Міністерство освіти і науки України
Національний університет «Києво-Могилянська Академія»
Факультет правничих наук
Кафедра кримінального та кримінального процесуального права

Магістерська робота

освітній ступінь – магістр

на тему: «Інформаційні дії у кримінальному праві: питання теорії і практики»
«Information Actions in Criminal Law: Issues of Theory and Practice»

Виконала: студентка 2-го року навчання
Спеціальності
081 Право
Чорна Вікторія Володимирівна
Керівник Багіров С.Р., доцент
Рецензент _____

Магістерська робота захищена з оцінкою _____
Секретар ЕК _____
«___»_____2024 р.

Київ – 2024

ЗМІСТ

KMA LAW Факультет правничих наук

Декларація академічної доброчесності

Я Чорна Вікторія Володимирівна, студентка 2 року навчання магістерської програми за спеціальністю «Право» факультету правничих наук НаУКМА підтверджую таке:

- написана мною магістерська робота на тему «Інформаційні дії у кримінальному праві: питання теорії і практики» відповідає вимогам академічної доброчесності та не містить порушень, передбачених п. 3.1. Положенням про академічну доброчесність здобувачів освіти у НаУКМА, зі змістом якого я ознайомлений;

- я заявляю, що надана мною для перевірки електронна версія роботи є ідентичною її друкованій версії.

10.05.2024 _____ Чорна В. В.

ВСТУП

В епоху стрімкого розвитку технологій, що беззаперечно впливає на суспільство, необхідно не лише розглядати нові можливості для людства, але й усвідомлювати загрози, що супроводжують цей процес. Поняття «інформація» є дуже широким і навіть неосяжним в певній мірі. Саме тому дослідження інформаційних дій є досить багатогранним і складним.

Сьогодні, коли інформаційна війна стала не просто фразою, а реальністю, стає очевидним, що інформація має надзвичайний вплив на свідомість та поведінку людей. Важко осягнути, наскільки сильно різні форми інформаційних дій здатні впливати на суспільно-важливі процеси, часто – безповоротно. Інтернет, як один з найпотужніших інструментів, значно збільшує цей вплив, що може нести нові загрози, як для кожної окремої особи, так і для суспільства в цілому. Зазначене й формулює актуальність цієї роботи. Так, Інтернет створює нові можливості для зловмисників, починаючи від викрадення даних, завершуючи поширенням дезінформації та фейків. Останнє, створює потенційно шкідливий вплив на громадську думку і процеси прийняття рішень, що може нести небезпеку для держави в цілому. На жаль, практика показує, що такими інформаційними діями нехтувати не можна, однак чи можливо створити ефективні правові механізми для врегулювання та запобігання зазначених проблем?

Без заперечень, в ногу із розвитком технологій, необхідно розробляти нові механізми для запобігання і протидії суспільно небезпечним інформаційним діям. Більше того, із стрімким розвитком штучного інтелекту, виникають нові виклики, щодо регулювання інформаційних дій. Однак, перш за все, важливим є вивчення такого явища, як інформаційні дії, що і є предметом дослідження даної роботи.

Наукова спільнота і держави світу все частіше звертають увагу на нові виклики, що прямо пов’язані із інформаційними діями, проте багато аспектів залишаються невивченими. Тому, метою даної роботи є ретельний аналіз концепції інформаційних дій у кримінально-правовому значенні, дослідження теоретичних та практичних підходів до вивчення та врегулювання існуючих проблем, а також спроба сформувати рекомендації, щодо удосконалення

правового регулювання інформаційних дій, зокрема в кримінальному законодавстві.

Враховуючи специфічний характер інформаційних дій та складність однозначно визначити загальне поняття та його ознаки, особливої уваги заслуговує питання визначення методів дослідження інформаційних дій у кримінальному праві.

В межах дослідження інформаційних дій також варто зупинитися і на питанні щодо необхідності впровадження нового інституту в кримінальному праві. Чи варто впроваджувати інститут інформаційних дій для їх ефективного регулювання, або ж достатнім є внесення точкових змін в існуючі норми? Це питання видається досить цікавим і безперечно є важливим та має бути дослідженим в даній роботі.

У світлі вказаного, особливої актуальності набуває проблема визначення кримінально-правового значення інформаційних дій. Дослідження даного питання потребує визначення основних проблем і викликів, що утворюються внаслідок розвитку інформаційних дій та їх значного впливу на суспільство, попереднього аналізу національного законодавства та іноземного досвіду правового регулювання інформаційних дій.

Лише на основі ґрунтовного аналізу вказаних аспектів можливо сформувати якісні та ґрунтовні рекомендації, щодо удосконалення правового регулювання інформаційних дій в кримінальному законодавстві.

Таким чином, метою роботи є не лише дослідження інформаційних дій, як явища, їх вплив та кримінально-правове значення, а й формування дієвих механізмів, що потенційно вирішуватимуть існуючі проблеми.

З аналізу наукової літератури вбачається, що інформаційні дії викликають особливий інтерес в науковців з різних галузей. Так, інформаційні дії в тій чи іншій мірі досліджували науковці Б.О. Соловйов, О.В. Кохановська, О.О. Кулініч, М.В. Карчевський, Д.С. Азаров, О.С. Ховпун, О.В. Домбровська, Г.В. Муляр, І.В. Панова, А.Ю. Нашинець-Наумова, В.С. Батиргареєва, М. Юнгер, Р. Вірінга, П. Гартел та багато інших. Однак в той же час, відсутній єдиний комплексний

підхід до визначення поняття та ознак інформаційних дій, а з урахуванням швидкого розвитку цифрових технологій, деякі з існуючих напрацювань швидко втрачають свою практичну актуальність.

Саме тому, не виникає жодних сумнівів, що дослідження інформаційних дій в кримінальному праві має як наукове так і практичне значення.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ДІЙ

1.1. Огляд сучасних наукових концепцій щодо дослідження інформаційних дій.

В сучасній науковій літературі існує ряд концепцій та підходів, що спрямовані на дослідження інформаційних дій. Хоча дана тема є актуальною та вивчається в рамках різних наукових галузей, однак до сьогодні відсутній єдиний комплексний підхід до визначення поняття та ознак інформаційних дій.

Так, інформаційні дії можна розглядати та досліджувати в аспекті цивільно-правових відносин, де інформаціє виступає об’єктом цивільних прав. Зокрема, дану концепцію досліджували такі науковці, як Б.О. Соловйов, О.В. Кохановська, О.О. Кулініч та багато інших.

Так, на думку Б.О. Соловйова якісне регулювання інформаційних відносин, а відповідно й інформаційних дій залежить від регулювання загальних засад цивільного законодавства. Науковець розглядає концепцію, відповідно до якої саме додаткове закріплення таких принципів, як «свобода інформації та інформаційного обміну» і «неприпустимість свавільного втручання у сферу інформації про особу, персональних даних» забезпечить базис якісного правового регулювання приватноправових відносин в цілому [1].

Важко не погодитись з таким підходом, так як в цифровому світі, де інформація має настільки сильний вплив, неможливо говорити про спеціалізовані підходи до вирішення існуючих проблем, коли в нормативно-правових актах не завжди закріплені базові засади та принципи що стосуються інформації та інформаційних дій.

Також, інформацію, як явище та категорію інформаційного права досліджував Б.А. Кормич. В своїй роботі автор, серед іншого, розглядав інформацію у сфері економіки, як цінний актив із значним комерційним значенням та продукт інтелектуальної праці суспільства. Б.А. Кормич визначав інформацію як «неречовий продукт інтелектуальної діяльності людини і

суспільства», а «виробництво і розповсюдження інформації … є одним із головних напрямів розвитку економіки» [с. 8, 2].

Науковець притримується максимально людиноцентричного підходу, звертаючи увагу, що саме людина завдяки своєму мисленню здатна перетворити сукупність даних на те, що вважається інформацією.

Враховуючи, що дана робота була написана автором до різкого розвитку штучного інтелекту, такий підхід видається досить зрозумілим, однак враховуючи існуючі технології, доцільно зауважити, що на сьогоднішній день не лише людина здатна перетворити сукупність даних на інформацію.

Комп'ютерні технології та існуючі програми вже давно довели, що мають здатність не лише відтворювати інформацію, а й створювати її на основі певного аналізу.

Найбільш практичний підхід до дослідження інформації та інформаційних дій все ж таки зустрічається в наукових роботах в галузі кримінального права.

Так, у своїй спільній праці «Кримінальні правопорушення у сфері інформаційних технологій: особливості розслідування» О.С. Ховпун, О.В. Домбровська та Г.В. Муляр розглядають інформацію як спосіб скоєння кримінальних правопорушень, як засіб (в якості недостовірних даних, які використовує особа з метою впливу на предмет злочинного посягання); та відповідно як частину об'єктивної сторони кримінального правопорушення, що допомагає в реалізації умислу [с.286, 3].

Найбільш комплексною роботою щодо злочинів в сфері комп'ютерної інформації видається монографія Д.С. Азарова «Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)» [4]. Робота має здебільшого практичний характер і є цікавою та цінною для подальшого дослідження інформаційних дій. Як вбачається з дослідження науковця, як для криміналізації суспільно небезпечних діянь в сфері комп'ютерної інформації, так і для криміналізації загалом інформаційних дій необхідним є системний підхід.

Видається, що системного підходу необхідно дотримуватись і при дослідження теоретичних аспектів такого явища, як інформаційні дії.

В контексті інформаційної безпеки та захисту інформаційного простору інформацію досліджувало чимало науковців, як українських, так і іноземних, а саме: І.В. Панова, А.Ю. Нашинець-Наумова, В.С. Батиргареєва, М. Юнгер, Р. Вірінга, П. Гартел та інші.

І.В. Панова в своїй статті «Захист від впливу інформації, що є шкідливою для особи, як принцип інформаційного права» [5] слушно звертає увагу на те, що, в результаті глобальної інформатизації суттєво посилюється інформаційний тиск на психіку людини [5, с. 71], тим самим зміщуючи акцент дослідження впливу інформації саме на людину, як особистість, а не суспільство в цілому та/або державні інтереси.

Іноземні науковці, в свою чергу активно досліджували та досліджують інформацію як явище в кіберпросторі. Так, Юнгер, Р. Вірінга, П. Гартел в свої роботі «Cyber-crime Science = Crime Science + Information Security» [6] звертають особливу увагу на визначенні відмінностей між злочинами та кіберзлочинами. Вони зазначають, що «Cyber-crime usually is non-local, traditional crimeusually is local» [6, с. 30], тобто, кіберзлочинність, на відміну від інших злочинів зазвичай не обмежується територіальною юрисдикцією однієї держави, що зумовлено, зокрема впливом інформації та її неосяжності, як річчі. Науковці підтримують ідею системного підходу та пропонують застосовувати більш інноваційні засоби боротьби, які можливо створити лише досконало дослідивши природу інформаційних дій та їх кримінально-правове значення.

В монографії А.Ю. Нашинець-Наумова «Інформаційна безпека: Питання правового регулювання» [7] науковиця розглядає поняття інформаційної безпеки через різні теоретичні підходи та зауважує, що не дивлячись на згадки досліджуваного поняття в багатьох нормативних актах, як національних, так і міжнародних, жоден з них не дає визначення поняттю [7, с. 26]. Безсумнівно, це може призводити до неоднозначного трактування інформаційної безпеки.

Теж саме стосується і інформаційних дій в цілому. Відсутність єдиного комплексного підходу до визначення даного поняття створює чимало труднощів в правовому регулюванні цього явища.

Досить цікавою для дослідження інформаційних дій також є праця А.А. Тер-Акопова «Преступление и проблемы нефизической причинности в уголовном праве» [8], в якій автор розглядає питання про існування та визнання причин, що не є фізичними, як підстави кримінальної відповідальності за вчинення злочинів. Як зазначає автор, кримінальний закон не завжди виходить з однозначної причинності, адже в багатьох складах злочинів, як підстава для кримінальної відповідальність є не завдання шкоди, а створення для цього усіх умов [8].

Для визначення причинного зв’язку в таких випадках, як зазначає А.А. Тер-Акопов, необхідно використовувати теорію соціально-правового детермінізму, яка пояснює наявність залежностей, які виникають.

Видається, такий підхід слід застосовувати й в контексті дослідження інформаційних дій, зокрема їх практичного значення, адже детермінізм базується на причинності, що передбачає обумовленість всіх явищ і процесів. Так, застосування такого підходу може допомогти виявити ті фактори, які потенційно можуть вплинути або впливають на результати інформаційних дій, такі як зовнішні обставини, технічні чи соціальні аспекти. Це може сприяти кращому розумінню можливих наслідків інформаційних дій, що беззаперечно слід врахувати під час розробки механізмів регулювання інформаційних дій.

Тут доречно згадати ще одну роботу, в якій досліджується питання причинних зв’язків та питання «інформаційної причинності». Так, в своїй дисертації «Теоретичні проблеми причинно-наслідкового зв'язку в кримінальному праві (філософсько-правовий аналіз)» Н.М. Ярмиш зазначала:

> Інформація служить не причиною змін стану або поведінки людини, а всього лише носієм причини. Причина ж формується як результат взаємодії інформації зі свідомістю людини. Проблема інформаційної причинності тісно переплітається з проблемою свободи волі, що є іншою стороною питання про можливість вибору особою того чи іншого варіанта поведінки. [9, с. 9]

Зазначене, додатково підкреслює значення застосування концепції соціально-правового детермінізму при дослідженні як теоретичних, так і практичних питань інформаційних дій.

