on special tribunal for Russia and on cultural genocide. *Ukrainska Pravda*: of website. URL: <https://www.pravda.com.ua/eng/news/2024/06/26/7462780/> (дата звернення: 27.06.2024).

ноциду, що призводить до масових жертв, часткового або повного знищення національної, етнічної, расової або релігійної групи.

Перші зафіксовані в правовому сенсі публічні заклики до геноциду були розглянуті на Міжнародному трибуналі в Нюрнберзі в 1946 р., коли Юліуса Штрейхера, редактора антисемітського щотижневого журналу «Der Sturmer», було обвинувачено в злочині проти миру, а Ханса Фріче, який вів щотижневу передачу «Говорить Ханс Фріче», – за воєнні злочини¹. Історичним прикладом також є випадок, зафіксований у вироку Міжнародного кримінального трибуналу щодо злочинів у Руанді, коли в передачі на радіо RTLM містилися етнічні стереотипи, які поширювались у спосіб, що пропагує презирство та ненависть до населення тутсі, знищення окремої етнічної групи (геноциду). У цих передачах слухачів закликали шукати ворога зі зброєю в руках, транслиували імена тутсі, їхніх сімей та політичних опонентів хуту, що призвело до їх вбивств та сплеску жорстокості².

Подібна ситуація простежується й в Україні, коли ще до початку російської агресії проти України в 2014 р. «рупори Кремля» в ЗМІ реалізовували інформаційну політику невизнання української ідентичності, культури, створення стереотипу «єдиного народу», нав'язуючи агресивний воєнний спосіб вирішення «українського питання», зокрема шляхом повного знищення української державності, національної, мовної, культурної, історичної та релігійної ідентичності.

Публічні заклики до вчинення геноциду як окреме діяння міститься не тільки в Конвенції про запобігання злочину геноциду та покарання за нього 1948 р., але й, як вже було зазначено, у ч. 2 ст. 442 КК. Цікаво, що Римський статут МКС не включає публічні заклики до вчинення геноциду як його окремої форми (ст. 6), однак має окрему вказівку щодо індивідуальної кримінальної відповідальності та покарання за такі дії (ст. 25).

¹ Timmermann W. K. Incitement in International Criminal Law. *International Review of the Red Cross*. 2006. Vol. 88. No. 864. P. 827.

² Опришко Л. Відповідальність ЗМІ за геноцид. Приклад Руанди. ЖТА: вебсайт. URL: <https://www.jta.com.ua/trends/vidpovidalnist-zmi-za-henotsyd-pryklad-ruandy/> (дата звернення: 27.06.2024).

Складність цієї проблеми пов'язується також із розмежуванням таких публічних закликів до геноциду (ст. 442 КК) із пропагандою війни («публічні заклики до агресивної війни», ст. 436 КК), злочином агресії («планування, підготовка, розв'язування агресивної війни», ст. 437 КК), воєнними злочинами (порушення звичаю війни щодо заборони «наказу не залишити нікого в живих», ст. 438 КК). Від первинної та наступної кваліфікації різного роду публічних закликів, що спричинили російську агресію, розв'язування війни та її ведення з порушенням законів та звичаїв, залежать і особливості розслідування таких діянь. Так, Офіс Генерального прокурора надав список підозрюваних у магістральній справі «24 лютого», в якому фігурують «розпалювачі війни та пропагандисти Кремля»¹. Така правова оцінка дій осіб, зазначених у списку, наближає кваліфікацію вчиненого ними до злочину агресії за ст. 437 КК. Водночас коли здійснені певними особами заклики починають стосуватися повного чи частково знищення української національної групи та/або ідентичності має відбутися перекваліфікація вчиненого на ст. 442 КК.

¹ Список підозрюваних магістральній справі «24 лютого». *Офіс Генерального прокурора*: оф. вебсайт. URL: <https://gp.gov.ua/detectable> (дата звернення: 27.06.2024).

