Київський національний торговельно-економічний університет

Кафедра загальноправових дисциплін

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА РОЗГОЛОШЕННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ»

Студента 2 курсу, 7м групи,
спеціальності 081 «Право»,
спеціалізації «Правове забезпечення
безпеки підприємницької діяльності» Кураси Яна Владиславовича

Науковий керівник
д.ю.н.,професор Ладиченко Віктор Валерійович

Керівник освітньої програми
к.ю.н., професор Крегул Юрій Іванович

Київ 2018

ЗМІСТ

ВСТУП

Актуальність теми. Конституція України у статті 34 закріпила право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб, за винятком спеціально визначених у законі обставин. Таке обмеження здійснюється за допомогою правового інституту інформації з обмеженим доступом, яка, у свою чергу, поділяється за чинним законодавством на конфіденційну, таємну та службову.

Важливим елементом механізму забезпечення режиму інформації з обмеженим доступом є юридична відповідальність, що виступає своєрідним гарантом. Від якості правових норм, що передбачають відповідальність за порушення режиму інформації з обмеженим доступом, їх відповідності реаліям життя та потребам сучасності залежить інформаційна безпека особи, громади, суспільства та держави.

Актуальність правового захисту інформації з обмеженим доступом зумовлена об'єктивним зростанням кількості інформаційних загроз та шляхів протидії їм в процесі побудови інформаційного суспільства.

Теоретичне підґрунтя випускної кваліфікаційної роботи складають наробки таких правознавців: Г. Андрощук, В. А. Глуховеря, І. Грищенко, Л. Колобов, О. Коренюк, О. О. Кулініч, А. І. Марущак та багато інших.

Проте, окреслена вище наукова проблема не знайшла й досі комплексного вирішення.

Мета і завдання. Метою випускної кваліфікаційної роботи є комплексне дослідження притягнення до юридичної відповідальності за розголошення інформації з обмеженим доступом, розроблення пропозицій щодо вдосконалення законодавства в інформаційній сфері. Відповідно до цієї мети були поставлені такі завдання:

- розглянути поняття та зміст інформаційних правовідносин;
- проаналізувати інформаційне законодавство зарубіжних країн та країн

ЄС;

- дослідити розподіл інформації за порядком доступу, поняття та ознаки інформації з обмеженим доступом, сфери впливу, доступ/обмеження доступу до інформації з обмеженим доступом (конфіденційної, службової та таємної інформації);

- з'ясувати порядок надання носіям інформації грифу «ДСК»;

- проаналізувати інформацію як предмет злочину;

- розглянути юридичну відповідальність (кримінальну, адміністративну, цивільну) за правопорушення в сфері інформації з обмеженим доступом;

- дослідити забезпечення охорони (захист) інформації з обмеженим доступом;

- проаналізувати відповідальність у сфері інформаційної безпеки в сучасних умовах.

Об'єктом випускної кваліфікаційної роботи виступають суспільні відносини, пов'язані з реалізацією права на інформацію як невід'ємного, основоположного та фундаментального права людини.

Предметом випускної кваліфікаційної роботи є юридична відповідальність за розголошення інформації з обмеженим доступом.

Методи випускної кваліфікаційної роботи ґрунтуються на основі комплексного підходу до вивчення предмета дослідження. Методологічну основу становить низка загальнонаукових і спеціально-наукових методів. Зокрема, діалектичний метод дозволив охарактеризувати сучасні концепції права на інформацію у різних його формах, його взаємодію та взаємозв'язки з іншими правовими явищами. Логічний - допоміг у формулюванні таких понять, як «інформаційні правовідносини», «інформація» тощо. Метод аналізу і синтезу дозволив класифікувати види інформації за порядком доступу тощо. Метод правового прогнозування використовувався для визначення конкретних перспектив притягнення до юридичної відповідальності за розголошення інформації з обмеженим доступом в

Україні та розроблення пропозицій щодо вдосконалення законодавства у цій сфері.

Наукова новизна полягає в змістовному дослідженні основних проблем адміністративно-правових відносин у сфері притягнення до юридичної відповідальності за розголошення інформації з обмеженим доступом, а також у визначенні і теоретичному обґрунтуванні напрямків удосконалення чинного інформаційного законодавства.

Практичне значення одержаних результатів полягає в тому, що їх зміст у багатьох аспектах може бути використаний у:

- науково-дослідній сфері – для подальшої розробки даної проблеми і вивчення особливостей адміністративно-правових відносин у сфері притягнення до юридичної відповідальності за розголошення інформації з обмеженим доступом;

- правотворчості – під час внесення змін і доповнень до чинного законодавства, призначеного регламентувати адміністративно-правові відносини у сфері притягнення до юридичної відповідальності за розголошення інформації з обмеженим доступом;

- правозастосуванні – як теоретичний фундамент для суб'єктів вказаних правовідносин при вирішенні практичних проблем, пов'язаних із правом на інформацію з обмеженим доступом, інформаційною безпекою, правом доступу до інформації тощо;

- навчальному процесі – при підготовці методичних рекомендацій, посібників та підручників, а також при викладенні дисциплін.

Структура випускної кваліфікаційної роботи обумовлена метою і предметом дослідження та авторським підходом до розгляду обраної теми. Дана робота складається зі вступу, трьох розділів, що включають в себе дев'ять підрозділів, висновків, а також списку використаних джерел. Повний обсяг роботи становить 100 сторінок. Список використаних джерел складається із 80 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ПРАВА ЛЮДИНИ НА ДОСТУП ДО ІНФОРМАЦІЇ

1.1. Поняття та зміст інформаційних правовідносин

Україна сьогодні переживає період формування суспільства нового типу – інформаційного суспільства. Зважаючи на ту роль, що відводиться людині, її правам та свободам у правовому і інформаційному світі, який змінюється, юридична наука повинна сформулювати нові підходи до праворозуміння, у яких точкою відліку в правовій системі координат буде не норма права або інший зовнішній щодо людини об'єкт, а сам суб'єкт права. Таке суб'єктне сприйняття права вимагає доповнення і переробки деяких теоретичних положень, перегляду існуючих правових конструкцій, зокрема визнання інформаційних правовідносин.

Насамперед, зауважимо, що у науковій літературі відсутній єдиний підхід щодо визначення поняття інформаційних правовідносин. Так, зокрема, І. В. Безверхні, Л. В. Перевалова зазначають, що інформаційними правовідносинами можуть вважатися суспільні відносини, які виникають з приводу одержання, перероблення, використання або зберігання інформації [27]. На думку О. І. Яременко, інформаційні правовідносини – суспільні відносини, які регулюються нормами права і виникають, розвиваються та припиняють свою дію в інформаційному просторі між суб'єктами права, які наділені інформаційними правами та обов'язками [78, с.158]. М. І. Дімчогло визначає інформаційні правовідносини як суспільні відносини щодо інформації, які формуються і розвиваються під впливом здобутків науково-технічного прогресу в галузі інформаціології, правової інформатики, телематики, кібернетики, комп'ютерних наук, у різних видах діяльності людей [33, с.3]. Перов Д. А., Климентьев А. П. вважають, що інформаційні правовідносини – це відносини між суб'єктами, коло яких законодавчо

визначене, з приводу вчинення певних дій щодо інформації (отримання, пошук, зберігання та ін.) [58, с.83].

Отже, інформаційні правовідносини – це врегульовані інформаційно-правовою нормою інформаційні суспільні відносини, сторони якого виступають як носії взаємних прав і обов'язків, встановлених і гарантованих інформаційно-правовою нормою.

До основних елементів інформаційних правовідносин належать:

1) об'єкт – те, з приводу чого виникають інформаційні правовідносини;

2) суб'єкт – сторін інформаційних правовідносин, які володіють певною правосуб'єктністю для реалізації інформаційних правовідносин;

3) зміст інформаційних правовідносин – комплексу суб'єктивних прав та юридичних обов'язків, що закріплюється за суб'єктами інформаційних правовідносин для здійснення інформаційної діяльності [65, с.184].

Об'єктами інформаційних правовідносин є: документована інформація, інформаційні продукти і послуги; виключні права; елементи інформаційної безпеки (інформаційні права і свободи особи, стан захищеності особи, захищеність інформації, інформаційних ресурсів, інформаційних продуктів і т.п.); інформаційні технології і засоби їх забезпечення (в тому числі програми для ЕОМ), інші об'єкти в інформаційній сфері; права, обов'язки і відповідальність суб'єктів правовідносин при здійсненні інформаційних процесів.

Концепція об'єкта інформаційних правовідносин допускає існування множини об'єктів:

1) інформація;

2) матеріальні блага, інформаційні системи, інформаційні ресурси, бази даних, засоби забезпечення автоматизованих інформаційних систем та їх технологій, засоби обчислювальної техніки і зв'язку;

3) нематеріальні особисті блага (таємниця приватного життя, особиста і сімейна таємниця, честь, гідність, ділова репутація);

4) поведінка та дії суб'єктів інформаційних правовідносин [77, с.13].

Шевчук О. М. [76, с.15] виокремлює особливі інформаційні відносини, безпосереднім об'єктом яких є інформація в електронно-цифровій формі. Основним предметом правового регулювання цих відносин виступають соціальні (суспільні) відносини, які виникають у процесі створення, перетворення і споживання інформації на базі застосування автоматизованих інформаційних технологій. Вони становлять особливий різновид інформаційних відносин, які називають інформаційно-комп'ютерними, а зазначену діяльність відносять до сфери комп'ютерної інформації. Їхня специфіка зумовлена особливостями самої природи інформації на машинних носіях і безпосередній технології її обробки.

Впровадження інформаційних технологій супроводжують такі суспільні відносини, які виникають при:

- забезпеченні конституційних прав на інформацію, що забезпечуються за допомогою автоматизованих інформаційних технологій;

- розробці, впровадженні та експлуатації комп'ютерних систем і мереж, а також телекомунікаційних мереж;

- створенні, поширенні, передачі, купівлі-продажу програмного забезпечення для електронно-обчислювальних машин та інших засобів забезпечення автоматизованих інформаційних систем;

- формуванні й використанні інформаційних ресурсів, що включають електронні бази даних;

- установленні й дотриманні режиму доступу до комп'ютерної інформації і проведенні інших заходів інформаційної безпеки;

- міжнародному обміні комп'ютерною інформацією.

Суб'єктами інформаційних відносин є: фізичні особи, юридичні особи, держава.

У Законі України «Про інформацію» дається розшифровка поняття «суб'єкти інформаційних правовідносин» (п. 4 ч. 1 ст. 1), до яких відносять органи державної влади, органи місцевого самоврядування, інших суб'єктів,

що здійснюють владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Щодо об'єднань громадян, то їхнє термінологічне тлумачення є дещо ускладненим. Поняття «об'єднання громадян» було зафіксовано в Законі України «Про об'єднання громадян» від 16 червня 1992 року № 2460-XII. Так, ч. 1 ст. 1 визначала, що об'єднанням громадян є добровільне громадське формування, створене на основі єдності інтересів для спільної реалізації громадянами своїх прав і свобод. Проте вказаний закон втратив чинність з прийняттям Закону України «Про громадські об'єднання» від 22 березня 2012 року № 4572-IV. Поняття «об'єднання громадян» було фактично замінено на поняття «громадські об'єднання». Такий висновок випливає з порівняння визначень. Так, ч. 1 ст. 1 Закону України «Про громадські об'єднання» характеризує громадські об'єднання як добровільне об'єднання фізичних осіб та/або юридичних осіб приватного права для здійснення та захисту прав і свобод, задоволення суспільних, зокрема економічних, соціальних, культурних, екологічних та інших інтересів. Таким чином, для узгодження термінології в Законі України «Про інформацію» потрібно замінити словосполучення «об'єднання громадян» на «громадські об'єднання».

Фізичні особи, що виступають як суб'єкти інформаційних правовідносин, можуть бути виключно громадянами України, іноземцями, особами без громадянства. Як фізичні, так і юридичні особи, що виступають суб'єктами інформаційних правовідносин, володіють інформаційною правоздатністю та інформаційною дієздатністю. Інформаційна правоздатність (здатність мати інформаційні права) для фізичних осіб наступає з моменту народження, а інформаційна дієздатність (здатність своїми діями набувати прав та обов'язків) – у більшості випадків з настанням повноліття, але іноді – в інший час (наприклад, користувачами бібліотеки або відвідувачами музеїв можуть бути навіть малолітні особи). Інформаційна правоздатність та інформаційна дієздатність юридичних осіб виникають

одночасно з моменту державної реєстрації новоствореної юридичної особи. Крім двох зазначених характеристик правового статусу суб'єктів інформаційних правовідносин, варто вказати і на ще одну – інформаційну деліктоздатність, тобто здатність нести відповідальність за свої дії. Розділ IV Закону України «Про інформацію» встановлює основні положення щодо відповідальності за порушення законодавства про інформацію. Зокрема, передбачено, що такі порушення тягнуть за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність, але також визначено і підстави звільнення суб'єктів інформаційних правовідносин від відповідальності.

Учасники інформаційних відносин зобов'язані:

- поважати інформаційні права інших суб'єктів;

- використовувати інформацію згідно з законом або договором (угодою);

- забезпечувати доступ до інформації усім споживачам на умовах, передбачених чинним законодавством;

- зберігати інформацію в належному стані впродовж встановленого терміну і надавати іншим громадянам, юридичним особам або державним органам у передбаченому законом порядку;

- компенсувати шкоду, заподіяну при порушенні законодавства про інформацію.

Третім елементом структури інформаційних правовідносин є зміст, під яким розуміється визначена сукупність суб'єктивних прав та юридичних обов'язків, що належать суб'єкту інформаційних правовідносин. Варто відмітити, що одному колу суб'єктів інформаційних правовідносин притаманна наявність більшої кількості обов'язків (органу державної влади або місцевого самоврядування), а іншим – кількості прав(фізичні особи). Наприклад, порівняємо зміст інформаційних правовідносин, суб'єктом яких є Адміністрація Державної служби спеціального зв'язку та захисту інформації

України Департаменту технічного захисту інформації та суб'єкти права інтелектуальної власності.

Відповідно до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України Департаменту технічного захисту інформації (затвердженого указом Президента України від 30 червня 2011 року № 717) за цим суб'єктом закріплено понад 80 обов'язків та близько 24 прав. Тоді як автори, винахідники або виконавці володіють цілою низкою особистих немайнових та майнових прав, закріплених у цивільному законодавстві, а обов'язків у них порівняно мало та й ті, як правило, носять загальноюридичний характер [65, с.186].

1.2. Інформаційне законодавство зарубіжних країн та країн ЄС

Інформаційне право, як наука має на меті розробку способів найбільш ефективного і повного забезпечення інформаційних процесів в Україні, захисту громадян, суспільства, держави від шкідливої, небезпечної інформації, захист прав і свобод споживачів інформації в інформаційній сфері. На виконання цієї мети, розроблена система правового регулювання інформаційних відносин, яка складається з двох частин: приватноправове регулювання, що здійснюється на рівні звичаїв, угод, традицій, норм суспільної моралі тощо; публічно-правове, державне регулювання, що здійснюється на рівні держави у вигляді інформаційного законодавства.

Сьогодні в світі актуальним питанням є проблема захисту інформації та інформаційного простору. Її розглядають не тільки на рівні однієї країни, але і на саммітах глобальних співтовариств та організацій, таких як НАТО, ЄС, Велика вісімка тощо. Відбувається це, головним чином, тому, що до їх складу входять провідні країни світу (США, Російська Федерація, передові країни Західної Європи та Азії).

Країною з розвинутою системою захисту інформаційного простору є США. Американці перші, хто зрозумів вислів про володіння інформацією,

оскільки вони одними з перших у світі запровадили систему захисту інформації на законодавчому рівні. У Сполучених Штатах Америки закони, що стосуються сфери захисту інформації діють з 1974 року [28].

Зазначимо, що законодавство у напрямку захисту інформації цієї країни, перш за все, визначає об'єкти правової охорони в інформаційній сфері, порядок реалізації права власності на інформаційні об'єкти, права і обов'язки власників, правовий режим функціонування інформаційних технологій; категорії доступу окремих суб'єктів до певних видів інформацій, встановлює категорії секретності, поняття «конфіденційної інформації» та межі його правового застосування [28].

Інформаційне законодавство Сполучених Штатів Америки - це той орієнтир, на який повинні слідувати країни у своїх спробах збудувати хорошу базу інформаційного законодавства. У цій країні законодавці змогли створити систему законів стосовно безпеки інформації з такою лаконічністю та узагальненням, що за необхідності реагування на проблему буде миттєве.

Законодавча система США з безпеки інформації є однією з найнадійніших у світі, що робить її майже досконалою та такою, на яку всі повинні рівнятися. Інформація в США може бути захищена за допомогою правових засобів захисту інтелектуальної власності, й взагалі інформація розглядається як об'єкт права інтелектуальної власності, навіть, коли йдеться про масову інформацію. Зазначимо, що в США існують чотири основних закони з приводу інтелектуальної власності: закон про авторське право, патентний закон, закон про торгову марку, закон про торговий секрет [40]. Ці закони є федеральними і поширюються на всі штати.

Важливе значення в системі законодавства США в інформаційній сфері відіграють судові прецеденти. Особливий інтерес з приводу з'ясування питань регулювання інформаційних відносин становлять рішення саме щодо права власності та інтелектуальної власності на інформацію. Згідно законодавства США існує два види комерційної таємниці - це технологічна інформація (має самостійну економічну вартість внаслідок власної

унікальності та за рахунок неможливості її одержання законним шляхом іншими особами, й які можуть отримати економічний еквівалент від її використання та розкриття) та ділова інформація (є об'єктом діяльності, що обґрунтовується за обставин, які вимагають її збереження в таємниці).

У США комерційна таємниця спочатку була сферою, що традиційно регулювалась загальним правом окремих штатів. Першою спробою «кодифікації» розробленого судами права комерційної таємниці був Перший Звід права деліктів 1939 р. Сучасніший підхід було закріплено Третім Зводом права деліктів 1993 р.. Охорона комерційної таємниці відбувається в межах делікту незаконного заволодіння комерційною таємницею, який, у свою чергу, є складовою делікту недобросовісної конкуренції. Зараз у більшості юрисдикцій США комерційна таємниця охороняється законами. 42 штати та Округ Колумбія прийняли ту чи іншу версію Уніфікованого Закону про комерційну таємницю (Uniform Trade Secrets Act) 1979 р. У Каліфорнії положення Закону включені в Цивільний кодекс. Законодавчі положення доповнюються договірним захистом, який виступає додатковим. Виділяють такі чотири основні елементи режиму комерційної таємниці в США: по-перше, це повинна бути «обмежена інформація», тобто інформація, яку можна відрізнити від загально відомих знань та навичок; по-друге, елемент «секретності» – інформація не є добре відомою або такою, яку можна легко отримати; по-третє, інформація повинна мати економічну цінність, що полягає у наданні певної конкурентної переваги; по-четверте, володілець повинен вжити розумних зусиль для того, щоб зберегти інформацію в таємниці.