Наведений огляд не є вичерпним, однак з вищезазначеного вже можна сміливо зробити висновок, що усі концепції щодо дослідження інформаційних дій, так чи інакше зводяться до дослідження інформації, як досить широкого і комплексного явища, через призму впливу інформації як на людину, так й на суспільство в цілому.

Більшість науковців розглядають інформаційні дії з практичної точки зору, іноді ігноруючи факт непередбачуваності впливу інформації на наслідки таких дій, поведінку людини та її сприйняття. В той же час, визначення причинного зв'язку між інформаційними діями та їх наслідками є значно складнішим питанням, ніж визначення поняття інформації та її місце в тій чи іншій галузі права. Безсумнівно, без визначення причинного зв'язку буде неможливо сформувати практичні працюючі механізми та заходи щодо вирішення наявних викликів, зумовлених недосконалим регулюванням інформаційних дій.

Таким чином, видається, що застосування системного підходу та теорії соціально-правового детермінізму дозволить дослідити інформаційні дії найбільш комплексно та ефективно.

1.2. Розвиток і еволюція дослідження інформаційних дій в історичному контексті.

При розгляді сучасних підходів до вивчення інформаційних дій важливо враховувати історичний контекст їх розвитку. Ігнорування історичної ретроспективи означало б нехтування важливим джерелом інформації щодо розуміння проблеми дослідження таких дій.

Аби уникнути будь-яких упущень, видається необхідним звернутись до витоків еволюції досліджень інформаційних дій та подій, що сприяли такому інтересу науковців до даної теми.

Як зазначає Н. Литвин, в своїй роботі «Інформаційне суспільство як головний пріоритет перспективного розвитку держави»:

> Україна має власну історію розвитку базових засад інституту інформаційного суспільства: діяльність всесвітньо відомої школи кібернетики; розроблення на

> початку 90-х років минулого століття концепції та програми інформатизації; створення різноманітних інформаційно-комунікаційних технологій і загальнодержавних електронних інформаційно-аналітичних систем різного рівня та призначення [с.158, 10].

Однак, визначальний вплив на розвиток наукової діяльності в сфері інформаційних дій, все ж таки, мало прийняття лідерами одних з найбільш розвинених держав світу «Хартії глобального інформаційного суспільства» в Окінаві 22 липня 2000 р.

Це фактично перший документ, що на міжнародному рівні визнав, що всі люди без винятку, мають право користуватися перевагами глобального інформаційного суспільства, а стійкість такого суспільства ґрунтується на демократичних цінностях, серед яких вільний обмін інформацією і знаннями. [11].

З того часу науковці почали активно досліджувати поняття інформаційного суспільства, зачіпаючи питання визначення інформації в цілому.

З цього питання цікавою роботою видається праця В.І. Пожуєва «Розвиток концептуальних засад інформатизації сучасного українського суспільства». Науковець досліджував різні концепції та підходи до дослідження інформатизації суспільства та зазначав, що концепція інформаційного суспільства це нова історична фаза розвитку цивілізації, в якій головними продуктами виробництва є інформація і знання [с. 6, 12]. У висновках своєї роботи автор слушно зауважив:

> Державне регулювання повинно забезпечити системність, комплексність і узгодженість розвитку інформатизації країни з використанням при цьому традиційних та нетрадиційних форм і методів супроводження та контролю [с. 15, 12].

Ця теза залишається актуальною і сьогодні, особливо в контексті регулювання інформаційних дій.

Сьогоднішні реалії показують, що інформаційний простір постійно розвивається, із зростанням технологічних можливостей з'являються нові виклики та загрози. Тому державне регулювання повинно бути гнучким і адаптованим до змін, здатним реагувати на еволюцію інформаційних процесів.

Наступним важливим кроком міжнародної спільноти стало прийняття державами-членами Ради Європи Конвенції про кіберзлочинність 23 листопада 2001 року, яку в 2005 році ратифікувала Україна.

Це стало поштовхом для нових досліджень в сфері кібербезпеки, кіберзлочинності та злочинів у сфері комп’ютерної інформації.

Однією з цікавих і досить фундаментальних праць є монографія Д.С. Азарова написана в 2007 році на тему: «Злочини у сфері комп’ютерної інформації (кримінально-правове дослідження)» [4].

Також темі безпеки в інформаційному просторі присвятили свої роботи такі науковці як І.В. Панова, А. Нашинець-Наумова, О. Амелін та багато інших. Їй роботи датуються від 2003 року і зачіпають такі важливі питання, як злочини у сфері інформаційних відносин в міжнародно-правових актах, захист інформаційного простору України засобами кримінального права, тощо.

Вже пізніше з’являються роботи науковців, присвячені практичному вирішенню проблем пов’язаних з кримінальними правопорушеннями у сфері інформаційних технологій. Зокрема, робота Ховпун О., Домбровська О., Муляр Г., що згадувалась раніше.

З аналізу наукових робіт в ретроспективі вбачається, що акценти в дослідженні інформаційних дій змінювалися протягом різних етапів розвитку технологій та інформаційного суспільства. Увага науковців приділялася різноманітним аспектам інформаційних дій відповідно до викликів, які поставали перед людством.

Хоча багато дослідників проводили побічні дослідження у цій області, комплексних робіт, присвячених безпосередньому дослідженню інформаційних дій, зокрема в кримінальному праві, виявилось недостатньо. Відсутність інтегрованих підходів може бути пов'язана зі складністю самого предмету дослідження, який охоплює різноманітні аспекти людської поведінки, технологічного розвитку та соціокультурних впливів.

Результати даного аналізу наочно підкреслюють необхідність подальших досліджень у сфері інформаційних дій. Теоретичні аспекти цього дослідження вимагають глибшого розуміння, оскільки вони відображають складні механізми взаємодії людей з інформацією та технологіями. Таке розуміння може сприяти розвитку більш ефективних стратегій управління інформацією.

1.3. Критичний аналіз підходів до визначення поняття та ознак інформаційних дій.

Як було зазначено раніше, чимало науковців досліджували питання, що прямо чи опосередковано пов’язані з інформаційними діями.

В свої роботах науковці в першу чергу досліджували поняття інформації та розуміння місця інформації в різних галузях. Однак, метою даного розділу є не лише огляд та аналіз напрацювань науковців, а й спроба сформулювати власне поняття інформаційних дій та чітко визначити їх ознаки. Для досягнення поставленої мети, видається логічним прокоментувати існуючі підходи та визначення інформації та інформаційних дій з критичної точки зору.

В своїй роботі С. Демченко «Підходи до змісту поняття «інформація»: кібернетичний, філософський, правовий» [13] розглянула декілька підходів до визначення поняття «інформація».

Автор, в контексті філософського підходу, розглядає інформацію як будь-який переданий зміст, тобто те, що може передатись як змістовність [с.37, 13]. Що ж стосується визначення інформації за правовим підходом, С. Демченко звертає увагу на визначення надані законодавцем в Законі України «Про інформацію» від 02.10.1992 р. та Цивільному кодексі України, відповідно до яких інформація визначається як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [14].

З вказаного логічно зробити висновок, що за правовим підходом, будь-які відомості можуть вважатися інформацією лише коли набувають певного зовнішнього вираження.

Однак, такий підхід до визначення поняття інформації видається досить обмеженим, так як не охоплює всю багатогранність цього явища та не враховує роль інформації, яка може бути вбудована в системи чи процеси, такі як шифри, алгоритми або навіть біологічні механізми.

В той же час, з урахуванням специфіки правового підходу, дане визначення є достатньо чітким та зрозумілим для подальшого правозастосування.

Більш широким є визначення наведене в термінологічній енциклопедії О.О. Селівановою:

> Інформація (від лат informare - зображувати, повідомляти) - сукупність знань, образів, відчуттів, наявних у свідомості людини або штучному інтелекті, які поступають по різних каналах передачі, переробляються й використовуються в процесі життєдіяльності людини й роботі автоматичних комп'ютерних систем [15].

Надане визначення враховує різноманітність форм, у яких може бути представлена інформація і видається досить комплексним та вдалим.

В контексті досягнення мети цієї роботи, вважливо дослідити та врахувати як науковці визначають інформацію саме в контексті кримінального права.

Так, Д.С. Азаров в своїй роботі досліджував питання щодо визнання інформації предметом злочину, його засобом та знаряддям [4].

Тут слід зазначити, що спірні питання виникають стосовно предмету злочину. У випадках, коли мова йде про злочини проти права власності, де предметом є інформація, а не її носій, при визначенні завданої шкоди важливо враховувати зокрема цінність викраденої інформації. В той же час, таку цінність досить складно визначити, адже інформація не є річчю.

Так само складно визнати інформацію знаряддям вчинення злочину, зокрема в традиційному розумінні [4, ст. 247-248].

В загальноприйнятому розумінні, знаряддя - це речі матеріального світу, якими може заподіюватись або заподіяна певна шкода. І хоча інформація може бути втілена у різних формах, таких як символи, електронні сигнали тощо, може міститись на різних носіях, в той же час, вона не має фізичної матеріальності і може існувати незалежно від конкретних носіїв.

Слід зазначити, що інформацію, як знаряддя злочину досліджувала також Д. Прокоф′єва в свої статті «Інформація як знаряддя вчинення злочину та злочини проти інформаційної безпеки», авторка вказує, що «знаряддям скоєння злочину може виступати – інформаційна зброя» [16, с. 31] і навіть виділяє різновиди інформації та інформаційних впливів, що можуть виступати в якості знаряддя

вчинення злочинів, серед яких погроза, завідомо неправдива інформація та деякі інші.

Однак знову ж таки, визначення інформації як знаряддя злочину є досить дискусійним і філософським, адже сама по собі інформації є досить специфічним явищем, як і дії інформаційного характеру, наслідки яких можуть бути непередбачуваними.

Цікавою видається думка, що «інформація формує інформаційну зброю, якщо включається до цілеспрямованої програми впливу на систему-мішень, яка має бути здатною призвести до досягнення запланованих суб′єктом впливу кінцевих результатів» [16, с. 31], однак тут виникає питання чи обов'язково інформація має виражати цілеспрямовану програму впливу аби визнаватись «зброєю», і відповідно знаряддям. Чи допускається кримінальними нормами нецілеспрямований інформаційний вплив, як знаряддя злочину?

Тут варто зауважити, що інформація сама по собі не може мати намірів чи цілей. Вона набуває значення та впливу лише у контексті свого використання. Таким чином, щоб інформація стала «зброєю», її потрібно свідомо використовувати для досягнення певних цілей або впливу на систему-мішень. В той же час, нецілеспрямоване використання також може призвести до впливу на системи, так як інформація є досить потужним інструментом, який може впливати на думки, переконання та поведінку людей.

Як вірно підмічає автор, цитуючи С.П. Расторгуєва «будь-яка інформація, що надходить на вхід системи інформації неминуче змінює систему. Цілеспрямований ж, умисний інформаційний вплив може привести систему до незворотних змін та самознищенню» [16, с. 31]. Надходження цієї інформації здійснюється внаслідок певних дій, які, як ми можемо припускати, є інформаційними діями.

Науковці О.С. Ховпуна, О.В. Домбровської та Г.В. Муляр в своїй роботі «Кримінальні правопорушення у сфері інформаційних технологій: особливості розслідування» [17] досліджували інформацію, як спосіб та засіб злочинного діяння. На відміну від Д. Прокоф′євої, в цій роботі автори визначають

інформацію, як спосіб вчинення злочину, зокрема за допомогою погроз або обману.

Однак дана позиція видається менш переконливою у зв'язку з тим, що спосіб вчинення злочину передбачає все ж таки вчинення (або не вчинення) певної дій, в той час як інформація, як явище не має ніякого впливу на інших людей без її використання, на відміну від інформаційних дій.

Таким чином, хоча інформація беззаперечно є важливим явищем в розрізі певних правопорушень, її роль у таких випадках значно відрізняється від ролі інформаційних дій, які можуть виступати способом вчинення злочину.

Щодо більш ґрунтовного аналізу самого поняття «інформаційні дії», слід зазначити, що науковці досить рідко використовують такий термін, хоча у літературі й зустрічаються поняття, які потенційно можуть ототожнюватись із інформаційними діями. Такими є «інформаційна діяльність», «дії в інформаційному просторі», «інформаційний вплив».

Однією з небагатьох робіт, де надається визначення інформаційним діям є підручник В. В. Сташиса та В. Я. Тація, відповідно до якого інформаційні дії визначаються як «передача відповідної інформації іншим особам, що виражається в словесній (вербальної) формі, а також у формі різних дій, що несуть інформацію: жестів і виразних рухів (міміка і пантоміміка)» [18, ст. 116].

Майже ідентичне визначення дає Р.В. Куцій, посилаючись на роботи М.І. Панова та О.В. Кириченко зазначаючи, що «інформаційними в теорії кримінального права вважають дії, що полягають у передачі інформації іншим особам і завжди виражаються у словесній (вербальній) формі, а також у будь-яких діях, що несуть інформацію: смислових жестах, виразних рухах (міміка)» [19, с. 131].