Висновки до розділу IV

1. У здійсненому дослідженні вдалося виокремити інформаційні кримінально-протиправні діяння, що посягають на мир, безпеку людства та міжнародний правопорядок. Розкриття змісту форм інформаційних кримінально-протиправних діянь, що посягають на мир, безпеку людства та міжнародний правопорядок, можливе лише шляхом звернення до міжнародних конвенцій та додаткових протоколів до них, а також до звичаєвого міжнародного гуманітарного права. Враховуючи інтенсивність продовжуваної російської агресії проти України, системне порушення ворогом законів та звичаїв війни, важливого значення набуває напрям наукових досліджень суспільно небезпечних діянь, визнаних злочинами міжнародним правом та вчинення яких пов'язано з використанням інформації. Їх здійснення стає передумовою вчинення ще більш тяжких діянь: злочину агресії, воєнних злочинів, геноциду та злочинів проти людяності.

2. Аналіз таких злочинів, як пропаганда війни (ст. 436 КК), виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436¹ КК), виправдовування, визнання правомірною, заперечення збройної агресії РФ проти України, глорифікація її учасників (ст. 436² КК) дозволив установити проблеми судового тлумачення, що пов'язані з надмірним покладанням на висновки судово-експертних досліджень та спеціалістів, високим рівнем політизованості щодо окремих видів цих злочинів і суб'єктів їх вчинення, а також наявність спірних питань щодо кваліфікації цих злочинів. Усі ці проблеми призводять до складнощів при встановленні ступеня тяжкості вчинених діянь як в Україні, так і в інших державах (Польща, Угорщина).

3. Виявлення різних підходів щодо визначень «злочин агресії» на міжнародному рівні та «планування, підготовка, розв'язування та ведення агресивної війни» на національному рівні (ст. 437 КК) дало можливим сформулювати ряд рекомендацій стосовно кваліфікації цих злочинів. Так, визначення «злочин агресії» допевне складало-

ся як таке, що мало на меті забезпечити переслідування суб'єктів-лідерів держав-агресорів міжнародним кримінальним трибуналом (судом). На національному ж рівні можливостей щодо формально-юридичного переслідування суб'єктів-лідерів більше, тому що, зокрема, в КК суб'єкта визначено узагальнено, а підходи щодо розуміння спеціального суб'єкта (лідера) тільки формуються судовою практикою (передусім Верховним судом).

4. Розгляд воєнних злочинів (ст. 438 КК) зробив можливим надання орієнтовного переліку інформаційних кримінально-протиправних діянь, що посягають на мир та міжнародний правопорядок шляхом порушень законів та звичаїв війни. Вдалося довести, що вони становлять окрему групу діянь як на національному, так і міжнародному рівні (неналежне використання прапора парламентаря, прапора чи військових знаків розрізнення та форми ворога або ООН, а також розпізнавальних емблем, встановлених Женевськими конвенціями; заява про те, що пощади не буде; оголошення скасованими, призупиненими або недопустимими в суді прав і позовів громадян ворожої сторони; набір або вербування дітей віком до п'ятнадцяти років до складу національних збройних сил або використання їх для активної участі в бойових діях тощо). На рівні національного законодавства вчинення таких діянь визнано воєнними злочинами (ст. 438 КК) та незаконним використанням символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала (ст. 445 КК).

5. Дослідження норм ст.ст. 435 та 445 КК, за яких злочинні діяння, ними визначені, пов'язані із незаконним використанням символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала, дало можливим констатувати їх відповідність міжнародним актам, а також віднести до інформаційних кримінально-протиправних правопорушень. Однак, зазначені в них діяння викладені неконкретизовано та відзначаються формальним дублюванням одне одного. Тому для їх застосування вкрай важливим є звернення до міжнародних норм та звичаїв ведення війни.

6. Публічні заклики до вчинення геноциду визнані злочином в нормі ч. 2 ст. 442 КК. Діяння, що наведене в цій нормі, відповідає положенням Конвенції 1948 р. про запобігання злочину геноциду

та покарання за нього. При цьому встановлено, що Римський статут МКС, який ґрунтується в цьому питанні на положеннях зазначеної конвенції, не включив до числа своїх норм публічні заклики до вчинення геноциду як його окремої форми (ст. 6), між тим містить вказівку щодо індивідуальної кримінальної відповідальності та покарання за такі дії (ст. 25). Також звернута увага на складність відмежування геноциду, пов'язаного з публічними закликами до його вчинення, від публічних закликів до агресивної війни (ст. 436 КК), планування, підготовки, розв'язування агресивної війни (ст. 437 КК), порушення звичаю війни щодо заборони «наказу не залишати нікого в живих» та інших подібних воєнних злочинів (ст. 438 КК). Наголошено, що у випадках, коли публічні заклики стосуються повного або часткового знищення саме національної, етнічної, расової чи релігійної групи має відбуватися кваліфікація за ст. 442 КК (геноцид).