Згідно з частиною четвертою ст. 1 Уніфікованого Закону США про комерційну таємницю: «Комерційною таємницею» є інформація, у тому числі формула, зразок, компіляція, програма, пристрій, метод, техніка або процес, яка:

1) має самостійну економічну цінність, дійсну або потенційну, у силу того, що не є загально відомою або легко доступною з використанням

необхідних засобів для осіб, які можуть отримати економічну вигоду від її розкриття або використання;

2) є предметом зусиль, що є розумними за відповідних обставин для збереження її секретності». Серед особливостей законодавства США про захист комерційної таємниці варто відзначити величезну увагу законодавця до кримінальної відповідальності, як найбільш ефективного засобу забезпечення прав й інтересів власника комерційної таємниці. Існує значна кількість кримінальних законів, що стосуються незаконного заволодіння комерційною таємницею, основним з яких є федеральний Закон про Економічний шпіонаж 1996 р.

Вважається, що передбачена законом цивільна відповідальність (відшкодування збитків) недостатня для запобігання інформаційним злочинам. Таким чином, захист комерційної таємниці здійснюється не тільки в приватних але й в публічних інтересах – з метою забезпечення конкурентноздатності національної економіки. За порушення прав володільця комерційної таємниці, закон передбачає покарання у вигляді позбавлення волі строком до десяти років і штрафу в розмірі до півмільйона доларів США. Якщо суб'єктом злочину є юридична особа, штраф може досягати п'яти мільйонів доларів США. Підвищені покарання передбачені також, якщо крадіжка комерційних секретів здійснюється в інтересах іноземних громадян й організацій. Окрім того, закон передбачає конфіскацію будь-якої власності, придбаної з порушенням прав володільця комерційної таємниці, а також використаної для здійснення відповідних злочинних діянь [56, с.137-138].

Слід зазначити, що персональна інформація, в Сполучених Штатах розглядається відповідно до концепції «privacy». Ця концепція реалізується через Стандарт CSA, який було прийнято у 1996 році. Цей нормативно-правовий документ використовується в Америці головним чином тому, що поширюється на всі країни-члени НАТО Стандарт CSA містить наступні

принципи регулювання суспільних відносин, що виникають з приводу персональних даних:

1. Відповідальність. Організація відповідальна за ті персональні дані, що знаходяться під її контролем, і має призначати особу або осіб, які відповідають за відповідність дій організації принципам законодавства.

2. Ідентифікація мети. Мета, задля якої збирається інформація, має бути ідентифікована організацією до початку процесу збирання інформації.

3. Згода. Усвідомлення та згода особи на збирання інформації про неї є обов'язковою умовою збирання, використання чи поширення (розкриття) персональних даних, крім випадків, де це недоречно.

4. Обмежене збирання. Збирання персональної інформації має бути обмежене до межі тієї мети, яка визначена (ідентифікована) організацією. Інформація може збиратися лише для справедливої та законної мети.

5. Обмежене використання, поширення, зберігання. Персональна інформація не повинна використовуватись або поширюватись не з тією метою, для якої вона була зібрана, окрім випадків згоди особи або вимоги закону. Персональна інформація не повинна зберігатися довше, ніж це необхідно для досягнення зазначеної мети.

6. Точність. Персональна інформація має бути точною, повною та сучасною, щоб досягти мети, задля якої інформацію було зібрано.

7. Безпека. Персональна інформація має бути захищена за допомогою забезпечення такого рівня безпеки, який відповідає вимогам «чутливості» (sensitivity) інформації.

8. Відкритість. Організація має зробити доступною для особи специфічну інформацію про її (організації) політичне та практичне відношення до управління персональною інформацією.

9. Особистий доступ. На вимогу особи вона має бути проінформована про існування, використання та поширення її персональної інформації, і такій особі має бути наданий доступ до інформації. Особа має бути в змозі

перевірити точність і повноту інформації та виправити таку інформацію в разі необхідності.

10. Перевірка відповідності. Особа повинна мати можливість направити завдання з перевірки, що стосується відповідності принципам законодавства, особам чи особі, відповідальним за відповідність діяльності організацій принципам законодавства [40].

Ще одним прикладом інформаційного законодавства є закони, прийняті країнами-членами Європейського Союзу, під які теперішні претенденти на вступ до ЄС переробляють або приймають доповнення до свого законодавства. У 1995 році Європейським Союзом була прийнята Директива щодо Захисту особистості з дотриманням режиму персональних даних і вільного руху таких даних. Директива спрямована на впорядкування практики захисту інформації в межах Європейського Союзу. Однією з вимог, адресованих державам-учасникам, є вимога прийняти закони щодо захисту персональної інформації як в публічному, так і в приватному секторі.

Зазначені закони мають також включати тимчасове блокування переміщення інформації до держав – не членів Європейського Союзу, які не встановили «адекватного» рівня захисту інформації. В доповнення цієї Директиви у 1996 році була прийнята Директива, яка забезпечує гармонізацію в державах - членах, умов, необхідних для того, щоб гарантувати еквівалентний рівень захисту фундаментальних прав і свобод, у тому числі специфічного права на секретність стосовно обробки персональних даних у секторі телезв'язку та гарантувати вільний рух таких даних, та обладнання телезв'язку та послуг у Співдружності. Положення Директиви регламентують також порядок обробки інформації та надання її за запитом. Передбачається обов'язкове знищення інформації або надання їй характеру анонімної після надання на запит, або після досягнення іншої мети, погодженої з абонентом. Обробка даних щодо рахунків може тривати лише до закінчення періоду, протягом якого по рахунках має бути сплачено. Можливість обробки торгівельних даних та інформації розрахунків має бути

обмежена діяльністю осіб, які діють відповідно до повноважень постачальників публічно доступного обслуговування телезв'язку, запитами клієнта, виявленням шахрайства та вдосконаленням управління послугами телезв'язку.

При здійсненні зазначеної діяльності, можливість обробки інформації має відповідати рівню необхідності такої обробки для досягнення встановленої мети. Персональні дані, що містяться в друкованих або електронних довідниках абонентів, які є доступним для громадськості або можуть стати доступними шляхом запиту, мають бути обмежені тією інформацією, яка дозволяє ідентифікувати конкретного абонента, якщо останній не дав згоди на публікацію додаткової інформації.

Держави-учасники можуть дозволити операторам мереж зв'язку вимагати платні від абонентів, які бажають, щоб інформація щодо адреси або статі не була внесена до довідника, якщо встановлена сума буде помірною та не заважатиме здійсненню такого права. Країни-учасники можуть обмежити застосування цього положення до абонентів.

Із метою реалізації чинної Директиви, держави-учасники мають гарантувати добровільне обладнання зв'язку не встановлені жодні примусові вимоги щодо певних технічних особливостей, які б могли перешкоджати вільному розміщенню обладнання на ринку та його обігу між Державами-учасниками. Відповідно до Директиви щодо Захисту особистості з дотриманням режиму персональних даних і вільного руху таких даних 95/46/ЕС і конкретизуючої її Директиви від 1996 року, були внесені зміни до національного Законодавства держав-учасників Європейського Союзу.

Країни-учасники Європейського Союзу мають у певному сенсі злагоджену систему захисту інформації, але в той же час вона є розгалуженою, тому що, як зазначалося вище, хоча існує Директива щодо Захисту особистості з дотриманням режиму персональних даних і вільного руху таких даних, яка в принципі врегульовує певні питання, але при цьому майже кожна країна ЄС має свої закони, положення, інструкції, щодо

врегулювання питань безпеки інформації. Така система має і свої переваги, та свої недоліки. Недолік полягає у тому, що обмін інформацією між країнами ускладнюється через певні неспівпадання у нормативних актах країн, про що було зазначено вище. Така ж проблема існує й у відносинах ЄС і України, оскільки інформаційне законодавство взагалі не співпадає з визначеннями понять у законодавстві Європейського Союзу [29, с.129-130].

У розвинутих країнах Європи охорона конфіденційної комерційної інформації має свою довгу історію, хоча підходи різняться залежно від країни. Найрозвинутішу систему охорони має Великобританія, що пов’язано з промисловою революцією та традицією прецедентного права. Саме з англійської системи бере початок відповідне законодавство США. У Великобританії відсутній законодавчий захист комерційної таємниці, відповідно, не існує легального визначення цієї таємниці. Натомість, правове регулювання цих відносин розвивалось впродовж останніх століть на основі судових прецедентів та отримало назву конфіденційного права (law of confidence). Отже, охорона комерційної таємниці ґрунтується на концепції «порушення довіри». У рішенні Seager v. Copydex LTD вона була сформульована наступним чином: «Право, що застосовується до цього випадку, не залежить від якоїсь угоди. Воно залежить від широкого принципу справедливості, що полягає в тому, що той, хто отримав інформацію конфіденційно не повинен недобросовісно здобувати з неї вигоду. Він не повинен використовувати її на шкоду тому, хто передав йому цю інформацію, якщо останній не дав своєї згоди».

Таким чином, головним принципом є довіра між законним володільцем таємниці та отримувачем конфіденційної інформації. Значна кількість судових справ щодо захисту комерційної таємниці пов'язана з трудовими відносинами. Це обумовлено доступом працівників до конфіденційної інформації під час виконання трудових обов'язків. Встановлені судовою практикою відповідні правові принципи, покликані забезпечити належний баланс між правом власника підприємства захищати свої таємниці й правом

працівника використати свій професійний досвід у власних інтересах та інтересах інших працедавців. Серед основних правил, встановлених для працівників (у т.ч. і колишніх), виділяється наступне – обов'язок збереження конфіденційної інформації може бути встановлений у спеціальних положеннях трудового договору, у разі відсутності таких умов цей обов'язок витікає із загальних вимог добросовісності й лояльності.

Вирішуючи спори між працівником і власником, судами враховується природа конкретних трудових відносин, статус працівника, рівень доступності конфіденційної інформації та вжиті працедавцем заходи щодо її захисту. Після припинення трудових відносин вимоги до колишнього працівника, щодо збереження комерційної таємниці, істотно звужуються. З метою запобігання розголошення комерційної таємниці власники підприємств включають у трудовий договір спеціальні положення, що забороняють працівнику приймати участь у конкурентній боротьбі проти роботодавця. З огляду на те, що подібні положення істотно обмежують розвиток підприємницької діяльності, вони враховуються лише за умов, якщо власник доведе, що були наявні підстави для застосування цих положень щодо строків, обсягів й територіальних рамок.

Очевидно, що наведені положення трудового договору не використовуються для обмеження конкуренції, а лише захищають законні інтереси працедавця як володільця, незважаючи на те, що працівник вніс певний вклад у створення цієї власності. Таким чином, умови збереження комерційної таємниці не можуть виходити за рамки розумного захисту інтересів колишнього працедавця, що, відповідно, обмежує їх обсяг й час дії.

В судовій практиці Великобританії, у справах про захист комерційної таємниці, і значне поширення отримали тимчасові (проміжні) методи судового захисту. Розголошення комерційної таємниці може призвести до значних збитків (і навіть припинення підприємницької діяльності потерпілого), при цьому, розкрита інформація, природно, не може бути знову засекречена. В зв'язку з цим значна кількість позовів подається з метою

запобігання незаконному використанню конфіденційної комерційної інформації або її розголошенню ще до того, як це спричинить майновий збиток. Законодавство Франції містить поняття промислових або виробничих секретів (secret de fabrique) та комерційної таємниці (secret de commerce). Перша категорія походить з французького кримінального кодексу та включає конфіденційну інформацію, що має виробниче застосування та може становити комерційну цінність. Комерційна таємниця прямо не визначається законодавством, але висвітлює ширші, порівняно з виробничими секретами, поняття і може відноситися до організаційної структури підприємства, списку постачальників, особових справ персоналу, контрактів з іншими організаціями, списків клієнтів, планів розвитку бізнесу, схеми дистрибуції тощо. Виробничі та комерційні секрети не вважаються власністю у Франції і отримують захист в якості деліктів з недобросовісної конкуренції та договірних зобов'язань [56, с.137].

Для законодавства Німеччини характерна детальна розробленість системи понять різних видів таємниць, чіткі формулювання їх визначень у федеральному законодавстві. Так, відповідно до закону про умови і процедури перевірки благонадійності у ФРН (1994) секретною інформацією є факти, вироби та відомості незалежно від форми їх представлення, які в державних інтересах повинні зберігатися в таємниці та яким наданий державним органом чи за його дорученням ступінь секретності, котрий відповідає необхідному рівню захисту: «цілком таємно», «таємно», «конфіденційно» чи «для службового користування».

У систему секретної інформації Німеччини входить державна таємниця (відомості з грифом «цілком таємно» і «таємно») та відомча таємниця (відомості з грифом «конфіденційно» і «для службового користування»), охорона яких, на відміну від інших видів таємниць, що становлять секретну сферу приватних осіб, зумовлена інтересами зовнішньої безпеки держави. У Кримінальному кодексі Німеччині передбачені норми, які регулюють

питання покарання в разі розголошення державної таємниці (§§ 93 – 95, 97 КК) та розголошення відомчої таємниці (§ 353 b).

Відповідно до Федерального відомчого закону (1953 р.) відомчою таємницею є «факти або відомості, збереження яких у таємниці обумовлене приписом закону чи постанови державного органу і які доступні лише обмеженому колу осіб». Під «обмеженим колом осіб», на нашу думку, слід розуміти безпосередніх «секретоносіїв», тобто таких осіб, яким таємниця була довірена чи стала відома по службі. До них належать переважно службовці державних органів. У кримінальному законодавстві Німеччини встановлена диференційована відповідальність за розголошення секретної інформації залежно від форми вини.

Зазначимо, що в перевірці благонадійності відповідно до нормативно-правових актів бере участь федеральне відомство з захисту конституції, а у сфері повноважень міністерства оборони – військова контррозвідка відповідно до закону про військову контррозвідку. Федеральна розвідувальна служба, федеральне відомство з захисту конституції та військова контррозвідка здійснюють перевірку благонадійності своїх кандидатів і співробітників самостійно. З метою належного відбору громадян та забезпечення безпеки проводиться: проста перевірка; розширена перевірка благонадійності; розширена перевірка благонадійності з аналізом відомостей.

У кінці 90-х років XX століття в Німеччині значно посилено поліцейський і контррозвідувальний режим стосовно іноземних громадян, особливо з пострадянських країн, які перебували там по лінії торгово-економічних і науково-технічних зв’язків. За ними здійснювалося спостереження як у службовий, так і позаслужбовий час. Слід зазначити, що спецслужби Німеччини активно взаємодіють із прикордонними військами, поліцейськими службами федеральних земель, митними органами, спілками підприємців, а також з іншими установами й відомствами, які відповідно до законодавства держави зобов’язані надавати відомості про іноземних

громадян. Крім того, вони сприяли через Федеральний союз німецької промисловості боротьбі з промисловим шпигунством.

Також спецслужби Німеччини проводять контррозвідувальні заходи у великих промислових фірмах, що підтримують ділові зв'язки з економічно розвинутими державами. Персонал фірм підлягає так званій «триступеневій» системі перевірки, яка раніше застосовувалася тільки до державних службовців. Саме тому збираються відомості не лише про особу, яка перевіряється, а й про її родичів.

У грудні 1989 року в Німеччині прийнято нове положення про порядок виїзду секретоносіїв за кордон. Згідно з ним усі особи, які мали доступ до секретної інформації, зобов'язані заздалегідь повідомляти співробітників, відповідальних за забезпечення режиму секретності, про свій намір відвідати іноземну державу [68, с.9-10].

1.3. Правове регулювання різних видів інформації

Аналізуючи інформацію як об'єкт правовідносин, треба розглянути інформацію, що заходиться в обігу, і з приводу, чи у зв'язку з якою і виникають суспільні відносини, пов'язані з реалізацією права на інформацію, як невід'ємного, основоположного та фундаментального права людини, і такі, що підлягають регулюванню нормами права.

Така інформація поділяється на три групи:

1) інформація, що заходиться у цивільному обігу, тобто та, з приводу якої виникають в першу чергу майнові відносини;

2) інформація, що заходиться в адміністративному обігу, тобто та, за допомогою якої регулюються суспільні відносини, в тому числі і в інформаційній сфері (зокрема, інформація, що міститься у нормах права);

3) інформація, яка знаходиться у суспільному (публічному) обігу, що являє собою відомості інформаційного характеру, чи масова інформація, призначена для інформування населення.

Необхідно чітко розмежовувати два поняття інформації:

1) публічна;

2) інформація з обмеженим доступом.

Публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом України «Про доступ до публічної інформації». Статтею 5 розділу II Порядок доступу до інформації даного Закону визначено шляхи доступу до інформації, а саме: систематичне та оперативне оприлюднення інформації в офіційних друкованих виданнях, на офіційних веб-сайтах в мережі Інтернет, на інформаційних стендах та надання інформації за запитами на інформацію, у будь-який інший спосіб. Якщо інформація вважається відкритою, отримати доступ до неї мають право всі громадяни України, незалежно від того стосується їх ця інформація безпосередньо чи ні.

За загальним правилом, публічна інформація є відкритою. Винятки з цього правила встановлюються законом (частина друга статті 1 Розділу I Закону [4]; частина друга статті 20 Розділу II Закону [3]. Положенням статті 21 Розділу II Закону [3], зокрема, встановлено види інформації, до якої може бути обмежено доступ: конфіденційна, таємна та службова інформація, та сукупність вимог, дотримання яких є обов'язковим для обмеження доступу до таких видів інформації.

Обмеження доступу до інформації здійснюється відповідно до Закону України «Про інформацію» при дотриманні сукупності таких вимог:

1) тільки в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам,

для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Порядок забезпечення доступу до публічної інформації у Вищому спеціалізованому суді України з розгляду цивільних і кримінальних справ здійснюється на підставі Закону та регулюється Положенням про забезпечення доступу до публічної інформації у Вищому спеціалізованому суді України (далі - ВССУ) з розгляду цивільних і кримінальних справ від 16 травня 2011 р. № 15/0/14-11. Відповідно до зазначеного Положення інформація про діяльність зазначеного суду може надаватися в усній формі та у вигляді документованої інформації, в тому числі у вигляді електронного документа. Надання публічної інформації про діяльність ВССУ запитувачам інформації, а також розміщення вказаної інформації на веб-сайті ВССУ та інформаційних стендах ВССУ забезпечують керівники структурних підрозділів апарату ВССУ за відповідними напрямами діяльності.

Правовий режим інформації з обмеженим доступом полягає в тому, щоб охороняти відомості, вільний обіг яких може порушити права та інтереси держави, суспільства та окремої особи, забезпечити інформаційну незалежність суб'єктів приватного права у відносинах із державою і між собою, узгодити публічну потребу у свободі інформації та право кожного на збереження таємниці [79,с. 13].

Обмеження доступу до інформації здійснюється відповідно до Закону України «Про доступ до публічної інформації» при дотриманні сукупності таких вимог: тільки в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав

інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; розголошення інформації може завдати істотної шкоди цим інтересам; шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Отже, законодавчо закріплені випадки визначення інформації з обмеженим доступом. Інформація з обмеженим доступом має надаватися власником чи розпорядником інформації, якщо він правомірно оприлюднив її раніше. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

Відповідно до Закону України «Про інформацію, інформація з обмеженим доступом – це інформація, що не може бути відкрито, оприлюдненою доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону.