Дане поняття можливо доповнити тим, що інформація може передаватись не лише іншим особам, а й комп'ютерним системам.

Після критичного аналізу різних наукових підходів до визначення поняття інформаційних дій, можна виділити кілька ключових ознак, які характеризують ці дії.

По-перше, інформаційні дії включають в себе процес передачі інформації від одного джерела до іншого, а також сприйняття цієї інформації отримувачем. Це може відбуватися як в мовній (вербальній) формі, так і через інші комунікаційні канали, такі як електронні повідомлення, соціальні мережі тощо.

По-друге, інформаційні дії охоплюють опрацювання та обробку інформації, що може включати аналіз, інтерпретацію та оцінку отриманих даних.

По-третє, інформаційні дії передбачають можливість обміну інформацією між різними сторонами або учасниками. При цьому, обмін може відбуватись як між людьми, так й між комп'ютерними системами.

Також, інформаційні дії включають в себе процес отримання інформації, що може бути здійснений як активним пошуком, так і прийняттям інформації, що надходить випадковим чином або безпосередньо.

Таким чином, можливо сформулювати наступне визначення:

Інформаційні дії - це процес передачі, сприйняття, опрацювання інформації та її обміну між різними джерелами та отримувачами, який може включати передачу інформації у вербальній чи невербальній формі або через різноманітні комунікаційні канали. При цьому, такі дії також передбачають або можуть передбачати аналіз, інтерпретацію та оцінку отриманої у результаті активного пошуку або пасивного сприйняття інформації.

Доречним в даному випадку видається розуміти поняття «інформації», як сукупність знань, образів, відчуттів, наявних у свідомості людини або штучному інтелекті, які поступають по різних каналах передачі, переробляються й використовуються в процесі життєдіяльності людини й роботі автоматичних комп'ютерних систем.

1.4. Виклики в дослідженні інформаційних дій та визначення методів дослідження інформаційних дій у кримінальному праві.

Як зазначалось раніше, наукова спільнота і держави світу все частіше звертають увагу на нові виклики, що прямо пов’язані із інформаційними діями, проте багато аспектів залишаються невивченими та недоопрацьованими.

Перш за все труднощі в дослідженні інформаційних дій полягають в складності самого предмета дослідження.

Як вбачається з наведеного раніше аналізу, визначити поняття «інформаційні дії» є досить складним завданням. В більшій мірі це обумовлено складністю визначення поняття «інформації» та її ознак, розуміння впливу інформації та наслідків такого впливу. Відповідно, ускладнення у дослідженні теоретичних аспектів інформаційних дій зумовлюють неабиякі проблеми в дослідженні і практичних аспектів такого явища, особливо в призмі кримінального права, адже без сумніву, інформаційні дії можуть призводити до страшних наслідків і порушувати права як окремих осіб, так і шкодити суспільству в цілому. Складність визначення причинного зв’язку між такими діями та завданою шкодою, тобто наслідками, породжує чимало проблем у кваліфікації кримінальних правопорушень і ще більше в їх розслідуванні.

Для вирішення проблем, необхідним є чітке їх визначення. Так, основні виклики, які виникають у зв'язку з дослідженням інформаційних дій, можна узагальнити наступним чином:

1) Теоретичні виклики: спричинені неможливістю чітко і комплексно визначити поняття інформації та інформаційних дій.

2) Теоретично-практичні виклики: полягають у відсутності зрозумілої і ефективної методології для дослідження інформаційних дій, що ускладнює як теоретичні дослідження, так і практичну роботу (розробку механізмів регулювання інформаційних дій, визначення місця інформації в правовому полі, тощо).

3) Практичні виклики: що є наслідком раніше зазначених аспектів та пов’язані з труднощами у створенні чіткого правового регулювання. Видається майже неможливим передбачити такі законодавчі механізми, що враховували б

інтереси суспільства, не порушуючи та/або обмежуючи права окремих осіб без розуміння методології дослідження інформаційних дій.

В даній роботі вже були розглянуті теоретичні аспекти дослідження інформаційних дій, що становить важливу базу для подальшого пошуку вирішення теоретично-практичних викликів.

Основна проблема, полягає у визначенні ефективних методів для дослідження інформаційних дій. В даному випадку методи слід розуміти, як підходи, засоби або прийоми теоретичного та експериментального дослідження або практичного втілення явища чи процесу [20, 58с.].

В своїй роботі А. С. Бондарчук звертає увагу, що дослідники класифікують всі методи за сферою дії на чотири групи:

1) філософські (діалектичний, феноменологічний, герменевтичний);

2) загальнонаукові (системний, порівняльний, історичний);

3) спеціальнонаукові;

4) дисциплінарні [21].

В даній роботі видається не досить коректним спиратись на одну групу методів. Більш ефективним для дослідження такого складного предмету є застосування певної комбінації методів, серед яких, зокрема, діалектичний, історичний, порівняльно-правовий, системний, соціологічний, статистичний та інші. Такий вибір зумовлений наступним.

Діалектичний метод, дозволить розглянути відповідне кримінально-правове явище у розвитку та з урахуванням базових законів діалектики (переходу кількісних показників у якісні; заперечення заперечення; єдності і боротьби протилежностей).

Історичний метод передбачає дослідження інформаційних дій у їх історичному контексті, зокрема, вивчення їх впливу на суспільні відносини в минулому та на сучасному етапі.

Порівняльно-правовий метод допоможе порівняти інформаційні дії, їх визначення та правове регулювання в межах національного законодавства, в порівнянні з нормативним регулюванням в інших державах, а також в ретроспективі, що надасть можливість краще зрозуміти суть даного явища та наявні

проблеми, які виникають на практиці. Більше того, без порівняльно-правового методу аналіз будь-якого явища чи процесу кримінально-правової дійсності не буде всебічним та об’єктивним, отже його застосування є необхідним в межах даного дослідження.

Системний метод зумовлює всебічний аналіз таких складних динамічних цілісностей, частини яких перебувають між собою в органічній єдності та взаємодії. Зокрема, в призмі дослідження інформаційних дій, цей метод дозволить продемонструвати взаємозв’язок та взаємообумовленість норм Кримінального кодексу України, якими передбачена відповідальність за вчинення відповідних дій, що підпадають під поняття «інформаційні дії».

Соціологічний метод дозволить провести аналіз соціальних умов, факторів та феноменів, які визначають значимість інформаційних дій в кримінально-правовому аспекті.

Статистичний метод дозволить акумулювати та аналізувати статистичну інформацію щодо досліджуваної теми, отриману з української та зарубіжної правозастосовної практики.

Таким чином, наразі перед нами постає чимало викликів в дослідженні інформаційних дій, зокрема в кримінальному праві, що підкреслює необхідність подальшої роботи над даною темою.

Одним із таких викликів є визначення концептуальних та методологічних засад аналізу інформаційних дій у кримінальному праві.

Для цього важливо використовувати широкий спектр методів, серед яких: діалектичний, історичний, порівняльно-правовий, системний, соціологічний, статистичний, що в свою чергу передбачають вивчення та аналіз теоретичних джерел та напрацювань науковців, аналіз правового регулювання в Україні та інших державах, аналіз судової практики, тощо.

Важливо зауважити, що комплексне застосування цих методів є необхідним для досягнення більш повного та об'єктивного розуміння та дослідження теми. Використання цього різноманіття методів дозволить отримати більш глибокий та комплексний погляд на інформаційні дії в кримінальному праві.

***

Таким чином, інформаційні дії є досить комплексним явищем, що визначається, як процес передачі, сприйняття, опрацювання інформації та її обміну між різними джерелами та отримувачами, який може включати передачу інформації у вербальній чи невербальній формі або через різноманітні комунікаційні канали. При цьому, такі дії також передбачають або можуть передбачати аналіз, інтерпретацію та оцінку отриманої у результаті активного пошуку або пасивного сприйняття інформації.

Розвиток технологій та зміна соціальних умов створює нові виклики для дослідження інформаційних дій, зокрема в контексті кримінального права. Водночас, багато хто з науковців розглядаючи інформаційні дії з практичної точки зору, ігнорують факт непередбачуваності впливу інформації на наслідки таких дій, поведінку людини та її сприйняття.

Застосування системного підходу та теорії соціально-правового детермінізму дозволить дослідити інформаційні дії найбільш комплексно та ефективно, враховуючи їх вплив на суспільство.

Окрім того, існуючі наукові дослідження в області інформаційних дій в кримінальному праві мають певні недоліки і не охоплюють всі аспекти цього явища. З огляду на це, необхідним є застосування інтегрованого підходу та проведення подальших досліджень для отримання більш повного розуміння проблематики. Для цього важливо використовувати широкий спектр методів, серед яких: діалектичний, історичний, порівняльно-правовий, системний, соціологічний та статистичний.

Результати аналізу, здійсненого в даному розділі, наочно підкреслюють необхідність подальших досліджень у сфері інформаційних дій.

РОЗДІЛ 2. ІНФОРМАЦІЙНІ ДІЇ У КРИМІНАЛЬНО-ПРАВОВОМУ РОЗУМІННІ

2.1 Сучасні виклики в правовому регулюванні інформаційних дій в Україні.

Попередньо були розглянуті виклики щодо дослідження теоретичного аспекту інформаційних дій, запропоноване власне визначення поняття «інформаційні дії» та виділено основні методи дослідження даного явища, що дає змогу розглядати практичні проблеми правового регулювання більш комплексно та ґрунтовно.

Події сьогодення дали зрозуміти, що правове регулювання інформаційних дій є дуже важливим і недооціненим механізмом забезпечення захисту прав людини та навіть безпеки держави.

З початку вторгнення російської федерації на територію України ще в 2014 році стало зрозумілим, що правове регулювання інформаційних дій не є досконалим. Поширення пропаганди, фейків та протидержавних наративів було звичайним явищем і ввело чимало людей в оману. Наслідки таких інформаційних дій є досить масштабними та впливають на українців і зараз. Інформація стала не лише можливістю для розвитку та пошуку нових ідей, створення нових технологій, вирішення екологічних проблем, а перетворилась в зброю, яка, як виявилось має високу ефективність.

І.М. Сопілко в своїй роботі «Інформаційна війна проти України та правові засоби протидії злочинним діям» зазначає, що відомі такі форми інформаційної війни як «мережева війна, семантична війна та ідеологічна диверсія» [с. 110, 22]. Однак, акцентує, що незалежно від виду, як зброя завжди виступає безпосереднє використання інформації.

Для того, аби використання інформації таким чином не мало вплив на суспільство, законотворцям необхідно звернути особливу увагу забезпеченню інформаційної безпеки.

Основною і ефективним способом такого забезпечення є перетворення стратегічних аспектів національної інформаційної політики у конкретне та ефективне інформаційне законодавство.

В межах аналізу сучасних викликів у правовому регулюванні інформаційних дій важливо враховувати вплив швидкого розвитку штучного інтелекту. Цей розвиток відбувається настільки стрімко, що штучний інтелект стає не лише здатним до обробки та надання вже існуючої інформації, але й до генерації нової інформації на основі самонавчання.

Це створює перед законодавцями нові виклики. Так, необхідно розробляти правові механізми, які б забезпечували адекватний захист прав та інтересів громадян у контексті використання штучного інтелекту. Враховуючи його здатність до самонавчання, необхідно забезпечувати контроль за процесом його навчання та діяльності, щоб уникнути можливих негативних наслідків.

Окрім вказаного, з розвитком і еволюцією досліджень інформації та інформаційних дій, не втрачає свою актуальність й проблема визначення причинно-наслідкового зв’язку.

Встановлення причинного зв’язку між діями інформаційного характеру та суспільно небезпечними наслідкам є досить складним процесом, так як самі дії фізично не впливають на людину. Такий зв’язок фактично є нефізичним, тому виявлення причинно-наслідкового зв'язку в цьому випадку стає не таким очевидним і вимагає глибокого аналізу.

Слід зазначити, що відсутність прямого фізичного впливу не робить інформаційні дії менш важливими або менш небезпечними для суспільства. Навпаки, інформаційні дії можуть мати значний соціальний та психологічний вплив, що в свою чергу впливатиме на рішення та поведінку людей та груп. Це може спричиняти різноманітні наслідки, від соціальної дезорієнтації до вчинення кримінальних діянь. Більш детально проблема визначення причинно-наслідкового зв’язку між інформаційними діями та суспільно небезпечними наслідками буде досліджена пізніше.

Таким чином, правове регулювання інформаційних дій не є досконалим, що підтверджується існуючими проблемами, які і зараз несуть значні ризики для окремих осіб та суспільства в цілому.

Війна, важливою складовою якої є інформаційна війна, стрімкий розвиток технологій та штучного інтелекту вимагають прийняття швидких рішень з боку законодавця, які далеко не завжди є досконалими та ефективними.

Враховуючи, що інформаційні дії можуть включати процес передачі, сприйняття, опрацювання інформації та її обміну, аналіз, інтерпретацію та оцінку отриманої інформації, процес правового регулювання стає ще складнішим, оскільки необхідно враховувати різноманітність інформаційних дій та їх потенційні наслідки для суспільства.