Авторський колектив

РОЗДІЛ I

- В. І. БОРИСОВ** – акад. НАПрН України, д-р юрид. наук, проф., радник при дирекції Інституту (вступні положення; підрозд. 1.2.; висновки)
- О. О. ПАЩЕНКО** – д-р юрид. наук, доц., зав. відділом Інституту (вступні положення; підрозд. 1.1.; висновки)
- Н. В. НЕТЕСА** – канд. юрид. наук, ст. дослідник, учений секретар Інституту (підрозд. 1.3.; висновки)
- В. В. ФЕДОСЄЄВ** – канд. юрид. наук, ст. наук. співроб. Інституту (підрозд. 1.4.; висновки)

РОЗДІЛ II

- Д. П. ЄВТЄЄВА** – канд. юрид. наук, ст. дослідник, заст. директора з наук. роботи Інституту (вступні положення, підрозд. 2.1. у співавт. з Д. О. Куковинець, висновки)
- В. В. БАЗЕЛЮК** – канд. юрид. наук, доц., наук. співроб. Інституту (вступні положення, підрозд. 2.2., висновки)
- Д. О. КУКОВИНЕЦЬ** – мол. наук. співроб. Інституту (вступні положення, підрозд. 2.1. у співавт. з Д. П. Євтеєвою, висновки)

РОЗДІЛ III

- М. В. КАРЧЕВСЬКИЙ** – д-р юрид. наук, проф., гол. наук. співроб. Інституту (вступні положення, підрозд. 3.1, 3.2., висновки у співавт. з В. В. Федюком)
- В. В. ФЕДЮК** – мол. наук. співроб. Інституту (вступні положення, підрозд. 3.1, 3.2., висновки у співавт. з М. В. Карчевським)

РОЗДІЛ IV

- В. І. БОРИСОВ – акад. НАПрН України, д-р юрид. наук, проф., радник при дирекції Інституту (вступні положення; підрозд. 4.3. у співавт. з М. В. Шепітьком; висновки)
- М. В. ШЕПІТЬКО – д-р юрид. наук, проф., пров. наук. співроб. Інституту (вступні положення, підрозд. 4.2.; підрозд. 4.3. у співавт. з В. І. Борисовим; підрозд. 4.4.; підрозд. 4.5. у співавт. з В. В. Базелюк; висновки)
- В. В. БАЗЕЛЮК – канд. юрид. наук, доц., наук. співроб. Інституту (підрозд. 4.5. у співавт. з М. В. Шепітьком, висновки)
- К. А. НОВІКОВА – канд. юрид. наук, ст. наук. співроб. Інституту (підрозд. 4.1., висновки)

Для нотаток

Для нотаток

Наукове видання

**Борисов Вячеслав Іванович,
Пащенко Олександр Олександрович,
Євтєєва Дарина Петрівна та ін.**

КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Монографія

Видається в авторській редакції

Підписано до друку 16.12.2024.

Формат 60×84/16. Ум. друк. арк. 19,06. Обл.-вид. арк. 21,23.

Тираж 100 пр. Зам. № 240

ТОВ «Видавничий дім «Право»,

вул. Харківських Дивізій, 11/2, м. Харків, Україна

Для кореспонденції: а/с 822, м. Харків, 61023, Україна

Тел.: (050) 409-08-69, (067) 574-81-20, (063) 254-50-84

Вебсайт: <https://pravo-izdat.com.ua>

Е-mail для замовників послуг: verstka@pravo-izdat.com.ua

Е-mail для покупців: sales@pravo-izdat.com.ua

Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023

Виготовлено ТОВ «Промарт»,

вул. Весніна, 12, Харків, 61023, Україна

Тел. (057) 717-25-44

Свідоцтво суб'єкта видавничої справи ДК № 5748 від 06.11.2017