На відміну від суто внутрішньодержавних нормативно-правових актів України, де відсутнє визначення поняття «інформація з обмеженим доступом», в окремих міжнародних угодах, учасником яких є Україна, знайшло своє відображення дане визначення. Є чимала кількість міжнародних документів, що встановлюють правила обігу інформації з обмеженим доступом між Україною та іншими державами, обмін якою здійснюється між ними чи між державними органами та приватними установами під їх юрисдикцією, або спільно створеними ними. Слід зауважити, що назва такої інформації також є неусталеною: в одних угодах вказується на взаємну охорону «інформації з обмеженим доступом», у других – на взаємну охорону «секретної інформації», в третіх – на взаємну охорону «таємної інформації». Аналіз змісту норм вищезазначених документів дає змогу дійти висновку, що, незважаючи на різну назву, мова йде саме про встановлення міжнародного співробітництва України та іншої держави у

сфері інформації з обмеженим доступом як більш широкої категорії [69, с.167-168].

На 2010 рік Україна підписала угоди, що закріплюють правила обігу інформації з обмеженим доступом, з Йорданським Хашимітським Королівством, Румунією, Македонією, Словенією, Угорською Республікою, Алжирською Народною Демократичною Республікою, Словацькою Республікою, Литовською Республікою. Так, першою такою угодою була Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом від 5 червня 2003 року, де інформація з обмеженим доступом визначається як інформація та матеріали незалежно від їх форми, природи та способу передачі, яким встановлені певні ступені обмеження доступу та надані відповідні грифи обмеження доступу, і які в інтересах національної безпеки та згідно з національним законодавством Сторін підлягають охороні від несанкціонованого доступу [13].

В угоді між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом закріплено інше визначення: «інформація з обмеженим доступом» – інформація у будь-якій формі та будь-які документи, матеріали, вироби, речовини або фізичні поля, на/в яких представлена інформація, яка в інтересах національної безпеки держав Сторін та відповідно до їхнього національного законодавства підлягає охороні від несанкціонованого доступу, включаючи інформацію, яку спільно створено юридичними особами держав Сторін в рамках співробітництва та доступ до якої обмежено на основі вимог національного законодавства держав Сторін та відповідно до критеріїв цієї Угоди [16].

Втім, як доречно зауважує В. Ю. Баскаков, на законодавчому рівні відсутнє уніфіковане визначення інформації з обмеженим доступом. У вітчизняному законодавстві застосовується кілька десятків термінів на позначення того чи іншого виду інформації з обмеженим доступом (секретна

інформація, таємна інформація, конфіденційна інформація, конфіденціальна інформація, нерозкрита інформація, незагальновідома інформація тощо), що ускладнює реалізацію норм права в практичній площині [26].

Що ж стосується наукового тлумачення поняття «інформація з обмеженим доступом», то серед науковців відсутній єдиний підхід. Так, Н. Мороз вважає, що інформація обмеженого доступу – це інформація, що має правовий режим, який передбачає обмеження її використання на підставі закону або договору [53, с .288]. О. О. Кулініч інформацію з обмеженим доступом визначає, як нематеріальне благо, що являє собою результат інтелектуальної діяльності людей, який існує в будь-якій об'єктивній формі у вигляді відомостей, які відомі тільки визначеному колу осіб та володіють у силу цього особливою цінністю та здатністю бути предметом майнових і особистих немайнових відносин [47, с.150]. А. І. Марущак інформацію обмеженого доступу тлумачить, як відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України і доступ до яких правомірно обмежений власником таких відомостей [50, с.45]. На думку В. Ю. Баскакова, під інформацією з обмеженим доступом слід розуміти відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено відповідно до законодавства України її власником чи добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) у зв'язку з її особливою цінністю для них на законних підставах [26]. П. В. Скок пропонує під терміном інформація з обмеженим доступом розуміти встановлений законодавством України перелік відомостей конфіденційного, секретного або таємного характеру, правовий статус яких визначений за допомогою відповідних юридичних процедур і доступ до яких обмежується певним колом осіб [69, с.168].

Обмеження доступу до інформації здійснюється в інтересах національної безпеки або охорони законних прав фізичних та юридичних осіб. Таку інформацію можна називати в деякій мірі «чутливою». Інформація

з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Обмежується доступ до інформації, а не до документу. Відповідно, якщо в одному документі міститься відкрита і закрита інформація, перша може бути надана на ознайомлення зацікавленій особі у вигляді окремого документу.

Загалом, в Україні налічується близько 20 видів інформації з обмеженим доступом (банківська, лікарська, адвокатська таємниця, таємниця сповіді).

Інформація з обмеженим доступом має самостійне правове значення і наділена властивостями, що істотно відрізняють її від інших видів інформації. Більшість дослідників окреслюють її характерні риси:

1) зміст інформації з обмеженим доступом складають знання, повідомлення, відомості про соціальну форму руху матерії і про всі інші її форми у той мірі, у якій вони використовуються суспільством, особою;

2) відомості, що складають зміст інформації з обмеженим доступом по своїй суті ідеальні (нематеріальні);

3) інформація з обмеженим доступом існує винятково в рамках взаємодії суб'єктів суспільних відносин: окремих індивідуумів, їх груп, а також таких соціальних утворень, як держава, муніципальні утворення і юридичні особи;

4) інформація з обмеженим доступом нерозривно не пов'язана з матеріальним носієм. Вона є самостійним об'єктом правового регулювання, що не залежить від конкретної форми її матеріального носія;

5) інформація з обмеженим доступом має кількісні і якісні характеристики. Співвідношення кількісних і якісних властивостей інформації має нелінійний характер (якість інформації з обмеженим доступом не залежить від її кількості);

6) інформація з обмеженим доступом не є загальнодоступною;

7) інформація з обмеженим доступом відома і використовується чітко визначеним колом осіб;

8) суб’єкт інформації вживає заходів, що спрямовані на обмеження вільного доступу третіх осіб до інформації;

9) інформація з обмеженим доступом має особливу соціальну цінність у силу її дійсної або потенційної невідомості третім особам. Поширення такої інформації може спричинити заподіяння істотної шкоди зацікавленим особам;

10) зміст інформації з обмеженим доступом відповідає обмеженням, установленим законодавством [47, с. 72-73].

Приймаючи до уваги вищевикладене, схематично поділ інформації за правовим режимом доступу включає в себе відповідно до статті 6 розділу II Закону [4] три такі категорії:

1. Конфіденційну інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Особи, які володіють конфіденційною інформацією, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. До кола конфіденційної інформації у сфері господарської (підприємницької) діяльності відноситься інформація, що визнається такою законом (ст. 862 ЦК України), комерційна таємниця (статті 505-508 ЦК) та «ноу-хау» (ст. 1 Закону України «Про інвестиційну діяльність»).

2. Таємну інформацію, доступ до якої обмежується законом відповідно до частини другої статті 6 Закону [3], в інтересах національної

безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

До кола таємної інформації відносяться, зокрема: секретна інформація, що визнається державною таємницею в установленому Законом України «Про державну таємницю» порядку; інформація, що визнається банківською таємницею (ст. 1076 ЦК , статті 60-62 Закону України «Про банки і банківську діяльність»); відомості, що становлять лікарську таємницю (ст. 40 Основ законодавства України про охорону здоров'я,) таємницю усиновлення (ст. 226 Сімейного кодексу України), адвокатську таємницю (ст. 9 Закону України «Про адвокатуру») та таємницю вчинюваних нотаріальних дій (ст. 8 Закону України «Про нотаріат»).

3. Службову інформацію:

- що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідних записках, рекомендаціях, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень,

- зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що не віднесена до державної таємниці.

Ознаками віднесення відомостей до службової таємниці можуть бути такі: обмеження на поширення інформації про діяльність органу публічного управління або підвідомчих їм юридичних осіб обумовлено законом або службовою необхідністю; інформація є конфіденційною для інших осіб, але стала відомою державним службовцям або службовцям органів місцевого самоврядування, посадовим особам інститутів громадянського суспільства в силу виконання ними своїх посадових обов'язків [35, с.7003].

В контексті цього можна зробити висновок, що службова таємниця – це правовий режим захисту конфіденційної інформації, що стала відомою посадовим особам органів публічного управління у силу виконання ними своїх обов'язків і службова інформація про діяльність органу публічного управління, за винятком тієї інформації про діяльність публічного органу, доступ до якої не може бути обмежено на підставі закону.

За умови, що публічна інформація підпадає під одну із вищезазначених категорій, тоді ця публічна інформація може бути віднесена до службової інформації після застосування трискладового тесту.

Відповідно до Закону [4] та абзацу четвертого частини першої статті 47 із змінами, внесеними згідно із Законом [2] визнано інформацією з обмеженим доступом та не підлягає відображенню у відкритому доступі зазначені у декларації відомості щодо реєстраційного номера облікової картки платника податків або серії та номера паспорта громадянина України, місця проживання, дати народження фізичних осіб, щодо яких зазначається інформація в декларації, місцезнаходження об'єктів, які наводяться в декларації (крім області, району, населеного пункту, де знаходиться об'єкт).

1.4. Порядок надання носіям інформації грифу «ДСК»

Документам, що містять службову інформацію, присвоюється гриф «Для службового користування».

Питання щодо необхідності присвоєння документу грифа «Для службового користування» вирішується виконавцем або посадовою особою, яка підписує документ, відповідно до переліку відомостей та з дотриманням вимог частини другої статті 6 та статті 9 Закону України «Про доступ до публічної інформації».

Ч.2 ст.6 передбачає, що обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) заподіяна шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

У ст.9 зазначається, що до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі [4].

До прийняття рішення про присвоєння документу грифа «Для службового користування» виконавець або посадова особа, яка підписує документ, повинні:

1) перевірити, чи належить інформація, яку містить документ, до категорій, визначених у частині першій статті 9 Закону України «Про доступ до публічної інформації»;

2) встановити, чи належить відповідна інформація до такої, доступ до якої згідно із законом не може бути обмежено, в тому числі шляхом віднесення її до службової інформації;

3) перевірити дотримання сукупності вимог, передбачених частиною другою статті 6 Закону України «Про доступ до публічної інформації» [12].

В окремих випадках питання щодо необхідності присвоєння документу грифа «Для службового користування» може бути розглянуто комісією з питань роботи із службовою інформацією за поданням посадової особи, яка підписуватиме документ.

Службовою інформацією є інформація, що міститься в: документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію; доповідних записках; рекомендаціях якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; інформація, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Якщо публічна інформація підпадає під одну із названих категорій, то ця публічна інформація може бути віднесена до службової інформації після застосування трискладового тесту, визначеного в статті 6 Закону України «Про доступ до публічної інформації».

У кожному конкретному випадку при вирішенні питання щодо віднесення публічної інформації до службової, має бути обґрунтовано:

1) якому саме з інтересів загрожує надання розголошення інформації (наприклад, інтересам національної безпеки, територіальної цілісності);

2) в чому саме буде полягати шкода в разі розголошення цієї інформації;

3) чому шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

На документах, що містять службову інформацію з:

мобілізаційних питань, додатково проставляється відмітка «Літер «М»;

питань криптографічного захисту службової інформації, - відмітка «Літер «К»;

питань спеціальної інформації, - відмітка «СІ».

Категорії документів, на яких проставляється відмітка «Літер «К», визначаються нормативно-правовими актами Адміністрації Держспецзв'язку [12].

Важливо зазначити, що «Гриф «Для службового користування» чи інші грифи, що передбачають обмеження доступу до документа або інформації в ньому, які були надані до набрання чинності Законом України «Про доступ до публічної інформації», крім грифів секретності, втрачають чинність, а відповідні документи підлягають розкриттю та наданню на запит, через один рік після набрання чинності цим Законом, якщо зазначені грифи не були переглянуті та підтверджені відповідно до Закону України «Про доступ до публічної інформації» [70, с.14].

РОЗДІЛ 2
ПРАВОВИЙ РЕЖИМ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ

2.1. Інформація, як предмет правопорушення

Станом на сьогодні, поняття «інформація» вживається у всіх без винятку галузях. Обсяг наукових знань, за оцінкою фахівців, подвоюється кожні п’ять років. Тож, можна сказати, що XXI століття буде тотально-інформаційним, паралельно перекладеним на «цифру» (total information digital world). Інформація, в нашу, як було тільки що зазначено, інформаційну епоху, це – спадок, надбання і найцінніший глобальний (стратегічний) ресурс; засіб комунікації людей та деколи об’єкт їх діяльності; продукт суспільного виробництва, результатом якого стають новітні технології.

Наприкінці XX століття змінюється розуміння феномену інформації та її соціально-політичне значення. Це пов’язано з процесом формування інформаційного суспільства, передумовою становлення та розвитку якого стала інформаційна революція. Можна стверджувати, що в умовах сучасного глобального суспільства інформація стає стратегічним соціально-політичним продуктом. Здатність суспільства та його інститутів збирати, накопичувати та використовувати інформацію, забезпечувати свободу інформаційного обміну є важливою передумовою соціального та технологічного прогресу, чинником національної безпеки, підґрунтям успішної внутрішньої та зовнішньої політики [49,с.93].

Інформація – від лат. informatio – ознайомлення, роз’яснення, уявлення, поняття. Інформація визначається як відомості про навколишній світ, що протікають у його процесах; повідомлення, що інформують про стан справ, чи чогось іншого [48,с.61].

Інформація є однією із найважливіших категорій системи суспільних відносин, що зумовлює численність дефініцій інформації. Саме через

складність і неоднозначність цього поняття, уявлення про яке має тенденцію постійно змінюватися у процесі безкінечного науково-технічного прогресу, існують численні підходи до визначення терміну «інформація» у залежності, наприклад, від рівня розуміння – побутового чи професійного, або від галузі знання.

Загальновизнана дефініція інформації відсутня у сучасній філософсько-методологічній думці, теоретичних та прикладних науках. Із правової точки зору, незважаючи на відсутність однозначного трактування змісту досліджуваної категорії, на розуміння її понятійної сутності залежно від контексту вживання і панування ідей її «невизначеності», поняття «інформація» повинно мати формалізовану, аксіоматичну форму, бути нормативно закріпленим, оскільки відсутність чіткого, регламентованого поняття може призвести до юридичних колізій під час його застосування.

Законодавець визначає інформацію через такі поняття, як «відомості» та «дані», що не є тотожними за своєю суттю, але часто використовуються як синоніми [74, с.119]. Так, Закон України «Про захист економічної конкуренції» визначає, що інформація − відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості [21].

В ЗУ «Про інформацію» зазначено, що інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [22].

На думку О.В.Харенко, така дефініція має певні недоліки. По-перше, акцентується увага на тому, що обов'язковою умовою для даних та відомостей є можливість їх закріплення на матеріальних носіях (на будь-якому матеріальному об'єкті чи середовищі, що може протягом певного

терміну зберігати, тобто нести у своїй структурі занесену у/на нього інформацію, наприклад, камені, дереві, папері, металі, пластику, магнітних матеріалах, напівпровідниках тощо) або відображення даних в електронній формі, тобто фіксація на електронному носії з використанням засобів обчислювальної техніки і можливістю передачі за допомогою електрозв'язку. Але якщо проаналізувати поняття «дані», стане зрозумілим, що дані передбачають їх автоматичну обробку електронно-обчислювальними пристроями, а тому є очевидною їх якість бути відображеними в електронній вигляді. По-друге, враховуючи, що термін закріплює під інформацією лише «відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді», може ускладнитися його правозастосування у цивільно-правових відносинах, де інформація є нематеріальним благом (глава 15 Цивільного кодексу України) і не зводиться до матеріального (фізичного) об'єкту, на якому вона зафіксована, або до відображення її в електронному вигляді [74,с.120-121].

А. Колодюк визначає інформацію, як

- дані, що характеризують ознайомлення зі станом справ, відомості про будь-що, які передаються людьми;

- дані, нерозривно зв'язані з управлінням, сигналами, що поєднують синтаксичні, семантичні та прагматичні характеристики;

- передача, відображення розмаїтості в будь-яких об'єктах і процесах [42, с.38–39].

О.В.Харенко вважає, що з точки зору права, інформація – це знакові комбінації у формі відомостей та/або даних, що є об'єктами публічного або приватного інтересу. Це визначення об'єднує у собі такі особливості:

1) закріплює, що інформація має знакову форму, що охоплює всеосяжність форм фіксації та передачі інформації у людському суспільстві;

2) підтверджує, що інформація має смисл, є цінною та корисною;

3) не має прив'язки до обов'язкової здатності бути закріпленою на матеріальному носії або відображеною в електронній формі, що сьогодні є

недоречним, адже, по-перше, не можливо і не потрібно встановлювати вичерпний перелік форм зберігання та способів передачі інформації (науково-технічний розвиток постійно відкриває нові можливості), а, по-друге, ця прив'язка є недоцільною, обмежуючою; крім того, дані вже передбачають технічний пристрій для їх запису, зберігання, передачі та обробки, а сприймання відомостей сенсорною системою людини, безумовно передбачає можливість їх фіксації на придатному носії);

4) враховує поділ на ієрархічні рівні інформації, зокрема, поняття відповідає державному рівню, має державно-правовий характер та відображає інформацію як об'єкт суспільних відносин, що потребує правового захисту [74,с.122].

К. І. Бєляков підкреслює, що визначення категорії, яка розглядається, залежить, перш за все, від конкретної галузі знань чи суспільного життя, у якій ведеться дослідження (предметна галузь суспільних відносин, організація управління соціальною системою тощо), а також характеру завдань, для яких вводиться це поняття [39,с.12].

Насправді спеціальних наукових визначень поняття «інформація» настільки чимало, і вони так багато разів змінювалися, а межі поняття то розширювалися, то звужувалися, що багато дослідників зробили висновок про те, що загального визначення інформації існувати не може. Так, Клод Шеннон, один із творців математичної «Теорії інформації», зазначив, що різні автори у загальній області інформаційної теорії надали різноманітні значення слову «інформація». Можливо, більшість із них виявиться достатньо корисною за певних обставин і заслуговуватиме визнання і наступного дослідження. Але не можна очікувати, що єдине визначення інформації може задовольнити її численні застосування у цій загальній області [80,с.180].

Аналіз вітчизняної правової доктрини свідчить, що більшість науковців дублюють недосконале законодавче визначення «інформація» через поняття

«відомості», «дані», або недоцільно застосовують поняття «знання»: зокрема під інформацією розуміють:

1) відомості, що передаються усним, письмовим або іншим способом, зокрема за допомогою умовних сигналів, технічних засобів і т.п. [38,с.24];

2) відомості (а не дані) про події та явища, які можуть бути пізнані особою та передані іншій особі у вигляді, придатному для сприйняття [59,с.9];

3) відомості про об'єктивно існуючі явища, які використовуються більш, ніж однією особою, незалежно від форми та способу надання у суспільних відносинах [62,с.7];

4) відомості, що передаються усним, письмовим або іншим способом, зокрема за допомогою умовних сигналів, технічних засобів і т.п. [67,с.24];

5) певну суму знань про той чи інший об'єкт, які можна використати в доцільній діяльності людини [61,с.172] тощо.