При цьому, в аспекті правового регулювання інформаційних дій в кримінальному законодавстві, не менш значною є проблема встановлення причинно-наслідкового зв’язку між інформаційними діями та суспільно небезпечними наслідками, що створює нові виклики та потребує значної уваги з боку наукової спільноти та законодавців.

2.2 Аналіз правового регулювання інформаційних дій у кримінальному законодавстві України та світовий досвід.

Кримінальне законодавство України не виділяє інформаційні дії в окремий інститут права.

Кримінальним кодексом України встановлюється відповідальність за правопорушення в сфері інформації та комп’ютерних технологій, однак, особливістю поточної моделі захисту відносин в інформаційному просторі є те, що відповідні норми закладені в різних розділах Особливої частини Кримінального кодексу України.

Інформаційні дії в кримінальному законодавстві в більшій мірі характеризуються як передача, інформації та її обмін між різними джерелами та отримувачами у вербальній чи невербальній формі або через різноманітні комунікаційні канали.

Зокрема до таких дій можна віднести правопорушення пов'язані з використанням електронно-обчислювальних машин або комп'ютерних технологій, правопорушення, що не пов'язані з використанням таких систем та технологій, однак засобом їх вчинення є інформація, а інформаційні дії – способом, а також в окрему групу можна визначити правопорушення що несуть загрозу демократичним засадам та національній безпеці.

До першої групи правопорушень можна віднести наступні дії: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361), створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електроннообчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2); 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); 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); 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) [23].

До переліку кримінальних правопорушень, в яких інформація є засобом вчинення злочину, а інформаційні дії – способом можна віднести: порушення недоторканності приватного життя (ст. 182 КК України) [23], а саме «шляхом незаконного збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації»; шахрайство (ст. 190 КК України) [23], яке може вчинятись по-перше, шляхом

обману, а по-друге - із використанням електронно-обчислювальної техніки; доведення до самогубства (ст. 120 КК України) [23], зокрема внаслідок шантажу та деякі інші.

Окрему увагу слід звернути на кримінальні правопорушення, способом вчинення яких є погроза.

По своїй природі, погроза виражається в передачі інформації про намір вчинення певних небажаних для іншої особи дій. Однак для того, щоб така дія, як погроза, підпадала під кримінальну відповідальність, важливим є як вираження такої інформації, так і її доведення до іншої особи.

Р.В. Куций в своїй наукові статті «Ознаки зовнішнього прояву погрози як способу вчинення злочину», аналізуючи норми Кримінального кодексу України наголошує на тому, що для криміналізації діяння важлива наявність форми вираження погрози, інакше, інформація, яка не набула форми та не стала доступною для сприйняття одержувача - не є вираженою, а відповідно і не є погрозою [19].

Особливу увагу також слід звернути на третю групу правопорушень, що несуть загрозу демократичним засадам та національній безпеці. Більшість таких дій також є кримінально караними.

Як зазначив доцент кафедри політології Технічного університету Вірджинії та член Ініціативи інформаційної довіри та суспільства А. Брантлі [24, с. 158] ще до Революції Гідності в Україні було понад 22 закони, пов’язані з інформаційною та кібербезпекою, однак незважаючи на ці закони, їх фактичне виконання було суб’єктивним та вибірковим.

Так, було створено Міністерство інформаційної політики України та прийнято ряд інших важливих рішень, в тому числі криміналізовано дії інформаційного характеру, такі як виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436-1) [23].

З початком повномасштабного вторгнення росії на територію України ще деякі дії інформаційного характеру були криміналізовані.

Зокрема, з’явилась стаття 114-2 [23], яка передбачає відповідальність 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 та стаття 436-2 - виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників.

Таким чином, в національному законодавстві прослідковуються реакції на нові виклики в інформаційному просторі, зокрема було криміналізовано інформаційні дії, що стосуються не лише кіберпростору та кібербезпеки, а й дії, що пов’язані з передачею інформації, з використанням якої може пов’язуватися вчинення злочину. В той же час, назвати національне правове регулювання інформаційних дій досконалим, на жаль, важко. Існує чимало упущень, які краще досліджувати з урахуванням міжнародного досвіду та судової практики.

Міжнародна спільнота також досить активно реагує на сучасні виклики, що зумовлені різними формами інформаційних дій, які є або можуть бути суспільно-небезпечними.

Одним з основних міжнародних нормативно-правових документів, що регулюють суспільні відносини в інформаційному просторі є Конвенція про кіберзлочинність від 23 листопада 2001 року. Даний акт був прийнятий Радою Європи, як відповідь на зміни, спричинені активним розвитком цифрових технологій та глобалізацією комп'ютерних мереж [25].

Проте, як вбачається з назви Конвенції, сфера її регулювання обмежується кіберпростором і не визначає поняття інформаційних дій як таких.

О.В. Амелін у свої праці «Злочини у сфері інформаційних відносин в міжнародно-правових актах» досліджував питання кіберзлочинності і розглядав правове регулювання в міжнародник актах. Автор звертає увагу, що Управління ООН з наркотиків і злочинності в опублікованому 2013 року звіті «Всебічне дослідження проблеми кіберзлочинності та відповідних заходів з боку держав-членів, міжнародного співтовариства і приватного сектора» зазначає, що поняття

«кіберзлочинність» залежить від контексту і мети вживання цього терміна [26]. Водночас, окрім злочинів проти конфіденційності, цілісності та доступності даних, дане поняття включає будь-які дії, спрямовані на нелегальне вилучення прибутку, контент-злочини та інші протиправні діяння в кіберпросторі.

В той же час, очевидно, що досліджуваний міжнародний акт не охоплює усі інформаційні дії, що є суспільно-небезпечними.

Цікавим в дослідженні інформаційних дій є законодавство Франції. Тут розрізняються дві категорії дій інформаційного характеру: інформаційний злочин (infraction informatique) і комп'ютерний злочин (criminalité informatique).

В роботі Жака Франсійона, яка присвячена правопорушенням передбаченим законодавством про інформацію та комунікацію [27] науковець досліджував норми Кримінального кодексу Франції та окремі судові кейси. Як зазначав автор, чимало проблем на практиці виникає у вирішенні питань підслідності інформаційних злочинів. Так, в його роботі розглядався випадок, пов’язаний з расистськими або антисемітськими повідомленнями, розміщеними в соціальній мережі Twitter.

Асоціації, які борються з расизмом і ксенофобією, активно відреагували на расистські повідомлення та запросили каліфорнійську компанію Twitter Inc. та її французьку дочірню компанію Twitter France, передати їм дані, які дозволять ідентифікувати авторів твітів, що підпадають під склади злочинів проти людяності та розпалювання расової ненависті [27].

Позиція суду ґрунтувалась, на тому, що автори спірних твітів, підпадають під кримінальне законодавство Франції відповідно до статті 113-2 Кримінального кодексу, згідно з якою злочин вважається вчиненим на території Республіки [27].

Інший випадок, який розглядає автор, стосується провокації глядачів на ворожнечу під час спортивного заходу. Відповідальність за такі дії інформаційного характеру передбачені ст. L. 332-6 і L. 332-21 Спортивного кодексу.

Дана ситуація стосується інформаційних дій, які виражались демонстрацією банера з образливим написом. По даній справі суд зауважив, що з тлумачення

інформації з банеру було зроблено висновок, що напис характеризує наклепницьку компанію, спрямовану на підбурювання публіки, присутньої на трибунах, до ненависті чи насильства проти групи людей [27].

Таким чином, відповідальність за інформаційні дії, що є суспільно-небезпечними встановлюється не лише Кримінальним кодексом, а й іншими нормативно-правовими актами, такими як Спортивний кодекс Франції. При цьому, особи несуть відповідальність за поширення або демонстрацію інформації, що порушує права та інтереси інших, не зважаючи на наявність чи відсутність суспільно небезпечних наслідків.

Інший досвід правового регулювання в Польщі. Кримінальний кодекс Польщі (далі - ККП) також містить положення, що передбачають відповідальність за інформаційні злочини. При чому, ці діяння, як і в Україні, передбачені в окремих розділах. Зокрема, ККП криміналізовані такі інформаційні дії: розголошення та незаконне використання інформації, яка є таємною або охороняється законом (статті 263 і 264 ККП), поширення матеріалів, які містять насильницьку, сексуальну або ксенофобську інформацію, а також поширення інформації, що пропагує насильство та дискримінацію (статті 173, 178, 193, 270 - 274 ККП), комп'ютерна злочинність, яка включає в себе злочини, пов'язані з порушенням функціонування комп'ютерної системи, несанкціонований доступ до комп'ютерних даних, введення в оману користувачів комп'ютерів, шахрайство через комп'ютерні мережі та інші злочини (статті 287 КК Польщі) [28].

Найбільш розгалужене правове регулювання інформаційних дій в Сполучених Штатаї Америки. Тут існує купа розрізнених федеральних і державних законів та ціла низка нормативно-правових актів, кожен з яких призначений лише для захисту певних типів даних. Закони позначаються такими абревіатурами, як HIPAA [29] (Закон про перенесення та підзвітність медичного страхування), FCRA [30] (Закон про справедливу кредитну звітність), FERPA [31] (Закон про права сім’ї на освіту та конфіденційність), GLBA [32] (Закон Грамма-Ліча-Блілі), ECPA [33] (Закон про конфіденційність електронних комунікацій),

COPPA [34] (Правила захисту конфіденційності дітей в Інтернеті) та VPPA [35] (Закон про захист конфіденційності відео).

Як вбачається з аналізу законодавства США, особливу увагу держава приділяє захисту персональних даних. Однак, враховуючи відсутність єдиного нормативного акту та часто дуже значні відмінності в нормативних актах різних штатів, робити висновки про ефективність чи неефективність правового регулювання інформаційних дій досить складно.

Таким чином, більшість держав прагне створити комплексне законодавство, яке б регулювало інформаційні дії різних форм та видів.

Для України може бути цінним досвід досліджуваних країн, зокрема в аспекті захисту персональних даних, боротьби з дискримінацією та ворожнечею в інформаційному просторі. В той же час, не слід забувати, що «сліпе» впровадження досвіду інших країн в національне законодавство не матиме ефективності. Більше того, в умовах війни українське законодавство має реагувати на нові виклики, які для більшості розвинутих країн не є актуальними.

Зокрема, важливо враховувати унікальні обставини, такі як гібридна війна, агресивна інформаційна пропаганда та кібератаки, що останнім часом проявляються в різних формах і досить великих масштабах. Ці виклики потребують специфічного правового регулювання, передбачення спеціальних заходів забезпечення безпеки, захисту від дезінформації та маніпуляцій у медіа та соціальних мережах. Забезпечення стійкості та безпеки інформаційного простору залишається найбільш актуальним напрямком подальшого розвитку правового регулювання України.

2.3 Класифікація видів інформаційних дій в контексті кримінального права.

Спроби класифікувати дії інформаційного характеру спостерігаються як в міжнародних актах, так і в наукових дослідженнях.

Так, в Конвенції про кіберзлочинність виділено чотири види кримінальних правопорушень:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, до яких віднесено незаконний доступ, нелегальне перехоплення, втручання в дані та втручання в систему;

2) правопорушення, пов'язані з комп'ютерами, а саме підробка та шахрайство, пов'язані з комп'ютерами;

3) правопорушення, пов'язані зі змістом, зокрема правопорушення, пов'язані з дитячою порнографія);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [25].

Проте, як зазначалось раніше, Конвенція обмежуються лише кіберпростором та не регулює усі інформаційні дії, що є або можуть визначатись суспільно-небезпечними.

З аналізу наукової літератури вбачається, що більшість робіт присвячено все ж таки вивченню кібербезпеки, кіберпростору, кіберзлочинності. Таку проблему висвітлює й В.С. Батиргареєва, звертаючи увагу, що «чимало злочинів, зокрема так званої загальнокримінальної спрямованості, все одно залишаються поза межами досліджень, оскільки до уваги беруться лише діяння в кіберпросторі» [36, с. 114].

Однак все ж таки зустрічаються роботи, які досліджують інформаційні дії в більш широкому значенні, не обмежуючись лише кіберпростором.

Так, Д. Прокоф′єва в свій роботі «Інформація як знаряддя вчинення злочину та злочини проти інформаційної безпеки», спробувала виділити різновиди інформації (інформаційних впливів), зачіпаючи не лише кіберпростір [16]. Зокрема науковця виділила такі види інформаційного впливу в кримінальному праві, як: погрози, завідомо неправдива інформація, заборонена інформація та інформаційні впливи, що завідомо призводять до злочинних наслідків, ентропійний вплив [16].

В той же час, в межах дослідження інформаційних дій не вдалось знайти жодної роботи, де б визначалась класифікація інформаційних дій. На основі аналізу національного, міжнародного та іноземного регулювання інформаційних

дій, а також наукових підходів дослідження таких дій, стає можливим здійснити власну класифікацію.

Перш за все, враховуючи сферу застосування кримінального права, слід визначати інформаційні дії як правомірні та ті, що порушують права та інтереси особи, суспільства, держави. При цьому, при визначенні неправомірності, в наукових цілях та в цілях удосконалення правового регулювання, слід враховувати не лише прямо закріплені в кримінальному законодавстві діяння, а й ті, що самі собою порушують, або можуть порушувати права та інтереси особи, групи осіб та держави.