Проблему відсутності однозначного трактування змісту досліджуваного поняття пояснюють тим, що «сучасні визначення категорії «інформація» намагаються відобразити спочатку філософську суть, а потім – найважливіші властивості сфери суспільних відносин» [36, с.7].

2.2. Юридична відповідальність за правопорушення в сфері інформації з обмеженим доступом

Юридичну відповідальність за порушення правил використання, поширення, зберігання конфіденційних та таємних відомостей повинні нести всі винні суб'єкти, що вступають в інформаційні правовідносини. Тобто, до відповідальності можуть притягатися працівники державних органів, фізичні та юридичні особи.

Відповідно до ст.27 ЗУ «Про інформацію» [3], порушення законодавства України про інформацію тягне за собою дисциплінарну,

цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

Інститут адміністративної відповідальності в інформаційній сфері є частиною системи інформаційного правопорядку, який закладає правові підвалини для нормального функціонування та розвитку інформаційного суспільства. При цьому, інститут адміністративної відповідальності в інформаційній сфері також має своєрідну специфіку правового регулювання, що зумовлено природою інформаційних правовідносин. За допомогою цього інституту здійснюється захист не тільки адміністративно-правових відносин, а й відносин, урегульованих нормами інших галузей права, зокрема інформаційного, банківського, фінансового, медіа-права тощо.

Адміністративна відповідальність – це вид юридичної відповідальності громадян і службових осіб, за вчинення ними адміністративних правопорушень [6]. Правову основу складу правопорушень, які є підставою притягнення осіб, які вчинили правопорушення до адміністративної відповідальності, закріплено в Законі України «Про інформацію» та інших спеціальних інформаційних законах, а в Кодексі України про адміністративні правопорушення, конкретизовані склади інформаційних правопорушень та адміністративних правопорушень, також визначені санкції за їх вчинення та сформовано механізм реалізації охоронних, а також захисних норм інформаційного законодавства, щодо забезпечення інформаційної безпеки та захисту інформації [6].

Адміністративна відповідальність за інформаційні правопорушення – це застосування до винної особи, яка вчинила правопорушення, заходів впливу, передбачених санкцією порушеної норми інформаційного права в певному регламентованому порядку.

Підставою адміністративної відповідальності є вчинення правопорушення (проступку), передбаченого нормами КУпАП та іншим законами, що регулюють порядок створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації.

Перелік заходів адміністративної відповідальності, що застосовуються до особи, яка вчинила адміністративне правопорушення в інформаційній сфері, є дещо ширшим і не завжди знаходить своє закріплення в нормах КУпАП, проте, за своєю юридичною природою, такі заходи є адміністративним стягненням і не виключають можливості настання адміністративної відповідальності. Повноваження органів, які в межах своєї компетенції наділені правом застосовувати адміністративні стягнення за адміністративні правопорушення в інформаційній сфері, визначаються в нормативних приписах КУпАП та інших нормативно-правових актах, якими врегульовано порядок створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації в Україні.

Особливістю інформації з обмеженим доступом в правових відносинах є зокрема те, що певні відомості створюються, збираються, надаються, захищаються тощо суб'єктами владних повноважень або для забезпечення функціонування такого суб'єкта, або для здійснення спеціального їх захисту.

Доцільно виділити наступні ознаки інформації з обмеженим доступом як об'єкта правового регулювання:

- правовий захист здійснюється щодо «матеріалізованої» інформації з обмеженим доступом, тобто відомості мають бути закріплені на матеріальних носіях або збережені в електронному вигляді;

- обмеження доступу до інформації здійснюється відповідно до Конституції України (ст. 34), інших законодавчих актів виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя та в інших випадках, встановлених законом;

- особлива цінність такої інформації в публічній сфері проявляється у забезпеченні державного управління в різних сферах суспільного життя;

- шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні;

- у зв'язку зі своєю цінністю така інформація потребує захисту від розголошення;

- наявність юрисдикційних та неюрисдикційних засобів охорони та захисту інформації (технічних, криптографічних тощо);

- можливість доступу, використання, зберігання визначеними суб'єктами адміністративно-правових відносин лише в межах, обсягах, встановленому законодавством порядку;

- певні відомості створюються, збираються, надаються, охороняються тощо суб'єктами владних повноважень для забезпечення функціонування такого суб'єкта або для здійснення спеціального їх захисту;

- за порушення режиму доступу до інформації з обмеженим доступом винні особи підлягають заходам державного примусу – притягаються до адміністративної відповідальності [44, с.96-97].

Адміністративна відповідальність за порушення правил у сфері використання інформації з обмеженим доступом на даний час передбачена такими статтями КУпАП:

1) ст. 163-9 «Незаконне використання інсайдерської інформації»;

2) ст. 163-10 «Порушення порядку внесення змін до системи депозитарного обліку цінних паперів»;

3) ч. 3 ст. 164-3 «Недобросовісна конкуренція»;

4) ст. 166-9 «Порушення законодавства щодо запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму»;

5) ст. 172-8 «Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень»;

6) ст. 186-3 «Порушення порядку подання або використання даних державних статистичних спостережень»;

7) ст. 188-31 «Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України»;

8) ст. 188-39 «Порушення законодавства у сфері захисту персональних даних»;

9) ст. 188-40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»;

10) ст. 195-5 «Незаконне зберігання спеціальних технічних засобів негласного отримання інформації»;

11) ст. 212-2 «Порушення законодавства про державну таємницю»;

12) ст. 212-3 «Порушення права на інформацію та права на звернення»;

13) ст. 212-5 «Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію»;

14) ст. 212-6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем» [6].

Таким чином, значна кількість норм КУпАП передбачає адміністративну відповідальність за порушення норм законодавства про інформацію з обмеженим доступом, проте це стосується далеко не всіх її видів. Так, адміністративно-правовому захисту підлягають: комерційна, службова, державна, фінансова таємниці та персональні дані як вид інформації з обмеженим доступом. Проте не передбачена адміністративна відповідальність за порушення режимів лікарської та медичної таємниці, таємниці усиновлення, податкової, досудового слідства, банківської та адвокатської таємниці, нотаріальної таємниці, таємниці нарадчої кімнати тощо [30,с.127].

Основною санкцією, що застосовується до порушників режиму того чи іншого виду інформації з обмеженим доступом, є штраф. Т.О. Коломоєць визначає адміністративний штраф, як універсальний вид адміністративного стягнення, один із найпоширеніших видів юридичних штрафних санкцій, якому притаманні загальні риси штрафної (каральної) санкції й певні специфічні ознаки: множинність органів адміністративно-штрафної юрисдикції, розмаїття суб'єктів, до яких застосовується штраф, порівняно невеликі розміри, досить спрощений порядок застосування, значний виховний, превентивний (поєднання загально-превентивного та конкретно-превентивного факторів), репресивний потенціал, оперативність процедури стягнення. У сукупності матеріальні й процесуальні властивості адміністративного штрафу свідчать про його самостійний характер у системі юридичних санкцій [43, с. 11].

Особливе місце у механізмі охорони та захисту інформаційних правовідносин займає інститут кримінальної відповідальності, що відображає наслідки невиконання або неналежного виконання особою норм інформаційного законодавства і тягне невідворотність реагування держави на вчинені кримінальні правопорушення (кримінальні проступки та злочини) [71, с.118].

Кримінально-правова відповідальність за правопорушення у сфері інформаційних правовідносин – становить правову основу кримінальної відповідальності, який закріплений Кримінальним кодексом України, що ґрунтується на Конституції України [8] та на загальновизнаних принципах і нормах міжнародного права. У чинному Кримінальному кодексі України з усього обсягу об'єктів інформаційних правовідносин виділені такі, що за своєю суспільною небезпекою виходять за межі дисциплінарного чи адміністративного правопорушень. Кримінальним законом закріплено понад 20 складів злочинів, що різняться між собою за об'єктом, предметом, об'єктивною стороною та головне загрожують інформаційній безпеці

суспільства і держави, відповідальність за які несуть як спеціальні так і загальні суб'єкти.

Отже, можна сказати, що ряд об'єктів інформаційних відносин перебувають у сфері кримінально-правового захисту з боку держави, що є додатковою гарантією забезпечення інформаційної безпеки людини, суспільства і держави.

Статті Кримінального кодексу України регламентують відповідальність за скоєння певних дій, що можуть мати значення для інформаційних відносин, хоча в диспозиціях таких статей про інформаційні відносини не згадується [60, с.70].

Чинне кримінальне законодавство не містить окремого розділу, родовим об'єктом якого є група однорідних суспільних відносин у сфері обігу інформації. Водночас норми Особливої частини КК України закріплюють склади злочинів, що посягають на встановлений законом порядок створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації.

Кримінальний кодекс України встановлює відповідальність за:

- порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер - ст. 163;

- ст. 182 - порушення недоторканності приватного життя, а саме незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації;

- ст. 114, 328, 329 - державної таємниці;

- ст. 330 - передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни;

- ст. 361-2 - несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних маши-

нах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

- ст. 145, 132 - порушення лікарської таємниці;

- ст. 159 - порушення таємниці голосування;

- ст. 168 - таємниці усиновлення;

- ст. 231, 232 - порушення комерційної або банківської таємниць;

- ст. 209-1 - розголошення інформації про фінансові операції, які підлягають внутрішньому або обов'язковому фінансовому моніторингу;

- ст. 232-1. - незаконне використання інсайдерської інформації.

Основними видами санкцій, що передбачені Кримінальним кодексом України за вчинення зазначених видів злочинів, є: штраф, громадські роботи, виправні роботи, обмеження волі, позбавлення права обіймати певні посади чи займатися певною діяльністю, конфіскація програмних та технічних засобів, які є власністю винної особи [9].

Такий розподіл норм, що захищають різні види інформації, не враховує класифікацію інформації за режимом доступу до неї. Негативним наслідком цього є те, що в законодавстві передбачається більш тяжке покарання за протиправні дії з інформацією із нижчим режимом захисту та, відповідно, меншою цінністю, ніж за порушення суворішого режиму відомостей. Так, комерційна таємниця, яка, по-суті, є конфіденційною інформацією приватних осіб, захищається кримінальним законом, а відповідна конфіденційна інформація держави, що захищається режимом службової таємниці, - ні [30, с.126].

На відміну від адміністративних правопорушень, злочини в інформаційній сфері характеризуються більш високим ступенем суспільної небезпеки, призводять до завдання реальної або потенційної істотної шкоди інтересам особи, держави, суспільства і передбачають можливість призначення покарання у вигляді позбавлення волі [34,с.101].

Цивільно-правова відповідальність за правопорушення у сфері інформаційних правовідносин – має обумовлений комплексний характер

інформаційного права, окремі норми якого закріплюються в цивільному законодавстві. Цивільно-правова відповідальність наступає у випадках, якщо була заподіяна шкода фізичним та юридичним особам внаслідок недотримання відповідних норм у сфері інформаційного права. Об'єктом цивільної відповідальності за правопорушення у сфері інформаційних правовідносин є майнові та особисті немайнові права фізичної або юридичної особи, які охороняються інформаційним та цивільним законодавством [60, с.69].

До ознак інформації з обмеженим доступом як об'єкта цивільно-правових відносин відносять наступне:

- зміст інформації з обмеженим доступом складають знання, повідомлення, відомості про соціальну форму руху матерії і про всі інші її форми у тій мірі, у якій вони використовуються суспільством, державою;

- інформація з обмеженим доступом є самостійним об'єктом правового регулювання, що не залежить від конкретної форми її матеріального носія;

- відомості, що складають зміст інформації з обмеженим доступом, за своєю сутністю ідеальні (нематеріальні);

- інформація з обмеженим доступом не є загальнодоступною;

- інформація з обмеженим доступом відома і використовується чітко визначеним колом осіб;

- суб'єкт інформації вживає заходів, що спрямовані на обмеження вільного доступу третіх осіб до інформації;

- інформація з обмеженим доступом має особливу соціальну цінність у силу її дійсної або потенційної невідомості третім особам, її поширення може спричинити істотну шкоду зацікавленим особам;

- зміст інформації з обмеженим доступом відповідає обмеженням, установленим законодавством [46, с. 16–17].

Реалізація цивільно-правової відповідальності – це передусім виконання обов'язку з відновлення порушеного права (становища) особи або компенсації нанесених правопорушенням шкоди, реальних збитків, упущеної

вигоди тощо, що забезпечується передбаченими нормами цивільного права заходами державного примусу (їх можливістю або безпосередньою реалізацією) [71, с.38].

У сфері інформаційних відносин цивільно-правова відповідальність може виникати із порушенням цивільних прав і зобов'язань, які мають безпосередню інформаційну залежність або об'єктом яких є інформація. Такі права й обов'язки, виходячи з їхньої інформаційної природи, сьогодні вже прийнято називати інформаційними правами й обов'язками. Слід звернути увагу на те, що «цивільне інформаційне право» та «цивільний інформаційний обов'язок» вітчизняним законодавством не визначаються, проте в основному акті цивільного законодавства України – Цивільному кодексі України [20]– міститься низка положень, які фактично їх закріплюють, а для захисту цивільних інформаційних прав ще й встановлюються особливі засоби. При цьому цивільні права та відповідні їм обов'язки, зокрема в інформаційній сфері, не вичерпуються їхнім переліком, визначеним законодавством.

Диспозитивність цивільних правовідносин зумовлює здатність особи (як фізичної, так і юридичної) мати цивільні права, які не встановлені Конституцією України та іншими актами законодавства, якщо вони не суперечать закону та моральним засадам суспільства (ст. 26, 91 ЦК України). Захисту на законних підставах підлягають всі цивільні права й інтереси особи (ст. 15, 16 ЦК України). Крім того, будь-яке суб'єктивне право однієї особи породжує відповідний обов'язок іншої особи (осіб), і навпаки. Тому взаємопов'язані цивільні права й обов'язки не завжди мають буквальне закріплення в одному акті цивільного законодавства. Зокрема, обов'язок продавця надавати покупцеві необхідну і достовірну інформацію про товар встановлено ст. 700 Цивільного кодексу України, що автоматично означає і право покупця на отримання цієї інформації, хоча воно безпосередньо цим законом не визначається. Проте для споживача (фізичної особи) право на інформацію про продукцію визначено і деталізовано в ст. 4 Закону України «Про захист прав споживачів».

Необхідно також враховувати, що природні риси інформаційних цивільних прав та обов'язків, а отже, і механізми їх охорони й захисту, зокрема цивільно-правова відповідальність, визначаються правовими властивостями інформації як об'єкта цивільних правовідносин, основними з яких є:

− нематеріальність (ціннісна самостійність інформації щодо носія); суб'єктивний характер (зумовленість інформації інтелектуальною діяльністю людини);

− неспоживність (можливість багаторазового використання);

– невід'ємність від суб'єкта (інформацію не можливо вилучити в суб'єкта, який її створив, передав, отримав тощо);

– здатність до безутратного відтворення, копіювання, збереження;

– необхідність об'єктивації для включення в правовий обіг (у формі відомостей про навколишній світ, зокрема про явища, події, процеси) [71, с.50-51].

Цивільний кодекс України відносить інформацію до нематеріальних об'єктів цивільних прав, що надає передусім немайнового характеру безпосередньому протиправному впливу інформаційного правопорушення. Навіть коли йдеться про майнову шкоду, спричинену таким правопорушенням, вона завдається саме через нематеріальну інформаційну сферу. Цивільні інформаційні обов'язки як в межах договірних, так і недоговірних відносин, як правило, пов'язані з необхідністю надання, повідомлення, закріплення певної інформації, невиконання чого може завдати особі шкоди та зумовити цивільно-правову відповідальність [71, с.51].

За порушення майнових прав інтелектуальної власності на комерційну таємницю чи прав на «ноу-хау», зокрема, шляхом добування протиправним способом чужої комерційної інформації, розголошення її без згоди особи, уповноваженої на те, чи схилення до її розголошення або використання чужої комерційної інформації без згоди уповноваженої особи, власник цієї

інформації має право на відшкодування завданих майнової та моральної шкоди відповідно до правил статей 1166 та 1167 ЦК. Така цивільна відповідальність може наставати і в разі вчинення дій, зазначених у главі 4 Закону України «Про захист від недобросовісної конкуренції».

РОЗДІЛ 3
ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНИХ УМОВАХ, ЩО СКЛАЛИСЯ В УКРАЇНІ

3.1. Сфери, що потребують забезпечення захисту від розголошення інформації з обмеженим доступом

Важливим показником стану захищеності інтересів особи, суспільства і держави є ступень забезпечення захисту інформації, доступ до якої обмежено з метою захисту прав і законних інтересів суб'єктів права на таємницю.

Інформація з обмеженим доступом, що цікавить розвідувальні органи іноземних держав, як правило, зосереджується:

- у політичній сфері: державні органи, органи управління зовнішньополітичною діяльністю, органи розвідки, органи з адміністративно-політичними функціями, суспільно-політичні організації, насамперед, що здійснюють міжнародні зв'язки, міжурядові політичні організації;

- в економічної сфері: державні органи, які здійснюють планування і керівництво економікою й окремими її галузями, державні установи, що планують і здійснюють зовнішні економічні зв'язки, міжурядові організації країн Співдружності незалежних держав у сфері економічних відносин, важливі підприємства промисловості, транспорту і зв'язку, наукові установи, які ведуть дослідження в галузі економіки;

- у військовій сфері: центральні управління Міністерства оборони України, Генеральний штаб, штаби видів Збройних сил, стратегічних угруповань військ, об'єднань, з'єднань, частин, військові частини оснащені новими видами зброї і бойової техніки, арсенали і склади зберігання цих видів зброї і техніки, установи, що займаються науково-дослідними і дослідно-конструкторськими роботами в галузі озброєння і військової техніки, іспитові полігони, засоби закритого оперативного зв'язку МО

України, підрозділи, що займаються стратегічними військовими перевезеннями;

- у науково-технічній сфері: державні органи планування і координації наукових робіт, Академія наук України, науково-дослідні інститути, що ведуть роботу на важливих напрямах розвитку науки і техніки.