Вже розуміючи характер інформаційних дій, доречно класифікувати їх за способом вчинення. Таким чином можна виділити дії, вчинені за допомогою електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та такі, що вчинені без такої допомоги (висловлення, проголошення, демонстрація жестами, тощо).

Як згадувалось раніше, важливою ознакою інформаційних дії є інформаційний зміст. Зміст також може впливати на визначення дій як правомірними, так і неправомірними. В контексті неправомірності, за змістом, інформаційні дії можна поділити на наступні:

- вираження погрози (зокрема, погроза вбивством, насильством, пошкодженням та знищенням майна, розголошенням відомостей, які ганьблять особу, чи які вона бажає зберегти в таємниці, вчиненням інших діянь, що посягають на права та інтереси людини);
- поширення/розголошення завідомо неправдивої інформації;
- поширення забороненої інформації (поширення державної таємниці, інформації з обмеженим доступом, особистої інформації, медичної таємниці, інформації про розташування військової техніки ЗСУ, тощо.)
- поширення пропаганди та дискредитації інших націй чи релігійних спільнот;
- поширення матеріалів, які порушують авторські права.

Даний перелік, звісно, не є вичерпним, але може бути основою для більш детальної класифікації інформаційних дій, зокрема й на підвиди.

Враховуючи, що інформаційні дії в контексті кримінального права в більшій мірі мають значення тільки тоді, коли інформація передається та сприймається певним суб'єктом та впливає на нього, важливою може бути класифікація таких дій за впливом на інтереси. Так, інформаційні дії можуть бути спрямовані на: інтереси конкретної особи (наприклад, особиста погроза), інтереси суспільства (наприклад, поширення пропаганди) та інтереси держави (прикладом є розголошення державної таємниці).

Класифікація інформаційних дій безумовно є важливим етапом у підготовці їх ефективного правового регулювання. Однак в аналізованих наукових джерелах щодо дослідження інформаційних дій та суміжних предметів, не було знайдено жодної класифікації інформаційних дій.

В той же час, чимало науковців визначає і класифікує інформацію та інформаційних вплив. На основі таких напрацювань, аналізу міжнародного та національного законодавства, стає можливим запропонувати власну класифікацію за різними критеріями.

Зокрема були виділені такі критерії, як: характер (правомірність) дій, спосіб вчинення, зміст інформації.

Таким чином існує багато критеріїв за якими можливо класифікувати інформаційні дії в кримінальному праві. Наведений перелік не є вичерпний і в подальшому може бути збільшений та допрацьований.

2.4 Встановлення зв'язку між інформаційними діями та їх наслідками.

Встановлення причинного зв'язку між діями інформаційного характеру та суспільно небезпечними наслідкам є досить складним процесом, так як самі дії фізично не впливають на людину, тобто є нефізичними.

Саме таку нефізичну причинність в своїй роботі «Преступление и проблемы нефизической причинности в уголовном праве» досліджував А.А. Тер-Акопов.

Автор розглядає питання існування та визнання причин, що не є фізичними, як підстави кримінальної відповідальності.

А.А. Тер-Акопов зазначав:

> сумніви виникають і у ситуаціях, коли відсутній фізичний зв’язок порушення з наслідком: є неправильна поведінка, є суспільно небезпечний наслідок, але не видно причинного зв’язку між ними. Більше того, виявляється, що наслідок став можливим завдяки діям певних проміжних факторів, які безпосередньо викликали негативний результат. Розрізненість порушення і наслідку іноді створює враження про відсутність причинного зв’язку між порушенням та наслідком» [8, с. 342-343].

Таким чином, для визначення причинного зв’язку дій інформаційного характеру необхідно відійти від «механічної» причинності. При цьому, важливим є здійснення об'єктивного аналізу причинно-наслідкових зв'язків, із врахуванням всіх можливих факторів, що впливають на ситуацію. Враховуючи специфіку інформаційних дій, таких факторів може бути достатньо багато, що ускладнює і без того складний процес встановлення причинного зв’язку.

Однак, враховуючи усі складності у встановленні причинного зв’язку, О. В. Таран в своїй праці «Проблема встановлення причинного зв’язку у злочинах проти безпеки виробництва» [37], на основі робіт таких науковців як А.А. Тер-Акопова, З.М. Соколовского, Ю. В. Баулина, М. С. Гринберга та Н.А. Князева, запропонувала кроки щодо визначення наявності або відсутності причинного зв’язку. Так було визначено наступні кроки:

1) ретельно дослідити механізм злочину; виявити проміжні явища (події, дії, обставини) стосовно початкового і кінцевого;

2) виокремити з проміжних ті явища (події, дії, обставини), які мають значення в цілому;

3) встановити співвідношення у часі проміжних явищ;

4) уявно послідовно виключити кожне з них, починаючи з найбільш близького до результату;

5) з’ясувати, чи мав би місце той самий результат за вказаних виключень, тобто чи могло дане порушення спричинити наявні шкідливі наслідки за умови відсутності іншої події (обставини, явища);

6) дослідити всі порушення, які мали шкідливі наслідки, а не обмежуватися тими, які були найближчими до цього наслідку, тобто врахувати всю сукупність чинників, які передували спричиненню шкоди;

7) сформулювати висновок про наявність або відсутність причинного зв’язку залежно від отриманих результатів [37, ст. 172].

Такі кроки дійсно можуть значно полегшити процес встановлення причинного зв’язку, однак не враховують усі можливі проблеми.

Зокрема, на практиці можуть виникати ситуації, коли інформаційні дії могли спричинити шкідливі наслідки за умови наявності іншої події, зокрема, як у випадку резонансної справи в Польщі щодо самогубства Міколая Філікса.

Мова йде про самогубство сина активної опозиціонерки, яка представляє партію "Громадянська платформа" в польському парламенті - Магдалени Філікс. П’ятнадцятирічний Міколай Філікс вчинив самогубство після публікації в ЗМІ інформації про насильство, вчинене проти хлопця.

Журналіст написав статтю про скандал, пов'язаний із насильством над дитиною в Західно-Поморському воєводстві, при цьому згадавши, що і засуджений, і очільник воєводства були членами тієї ж партії, що й Магдалена Філікс.

По справі щодо насильства над дитиною був винесений вирок. При цьому, судовий процес не був публічним, в межах захисту неповнолітніх жертв насильницьких злочинів. Однак новину активно підхопили й інші ЗМІ: телевізійний канал TVP Info, тижневик Gazeta Polska та регіональна газета Glos Szczeciński [38]. В результаті, інформація, яка з'являлася в ЗМІ, допомогла ідентифікувати неповнолітню жертву.

Через два роки після вчинення насильницького злочину та через тиждень після публікацій в ЗМІ, Міколай Філікс вчинив самогубство.

Тут постає логічне питання, що саме стало причиною смерті Міколая – публікація в ЗМІ чи сам факт вчинення насилля?

Станом на написання роботи, в публічному доступі відсутня будь-яка інформація щодо рішення суду по даній справі та кваліфікацію цього злочину. В

той же час, дана справа підсвічує чимало проблемних моментів в контексті встановлення причинного зв’язку між інформаційними діями та наслідками.

Єдиним можливим варіантом для вирішення цієї проблеми є врахування співвідношення дій у часі, однак в кримінальному праві не встановлений термін дії причини.

В розумінні українського законодавства, у доведенні до самогубства перевагу мають активні дії суб’єкта, оскільки, відповідно до ст. 120 КК України, самогубство особи має бути «наслідком жорстокого з нею поводження, шантажу, систематичного приниження її людської гідності або систематичного протиправного примусу до дій, що суперечать її волі, схиляння до самогубства, а також інших дій, що сприяють вчиненню самогубства» [23].

Однак доведення факту вчинення такого кримінального правопорушення шляхом вчинення дій інформаційного характеру, ускладнюється тим, що відсутній реальний контакт суб’єкта з потерпілим, а також відсутні положення у кримінально-правовій нормі, що конкретизують визначення таких дій злочинними, тобто такими, що доводять до самогубства.

Ще однією роботою, в якій досліджується питання причинних зв’язків є дисертація Н.М. Ярмиш «Теоретичні проблеми причинно-наслідкового зв'язку в кримінальному праві (філософсько-правовий аналіз)». Зокрема, науковиця розглядала питання «інформаційної причинності»[9].

Автор зазначала, що «інформація служить не причиною змін стану або поведінки людини, а всього лише носієм причини. Причина ж формується як результат взаємодії інформації зі свідомістю людини» [9, ст. 9].

Також, цікавим є те, що в аспекті інформаційної причинності у дослідженні Н.М. Ярош розглянула питання про причинний зв'язок при бездіяльності, доводячи те, що «бездіяльність здатна бути носієм причини винятково як інформаційний сигнал» [9, с. 10].

Таким чином, питання причинності в аспекті вчинення дій інформаційного характеру викликає особливий інтерес у науковців. Однак дана тема потребує

вивчення і нормативного врегулювання, адже на практиці складність визначення причинного зв’язку призводить до безкараності винних.

Таким чином, для встановлення причинного зв’язку між діями інформаційного характеру та суспільно небезпечними наслідкам необхідно відслідковувати, які саме дії мали вплив на потерпілу особу, часовий проміжок цих дій, які наслідки в результаті настали. При цьому необхідно детально проаналізувати, чи настали б суспільно-небезпечні наслідки, якби ті, чи інші дії не були вчинені. Важливо враховувати усі зовнішні і внутрішні фактори, які могли мати вплив на потерпілу особу, що є досить складним завданням.

Окремо можна додати ще кілька факторів, які слід враховувати при визначені причинно-наслідкового зв’язку, зокрема:

1) мета інформаційних дій та наслідки, які були очікувані чи досягнуті;
2) інтенсивність та повторюваність інформаційних дій (що, очевидно, може мати значно більший вплив на потерпілу особу);
3) інші виняткові обставини, що здатні змінити оцінку причинного зв'язку.

В будь-якому разі, встановлення причинного зв’язку між інформаційними діями та суспільно-небезпечними наслідками потребує ґрунтовного комплексного аналізу усіх обставин і факторів, що призвели або могли призвести до відповідних негативних наслідків.

В той же час, цей процес є абсолютно можливим, хоча й потребує встановлення більш чітких критеріїв оцінки причинно-наслідкового зв’язку.

***

Таким чином виявлено, що правове регулювання інформаційних дій не є ідеальним, і наявні проблеми становлять значний ризик для окремих осіб та держави в цілому. Сучасна інформаційна війна та стрімкий розвиток технологій та штучного інтелекту створюють необхідність у швидких та ефективних рішеннях з боку законодавців.

Оскільки інформаційні дії можуть охоплювати різноманітні процеси передачі, сприйняття, опрацювання та обміну інформацією, правове регулювання

таких дій стає складним завданням, що потребує уваги з боку наукової спільноти та законотворців.

Для подальшого розвитку правового регулювання інформаційних дій важливо вивчати досвід інших країн, однак необхідно уникати "сліпого" впровадження іноземного досвіду, а зосередитися на унікальних викликах та потребах України, зокрема у забезпеченні стійкості та безпеки інформаційного простору.

Класифікація інформаційних дій є важливим етапом у їх ефективному правовому регулюванні, але на даний момент в науковий джерелах не було знайдено жодної класифікації інформаційних дій. Тому, були запропоновані наступні критерії для класифікації таких дій: характер (правомірність) дій, спосіб вчинення, зміст інформації.

Також, у контексті кримінального законодавства важливо встановити причинно-наслідковий зв'язок між інформаційними діями та суспільно небезпечними наслідками, що потребує детального аналізу та врахування різних обставин. Так, для встановлення причинного зв’язку між діями інформаційного характеру та суспільно небезпечними наслідкам необхідно відслідковувати, які саме дії мали вплив на потерпілу особу, часовий проміжок цих дій, які наслідки в результаті настали. Додатково слід враховувати мету інформаційної дії та наслідки, які були очікувані чи досягнуті, інтенсивність та повторюваність інформаційних дій та інші виняткові обставини, що здатні змінити оцінку причинного зв'язку.

РОЗДІЛ 3. ПРАКТИЧНИЙ АСПЕКТ ІНФОРМАЦІЙНИХ ДІЙ У КРИМІНАЛЬНОМУ ПРАВІ

3.1 Кримінально-правове значення інформаційних дій.

Як вже визначено, інформаційні дії можуть впливати на права та свободи громадян, безпеку держави, а також на функціонування суспільства в цілому. З розвитком цифрових технологій, такі дії набули нових форм та ще більшого поширення.

І хоча використовувати такі можливості було б значно розумніше і вигідніше для подальшого розвитку людства, технологій та вирішення існуючих світових проблем, зловмисники радо використовують інформаційні дії суто у власних цілях та на шкоду іншим особам.

Найбільш ефективно запобігти злочинам в інформаційному просторі можливо саме засобами кримінального права.

В даному контексті слід розглянути поняття інформаційного злочину, так як воно є надзвичайно важливим в контексті захисту суспільства від негативних наслідків інформаційних дій, а також визначити необхідність створення інституту інформаційних дій в кримінальному праві.

Так, О.С. Павлова в своїй роботі «Поняття та види інформаційних правопорушень» надала досить вичерпне визначення поняттю «інформаційний злочин», а саме:

> …– це небезпечне для суспільства протиправне діяння (дія чи бездіяльність), винна в якому особа, яка має здатність до вчинення злочину, порушує вимоги законодавства у сфері інформаційної діяльності (у сфері створення, передача, використання, обробка, зберігання, захист інформації тощо) або в будь-якій іншій сфері з використанням інформаційних засобів і технологій, за які настає юридична відповідальність [39, с. 374].

В той же час дане визначення має деякі неточності, що можуть ускладнити практичне застосування такого визначення. Так, некоректним видається застосування терміну «особа, яка має здатність до вчинення злочину». Доречніше було б використати загальноприйняте поняття – суб'єкт злочину.

В той же час, надане О.С. Павловою визначення презюмує наявність правового регулювання у сфері інформаційної діяльності. Таке трактування є логічним, хоча по суті зв'язує кримінально-правові норми з іншими нормативно-правовими актами, що регулюють відносини у сфері інформаційної діяльності.

На жаль, такі нормативно-правові акти не завжди встигають адаптовувати під нові виклики, що потенційно може спричинити відсутність регулювання частини інформаційних діянь, що мають суспільно-небезпечний характер.

Таким чином, з урахуванням зауважень інформаційний злочин можна визначити як небезпечне для суспільства протиправне діяння (інформаційні дії або бездіяльність) вчинене суб'єктом злочину, що порушує права та свободи особи, групи осіб та/або держави шляхом використання інформаційних засобів і технологій, за які передбачена кримінальна відповідальність.

Для того, аби якісно визначити та передбачити в кримінальному законодавстві відповідальність за усі небезпечні для суспільства протиправні діяння, тобто врахувати усі можливі інформаційні злочини, які де-факто існують, однак поки не віднесені до злочинів в розумінні Кримінального кодексу України, видається необхідним розглянути питання формування окремого інституту в кримінальному праві, а саме інституту інформаційних дій.

Перш за все необхідно зважити всі переваги та недоліки створення такого додаткового інституту та в принципі визначити, чи існує в цьому потреба.

Так, з одного боку створення окремого інституту може забезпечити більш ефективне правове регулювання інформаційних дій в кримінальному праві, що дасть можливість для запровадження більш спеціальних норм, в тому числі щодо критеріїв визначення причинно-наслідкового зв'язку, передбачення додаткових норм щодо визначення підслідності інформаційних злочинів, які набули міжнародного характеру, передбачення додаткових та або спеціальних обмежень та санкцій за вчинення інформаційних злочинів.

Тобто, запровадження інституту інформаційних дій в кримінальному праві дозволило б ефективніше регулювати такі дії завдяки запровадженню ряду

спеціальних норм, що враховували б специфіку та унікальність інформаційних злочинів.

Однак, дана ідея має ряд недоліків, серед яких ризик дублювання правових норм, ризик обмеження правомірних дій внаслідок надмірного правового регулювання, технічні труднощі, зумовлені постійним розвитком технологій та необхідністю швидко реагувати на такі дії та вносити зміни в законодавство.

На даному етапі розвитку законодавства видається недоцільним створювати додатковий інститут, натомість слід більш ґрунтовно та системно підійти до удосконалення вже існуючих механізмів регулювання інформаційних дій та запобігання інформаційних злочинів. Можливим також є доповнення Загальної частини Кримінального кодексу України визначенням «інформаційний злочин» або «інформаційні дії» з метою встановлення спеціальних особливостей та критеріїв щодо встановлення причинно-наслідкового зв’язку для окремої категорії правопорушень.

В той же час, не можна недооцінювати кримінально-правове значення інформаційних дій, що полягає не лише в науковому інтересі дослідження такого явища, але й у необхідності створення дієвих механізмів регулювання цієї сфери, з урахування її швидкого розвитку та складності предмета регулювання.

3.2 Дослідження судової практики щодо розгляду справ, пов’язаних із інформаційними діями та визначення основних труднощів в судовій практиці України.

Як було визначено і досліджено раніше, Кримінальний кодекс України не виділяє правопорушення, що пов’язані з інформаційними діями в окремий розділ Особливої частини. Однак в межах дослідження судової практики, їх можна поділити на кілька груп, в залежності від характеру інформаційних дій та предмету посягання.

Так, до першої групи належать правопорушення, що пов’язані з використанням електронно-обчислювальних машин або комп’ютерних технологій.

Досить поширеним правопорушенням серед цієї групи є несанкціоноване втручання в роботу комп'ютерів, систем, та мереж, відповідальність за яке передбачена статтею 361 КК України.

При цьому слід зазначити, що диспозиція статті 361 КК України детально не розкриває способи вчинення таких правопорушень, передбачаючи відповідальність за будь-яке несанкціоноване втручання.

Тут слід додати, що Верховний Суд також звертав увагу на те, що «об`єктивна сторона кримінального правопорушення, передбаченого ст. 361 Кримінального кодексу України, охоплює не усі дії, які спричинили витік, втрату, підробку, блокування інформації, спотворення процесу обробки інформації чи до порушення встановленого порядку її маршрутизації. Кримінальна відповідальність за зазначеною статтею настає тільки в разі, коли такі наслідки мають місце у результаті несанкціонованого втручання в роботу мереж електрозв`язку. У такому разі несанкціоноване втручання у роботу мереж електрозв`язку є будь-якими діями, вчиненими без наданої власником згоди, унаслідок яких припиняється робота мережі електрозв`язку або ж змінюється режим такої роботи» [40].

Як показує судова практика, найчастіше злочинці використовують отриману інформацію, внаслідок такого втручання, для подальшого заволодіння майном потерпілої особи. При цьому, вказані дані можуть бути отримані, або викрадені різними способами, найпоширенішими з яких є отримання даних:

- за допомогою використання додаткових програм;
- шляхом безпосереднього викрадення документів особи;
- шляхом незаконного отримання даних, до яких особа не має права доступу.

Прикладом першого способу є використання шкідливого програмного засобу для підбору паролів, що розглядалось у справі №208/10010/21 Заводським

районним судом м. Дніпродзержинська Дніпропетровської області 18 січня 2022 року [41].

Прикладом випадку безпосереднього викрадення документів є судова справа № 127/35602/23, щодо якої Вінницький міський суд 25 січня 2024 року виніс обвинувальний вирок, що вже набрав законної сили. Суть справи полягає у вчинення одразу ряду кримінальних правопорушень, які характеризуються вчиненням в тому числі інформаційних дій. Винна особа, шляхом викрадення документів, отримала дані, до яких не мала права доступу та використала їх для отримання кредиту, вказавши неправдиву інформацію. Також, винна особа використала викрадені документи, а саме паспорт громадянина України та реєстраційний номер облікової карти платника податку, виданих на ім’я іншої особи, чим ввела в оману працівників банківської установи і повідомила, що бажає змінити фінансовий номер на власний номер телефону для здійснення входу до інтернет-банкінгу «Приват24». Після цього, особа здійснила несанкціонований вхід до облікового запису «акаунту», який є системою призначеною для дистанційного керування банківськими рахунками [42].

Шляхом незаконного отримання даних, до яких особа не має права доступу, скористався працівник центру обслуговування з ремонту мобільної техніку. Як вбачається з вироку Шевченківського районного суду м. Чернівці від 24.01.2023 року у справі № 727/21/23, винна особа отримала телефон потерпілої особи для ремонту, однак отримавши телефон із встановленими додатками «Дія» та «Приват 24» здійснила несанкціоноване втручання до облікового запису потерпілої особи в Порталі «Дія», підробивши відомості про засоби верифікації особи за допомогою сім-картки оператора стільникового зв`язку ПрАТ «Київстар», що належить останній, без її відома та дозволу, змінивши електронну пошту для авторизації, до якої мав доступ [43].

Таким чином, злочинні дії, пов'язані з отриманням інформації та її використанням для заволодіння майном потерпілих, є актуальною проблемою, яка вимагає уваги з боку законодавців і правоохоронних органів. Судова практика демонструє, що злочинці використовують різні способи для отримання

інформації, такі як викрадення документів, використання програмного забезпечення для підбору паролів та незаконне отримання даних. Ці дії є прикладами того, як інформаційні технології можуть бути використані для скоєння злочинів.

В той же час, за результатом аналізу судових рішень стає зрозумілим, чому законодавець не деталізує диспозицію ст. 361 КК України, зокрема можливими способами вчинення такого правопорушення. З урахуванням варіації та методів несанкціонованого втручання в роботу комп'ютерів, систем, та мереж, не можливо передбачити усі можливі дії, яким чином особа може отримати доступ до відповідних систем. Такі дії мають інформаційних характер та їх перелік є абсолютно невичерпаним.

В даному випадку можна сміливо стверджувати, що надмірний формалізм в регулюванні інформаційних дій міг би значно звузити сферу застосування відповідних положень Кримінального кодексу України.

Окрім правопорушення, відповідальність за яке передбачене ст. 361 КК України, досить поширеним є несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, відповідальність за що передбачена ст. 362 КК України.

Інформація є одним з найцінніших ресурсів у сучасному світі, водночас найменш захищеним. Однак, з розвитком технологій з’являються нові механізми захисту, що дозволяють в той же час відстежувати винних у розповсюдженні інформації з обмеженим доступом, що значну збільшує шанси викрити зловмисника.

Так, було викрито Головного державного ревізора-інспектора управління податкових перевірок ГУ ДПС у Дніпропетровській області. Як вбачається з вироку Жовтневого районного суду від 19 січня 2022 року у справі № 201/3277/21, винний, використовуючи свій службовий комп'ютер, отримав з інформаційно-телекомунікаційної системи «Податковий блок» реєстри виписаних податкових накладних поданих ТОВ «Атлантіс систем» та, розуміючи, що

отримані реєстри податкових накладних являються конфіденційною інформацією, а ТОВ «Атлантіс систем» не надавало згоди на її розповсюдження, в порушення ст. 21 Закону України «Про інформацію», в невстановлений слідством спосіб передав її службовим особам Товариства з обмеженою відповідальністю «Технопромзв'язок», тим самим допустивши несанкціонований збут інформації з обмеженим доступом [44].

Як вбачається з аналізу судової практики щодо правопорушень, що пов’язані з використанням електронно-обчислювальних машин або комп’ютерних технологій, як правило, такі правопорушення зазвичай вчиняються у сукупності з іншими, зумовленими корисливими мотивами.

Так, несанкціонованого втручання в роботу комп'ютерів, систем, та мереж найчастіше відбувається з метою отримання даних, до яких відсутній доступ та подальшого використання такої інформації для шахрайства та викрадення коштів.

У зв’язки з цим доцільно розглянути судову практику щодо правопорушення, що не пов’язані з електронно-обчислювальними машинами або комп’ютерними технологіями, але в яких інформація є засобом вчинення злочину, а інформаційні дії – способом.

Яскравим прикладом такого правопорушення є шахрайство.

Існує чимало судових рішень щодо шахрайства, відповідальність за яке передбачена ст.. 190 КК України, однак в контексті дослідження інформаційних дій, особливої уваги заслуговує аналіз способу вчинення даного правопорушення. Як відомо з диспозиції статті, шахрайство це - заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою шляхом обману чи зловживання довірою.

Для обману або зловживання довірою зловмисники завжди використовують інформацію, що може бути отримана, як цілком законно так й протиправним шляхом (як у випадках, несанкціонованого збуту або розповсюдження інформації).

Обман цілком підпадає під визначення інформаційної дії, що включає процес передачі та отримання інформації, її сприйняття. Саме вплив такої

інформаційної дії часто сприяє передачі майна або права на майно потерпілою особою, або третьою особою. Розвиток технологій та цифровізація адміністративних послуг лише сприяє появі нових видів шахрайства з використанням інформації та даних, що правомірно або неправомірно потрапляють у відкритий доступ.

Слід зазначити, що в 2023 році за неофіційною статистикою, що наводить моніторингова платформа «Опендатабот», було відкрито понад 82 тисячі проваджень за статтею 190 КК України, що є найвищим показником за останні 11 років [45].

Причиною такої сумної статистики, скоріш за все є доступність інформації, а саме особистих даних, контактних телефонів, тощо. З початком повномасштабного вторгнення, що вразило психологічний стан більшості українців, проблема правового регулювання такої доступності інформації стала більш очевидною.

При цьому, як зазначається в наведеній статистиці, лише 18% справ доходять до суду.

І хоча з початком повномасштабного вторгнення чимало інформації було прибрано з відкритого доступу, однак отримання необхідних даних через вже згадувану платформу «Опендатабот» та подібних до неї є досить простою процедурою, що полегшує шахраям можливість сформувати обман таким чином, аби потенційна потерпіла особа сприйняла таку інформацію як правдиву.

Показовою в даному випадку є справа № 173/2911/23 щодо якої Верхньодніпровський районний суд ухвалив вирок 22 лютого 2024 року.