Розвідувальні спрямування кожної зацікавленої іноземної держави щодо України націлені на наступні життєво важливі об'єкти національної безпеки, до яких відносяться:

- об'єкти політичної розвідки і діяльності іноземних держав щодо політичної стабільності і зовнішніх зв'язків України:

а) загальні об'єкти:

- політична система;
- політичний потенціал;
- плани щодо реалізації політичної стратегії;

б) спеціальні об'єкти:

- міжнародні позиції України;
- політичні відносини з іншими державами;
- зовнішні зв'язки з міжнародними організаціями, рухами тощо;
- національні та міжнародні відносини;
- процес розвитку демократії та становлення державності;
- політично-адміністративна діяльність України;
- формування загальнодержавної ідеології розвитку суспільства;
- антигромадські прояви у суспільстві;

в) об'єкти розвідувального проникнення:

- центральні органи державної влади і управління;
- органи управління зовнішньою діяльністю;
- органи зовнішньої розвідки;
- органи, що здійснюють адміністративно-державні функції всередині держави;

- політичні партії, громадсько-політичні, релігійні та культурологічні організації, що беруть участь в міжнародних зв'язках;

- міжнародні політичні організації, до складу яких входить Україна;

- об'єкти військової розвідки і діяльності іноземної держави щодо військової могутності та зовнішніх воєнно-політичних зв'язків України:

а) загальні об'єкти:

- воєнний потенціал;

- зовнішні воєнно-політичні відносини і воєннostратегічні позиції;

- воєнно-стратегічні плани вищого військового командування;

б) спеціальні об'єкти:

- боєготовність і боєздатність Збройних сил України;

- воєнно-мобілізаційні плани військового командування;

- озброєння, бойова техніка та заходи держави по їх розвитку;

- плани військового будівництва;

- українська військова наука та військове мистецтво;

- дислокація воєнних об'єктів;

- ймовірні театри воєнних дій та їх воєнно-інженерна підготовленість;

- плани ведення бойових дій у відповідних умовах та окремих регіонах;

- військове співробітництво з іноземними військовими, в тому числі і міжнародними організаціями, та перспективи їх розвитку;

- військова допомога іноземним державам, організаціям та рухам;

- військово-політичні зв'язки України з іноземними державами;

- воєнно-політичні заходи, які готуються на випадок актів агресії проти України, а також на випадок виникнення кризової ситуації в різних регіонах світу, де є життєво важливі інтереси України;

в) об'єкти розвідувального проникнення:

- Центральне управління Міністерства оборони;

- Генеральний штаб;

- штаби видів Збройних Сил;

- стратегічні угруповання військ;

- об'єднання, з'єднання частин;

- об'єднані міждержавні воєнні організації, структури, військові частини, які споряджені новими видами зброї та бойової техніки, арсенали і склади зберігання цих видів зброї та техніки;

- заклади, які займаються науково-дослідницькою діяльністю і випробувально-конструкторськими роботами у галузях озброєння і військової техніки;

- випробувальні полігони;

- засоби закритого оперативного зв'язку Міністерства оборони;

- заклади, які займаються військовими перевезеннями;

- оточення важливих військових об'єктів;

- об'єкти економічної розвідки і діяльності іноземних держав щодо економічної могутності зовнішньоекономічних зв'язків України:

а) загальні об'єкти:

- економічна система;

- економічний потенціал;

- кредитно-фінансова система;

- зовнішньоекономічні зв'язки;

- плани державних і владних структур щодо реалізації економічної стратегії України;

б) спеціальні об'єкти:

- конкретні галузі економіки;

- природні ресурси, стратегічні промислові ресурси (сировини та сільгосппродуктів, енергетичні та інші державні запаси для потреб оборони);

- народно-господарські плани, торгово-економічна і кредитно-фінансова система;

- потреби України у розвитку економічних зв'язків;

- плани держави щодо розвитку зовнішніх економічних зв'язків різного рівня, включаючи плани підготовки до укладання конкретних торгово-економічних угод;

- процеси економічної інтеграції і міжнародного розподілу праці в економічних міжнародних структурах, до яких входить Україна;

- торговельно-економічні відносини з іноземними державами;

в) об'єкти розвідувального проникнення:

- державні органи, що здійснюють планування і управління економікою та окремими її галузями;

- державні органи та інші організації, що задіяні у сфері зовнішньоекономічної та кредитно-фінансової діяльності;

- міжурядові організації в сфері економічних відносин;

- важливі підприємства промисловості, сільського господарства, транспорту та зв'язку, сховища матеріальних цінностей;

- наукові заклади, які проводять дослідження в галузі економіки;

- об'єкти науково-технічної розвідки і діяльності іноземних держав щодо підриву науково-технічного потенціалу, зовнішніх науково-технічних зв'язків України:

а) загальні об'єкти:

- науково-технічний потенціал України;

- зовнішні наукові зв'язки та державні плани розвитку науки і техніки;

б) спеціальні об'єкти:

- науково-технічний процес в Україні;

- напрями розвитку науки і техніки в Україні, які мають важливе народногосподарське і оборонне значення;

- система управління науковими дослідженнями в Україні;

- наукові винаходи, які мають важливе народно-господарське і оборонне значення, наукові ідеї і фундаментальні дослідження, які ініціюють винаходи, що здатні викликати стрімке зростання сукупного потенціалу держави і зміцнити її авторитет та позиції на світовій арені;

- важливі для розвитку науки випробувальні зразки обладнання;

- провідні українські вчені, які працюють на важливих напрямах розвитку науки;

- наукові зв'язки України з іноземними державами;

- потреби України у розвитку таких зв'язків;

в) об'єкти розвідувального проникнення:

- державні органи управління науковими роботами;

- Національна академія наук;

- науково-дослідні інститути, полігони галузевого профілю [52, с.142-144].

3.2. Комплекс дій по попередженню та захисту від розголошення інформації з обмеженим доступом

Захист інформації з обмеженим доступом – це комплекс дій власника інформації для збереження прав на її володіння й розповсюдження, а також сприяння життєдіяльності людини, суспільства та держави на основі створення органами управління безпечних умов, що обмежують розповсюдження й виключають або істотно ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв [54, с.114].

Адміністративно-правові заходи захисту інформації з обмеженим доступом можна визначити як сукупність методів, засобів і прийомів, спрямованих на захист інформаційної безпеки людини, суспільства й держави в усіх сферах життєво важливих інтересів. Сукупність їх полягає у виявленні, вилученні та нейтралізації негативних джерел, причин та умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації, а цілі й методи адміністративно-правового захисту інформації з обмеженим доступом здійснюються з огляду на її зміст. Тому зміст адміністративно-правового захисту інформації з обмеженим доступом ототожнюється з процесом забезпечення інформаційної безпеки як необхідності нормального функціонування держави, суспільства, окремої людини. А. Антонюк відносить до сфери безпеки інформації не захист інформації, а захист права власності на неї [25, с. 103].

Справді, захист інформації організовує та здійснює власник, користувач інформації або уповноважена ними особа (фізична чи юридична), а також держава в особі компетентних органів у межах своєї правоохоронної функції. Захистом інформації власник охороняє свої права на володіння й розповсюдження інформації, намагається запобігти незаконному заволодінню нею та використанню її на шкоду власним інтересам.

Система захисту може бути різною, на розсуд власника, а може й не мати такого захисту взагалі. Він здійснюється на основі диспозитивних методів, що входять у сферу цивільно-правого розгляду. Захист інформації стає предметом адміністративно-правового регулювання у випадках, коли обмеження доступу до інформації прямо передбачаються законами, коли ці обмеження пов'язуються із забезпеченням інформаційних прав і свобод людини, інформаційних аспектів національної, державної, громадської безпеки тощо, а суб'єктом застосування цих обмежень, що дуже важливо, є держава в особі її компетентних органів [51, с. 103].

Форми адміністративно-правового захисту інформації з обмеженим доступом традиційно можна класифікувати на юрисдикційні та неюрисдикційні. До перших належить захист порушених прав суб'єктів інформаційних правовідносин у судовому й адміністративному порядку, до других – технічні засоби захисту інформації з обмеженим доступом. Механізм захисту інформації з обмеженим доступом є повним поєднанням технічних і юрисдикційних засобів захисту інформації. Усі вони є правовими, оскільки встановлюються правовими актами управління, у тому числі нормативно-правовими.

Адміністративно-правове забезпечення інформації з обмеженим доступом – це діяльність щодо застосування юрисдикційних і неюрисдикційних форм її захисту.

Діяльність щодо технічного захисту інформації з обмеженим доступом повинна відповідати таким вимогам:

– наявності спеціальної освіти в осіб, які її здійснюють, або наявності в них спеціальної підготовки;

– відповідності виробничих приміщень, виробничого, випробувального й контрольно-вимірювального устаткування технічним нормам і вимогам, встановленим державними стандартами й нормативно-методичними документами щодо технічного захисту інформації з обмеженим доступом;

– використанню сертифікованих автоматизованих інформаційних систем і засобів їх захисту – використанню третіми особами програм для комп'ютерів чи баз даних на підставі договору з їх правовласником [54, с.114].

Юрисдикційні форми реалізації адміністративно-правових заходів захисту інформації з обмеженим доступом у суб'єктів господарювання реалізовуються з метою відновлення порушених прав суб'єктів інформаційних правовідносин. До цих заходів відносимо насамперед такі:

а) віднесення відомостей до інформації з обмеженим доступом;

б) документування інформації з обмеженим доступом, що є основою для реєстрації інформаційних ресурсів;

в) правовий захист інформації з обмеженим доступом, що виражається в існуванні інституту адміністративно-правової відповідальності за порушення законодавства про службову інформацію, який є однією з гарантій належної її реалізації та правового захисту [54, с.115].

Забезпечення захисту інформації з обмеженим доступом здійснюється як технічними, так і правовими заходами, що зосереджені в нормативних приписах чинного вітчизняного законодавства.

Зокрема, відповідно до ст.517 КПК України охорона державної таємниці під час кримінального провадження забезпечується дотриманням режиму секретності, що включає такі специфічні заходи, як: обмеження кола учасників особами, які мають допуск до державної таємниці та доступ до конкретної секретної інформації, заборона робити виписки та копії з

матеріалів, які містять державну таємницю тощо. Водночас положення ч. 7 ст. 517 КПК України чітко визначають, що здійснення кримінального провадження, яке містить державну таємницю, не є підставою для обмеження прав його учасників, крім випадків, передбачених законом та обумовлених необхідністю забезпечення охорони державної таємниці.

Законодавче врегулювання нового виду кримінального провадження, яке містить державну таємницю, безумовно, є важливим кроком у напрямі правового забезпечення охорони інформації з обмеженим доступом. Вбачається, що аналогічний підхід повинен бути збережений і при вирішенні питання забезпечення охорони інших видів інформації, доступ до якої обмежується з метою захисту прав і законних інтересів суб'єктів права на таємницю. У зв'язку із цим пропонується внести зміни до ч. 2 ст. *27* КПК України, нормами якої визначено підстави проведення закритого засідання. Зокрема, прийняття рішення про здійснення кримінального провадження у закритому судовому засіданні у випадках, передбачених пп. 3-5 ч.

Ст. 27 КПК України, повинно визначатися обов'язком, а не правом судді (слідчого судді), за умови надходження відповідного обґрунтованого клопотання від власника або володільця відповідної інформації. Запровадження такого порядку стане додатковим свідченням визнання пріоритету прав і законних інтересів особи у сфері кримінального судочинства і створить законодавче підґрунтя для подальшого вдосконалення забезпечення охорони інформації з обмеженим доступом [72, с.225].

Правовий захист в режимі комерційної таємниці має цілу низку переваг порівняно з іншими формами охорони. Це відсутність вимог про обов'язкову реєстрацію в Патентному відомстві, необмеженість строку охорони, оперативність отримання статусу охороняємого результату інтелектуальної діяльності, універсальність об'єктів охорони, відсутність необхідності сплати мита та оприлюднення сутності результату, що охороняється. Безумовно, що ці особливості роблять комерційну таємницю (ноу-хау) досить привабливим

засобом правової охорони результатів інтелектуальної діяльності на підприємствах усіх форм власності. Проте в роботі з секретом виробництва існують і складності, обумовлені невизначеністю механізму постановки ноу-хау на бухгалтерський баланс і додатковими витратами, які супроводжують цей етап роботи з ним. З одного боку, відповідно до п. 4 Положення по бухгалтерському обліку «Облік нематеріальних активів» (ПБУ 14/2007). До нематеріальних активів належать, наприклад, твори науки, літератури і мистецтва; програми для електронних обчислювальних машин, винаходи; корисні моделі, секрети виробництва (ноу-хау); товарні знаки і знаки обслуговування» Це означає, що теоретично секрети виробництва на баланс ставити можна [75].

Комплексний характер заходів щодо захисту інформації з обмеженим доступом обумовлює необхідність активної участі в цьому процесі багатьох державних органів. Так, зокрема, у забезпеченні охорони державної таємниці беруть участь органи законодавчої, виконавчої та судової влади, а Службу безпеки України Законом України "Про державну таємницю" визначено спеціально уповноваженим органом державної влади у сфері охорони державної таємниці. Всі суб'єкти забезпечення охорони державної таємниці діють виключно в межах повноважень, визначених Конституцією України, її законами та іншими нормативно-правовими актами [52, с.144].

Так, відомості, які становлять державну таємницю України, іноземної держави чи міжнародної організації, охороняються Законом України «Про державну таємницю», у якому зазначено, що секретна інформація до скасування рішення про віднесення її до державної таємниці та матеріальні носії такої інформації до їх розсекречування можуть бути передані іноземній державі чи міжнародній організації лише на підставі міжнародних договорів, згода на які надана Верховною Радою України, або письмового вмотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України. У разі, якщо

міжнародним договором, згода на укладення якого надана Верховною Радою України, установлено інші, ніж передбачені цим законом, правила охорони таємниці іноземної держави чи міжнародної організації, застосовуються правила міжнародного договору.

Практичні аспекти зазначених положень деталізовано в Указі Президента України від 14 грудня 2004 року № 1483/2004 «Про деякі питання передачі державної таємниці іноземній державі чи міжнародній організації», який був ухвалений з метою вдосконалення процедур із вирішення питань щодо передачі державної таємниці іноземним державам і міжнародним організаціям за умови забезпечення при цьому додержання інтересів національної безпеки України, національного законодавства про державну таємницю. Цей Указ містить положення щодо визначення порядку підготовки документів з метою передачі державної таємниці іноземній державі чи міжнародній організації та підготовки проектів міжнародних договорів про взаємну охорону секретної інформації. Цей порядок можна представити як певну взаємоузгоджену послідовність дій зацікавлених суб'єктів щодо передачі державної таємниці іноземній державі чи міжнародній організації. Зміни до цього указу були затверджені Указом Президента № 828/2014 від 27 жовтня 2014 року.

Якщо секретна інформація передається іноземній стороні винятково на підставі розпорядження Президента України без наявності двосторонньої угоди про взаємний захист секретної інформації, Служба безпеки України та відповідний орган іноземної сторони мають погодити усі аспекти здійснення такої передачі. Зокрема, для одержання дозволу на передачу секретної інформації іноземній стороні державний орган, орган місцевого самоврядування вносить Службі безпеки України пропозиції щодо доцільності такої передачі; підприємства, установи й організації державного сектора економіки подають пропозиції щодо передачі секретної інформації іноземній стороні до органу виконавчої влади, в управлінні якого вони перебувають; інші підприємства, установи й організації подають такі

пропозиції до замовників робіт, пов'язаних з відповідною державною таємницею.

Зазначені органи виконавчої влади та замовники робіт, пов'язаних із державною таємницею, здійснюють розгляд одержаних запитів, за результатами якого вносять Службі безпеки України пропозиції стосовно доцільності передачі секретної інформації іноземній стороні, яка порушує перед Радою національної безпеки і оборони клопотання щодо подання Президенту України пропозиції стосовно видання розпорядження про передачу секретної інформації іноземній державі чи міжнародній організації.

Рада національної безпеки й оборони України, визначаючи відповідність передачі секретної інформації інтересам забезпечення національної безпеки України, законодавству України, міжнародним договорам, за результатами розгляду поданих Службою безпеки України матеріалів вносить на розгляд Президенту пропозиції щодо видання розпорядження про передачу секретної інформації іноземній стороні.

На виконання розпорядження Президента Служба безпеки України видає державному органу, органу місцевого самоврядування, підприємству, установі дозвіл на передачу секретної інформації та погоджує проект виконавчого договору. Якщо ж за результатами розгляду пропозицій про передачу секретної інформації іноземній стороні цю передачу визнано такою, що не відповідає інтересам національної безпеки чи українському законодавству, Служба безпеки України повідомляє замовника робіт, пов'язаних із відповідною державною таємницею, від якого надійшла така пропозиція, про відмову в наданні дозволу та погодженні проекту виконавчого договору.

Якщо ж секретна інформація передається іноземній державі чи міжнародній організації на підставі міжнародного договору України, згоду на обов'язковість якого надано Верховною Радою України, її передача здійснюється згідно з процедурою, описаною відповідним міжнародним договором. У такому разі дозвіл на передачу секретної інформації має

оформляти Служба безпеки України за умови надання іноземною стороною зобов'язань або письмових гарантій щодо забезпечення охорони секретної інформації, зокрема недопущення її надання третій стороні [31, с.34-35].

Згідно зі статтею 8 угоди між Україною та Європейським Союзом сторони надають взаємну допомогу з питань безпеки інформації з обмеженим доступом, а також із питань, що становлять спільний інтерес у галузі безпеки. Органи відповідно до їхніх обов'язків мають проводити взаємні консультації та перевірки з питань безпеки для оцінки ефективності домовленостей про безпеку [17].

З метою досягнення цілей, зазначених у цій угоді, стосовно України уся кореспонденція надсилається начальнику центральної канцелярії документів ЄС Міністерства закордонних справ України, а щодо Європейського Союзу уся кореспонденція надсилається Раді, а потім начальник Канцелярії Ради пересилає її державам-членам і Європейській комісії. У виняткових випадках кореспонденція від однієї сторони, до якої мають доступ лише окремі компетентні посадові особи, органи або служби цієї сторони, може надсилатися лише до окремих компетентних посадових осіб, органів або служб іншої сторони, конкретно визначених як одержувачі, які матимуть до неї доступ з урахуванням їхньої компетенції та відповідно до принципу потреби в доступі за умовами службової діяльності. Про це на кореспонденції робляться відповідні позначки. Ця кореспонденція передається через начальника Канцелярії Ради Європейського Союзу та начальника Центральної канцелярії документів ЄС Міністерства закордонних справ України [1].

У статті 12 зазначеної угоди вказано, що уповноважені органи установлюють процедури, які виконуватимуться в разі доведеного або підозрюваного розголошення інформації з обмеженим доступом. Перед наданням інформації з обмеженим доступом відповідальні органи безпеки мають домовитися щодо способів охорони інформації. Усі інші угоди у сфері охорони секретної інформації, що укладаються обома сторонами, не повинні

суперечити положенням цієї угоди. Усі спірні питання між Україною та Європейським Союзом, що виникають стосовно тлумачення або застосування цієї угоди, мають вирішуватися шляхом проведення переговорів між ними [17].

На сьогодні правила обігу інформації з обмеженим доступом між Україною та державами Східної Європи регулюються угодами, укладеними з Литовською Республікою (2003) [13], Словацькою Республікою (2008) [16], Угорщиною (2008) [18], Румунією (2013) [15], Республікою Молдовою [14]. Першим таким договором була Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом від 5 червня 2003 р., у якій указано, що інформація з обмеженим доступом в інтересах національної безпеки та згідно з національним законодавством сторін підлягає охороні від несанкціонованого доступу. Зазначено, що угода укладена з метою зміцнення політичного, військового, економічного, юридичного, наукового та технологічного співробітництва між сторонами. Наголошується, що сторони підписали угоду, усвідомлюючи, що кінцеве співробітництво потребує обміну інформацією з обмеженим доступом між сторонами, а також керуючись прагненням забезпечити охорону всієї інформації з обмеженим доступом.