Так, винна особа із використанням придбаної \ сім-картки зареєструвався у мобільному додатку «Telegram» та здійснив пошук відкритих для вступу чатів з невеликою кількістю учасників. Вступив до чату «Sinevo», переглянув список учасників чату та з метою подальшого спілкування від імені та під виглядом одного з учасників чату, зберіг фотографію цієї особи (аватар) в пам`яті свого смартфону та заповнив у «Telegram» анкету на ім`я цієї ж особи, додавши до сторінки її фотографію. Шляхом обману, почав надсилати потерпілій особі

текстові повідомлення від імені її знайомої щодо якої використав інформацію з відкритих джерел, та попросив у потерпілої в борг грошові кошти в сумі 11 100.00 гривень. Потерпіла, будучи впевненою, що надсилає належні їй грошові кошти своїй знайомій у борг, після чого остання через деякий час поверне їй грошові кошти, добровільно перерахувала на вказаний у текстовому повідомленні банківський рахунок, грошові кошти у сумі 11 100 гривень за допомогою терміналу «ІЬох» [46].

Слід також додати, що обман, як інформаційна дія, в межах вчинення такого правопорушення, як шахрайство, часто супроводжується й іншими кримінальними правопорушеннями, що додатково кваліфікуються судом.

Зокрема, Верховний Суд в Постанові від 25 січня 2024 року у справі № 359/11048/19 зауважує, що «згідно з усталеною практикою суду касаційної інстанції, якщо обман чи зловживання довірою при шахрайстві полягають у вчиненні іншого злочину, дії винної особи належить кваліфікувати за відповідною частиною статті 190 КК України і статтею, що передбачає відповідальність за цей злочин. Зокрема, самовільне присвоєння владних повноважень або звання службової особи, викрадення, привласнення, пошкодження та підроблення документів, штампів і печаток з метою подальшого їх використання при шахрайстві, використання при шахрайстві завідомо підробленого документа, а також зловживання владою чи службовим становищем потребують додаткової кваліфікації відповідно за статтями 353, 357, 358 та 364 КК України» [47].

Як вбачається з судової практики, найчастіше при шахрайстві зловмисники використовують інформацію, що є у відкритому доступі. В переважній більшості випадків така інформація з’являється у публічному доступі добровільно власником відповідних даних. В той же час, існує чимало випадків, коли інформацію вдається отримати з реєстрів або інших джерел з використанням частини наявних в зловмисника даних, такі як номер телефона чи повне ім’я особи, її адреса, тощо.

Найбільш складними в дослідженні інформаційних дій є правопорушення, що пов’язані безпосередньо з воєнними діями та/або країною-агресором. Деякі з таких діянь були криміналізовані не так давно.

Зокрема, увагу привертає справа № 761/8306/22, де Шевченківський районний суд м. Києва встановив, що обвинувачуваний здійснив кримінальне правопорушення, передбачене ч. 2 ст. 436-2 КК України, вподобавши, а саме натиснув «Класс» під публікаціями певних матеріалів, у яких міститься глорифікація осіб, які здійснювали (здійснюють) збройну агресію російської федерації проти України, розпочату у 2014 році [48].

Зазначена справа демонструє, що навіть позначка «Класс» в соціальних мережах несе певну інформацію, зокрема в даному випадку – глорифікація агресорів.

Така практика стає все більш розповсюдженою і є досить сталою. Зокрема, Прилуцький міськрайонний суд Чернігівської області у справі №742/1628/23 визнав жінку винною у вчиненні кримінального правопорушення, передбаченого за ч. 2,3 ст. 436-2 КК України за «вподобайки» постів, що містили виправдовування збройної агресії рф проти України.

Наразі існує практика Верховного суду щодо подібної справи, а саме справа № 127/12127/22. Так, жінку було засуджено до позбавлення волі на 3 роки за репост та вподобання матеріалів що виправдовують збройну агресію рф в забороненій соціальній мережі «Вконтакте». При цьому, Верховний суд звернув увагу на «неможливість застосування інституту звільнення від відбування покарання з випробуванням, оскільки жінка вчинила кримінальні правопорушення, які відповідно до розділу XX КК України відносяться до кримінальних правопорушень проти миру, безпеки людства та міжнародного правопорядку в той час, коли відповідно до Указу Президента України № 64/2022 від 24 лютого 2022 року, у зв`язку з військовою агресією російської федерації проти України введено воєнний стан на всій території України, що свідчить про підвищену суспільну небезпечність цих правопорушень» [49].

Слід також звернути увагу на судову практику щодо кримінального правопорушення, передбаченого ч. 3 ст. 114-2 КК України. В ЄДРСР наявна велика кількість вироків щодо осіб, які несанкціоновано поширювали інформацію 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

Так, 22 травня 2023 року Чернігівський районний суд Чернігівської області визнав винною у вчинення злочину передбаченого ч.3 ст. 114-2 КК України громадянку України, що почала підтримувати постійний зв'язок за допомогою додатку «Telegram», з невстановленим в ході досудового слідства представником військових підрозділів зс рф на ім'я «Іван». При цьому, вона усвідомлювала, що «Іван» є представником військових формувань рф, приймає участь у збройній агресії проти України, а передача йому будь-яких відомостей військового чи оборонного характеру явно зашкодить національній безпеці України. Достовірно усвідомлюючи вказані обставини, особа прийняла протиправне рішення за грошову винагороду на регулярній основі надавати «Івану» як представнику рф відомості щодо переміщення, руху та розташування Збройних Сил України та інших військових формувань [50].

Таким чином, вбачається, що в судам доводиться розглядати величезну кількість правопорушень пов’язаних з інформаційними діями. При цьому суди звертають увагу на характер таких дій та характер самої інформації.

Слід звернути увагу, що ряд суспільно-небезпечних діянь поки не було криміналізовано, зокрема щодо поширення дезінформації, створення фейкових неправдивих матеріалів (такі як діпфейки, як у відео, так й аудіо форматі), тощо. Зрозуміло, що з огляду на це не існує й судової практики, щодо таких діянь.

В той же час, криміналізувати такі діяння є необхідним задля запобігання масштабування пробем пов’язаних з подальшим розвитком технологій. Так, в деяких країнах створення та поширення діпфейків, які можуть нашкодити чиїйсь репутації вже криміналізовано та існують випадки, коли осіб арештовували за підозру у вчинення таких дій. Зокрема, як вбачається з інформації в ЗМІ, жінку з

Пенсільванії заарештували за створення наклепницьких підроблених фотографій дівчат із команди підтримки її доньки. Її звинувачують у створенні діпфейків, зокрема фотографій і відео, на яких зображені троє дівчат з команди її доньки в непристойному стані [51].

На жаль, з практики вбачається, що досліджувані правопорушення є дуже поширеними в Україні. Причинами цього можуть бути як недосконаліть законодавства (надто м'яке покарання за злочинні дії, тощо), так і низька обізнаність у суспільстві щодо реальної загрози таких злочинів.

3.3 Шляхи удосконалення правового регулювання інформаційних дій в кримінальному законодавстві.

Розуміючи теоретичні та практичні аспекти інформаційних дій, можливо сформувати власні рекомендації, що дозволять удосконалити правове регулювання інформаційних дій в кримінальному законодавстві.

Однак перш за все, варто відмітити, що кримінальним законодавством досить вдало були врегульовані ті виклики, що виникли у зв'язку з початком повномасштабного вторгнення. Стала судова практика підтверджує чіткість норм та їх вдале формулювання. В той же час, видається, що вдалось би запобігти більшій кількості правопорушень, якби Кримінальним кодексом України була передбачена відповідальність за деякі діяння що посягають на національну безпеку завчасно, до початку повномасштабного вторгнення, а не як реакція на вже існуючу проблему.

Для забезпечення ефективного правового регулювання інформаційних дій необхідно враховувати складність чіткого визначення інформаційних дій та інформації, необмеженість поширення інформації територіально, досвід іноземних країн, наукові напрацювання, а також виклики, що постають перед нами зараз і постануть в найближчій перспективі. Таким чином, можливість для вдосконалення правового регулювання інформаційних дій в кримінальному законодавстві вбачається в наступному.

По-перше, необхідно на певному уніфікованому рівні визнати та визначити таке поняття, як інформаційні дії, або ж інформаційні злочини. Це видається необхідним з тієї точки зору, що при встановленні складу кримінального правопорушення, де об'єктивна сторона характеризується вчиненням інформаційних дій, виникають певні труднощі у визначенні причинно-наслідкового зв'язку. З огляду на це, уніфікація визначення такого або таких понять, дозволить передбачити чіткий алгоритм дій для встановлення такого зв'язку, що допоможе правоохоронцям та судам притягати до відповідальності винних осіб, навіть коли причинно-наслідковий зв'язок не є очевидним.

По-друге, необхідно посилити покарання за деякі з інформаційних дій, що криміналізовані, однак не дивлячись на це є дуже поширеними і завдають значну шкоду потерпілим особам. Зокрема, мова йде, в першу чергу, про шахрайство, через постійний ріст кількості випадків вчинення такого злочину.

По-третє, необхідно криміналізувати інформаційні дії, у відповідності із наявними викликами, в умовах стрімкого розвитку штучного інтелекту та воєнного стану в країні. Так, за допомогою штучного інтелекту можуть бути створені та фактично вже створюються пропагандиські, фейкові та неправдиві матеріали, в тому числі діпфейки, що можуть порушувати або вже порушують права окремих осіб, їх гідність та репутацію, а також можуть нести загрозу на рівні країни, поширюючи шкідливі наративи та неправдиву інформацію.

Таким чином, розробка комплексних заходів з урахуванням зазначених рекомендацій потенційно може удосконалити правове регулювання інформаційних дій в кримінальному законодавстві та вирішити ряд проблем, що наразі існують. Тут слід підкреслити, що враховуючи швидкість технологічного розвитку та штучного інтелекту, активні бойові дії та інформаційну війну, необхідно швидко реагувати на такі обставини та так само оперативно адаптовувати законодавство під нові реалії.

***

Таким чином, за результатом дослідження інформаційних дій в практичному аспекті можна дійти висновку, що на даному етапі розвитку

законодавства видається недоцільним створювати додатковий інститут інформаційних дій, натомість слід більш ґрунтовно та системно підійти до удосконалення вже існуючих механізмів регулювання інформаційних дій та запобігання інформаційних злочинів.

В той же час, не можна недооцінювати кримінально-правове значення інформаційних дій, що полягає не лише в науковому інтересі дослідження такого явища, але й у необхідності створення дієвих механізмів регулювання цієї сфери, з урахування її швидкого розвитку та складності предмета регулювання.

З аналізу судової практики, вбачається, що судам доводиться розглядати величезну кількість правопорушень пов'язаних з інформаційними діями. При цьому суди звертають увагу на характер таких дій та характер самої інформації.

Слід звернути увагу, що ряд суспільно-небезпечних діянь поки не було криміналізовано, зокрема щодо поширення дезінформації, створення фейкових неправдивих матеріалів, тощо. Криміналізація таких діянь є необхідним заходом задля запобігання масштабування проблем пов'язаних з подальшим розвитком технологій.

Розуміючи теоретичні та практичні аспекти інформаційних дій, можливо сформувати власні рекомендації, що дозволять удосконалити правове регулювання інформаційних дій в кримінальному законодавстві.

Можливість для вдосконалення правового регулювання інформаційних дій в кримінальному законодавстві вбачається у:

1) визнанні та визначенні на законодавчому рівні такого поняття, як інформаційні дії, або ж інформаційні злочини;

2) посиленні покарання за деякі з інформаційних дій, що криміналізовані, однак не дивлячись на це є дуже поширеними і завдають значну шкоду потерпілим особам;

3) криміналізації інформаційних дій у відповідності із наявними викликами в умовах стрімкого розвитку штучного інтелекту та воєнного стану в країні.

Лише розробка комплексних заходів може удосконалити правове регулювання інформаційних дій в кримінальному законодавстві та вирішити ряд проблем, що наразі існують.

ВИСНОВОК

Таким чином, в даній роботі були досліджені теоретичні та практичні аспекти інформаційних дій.

В результаті визначено основні наукові підходи до дослідження інформації та інформаційних дій, встановлена методика дослідження та проаналізовані фактори, що впливали на дослідження інформаційних дій в різний період.

Так, науковці застосовують різні підходи, однак застосування системного підходу та теорії соціально-правового детермінізму дозволить дослідити інформаційні дії найбільш комплексно та ефективно, враховуючи їх вплив на суспільство.

Як вбачається з аналізу напрацювань, існуючі наукові дослідження в області інформаційних дій в кримінальному праві мають певні недоліки і не охоплюють всі аспекти цього явища. З огляду на це, необхідним є застосування інтегрованого підходу та проведення подальших досліджень для отримання більш повного розуміння проблематики. Для цього важливо використовувати широкий спектр методів, серед яких: діалектичний, історичний, порівняльно-правовий, системний, соціологічний та статистичний.

В результаті було визначено ознаки та поняття інформаційних дій. Так, інформаційні дії є процесом передачі, сприйняття, опрацювання інформації та її обміну між різними джерелами та отримувачами, що може включати передачу інформації у вербальній чи невербальній формі або через різноманітні комунікаційні канали. При цьому, такі дії також передбачають або можуть передбачати аналіз, інтерпретацію та оцінку отриманої у результаті активного пошуку або пасивного сприйняття інформації.

З аналізу практичних аспектів, діючого кримінально законодавства, іноземного досвіду, виявлено, що правове регулювання інформаційних дій не є ідеальним, і наявні проблеми становлять значний ризик для окремих осіб та держави в цілому. Сучасна інформаційна війна та стрімкий розвиток технологій та штучного інтелекту створюють необхідність у швидких та ефективних рішеннях з боку законодавців.

Для подальшого розвитку та удосконалення правового регулювання інформаційних дій важливо вивчати досвід інших країн, однак впроваджувати такий досвід слід з урахуванням унікальних викликів та потреб України.

Класифікація інформаційних дій є важливим етапом у їх ефективному правовому регулюванні, але на даний момент в науковий джерелах не було знайдено жодної класифікації інформаційних дій. Тому, були запропоновані критерії для класифікації таких дій, зокрема: характер (правомірність) дій, спосіб вчинення, зміст інформації.

Також, у контексті кримінального законодавства особлива увага приділена причинно-наслідковому зв'язку між інформаційними діями та суспільно небезпечними наслідками. Так, для встановлення причинного зв’язку між діями інформаційного характеру та суспільно небезпечними наслідкам необхідно відслідковувати, які саме дії мали вплив на потерпілу особу, часовий проміжок цих дій, які наслідки в результаті настали. Додатково слід враховувати мету інформаційної дії та наслідки, які були очікувані чи досягнуті, інтенсивність та повторюваність інформаційних дій та інші виняткові обставини, що здатні змінити оцінку причинного зв'язку.

Слід зауважити, що не можна недооцінювати кримінально-правове значення інформаційних дій, що полягає не лише в науковому інтересі дослідження такого явища, але й у необхідності створення дієвих механізмів регулювання цієї сфери.

З аналізу судової практики, вбачається, що судам доводиться розглядати величезну кількість правопорушень пов’язаних з інформаційними діями. При цьому суди звертають увагу на характер таких дій та характер самої інформації.

В той же час, ряд суспільно-небезпечних діянь поки не було криміналізовано, зокрема щодо поширення дезінформації, створення фейкових неправдивих матеріалів, тощо. Однак, криміналізація таких діянь вбачається необхідним заходом задля запобігання масштабування проблем пов’язаних з подальшим розвитком технологій.

Розуміючи теоретичні та практичні аспекти інформаційних дій, за результатом дослідження цього явища, запропоновані наступні рекомендації, що дозволять удосконалити правове регулювання інформаційних дій в кримінальному законодавстві.

По-перше, необхідно на певному уніфікованому рівні визнати та визначити таке поняття, як інформаційні дії, або ж інформаційні злочини. Це дозволить передбачити чіткий алгоритм дій для встановлення такого зв'язку, що допоможе правоохоронцям та судам притягати до відповідальності винних осіб, навіть коли причинно-наслідковий зв'язок не є очевидним.

По-друге, необхідно посилити покарання за ті інформаційні дії, що є дуже поширеними і завдають значну шкоду потерпілим особам.

По-третє, необхідно криміналізувати інформаційні дії, у відповідності із наявними викликами, в умовах стрімкого розвитку штучного інтелекту та воєнного стану в країні. Так, за допомогою штучного інтелекту можуть бути створені та фактично вже створюються інформаційні матеріали, в тому числі діпфейки, що можуть порушувати або вже порушують права окремих осіб, їх гідність та репутацію, а також можуть нести загрозу на рівні держави, поширюючи шкідливі наративи та неправдиву інформацію.

Слід зауважити, що лише розробка комплексних заходів може удосконалити правове регулювання інформаційних дій в кримінальному законодавстві та вирішити проблеми, що наразі існують.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Соловйова Б.О. Інформація як об’єкт цивільних прав в оновленому Цивільному кодексі України: проблеми визначення та основних ознак. *Київський університет права НАН України: Часопис Київського університету права.* 2021. № 1. С. 207 – 211.
2. Кормич Б. А. Інформаційне право: підручник. Харків: БУРУН і К., 2011. 334 с.
3. Ховпун О.С., Домбровська О.В., Муляр Г.В. Кримінальні правопорушення у сфері інформаційних технологій: особливості розслідування. *Часопис Київського університету права*. 2020. № 3. С. 285 – 289.
4. Азаров Д. С. Злочини у сфері комп’ютерної інформації (кримінально-правове дослідження): монографія. К.: Атіка, 2007. 304 с.
5. Панова І. В. Захист від впливу інформації, що є шкідливою для особи, як принцип інформаційного права. *Право і Безпека*. 2010. № 3. С. 69 – 72.
6. Hartel P., Junger M., Wieringa R. Cyber-crime Science = Crime Science + Information Security. 2010. 53 p. URL: https://www.researchgate.net/publication/215826712_Cyber-crime_Science_Crime_Science_Information_Security (дата звернення: 18.03.2024).
7. Нашинець-Наумова А. Інформаційна безпека: питання правового регулювання: монографія. Київ, Видавничий дім «Гельветика», 2017. 167 с.
8. Тер-Акопов А.А. Преступление и проблемы нефизической причинности в уголовном праве. М.: Юркнига, 2003. 478 с.
9. Ярмиш Н. Теоретичні проблеми причинно-наслідкового зв'язку в кримінальному праві (філософсько-правовий аналіз) : автореферат. Харків, 2003. 39 с.
10. Литвин Н. Інформаційне суспільство як головний пріоритет перспективного розвитку держави. *Вісник національного університету «Львівська політехніка», серія Юридичні науки.* 2017. Вип. 876, № 1. С. 157 – 162 URL: https://science.lpnu.ua/uk/law/vsi-vypusky/vypusk-1-nomer-876-15-

2017/informaciyne-suspilstvo-yak-golovnyy-priorytet (дата звернення: 28.03.2024).

11. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції URL: https://westudents.com.ua/glavy/51796-1-osnovn-polojennya-oknavsko-hart-globalnogo-nformatsynogo-susplstva.html#google_vignette (дата звернення: 28.03.2024).
12. Пожуєва В.І. Розвиток концептуальних засад інформатизації сучасного українського суспільства. *Гуманітарний вісник ЗДІА*. 2010. Вип. 41. С. 4 – 17.
13. Демченко С. Підходи до змісту поняття «інформація»: кібернетичний, філософський, правовий. *Национальный юридический журнал: Теория и практика*. 2016. С. 35–38.
14. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення 27.07.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 01.04.2024).
15. Селіванова О.О. Сучасна лінгвістика: термінологічна енциклопедія. Полтава, 2006. 197 с.
16. Прокоф'єва Д. Інформація як знаряддя вчинення злочину та злочини проти інформаційної безпеки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. С. 31–36.
17. Ховпун О., Домбровська О., Муляр Г. Кримінальні правопорушення у сфері інформаційних технологій: особливості розслідування. *Часопис Київського університету права*. 2020. № 3. С. 285–288.
18. Кримінальне право України. Загальна частина: Підручник / За ред. М.І. Бажанова, В.В. Сташиса, В.Я. Тація. Київ – Харків: Юрінком Інтер, Право, 2002. 416 с.
19. Куций Р. Ознаки зовнішнього прояву погрози як способу вчинення злочину. *Науковий вісник Міжнародного гуманітарного університету*. 2014. Т. 2, № 12. С. 129–131.
20. Бурау Н.І., Антонюк В.С., Півторак Д.О. Методологія наукових досліджень у галузі: практикум. *КПІ ім. Ігоря Сікорського*, 2021. 58 с.

21. Бондарчук А.С. Методологічні засади дослідження кримінальної відповідальності за погрозу або насильство щодо журналіста. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 2 Вип. 16. С 116 – 128.
22. Сопілко І. М. Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України. *Юридичний вісник*. 2022. № 3 Вип. 64. С.108-115.
23. Кримінальний кодекс України : Кодекс України від 05.04.2001 р. № 2341-III : дата оновлення 28.03.2024 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 15.03.2024).
24. Cavelty M. D., Wenger A. Cyber Security Politics: навчальний посібник. *New York* : Routledge, 2022. 272 p. URL: https://library.oapen.org/bitstream/handle/20.500.12657/52574/9781000567113.pdf?sequence=1 (дата звернення: 16.03.2024).
25. Про кіберзлочинність: Конвенція Ради Європи від 23 листопада 2001 року. ETS № 185. Офіційний вісник України. 2007. № 65. Ст. 2535.
26. Амелін О. Злочини у сфері інформаційних відносин в міжнародно-правових актах. *Науковий часопис Національної академії прокуратури України*. 2016. № 2. С. 1–9.
27. Francillon J. Infractions relevant du droit de l'information et de la communication. URL: https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2013-3-page-559.htm (date of access: 17.03.2024).
28. Kodeks karny. *OpenLEX*. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683 (date of access: 17.03.2023).
29. Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC. *Centers for Disease Control and Prevention*. URL: https://www.cdc.gov/phlp/publications/topic/hipaa.html (date of access: 02.04.2024).

30. Federal Register :: Request Access. *Federal Register :: Request Access*. URL: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F (date of access: 02.04.2024).
31. Federal Register :: Request Access. *Federal Register :: Request Access*. URL: https://www.ecfr.gov/current/title-34/subtitle-A/part-99?toc=1 (date of access: 02.04.2024).
32. Gramm-Leach-Bliley Act. *Congress.gov*. URL: https://www.congress.gov/bill/106th-congress/senate-bill/900/text (date of access: 02.04.2024).
33. U.S. Code Chapter 119 - Wire And Electronic Communications Interception And Interception Of Oral Communications. *LII / Legal Information Institute*. URL: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119 (date of access: 02.04.2024).
34. Children's Online Privacy Protection. *Olrc Home*. URL: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title15-section6501&edition=prelim (date of access: 02.04.2024).
35. Wrongful disclosure of video tape rental or sale records. *LII / Legal Information Institute*. URL: https://www.law.cornell.edu/uscode/text/18/2710 (date of access: 02.04.2024).
36. Батиргареєва В. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право*. 2020. Т. 1, № 32. С. 110 – 117.
37. Таран О. В. Проблема встановлення причинного зв'язку у злочинах проти безпеки виробництва. *Юридичний вісник*. 2016. Т. 1, № 38. С. 168 – 173.
38. Лепярж Я. Убили словами. ДержЗМІ Польщі довели до суїциду підлітка? URL: https://www.dw.com/uk/ubili-slovami-derzzmi-polsi-doveli-do-suicidu-pidlitka/a-64944015 (дата звернення: 20.03.2024).
39. Павлова О.С. Поняття та види інформаційних правопорушень. *Юридичний науковий електронний журнал*. 2023, № 7. С. 372 – 375.

40. Постанова Верховного Суду від 09 грудня 2020 р., судова справа №726/2173/18. URL: https://reyestr.court.gov.ua/Review/93595905 (дата звернення 07.04.2024).
41. Вирок Заводського районного суду м. Дніпрозержинська Дніпропетровської області від 18 січня 2022 р., судова справа № 208/10010/21. URL: https://verdictum.ligazakon.net/document/102582175?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01 (дата звернення 07.04.2024).
42. Вирок Вінницького міського суду Вінницької області від 25 квітня 2024 р., судова справа № 127/35602/23. URL: https://reyestr.court.gov.ua/Review/116585423 (дата звернення 07.04.2024).
43. Вирок Шевченківського районного суду м. Чернівці від 24 січня 2023 р., судова справа № 727/21/23. URL: https://reyestr.court.gov.ua/Review/108593691(дата звернення: 07.04.2024).
44. Вирок Жовтневого районного суду від 19 січня 2022 р., судова справа № 201/3277/21. URL: https://verdictum.ligazakon.net/document/102592807?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01 (дата звернення 07.04.2024).
45. Кількість справ про шахрайство сягла історичного максимуму у 2023 році. 2024. URL: https://opendatabot.ua/analytics/fraud-2023 (дата звернення 07.04.2024).
46. Вирок Верхньодніпровського районного суду Дніпропетровської області від 22 лютого 2024 р., судова справа № 173/2911/23. URL: https://reyestr.court.gov.ua/Review/117188977 (дата звернення: 07.04.2024).
47. Постанова Верховного Суду від 25 січня 2024 р., судова справа № 359/11048/19. URL: https://reyestr.court.gov.ua/Review/116639688 (дата звернення: 07.04.2024).
48. Вирок Приморського районного суду міста Одеси від 07.06.2022 р., судова справа № 522/6419/22. URL: https://verdictum.ligazakon.net/document/104656718?links_npa=T01234

1%20912915&_ga=2.253198030.671472069.1679590278-1937893070.1655155266 (дата звернення: 07.04.2024).

49. Постанова Верховного Суду від 18 травня 2023 р., судова справа № 127/12127/22. URL: https://reyestr.court.gov.ua/Review/111096337 (дата звернення: 08.04.2024).
50. Оголошено вирок за несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України/ URL: https://cn.cn.court.gov.ua/sud2523/pres-centr/news/1426732/ (дата звернення: 08.04.2024)
51. Cheerleader mom is arrested for creating 'deepfake' images and videos showing her daughter's rivals 'naked, drinking and smoking' in a bid to have them kicked off the team. URL: https://www.dailymail.co.uk/news/article-9359823/Cheerleader-mom-created-deepfake-images-daughters-rivals-naked-drinking-smoking.html (дата звернення: 08.04.2024)