В Угоді між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом визначено, що охороняється інформація, яка в інтересах національної безпеки держав сторін та відповідно до їхнього національного законодавства підлягає охороні від несанкціонованого доступу, зокрема інформація, що спільно створена юридичними особами держав-сторін у процесі співробітництва та до- ступ до якої обмежено на основі вимог національного законодавства держав-сторін та відповідно до критеріїв укладеної угоди.

В Угоді між Кабінетом Міністрів України та Урядом Республіки Молдова про взаємний захист секретної інформації зазначено, що сторони забезпечують взаємний захист переданих та (або) створених у процесі

співробітництва відомостей у сфері оборони, економіки, науки та техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди безпеці та інтересам України та (або) Республіки Молдови і які відповідно до законодавства держав сторін віднесені до державної таємниці.

Загалом у проаналізованих документах визначено загальні принципи, правила та механізми обміну (передачі) секретною інформацією, зокрема зазначено, що одна сторона забезпечує конфіденційність відомостей, переданих іншою, якщо вони згідно з законодавством цієї сторони мають таємний (секретний) характер або розголошення їх змісту є небажаним. Ступінь таємності відомостей визначається стороною, яка їх передає.

Угоди про взаємну охорону інформації містять положення про те, що сторони згідно з їхнім національним законодавством уживають усіх необхідних заходів щодо охорони секретної інформації, яка передається чи створюється, або забезпечують таку ж охорону, яка передбачена в процесі обігу власної секретної інформації з відповідним ступенем секретності, а саме:

– порядок взаємної охорони секретної інформації (відповідно до національного законодавства сторін, актів міжнародних організацій, узгоджених правил);

– зобов'язання сторін щодо забезпечення охорони одержаної секретної інформації, насамперед недопущення доступу до неї третьої сторони, а також використання секретної інформації з метою, що не відповідає цілям передачі;

– порядок надання доступу до секретної інформації представникам сторін;

– зобов'язання щодо засекречування, зміни ступеня секретності, розсекречування секретної інформації (матеріальних носіїв такої інформації);

– порядок передачі секретної інформації;

– зобов'язання щодо взаємного інформування у випадку порушення вимог стосовно охорони секретної інформації та вжиття заходів щодо притягнення до відповідальності винних у цьому осіб;

– терміни, протягом яких сторони зобов'язуються забезпечувати взаємну охорону секретної інформації;

– вимоги до виконавчих договорів, що укладаються між уповноваженими суб'єктами сторін, щодо передачі секретної інформації (матеріальних носіїв такої інформації);

– порядок вирішення спірних питань;

– визначення органів сторін, на які покладається здійснення співробітництва за договором.

Не впливає на зобов'язання сторін, узяті за іншими міжнародними договорами, і вона не буде використовуватися проти інтересів, безпеки та територіальної цілісності інших держав та міжнародних організацій. У статті 1, як правило, містяться поняття, які використовуються в угоді, зокрема «інформація з обмеженим доступом», «секретна інформація», «ступінь обмеження доступу», «гриф обмеження доступу», «компетентний орган безпеки», «уповноважений орган», «сторона-джерело», «сторона-одержувач», «допуск до секретної інформації», «носії секретної інформації».

Далі зазначаються компетентні органи безпеки (чи національні органи безпеки) в обох державах, подекуди вказано їхні юридичні адреси. В Україні цим компетентним органом є Служба безпеки України. В угоді з Угорщиною стаття 5 присвячена опису діяльності компетентних органів у процесі охорони секретної інформації, зокрема передбачено консультування з окремих питань, інформування про будь-які зміни як у контактних даних, так і в питаннях роботи з інформацією, сприяння в проведенні спільних перевірок, мета яких – переконатися, що передана інформація з обмеженим доступом охороняється відповідним чином стороною-одержувачем. Як правило, окрема стаття відводиться для узгодження грифів обмеження доступу до інформації: окрім національних варіантів, пропонується також

еквівалент англійською мовою для уникнення непорозумінь під час тлумачення. У деяких угодах ця інформація є більш деталізованою, наприклад в угоді з Литовською Республікою розписано особливості захисту кожною стороною секретної інформації іншої за грифами доступу.

А в угоді з Угорщиною в статті 4 «Принципи охорони інформації з обмеженим доступом» зазначено особливості охорони інформації з обмеженим доступом відповідно до грифів секретності. У наступній статті визначено основні заходи з охорони секретної інформації, яка передається, отримується, створюється або розробляється в процесі співробітництва.

В угодах зазначено, що сторони не надають доступ до інформації з обмеженим доступом третій стороні без попередньої письмової згоди сторони-джерела. Інформація з обмеженим доступом використовується лише для цілей, для яких її передано. Зазначається, що одержана інформація може використовуватися стороною-отримувачем лише з тією метою, для якої вона була надана. В угоді з Литовською Республікою зафіксовано, що кожний національний орган безпеки чи компетентний орган веде список допусків осіб, що працюють у цьому органі, які уповноважені володіти доступом до такої інформації.

В угоді з Румунією визначено механізми знищення інформації у випадку необхідності: сторона-одержувач інформує сторону-джерело про знищення інформації з обмеженим доступом. У випадку невідворотної загрози інформація з обмеженим доступом знищується без попереднього дозволу, а компетентний орган безпеки сторони джерела негайно інформується про це. В угоді з Угорщиною вказано, що інформація з обмеженим доступом має знищуватися так, щоб неможливо було її відновити в цілому або частково.

Зазначено, що інформація з грифом, еквівалентним “Top Secret”, не знищується, а повертається стороні-джерелу, коли більше нема потреби в її використанні або коли закінчився термін її дії. Якщо інші процедури не погоджені компетентними органами безпеки, сторона-одержувач може

знищити інформацію з грифами, еквівалентними “Secret”, “Confidential” чи “Restricted”, після закінчення терміну обмеження доступу. Про це необхідно повідомити компетентний орган безпеки сторони-джерела. В угодах визначено також правила доступу до інформації. Зокрема, в угоді зі Словацькою Республікою зазначено, що лише сторона-джерело має повноваження змінювати ступінь обмеження доступу або скасовувати таке обмеження стосовно переданої інформації з обмеженим доступом . Така зміна або скасування обмежень щодо доступу до спільно створеної інформації з обмеженим доступом здійснюється на основі взаємної згоди держав-сторін. В угоді з Румунією вказано, що допуск надається за результатами перевірки відповідно до законодавства кожної сторони.

За запитом компетентні органи безпеки держав-сторін, беручи до уваги відповідне національне законодавство, сприяють один одному в проведенні процедур перевірки стосовно надання допуску та дозволу на проведення діяльності, пов’язаної з інформацією з обмеженим доступом. Окремо в угодах регламентуються візити сторін, що пов’язані з доступом до інформації.

У більшості угод просто вказано, що інформація з обмеженим доступом передається між договірними сторонами погодженими та захищеними інформаційними, комунікаційними, дипломатичними каналами або іншими шляхами, узгодженими компетентними органами безпеки. Проте в окремих випадках ці положення більш конкретизовані. Так, зокрема, в Угоді між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом вказано, що в особливих випадках національні органи безпеки (компетентні органи) можуть погодити передачу інформації з обмеженим доступом іншими каналами. У такому випадку мають виконуватись вимоги, зафіксовані в угоді: супроводжуюча особа повинна мати допуск обмеження доступу відповідного рівня; сторона-джерело зберігає список інформації з обмеженим доступом, яка передається, а копія цього переліку надається стороні-

одержувачу; інформація з обмеженим доступом упаковується і запечатується відповідно до національного законодавства сторони-джерела; отримання стороною-одержувачем інформації з обмеженим доступом підтверджується письмово. Якщо ж передбачається передача великої кількості інформації з обмеженим доступом, національні органи безпеки (компетентні органи) обох сторін взаємно погоджують і схвалюють засоби транспортування, маршрут та заходи безпеки для кожного такого випадку окремо. Зазначено, що електронна передача інформації з обмеженим доступом має здійснюватися лише у шифрованій формі (з використанням криптографічних засобів і пристроїв закриття інформації).

Зокрема, у статті 9 угоди з Румунією так описано особливості передачі інформації з обмеженим доступом: інформація з обмеженим доступом передається дипломатичними чи військовими кур'єрами або іншими засобами, узгодженими компетентними органами безпеки. Сторона-одержувач має письмово повідомити сторону-джерело про отримання інформації з обмеженим доступом. У випадку відправлення інформації великого обсягу компетентні органи безпеки можуть взаємно узгодити та затвердити засоби передачі, а також заходи безпеки для кожного такого випадку окремо. Водночас зазначено, що обмін інформацією з обмеженим доступом з використанням електронних засобів здійснюється відповідно до безпекових процедур, встановлених за взаємними домовленостями компетентними органами безпеки згідно з національним законодавством.

В угоді з Урядом Словацької Республіки більш деталізовано процедуру передачі інформації з обмеженим доступом. Зазначено, що, якщо сторона-джерело має намір передати інформацію з обмеженим доступом юридичній особі сторони-одержувача, вона попередньо надсилає запит компетентному органу сторони-одержувача стосовно підтвердження того, що юридична особа сторони-одержувача отримала згідно з національним законодавством сторони-одержувача допуск відповідного рівня та має необхідні можливості для забезпечення належної охорони інформації з обмеженим доступом. Це

підтвердження містить зобов'язання забезпечити, щоб усі заходи з охорони інформації з обмеженим доступом, які вживатиме перевірена юридична особа, відповідали вимогам національного законодавства в сфері охорони інформації з обмеженим доступом сторони-одержувача. Компетентний орган сторони-одержувача контролює виконання цих заходів. Також зазначено, що компетентний орган сторони-одержувача забезпечує, щоб його фізичні та юридичні особи поводилися з інформацією з обмеженим доступом іншої сторони як з власною інформацією з еквівалентним ступенем обмеження доступу.

В угоді вказано, що інформація з обмеженим доступом передається між сторонами дипломатичними каналами. Компетентний орган сторони-одержувача підтверджує у письмовій формі одержання інформації з обмеженим доступом та передає одержану інформацію з обмеженим доступом користувачу. Зазначено, що в особливих випадках і за взаємною згодою компетентні органи сторін можуть визначити інші способи передачі інформації з обмеженим доступом. А передача інформації з обмеженим доступом електронними шляхами здійснюється з використанням криптографічних засобів закриття інформації, схвалених компетентними органами сторін.

Зазначено, що компетентні органи сторін можуть домовитись щодо інших шляхів передачі інформації з обмеженим доступом, проте лише тієї, яка позначена грифом «Для службового користування» / "Vyhradene" / "Restricted". В угоді між Кабінетом Міністрів України та Урядом Республіки Молдова про взаємний захист секретної інформації зафіксовано, що рішення про передачу секретної інформації приймається у кожному окремому випадку відповідно до законодавства України та Республіки Молдова. В угоді зафіксовано таку процедуру передачі секретної інформації: якщо уповноважений орган однієї сторони має намір передати секретну інформацію уповноваженому органу іншої сторони, він попередньо запитує d

компетентного органу своєї сторони письмове підтвердження про те, що уповноважений орган має відповідний допуск [14].

Зазначено, що передача секретної інформації з однієї держави до іншої здійснюється згідно з вимогами, установленими законодавством держав-сторін, дипломатичними каналами, фельд'єгерською службою або з використанням спеціальних технічних засобів зв'язку, які забезпечують захист інформації, що передається. Відповідний уповноважений орган письмово підтверджує одержання секретної інформації. Для передачі секретної інформації значного обсягу уповноважені органи за погодженням з відповідними компетентними органами у кожному окремому випадку встановлюють способи транспортування, маршрут і форму супроводу [14].

Аналіз окремих положень зазначених вище угод дав підстави для висновку, що основною загрозою для системи охорони інформації з обмеженим доступом є «несанкціонований доступ» та, як наслідок, її розголошення. В угодах зафіксовано процедуру дій у випадку порушення правил безпеки та компрометації інформації з обмеженим доступом. Зазначено, що в такому випадку компетентний орган безпеки сторони-одержувача інформує компетентний орган безпеки сторони-джерела, забезпечує належне розслідування ситуації та здійснює необхідні заходи з обмеження та подолання наслідків відповідно до національного законодавства. За запитом компетентні органи безпеки обох держав мають сприяти один одному в розслідуванні. Окрім того, в угодах визначаються питання щодо витрат, а також розв'язання суперечок, що виникають у процесі використання інформації з обмеженим доступом.

У прикінцевих положеннях узгоджуються організаційно-процедурні питання щодо термінів дії угоди, процедури припинення її дії тощо. В угоді з Угорською Республікою вказано, що, незважаючи на припинення дії цієї угоди, поводження з усією інформацією з обмеженим доступом, переданою в рамках цієї угоди, та її охорона здійснюються відповідно до цієї угоди або вона повертається стороні-джерелу. Після припинення дії цієї угоди

інформація з обмеженим доступом, яку договірні сторони отримали на підставі попередніх домовленостей із зобов'язанням стосовно її повернення, повертається стороні-джерелу [18].

В угоді з Республікою Молдовою зазначено, що вона (угода) укладається на п'ять років і автоматично продовжується на наступні п'ятирічні періоди, якщо жодна зі сторін не повідомить дипломатичними каналами іншу сторону не менше ніж за шість місяців до закінчення відповідного терміну про свій намір припинити її дію. У разі припинення дії цієї угоди її положення продовжують застосовуватися стосовно до переданої та (або) створеної в процесі співробітництва сторін секретної інформації, поки не буде скасовано гриф секретності [14].

Водночас наголосимо, що аналіз положень міжнародних договорів України про взаємну охорону секретної інформації та матеріалів засвідчив, що ці міжнародні угоди більше спрямовані на захист інформації, ніж на її передачу. З положень цих договорів випливає, що передача інформації здійснюватиметься відповідно до національного законодавства держав, які є учасниками договору або правил процедури. Тобто, такі договори не є підставою для передачі секретної інформації, а лише можуть розглядатись як механізм забезпечення взаємного захисту секретної інформації у випадку прийняття рішення в межах указу (розпорядження) Президента України або міжнародного договору про таку передачу.

Водночас більшість положень, які визначені договорами про взаємний захист секретної інформації після набрання ними чинності, мають корелюватись з нормами національного законодавства з метою їх ефективного застосування, оскільки на цей час окремі їх положення не узгоджуються з законодавством про державну таємницю, кримінальним, адміністративним законодавством в частині забезпечення порядку передачі секретної інформації, прийняття відповідного рішення, відповідальності за невиконання або неналежне виконання зобов'язань, включаючи політичну, матеріальну та особистісну відповідальність тощо.

Водночас зазначимо, що такі угоди щодо обміну інформацією з обмеженим доступом укладені не з усіма державами Східної Європи, у такому випадку всі питання регулюються відповідно до нормативно-правової бази сторін, а також спільно укладених договорів про співробітництво. Тому в процесі передачі чи надання секретних матеріалів може виникнути низка проблем як організаційного, так і правового характеру. Зазначимо, що в статті 9 Закону «Про державну таємницю» Республіки Латвії та статті 24 Закону «Про державну таємницю» Республіки Молдови зазначено, що порядок надання відомостей, які містять державну таємницю, визначається Кабінетом Міністрів, що дає можливість у кожному конкретному випадку оперативно приймати рішення [32, с.155].

Захист інформації, що містить комерційну таємницю, від несанкціонованого використання має важливе правове значення: з моменту втрати конфіденційності майнові права особи на секрет виробництва припиняються. До способів легально дізнатися комерційну таємницю належать: незалежне відкриття, зворотний технічний аналіз, добросовісне придбання. Використання комерційної таємниці іншого суб'єкта господарювання є неправомірним за умови, якщо відомості, що її становлять, були зібрані незаконно – без згоди на те власника комерційної таємниці. Адміністративно-господарські санкції за неправомірне збирання, розголошення та використання комерційної таємниці передбачені Законом України «Про захист від недобросовісної конкуренції» від 07.06.1996 р.

Внаслідок незаконного розкриття комерційної таємниці її володілець зазнає таких негативних економічних наслідків: знижуються можливості продажу ліцензій, втрачається пріоритет у дослідженнях, зростають витрати на переорієнтацію діяльності дослідницьких підрозділів; труднощі під час закупівель сировини, інших компонентів нормальної виробничої діяльності; обмежується кооперація на ринку, зменшується імовірність укладання контрактів на вигідних умовах, проблеми під час виконання договірних зобов'язань. До інших причин необхідності надання інформації захисту як

комерційній таємниці слід віднести такі: суб'єкт господарювання має статус інноваційного та досягнув високого рівня науково-виробничої діяльності; без створення корпоративної та контрактної систем захисту комерційної таємниці претензії до правопорушників є безпідставними; це один із найбільш важливих інститутів права інтелектуальної власності для тих держав, що намагаються залучити іноземні інвестиції [55, с.109-110].

Склад та обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються самостійно її власником або керівником підприємства з дотриманням норм чинного законодавства, саме захист комерційної таємниці є найбільш важливим питанням у процесі використання такої інформації [41, с.9].

При прийнятті рішення про те, чи слід скористатися механізмом охорони комерційної таємниці, необхідно виходити з переваг і недоліків такої охорони в порівнянні з іншими засобами охорони ІВ. Переваги комерційної таємниці полягають в наступному:

1) вона не пов'язана з витратами на реєстрацію;

2) її дія не обмежена в часі;

3) її охорона починає діяти негайно;

4) для встановлення охорони не потрібно її розкриття або реєстрація у державному органі.

З іншого боку, її недоліки полягають у наступному:

1) якщо таємниця втілена в продукті, треті особи можуть самостійно розкрити укладену в ньому секретну інформацію і використовувати її на законних підставах шляхом «зворотного інжинірингу»;

2) якщо комерційна таємниця розкрита широкій публіці, охорона не надається;

3) охорона надається тільки від неналежного одержання, використання або розкриття конфіденційної інформації;

4) охорона комерційної таємниці є більш слабкою, ніж охорона патентів;

5) комерційна таємниця не забезпечує охорони від тих, хто самостійно приходить до аналогічної ідеї, що тримається в секреті. Як наслідок, незапатентована комерційна таємниця може бути запатентована іншою особою, якщо вона буде розкрита нею самостійно. У цьому комерційна таємниця відрізняється від патентів на винаходи, які охороняють власників патентів навіть від тих, кому вдалося самостійно розробити аналогічне технічне рішення.

Закон не передбачає покарання за добросовісне розкриття, яке включає виявлення такими законними способами, як:

1) самостійне створення; комерційна таємниця не забезпечує виключності, тому потенційно будь-хто може розкрити вашу комерційну таємницю самостійно і використовувати або запатентувати її;

2) зворотний інжиніринг; це звичайна практика, яка використовується для з'ясування механізму функціонування або складових частин продукту і яка полягає в тому, що конкурент вивчає продукт з метою його відтворення або навіть виготовлення більш досконалого продукту.

Однак, в даний час серед дослідників вже досить поширеною є думка про те, що охорона результатів інтелектуальної діяльності в режимі комерційної таємниці більш перспективна, ніж захист патентом. Адже патенти з самого початку були призначені для того, щоб стимулювати виведення винаходів з комерційної таємниці [23].

3.3. Відповідальність за розголошення у сфері інформаційної безпеки в сучасних умовах (наприклад, в зоні проведення АТО (з 30 квітня 2018 року формат Антитерористичної операції на Сході України змінено на формат Операції об'єднаних сил (ООС, United forces operation)

В Україні триває гібридна війна (війна із поєднанням принципово різних типів і способів ведення війни, які скоординовано застосовуються

задля досягнення спільних цілей) типовим компонентом для якої є загрожуюча державі ворожа пропаганда, яка має на меті підірвати довіру до влади, збройних сил, зміну території, існуючих кордонів, легалізацію бандитських та терористичних угруповань, розв'язання нових конфліктів у державі тощо. Пропаганда не охоплюється об'єктивною стороною злочину, передбаченого ст.109 КК України «Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади» [9].

У пропаганді відсутні: дії, вчинені з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади; змова про вчинення таких дій; публічні заклики до насильницької зміни чи повалення конституційного ладу або захоплення державної влади; розповсюдження матеріалів із закликами до таких дій.

Сьогодні в Україні відсутня кримінальна відповідальність за пропаганду в тому визначені, у якому вона сьогодні здійснюється. За пропаганду можливо притягнути лише на підставі ст.161 КК України, у випадку, якщо пропаганда, як різновид умисних дій, матиме своєю спрямованістю розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образа почуттів громадян у зв'язку з їхніми релігійними переконаннями. Проте, об'єктом цього злочину є порушення рівноправності громадян, а не державна (національна) безпека. Адже мета ворожої пропаганди – насильницька зміна чи повалення конституційного ладу або захоплення державної влади, тобто вона безпосередньо впливає на національну безпеку.

Пропаганда має на меті впливу на суспільну думку на користь певної спільної справи (згуртуванню у боротьбі з зовнішнім та внутрішнім ворогом, довіра до законно обраної влади, добровільна участь у частковій мобілізації, допомога пораненим, вимушеним переселенцям тощо) чи громадської позиції під час проведення Антитерористичної операції, тощо.

Родовим об'єктом злочинів проти основ національної безпеки – суспільні відносини, які забезпечують державну безпеку, конституційний

лад, суверенітет, територіальну цілісність і недоторканність, обороноздатність, тобто основи національної безпеки. Тобто відносини, що забезпечують саме існування України як суверенної, незалежної, демократичної, соціальної і правової держави [45, с.7].

В цілому, криміналізація посягань за пропаганду, що загрожує державі відповідає принципам криміналізації суспільно-небезпечних діянь, розробленим теорією кримінального права, а саме соціальних і соціально-психологічних принципів криміналізації, принципів, які визначають вимоги внутрішньої логічної несуперечливості системи норм кримінального права, несуперечливості між нормами конституційного, кримінального, а також інших галузей права.

Потрібно окремо підкреслити, що наявна пропозиція про доповнення КК України статтею про кримінальну відповідальність за пропаганду, що загрожує державі не суперечить Конвенції про захист прав людини і основоположних свобод від 04 листопада 1950 р., ст.10 «Свобода вираження поглядів» якою проголошено, що: «Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію й ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

Здійснення цих свобод, оскільки воно пов’язане з обов’язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров’я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду» [7].

Беручи до уваги зазначене, цілком підтримуємо пропозицію А. М. Притули доповнити Розділ І Особливої частини Кримінального кодексу України «Злочини проти основ національної безпеки» статтею наступного змісту, виклавши її, наприклад, у такому вигляді: «Стаття 1091. Поширення інформації чи відомостей, що становлять загрозу національним інтересам України Пропаганда іноземної держави, яка направлена на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади, а також поширення інформації чи відомостей, що становлять загрозу національним інтересам України, карається…» [63, с.102].

Слід зазначити, що поширення поглядів та аргументів з метою формування певної суспільної думки та(або) активізації певної бажаної діяльності щодо війни, яка не є агресивною, не утворює ознаки будь-якого злочину. Така сама діяльність щодо певних політичних, релігійних або філософських поглядів утворює окремі ознаки складу злочину, відповідальність за яких передбачена ст. 436 КК, якщо вони ідентифіковані як неонацизм.

Залишається відкритим питання, чи достатньо самоідентифікації прихильників цих поглядів, чи треба в якомусь формалізованому порядку (можливо, судовому або за допомогою експертизи) приходити до певного висновку, чи підпадають під кримінально-правову заборону супутні, суміжні течії, або витоки неонацизму.

Не однаковим є опис об’єктивної сторони розглядуваних злочинів. Так, в ч.1 ст. 436 КК прямо не міститься визначення, але з її назви випливає, що під кримінально-караною пропагандою війни, напевно, слід розуміти публічні заклики до агресивної війни або до розв’язування воєнного конфлікту, а також виготовлення матеріалів із закликами до вчинення таких дій з метою їх розповсюдження або розповсюдження таких матеріалів.

Між тим, диспозицією ч.1 ст.436 КК такі різновиди протиправної поведінки, як пропаганда ідеології, виготовлення та(або) розповсюдження матеріалів, передбачено в якості самостійних форм, з чого випливає, що в

цьому випадку та на відміну від ч.1 ст. 436 КК пропаганда не охоплює розповсюдження або виготовлення, тобто, вони не співвідносяться між собою як родове та видове поняття. Це не є прийнятним, адже, з точки зору системного підходу до розробки будь-якого нормативного акту та у конкретному випадку подальшого застосування КК у практичній правоохоронній діяльності, певні терміни не можуть бути вживані у різних значеннях.

Чинний КК ще в одній статті у редакції Закону України № 1707-УІ від 05.11.2009 передбачає відповідальність за діяльність, яка пов'язана з пропагандою, але ця ознака характеризує вже предмет злочину твори, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ч. 1 ст. 300 КК), кіно та відео продукція такої самої спрямованості (ч.2 ст.300 КК). Якщо виготовлення та(або) розповсюдження розглядати в якості форм пропаганди, тоді слід вважати пропагандою насильницької зміни чи повалення конституційного ладу або захоплення державної влади дії з розповсюдження відповідних матеріалів (ч.2 ст. 109 КК), пропагандою посягання на територіальну цілісність і недоторканність України розповсюдження матеріалів із закликами до вчинення таких дій (ч.1 ст.110 КК), терористичного акту розповсюдження або виготовлення матеріалів закликами до нього (ч. 1 ст.2582 КК), пропагандою дій, що загрожують громадському порядку виготовлення або розповсюдження матеріалів з публічними закликами до погромів, підпалів, знищення майна, захоплення будівель чи споруд, насильницького виселення громадян, що загрожують громадському порядку (ч.1 ст.295 КК), пропагандою порнографії виготовлення або розповсюдження творів, зображень або інших предметів порнографічного характеру (ч.1 ст.301 КК), пропагандою геноциду виготовлення матеріалів із закликами до нього з метою їх розповсюдження або розповсюдження таких матеріалів (ч.2 ст.442 КК) тощо.

Пропаганда певних політичних, філософських, наукових, мистецьких або інших поглядів, ідей, фактів, аргументів та інших відомостей для формування суспільної думки та свідомості, активізації певної бажаної діяльності тощо може відбуватися і без виготовлення певних матеріалів або їх розповсюдження (наприклад, заклики блаженного чи юродивого). Отже, пропаганду слід розглядати як окрему та самостійну форму діяльності по відношенню до виготовлення або розповсюдження певних матеріалів, тобто, як поняття, які мають певні обсяги перехрещення, але не поглинають одне інше.

Крім того, О. К. Тугарова наголошує на доцільності об'єднання в окремому розділі Особливої частини КК України злочинів у сфері обігу інформації, родовим об'єктом яких виступатиме інформаційна безпека людини, держави і суспільства. На нашу думку, пропозиція науковця є цілком слушною. Адже такий підхід забезпечить системний підхід у визначенні кола потенційних і реальних загроз інформаційній безпеці, та сприятиме довершеності положень кримінального законодавства України [72, с.65].

Вирішення потребує й питання відповідальності юридичних осіб за пропаганду війни в Україні. Як відомо, У 2014 році в кримінальному законодавстві України відбулася одна з найбільш значущих його реформ за часів незалежності: у ньому з'явився інститут заходів кримінально – правового характеру щодо юридичних осіб. Цей інститут був запроваджений законом України № 314-VII від 23 травня 2013 року. і ще до набрання чинності зазнав змін, унесених законом України № 1207-VII від 15 квітня 2014 року. Проект Закону України «Про внесення змін до деяких законодавчих актів України (щодо виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України стосовно відповідальності юридичних осіб)» в першу чергу був спрямований на забезпечення виконання рекомендацій Групи держав проти корупції (GRECO), Спеціального Комітету експертів Ради Європи з питань оцінки

заходів боротьби з відмиванням коштів (MONEYVAL), а також на вирішення питань про реалізацію низки міжнародних договорів України в частині встановлення відповідальності юридичних осіб. Прийняття проекту Закону України «Про внесення змін до деяких законодавчих актів України (щодо виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України стосовно відповідальності юридичних осіб)» має сприяти виконанню взятих Україною зобов'язань щодо встановлення відповідальності юридичних осіб за злочини, а також дозволить привести положення вітчизняного законодавства у відповідність з міжнародними стандартами у цій сфері. В той же час відсутність на сьогоднішній момент значної судової практики та керівних роз'яснень Пленуму Верховного Суду України в частині застосування законодавства про кримінальну відповідальність щодо юридичних осіб викликає низку проблемних питань, які потребують негайного вирішення, їх теоретичного обґрунтування та вироблення ефективних рекомендацій щодо їх застосування. В першу чергу це стосується застосування такого заходу кримінально – правового характеру як ліквідація та конфіскація майна [57].

Серед низки суспільно небезпечних діянь за вчинення яких передбачено вжиття кримінально – правових заходів до юридичної особи, п. 4 ч.1 ст. 96-3 КК України містить і пропаганду війни (ст. 436 КК України). Дані зміни до КК України, є як ніколи актуальними та своєчасними, адже вони є частиною розробки національного і міжнародного законодавства і політики щодо поширення пропаганди, пов'язаної з конфліктом в Україні і навколо неї. На необхідність такої розробки неодноразово було вказано на рівні різних нормативно – правових актів та різноманітних доповідей міжнародними інстанціями з безпеки в Європі та Світі.

Особлива увага при цьому звертається на коло юридичних осіб, що задіяні в інформаційній сфері. Так на небезпеку поширення закликів, щодо розв'язання агресивної війни чи збройного конфлікту, за допомогою засобів масової інформації неодноразово вказувалося в різноманітних європейських

джерелах. Проте застосування різноманітних заходів впливу на засоби масової інформації має бути здійснено з максимальною обережністю. Адже втручання держави в журналістську діяльність, в окремих випадках, може розглядатися як факт та набувати ознак цензури.

Відповідно до ст. 96-6 КК України до юридичних осіб судом можуть бути застосовані такі заходи кримінально – правового характеру: штраф; конфіскація майна; ліквідація. При цьому відповідно до ч. 2 ст. 96-6 КК України до юридичних осіб штраф та ліквідація можуть застосовуватися лише як основні заходи кримінально – правового характеру, а конфіскація майна – лише як додатковий.

Геополітичне положення України та проведення АТО (ООС) на території України, спонукає до вивчення організаційно-правових норм захисту інформації з обмеженим доступом у такому потужному військово-політичному утворенні, як НАТО. Як зазначено у статті «Проблемні питання правового регулювання обігу інформації з обмеженим доступом (державна таємниця та службова інформація)» за авторством О. О. Федоренка, С. О. Керсіцького, А. І. Курбатова [63], безпосередньо в самому НАТО існують інституції, завданням яких є моніторинг (нагляд) результатів та якості захисту інформації з обмеженим доступом у країнах-учасницях. Офіс безпеки НАТО (NOS), що відповідає за повну координацію питань інформаційної безпеки, доводить інформацію щодо застосування принципів і стандартів та виконує моніторинг національних систем захисту інформації.

Основними загрозами для інформації є її розголошення, витік і несанкціонований доступ до її джерел. Так, у військовій сфері можна виділити інформацію, що стосуються безпосередньо Збройних сил України, до якої, зокрема, віднесено відомості: про зміст оперативних планів і документів бойового управління директив, донесень та зведень; про підготовку військ до виконання оперативних (бойових) завдань; про стратегічне розгортання оперативно-мобілізаційних заходів; про зміст закритих навчальних програм у вищих військових навчальних закладах Збройних сил України. Розголошення

відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422) [9].

Слід підкреслити, що Прес-центр штабу антитерористичної операції на Донбасі неодноразово оприлюднював звернення з проханням не поширювати відомостей про хід АТО (ООС), не розголошувати жодної інформації і відомостей, фото- і відеоматеріалів, що стосуються ходу тактичних і оперативних дій (переміщення, зміна позицій, розкриття підрозділів, просування тощо). Оприлюднення інформації з обмеженим доступом може створювати загрозу безпеці і життя військовослужбовців, за що настає адміністративна та кримінальна відповідальність.

Адміністративна відповідальність передбачена за порушення законодавства про державну таємницю (ст. 2122 КУпАП України, за розголошення конфіденційної інформації, що є власністю держави (ст. 2125 КУпАП України). Зазначені статті розміщено у главі 15 КУпАП України «Адміністративні правопорушення, що посягають на встановлений порядок управління». В тій же главі 15 КУпАП України, частиною 3 ст. 1863 передбачена відповідальність за порушення порядку використання конфіденційної інформації, приховування або перекручення даних державних статистичних спостережень, а також використання їх в засобах масової інформації, для поширення в інформаційних мережах, на паперових, магнітних та інших носіях, в наукових працях тощо без посилання на їх джерело.

Необхідно акцентувати, що вже існують прецеденти коли Колегія суддів Солом'янського райсуду міста Києва визнавала винною в державній зраді військовослужбовців Національної гвардії України. Так, технік-оператор відділу інформаційного забезпечення Центральної бази зберігання Нацгвардії збирала і передавала спецслужбам РФ відомості, що становлять державну таємницю. Суд обрав їй міру покарання у вигляді чотирьох років позбавлення волі. Отже, якщо розголошена інформація не відповідала б будь-

якій з ознак, вказаних на початку статті, особа б не підлягала кримінальній відповідальності за ст. 328 [9].

З метою удосконалення інформаційного режиму в зоні проведення АТО (ООС) та попередження витоку інформації з обмеженим доступом, необхідно поглибити юридичну відповідальність як для військовослужбовців Збройних сил України, так і для волонтерів, які співпрацюють зі Збройними силами України, для осіб, які мешкають на тимчасово окупованій території та для тимчасово переміщених осіб – громадян України. Це надасть змогу підвищити відповідальність громадян за порушення законодавства про охорону інформації з обмеженим доступом.

Відповідним законотворчим органам (Комітету з питань законодавчого забезпечення правоохоронної діяльності Верховної ради України) необхідно поширити законотворчу діяльність та внести зміни до кодексів України щодо настання адміністративної та кримінальної відповідальності для військовослужбовців, волонтерів, осіб, які мешкають на тимчасово окупованій території відповідальності за розголошення інформації і відомостей, фото- і відеоматеріалів, що стосуються ходу тактичних і оперативних дій (переміщення, зміни позицій, розкриття підрозділів, просування і т.п.). На даний момент опрацьовується проект Закону України від 09.06.2015 р. №2050а «Про внесення змін до деяких законодавчих актів України щодо удосконалення інформаційного режиму проведення антитерористичної операції» [6], викликаний непоодинокими випадками розповсюдження в засобах масової інформації та соціальних медіа відомостей про розташування, розгортання та переміщення підрозділів Збройних сил України та інших військових формувань, стан їх бойової та мобілізаційної готовності, технічний стан озброєння та військової техніки, рівень оснащення, забезпечення та морально-психологічний стан військовослужбовців, стан оперативного обладнання територій, стан виконання робіт підприємствами оборонно-промислового комплексу та іншої

інформації, що ставить під загрозу успішне проведення Антитерористичної операції (Операції об’єднаних сил).

Вищезазначену мету передбачається досягти шляхом встановлення відповідної заборони (внесення змін до статей 17 та 25 Закону України «Про боротьбу з тероризмом») та визначенням кримінальної відповідальності за її порушення. Загальною правовою основою у сфері суспільних відносин, що стосуються проекту Закону [6], є Конституція України, Кримінальний кодекс України, Закон України «Про інформацію» та інші закони України і нормативно-правові акти.

ВИСНОВКИ ТА ПРОПОЗЦІЇ

Отже, найважливіші результати, одержані під час складання випускної кваліфікаційної роботи, що насамперед дають відповідь на окреслені завдання вищезазначеної роботи, полягають у такому:

1. Інформаційні правовідносини – це врегульовані інформаційно-правовою нормою інформаційні суспільні відносини, сторони якого виступають як носії взаємних прав і обов'язків, встановлених і гарантованих інформаційно-правовою нормою.

Зміст інформаційних відносин являє собою визначену сукупність суб'єктивних прав та юридичних обов'язків, що належать суб'єкту інформаційних правовідносин.

2. Інформаційне право, як наука, має на меті розробку способів найбільш ефективного і повного забезпечення інформаційних процесів в Україні, захисту громадян, суспільства, держави від шкідливої, небезпечної інформації, захист прав і свобод споживачів інформації в інформаційній сфері. На виконання цієї мети, розроблена система правового регулювання інформаційних відносин, що складається з двох частин: приватноправове регулювання, що здійснюється на рівні звичаїв, угод, традицій, норм суспільної моралі тощо; публічно-правове, державне регулювання, що здійснюється на рівні держави у вигляді інформаційного законодавства.

Законодавча система США з безпеки інформації є однією з найнадійніших у світі, що робить її майже досконалою та такою, на яку всі повинні рівнятися.

Ще одним прикладом інформаційного законодавства є закони, прийняті країнами-членами Європейського Союзу, під які теперішні претенденти на вступ до ЄС переробляють або приймають доповнення до свого законодавства.

3. За порядком доступу інформацію поділяють на три групи: інформація, що заходиться у цивільному обігу, тобто та, з приводу якої

виникають в першу чергу майнові відносини; інформація, яка заходиться в адміністративному обігу, тобто та, за допомогою якої регулюються суспільні відносини, в тому числі і в інформаційній сфері (зокрема, інформація, що міститься у нормах права); інформація, яка знаходиться у суспільному (публічному) обігу, що являє собою відомості інформаційного характеру, чи масова інформація, призначена для інформування населення.

До ознак інформації з обмеженим доступом відносять:

- така інформація має кількісні і якісні характеристики, не є загальнодоступною, використовується чітко визначеним колом осіб і саме завдяки цьому суб'єкт інформації вживає заходів, що спрямовані на обмеження вільного доступу третіх осіб до неї, її зміст відповідає обмеженням, встановленим законодавством;

- така інформація має особливу соціальну цінність завдяки її дійсної або потенційної невідомості (непоширенню) третім особам, що не спричинить істотної шкоди зацікавленим особам;

- така інформація існує винятково в рамках взаємодії суб'єктів суспільних відносин: окремих індивідуумів, їх груп, а також таких соціальних утворень, як держава, муніципальні утворення і юридичні особи.

За правовим режимом доступу інформація поділяється на три такі категорії:

Конфіденційну інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Таємну інформацію, доступ до якої обмежується, в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Службову інформацію, що міститься в документах суб'єктів владних повноважень (галузева чи відомча кореспонденція, доповідні та/або службові записки, рекомендації тощо), якщо вони пов'язані з розробкою напряму діяльності установ або зі здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; зібрана в процесі проведення оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, та є такою, що не віднесена до державної таємниці.

4. До прийняття рішення про присвоєння документу грифа «Для службового користування» посадова особа або уповноважений нею виконавець, який підписує документ, повинні:

4.1. Перевірити, чи належить інформація, яку містить документ, до категорій, визначених у частині першій статті 9 Закону України «Про доступ до публічної інформації».

4.2. Встановити, чи належить відповідна інформація до такої, доступ до якої згідно із законом не може бути обмежено, в тому числі шляхом віднесення її до службової інформації.

4.3. Перевірити дотримання сукупності вимог, передбачених частиною другою статті 6 Закону України «Про доступ до публічної інформації».

У кожному конкретному випадку при вирішенні питання щодо віднесення публічної інформації до службової, має бути обґрунтовано: якому саме з інтересів загрожує надання розголошення інформації (наприклад, інтересам національної безпеки, територіальної цілісності); в чому саме буде полягати шкода в разі розголошення цієї інформації; чому шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

На документах, що містять службову інформацію з: мобілізаційних питань – проставляється відмітка «Літер «М»; питань криптографічного захисту службової інформації – відмітка «Літер «К»; питань спеціальної інформації – відмітка «СІ». Категорії документів, на яких проставляється

відмітка «Літер «К», визначаються нормативно-правовими актами Адміністрації Держспецзв'язку.

5. Інформація є однією із найважливіших категорій системи суспільних відносин, що зумовлює численність її дефініцій. Із правової точки зору поняття «інформація» повинно мати формалізовану, аксіоматичну форму, бути нормативно закріпленим, оскільки відсутність чіткого, регламентованого поняття може призвести до юридичних колізій під час його застосування.

Так, інформація − будь-які відомості та/або дані, що можуть бути збережені:

– на матеріальних носіях (листування, книги, помітки, ілюстрації, карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, друковані пояснення осіб;

– в електронному вигляді (кіно-, відео-, мікрофільми, звукові записи (будь-які інші публічно оголошені чи документовані відомості), бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів).

Враховуючи, що термін закріплює під інформацією лише «відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді», може ускладнитися його правозастосування у цивільно-правових відносинах, де інформація є нематеріальним благом (глава 15 Цивільного кодексу України) і не зводиться до матеріального (фізичного) об'єкту, на якому вона зафіксована, або до відображення її в електронному вигляді.

Аналіз вітчизняної правової доктрини свідчить, що більшість науковців дублюють недосконале законодавче визначення «інформація» через поняття «відомості», «дані», або недоцільно застосовують поняття «знання», зокрема під інформацією розуміють:

- відомості, що передаються усним, письмовим або іншим способом, зокрема за допомогою умовних сигналів, технічних засобів тощо;

- відомості (не дані) про події та явища, що можуть бути пізнані особою та передані іншій особі у вигляді, придатному для сприйняття;
- відомості про об’єктивно існуючі явища, що використовуються більш ніж однією особою, незалежно від форми та способу надання у суспільних відносинах;
- відомості, що передаються усним, письмовим або іншим способом, зокрема за допомогою умовних сигналів, технічних засобів тощо;
- певний набір знань про той чи інший об’єкт, що можна використати в доцільній діяльності людини тощо.

Однозначного трактування змісту досліджуваного поняття можна дійти тільки через сутність найважливіших властивостей у сфері суспільних відносин.

Здатність суспільства та його інститутів збирати, накопичувати та використовувати інформацію, забезпечувати свободу інформаційного обміну є важливою передумовою соціального та технологічного прогресу, чинником національної безпеки, підґрунтям успішної внутрішньої та зовнішньої політики.

6) Наслідком розголошення інформації з обмеженим доступом є притягнення до юридичної відповідальності. За такі дії винна особа може бути притягнена до кримінальної, адміністративної та цивільної відповідальності.

Юридичну відповідальність за порушення правил використання, поширення, зберігання конфіденційних та таємних відомостей повинні нести всі винні суб’єкти, що вступають в інформаційні правовідносини.

Значна кількість норм КУпАП передбачає адміністративну відповідальність за порушення норм законодавства про інформацію з обмеженим доступом, проте це стосується далеко не всіх її видів. Так, правовому захисту підлягають: комерційна, службова, державна, фінансова таємниці та персональні дані як вид інформації з обмеженим доступом. Проте не передбачена адміністративна відповідальність за порушення

режимів лікарської та медичної таємниці, таємниці усиновлення, податкової, досудового слідства, банківської та адвокатської таємниці, нотаріальної таємниці, таємниці нарадчої кімнати тощо.

Особливе місце у механізмі захисту інформаційних правовідносин займає інститут кримінальної відповідальності, що відображає наслідки невиконання або неналежного виконання особою норм інформаційного законодавства і тягне невідворотність реагування держави на вчинені кримінальні правопорушення з основними видами санкцій (штраф, громадські роботи, виправні роботи, обмеження волі, позбавлення права обіймати певні посади чи займатися певною діяльністю, конфіскація програмних та технічних засобів, які є власністю винної особи).

Такий розподіл норм, що захищають різні види інформації, не враховує класифікацію інформації за режимом доступу до неї. Негативним наслідком цього є те, що в законодавстві передбачається більш тяжке покарання за протиправні дії з інформацією із нижчим режимом захисту та, відповідно, меншою цінністю, ніж за порушення суворішого режиму відомостей. Так, комерційна таємниця, яка, по-суті, є конфіденційною інформацією приватних осіб, захищається кримінальним законом, а відповідна конфіденційна інформація держави, що захищається режимом службової таємниці, - ні.

На відміну від адміністративних правопорушень, злочини в інформаційній сфері характеризуються більш високим ступенем суспільної небезпеки, призводять до завдання реальної або потенційної істотної шкоди інтересам особи, держави, суспільства і передбачають можливість призначення покарання у вигляді позбавлення волі.

Цивільно-правова відповідальність наступає у випадках, якщо була заподіяна шкода фізичним та юридичним особам внаслідок недотримання відповідних норм у сфері інформаційного права. Об’єктом цивільної відповідальності за правопорушення у сфері інформаційних правовідносин є майнові та особисті немайнові права фізичної або юридичної особи, які охороняються інформаційним та цивільним законодавством.

Реалізація цивільно-правової відповідальності – це передусім виконання обов'язку з відновлення порушеного права (становища) особи або компенсації нанесених правопорушенням шкоди, реальних збитків, упущеної вигоди тощо, що забезпечується передбаченими нормами цивільного права заходами державного примусу (їх можливістю або безпосередньою реалізацією).

7) Важливим показником стану захищеності інтересів особи, суспільства і держави є ступень забезпечення захисту інформації, доступ до якої обмежено з метою захисту прав і законних інтересів суб'єктів права на таємницю.

Інформація з обмеженим доступом, що цікавить розвідувальні органи іноземних держав, як правило, зосереджується в таких сферах: політичній, економічній, військовій, науково-технічній.

Розвідувальні спрямування зацікавленої іноземної держави щодо України націлені на наступні життєво важливі об'єкти національної безпеки, до яких відносяться:

– об'єкти політичної розвідки і діяльності іноземних держав щодо політичної стабільності і зовнішніх зв'язків України (політична система та потенціал, плани щодо реалізації політичної стратегії; міжнародні позиції України, політичні відносини з іншими державами, міжнародними організаціями, рухами тощо; процес розвитку демократії та становлення державності; політично-адміністративна діяльність України, формування загальнодержавної ідеології розвитку суспільства, антигромадські прояви у суспільстві);

– об'єкти розвідувального проникнення:

7.1. Центральні органи державної влади і управління, органи управління зовнішньою діяльністю, органи зовнішньої розвідки; органи, що здійснюють адміністративно-державні функції всередині держави: політичні партії, громадсько-політичні, релігійні та

культурологічні організації, що беруть участь в міжнародних зв'язках; міжнародні політичні організації, до складу яких входить Україна).

7.2. Центральне управління Міністерства оборони, Генеральний штаб, штаби видів Збройних Сил, стратегічні угруповання військ, об'єднання, з'єднання частин, об'єднані міждержавні воєнні організації, структури, військові частини, які споряджені новими видами зброї та бойової техніки, арсенали і склади зберігання цих видів зброї та техніки, випробувальні полігони, засоби закритого оперативного зв'язку Міністерства оборони.

7.3. Державні органи, що здійснюють планування і управління економікою та окремими її галузями, державні органи та інші організації, що задіяні у сфері зовнішньоекономічної та кредитно-фінансової діяльності, міжурядові організації в сфері економічних відносин, важливі підприємства промисловості, сільського господарства, транспорту та зв'язку, сховища матеріальних цінностей; наукові заклади, які проводять дослідження в галузі економіки).

7.4. Державні органи управління науковими роботами, Національна академія наук, науково-дослідні інститути, полігони галузевого профілю.

– об'єкти військової розвідки і діяльності іноземної держави щодо військової могутності та зовнішніх військово-політичних зв'язків України (військовий потенціал, зовнішні військово-політичні відносини і військово-стратегічні позиції, військово-стратегічні плани вищого військового командування; боєготовність і боєздатність Збройних сил України; військово-мобілізаційні плани військового командування, озброєння, бойова техніка та заходи держави по їх розвитку, плани військового будівництва, дислокація військових об'єктів, плани ведення бойових дій у відповідних умовах та окремих регіонах, військове співробітництво з іноземними військовими, в тому числі і міжнародними організаціями, та перспективи їх розвитку, військово-політичні заходи, що готуються на випадок актів агресії

проти України, а також на випадок виникнення кризової ситуації в різних регіонах світу, де є життєво важливі інтереси України);

– об’єкти економічної розвідки і діяльності іноземних держав щодо економічної могутності зовнішньоекономічних зв’язків України (економічна система, економічний потенціал, кредитно-фінансова система, зовнішньоекономічні зв’язки, плани державних і владних структур щодо реалізації економічної стратегії України; конкретні галузі економіки, природні ресурси, стратегічні промислові ресурси (сировини та сільгосппродуктів, енергетичні та інші державні запаси для потреб оборони), народно-господарські плани, торгово-економічна і кредитно-фінансова система, потреби України у розвитку економічних зв’язків, плани держави щодо розвитку зовнішніх економічних зв’язків різного рівня, включаючи плани підготовки до укладання конкретних торгово-економічних угод, процеси економічної інтеграції і міжнародного розподілу праці в економічних міжнародних структурах, до яких входить Україна, торговельно-економічні відносини з іноземними державами);

– об’єкти науково-технічної розвідки і діяльності іноземних держав щодо підриву науково-технічного потенціалу, зовнішніх науково-технічних зв’язків України (науково-технічний потенціал України, зовнішні наукові зв’язки та державні плани розвитку науки і техніки; науково-технічний процес в Україні, напрями розвитку науки і техніки в Україні, які мають важливе народногосподарське і оборонне значення, система управління науковими дослідженнями в Україні, наукові винаходи, які мають важливе народногосподарське і оборонне значення, наукові ідеї і фундаментальні дослідження, які ініціюють винаходи, що здатні викликати стрімке зростання сукупного потенціалу держави і зміцнити її авторитет та позиції на світовій арені, важливі для розвитку науки випробувальні зразки обладнання, наукові зв’язки України з іноземними державами).

8. Захист інформації з обмеженим доступом – це комплекс дій власника інформації для збереження прав на її володіння й розповсюдження, а також

сприяння життєдіяльності людини, суспільства та держави на основі створення органами управління безпечних умов, що обмежують розповсюдження й виключають або істотно ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв.

Форми адміністративно-правового захисту інформації з обмеженим доступом традиційно можна класифікувати на юрисдикційні та неюрисдикційні. До перших належить захист порушених прав суб'єктів інформаційних правовідносин у судовому й адміністративному порядку, до других – технічні засоби захисту інформації з обмеженим доступом. Механізм захисту інформації з обмеженим доступом є повним поєднанням технічних і юрисдикційних засобів захисту інформації. Усі вони є правовими, оскільки встановлюються правовими актами управління, у тому числі нормативно-правовими.

9. З метою удосконалення інформаційного режиму в зоні проведення АТО (з 30 квітня 2018 року формат Антитерористичної операції на Сході України змінено на формат Операції об'єднаних сил (ООС, United forces operation) та попередження витоку інформації з обмеженим доступом, необхідно поглибити юридичну відповідальність для кожної групи нижчезазначених осіб:

- для військовослужбовців Збройних сил України,
- для волонтерів, які співпрацюють зі Збройними силами України,
- для осіб, які мешкають на тимчасово окупованій території,
- для внутрішньо переміщених осіб – громадян України. Це надасть змогу підвищити відповідальність всіх без винятку громадян України за порушення законодавства про охорону інформації з обмеженим доступом в районах проведення бойових дій та на території так званих «зон безпеки».

Відповідним законотворчим органам (Комітету з питань законодавчого забезпечення правоохоронної діяльності Верховної ради України) необхідно поширити законотворчу діяльність та внести зміни до кодексів України щодо настання адміністративної та кримінальної відповідальності для

військовослужбовців, волонтерів, осіб, які мешкають на тимчасово окупованій території відповідальності за розголошення інформації і відомостей, фото- і відеоматеріалів, що стосуються ходу тактичних і оперативних дій.

На даний момент опрацьовується проект Закону України від 09.06.2015 р. №2050а «Про внесення змін до деяких законодавчих актів України щодо удосконалення інформаційного режиму проведення антитерористичної операції», викликаний непоодинокими випадками розповсюдження в засобах масової інформації та соціальних медіа відомостей про розташування, розгортання та переміщення підрозділів Збройних Сил України та інших військових формувань, стан їх бойової та мобілізаційної готовності, технічний стан озброєння та військової техніки, рівень оснащення, забезпечення та морально-психологічний стан військовослужбовців, стан оперативного обладнання територій, стан виконання робіт підприємствами оборонно-промислового комплексу та іншої інформації, яка ставить під загрозу успішне проведення антитерористичної операції.

Вищезазначену мету передбачається досягти шляхом встановлення відповідної заборони та визначенням кримінальної відповідальності за її порушення. Загальною правовою основою у сфері суспільних відносин, що стосуються проекту Закону, є Конституція України, Кримінальний кодекс України, Закон України «Про інформацію» та інші закони України і нормативно-правові акти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Домовленості про безпеку між Службою безпеки України та Управлінням безпеки Генерального секретаріату Ради ЄС і Департаментом безпеки Європейської Комісії стосовно захисту інформації з обмеженим доступом» від 11 жовтня 2005 року. [Електронний ресурс]. – Режим доступу : www.zakon3.rada.gov.ua/laws/show/994_859.

2. Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення прозорості у сфері відносин власності з метою запобігання корупції» № 597-VIII від 14.07.2015 р. // Відомості Верховної Ради. – 2015. - № 35. -Ст.343

3. Закон України «Про інформацію» від 02.10.1992№2657-XII // Відомості Верховної Ради України. – 1992. - №48. - Ст.650.

4. Закон України «Про доступ до публічної інформації» від 13.01.2011 р. №2939-VI // Відомості Верховної Ради. – 2015. - № 35. -Ст.343

5. Закону України «Про запобігання корупції» від 14.10.2014 р. №1700-VII // Відомості Верховної Ради. – 2015. - № 35. - Ст.343

6. Кодекс України про адміністративні правопорушення: від 07.12.1984 р. // ВВР Української РСР. – 1984. – Додаток до № 51. – Ст. 1122.

7. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. // Офіційний вісник України – 1998. – № 13

8. Конституція України від 28.06.1996 р. № 254// Відомості Верховної Ради України. – 1996. - № 30. - Ст. 141.

9. Кримінальний кодекс України від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. - № 25-26. Ст.131

10. Постанова Кабінету Міністрів Україні «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736.

11. Проект Закону про внесення змін до деяких законодавчих актів України щодо удосконалення інформаційного режиму проведення антитерористичної операції. Офіційний веб-портал Верховної ради України. Електронний ресурс: http://w1.c1.rada.gov.ua/pls/ zweb2/ webp roc4 _1? Pf 3511=55536.

12. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію затверджена Постановою КМУ від 19.10.2016 року №736

13. Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом від 5 червня 2003 року // Офіційний вісник України. – 2004. – № 25. – Ст. 1639

14. Угода між Кабінетом Міністрів України та Урядом Республіки Молдова про взаємний захист секретної інформації [Електронний ресурс]. – Режим доступу : http://www.ua-info. biz/legal/basese/ua-ameget.htm.

15. Угода між Кабінетом Міністрів України та Урядом Румунії про взаємну охорону інформації з обмеженим доступом [Електронний ресурс]. – Режим доступу : ligazakon. ua/l_doc2.nsf/link1/MU13180.

16. Угода між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом // Офіційний вісник України. – 2008. – № 99. – Ст. 3282.

17. Угода між Україною та Європейським Союзом про процедури безпеки, які стосуються обміну інформацією з обмеженим доступом» від 13 червня 2005 року. [Електронний ресурс]. – Режим доступу : www.zakon5.rada.gov.ua/laws/show/994_750.

18. Угода між Україною та Угорською Республікою про взаємну охорону інформації з обмеженим доступом // Офіційний вісник України. – 2008. – № 24. – Ст. 720.

19. Указ Президента України №47/2017 «Про рішення Ради національної безпеки і оборони України» від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

20. Цивільний кодекс України від 16.01.2003 № 435-IV // Відомості Верховної Ради України. – 2003. - №№ 40-44. - Ст.356

21. Адміністративне право України. Академічний курс : підруч. : у 2 т. / ред. колегія: В.Б. Авер'янов (голова). – К.: Юридична думка, 2004. – Т. 1. Загальна частина. –584 с.

22. Актуальні проблеми кримінального права : [навч. посіб.] / В. М. Попович, П. А. Трачук, А. В. Андрушко, С. В. Логін]. – К. : Юрінком Інтер, 2009. – 256 с.

23. Андрощук Г. Захист комерційної таємниці в зарубіжній правовій доктрині: стратегії забезпечення лояльності працівників / Г. Андрощук // Юридичний журнал: аналітичні матеріали. Коментарі. Судова практика. - 2012. - № 5. - С. 56-62.

24. Андрощук Г. Захист комерційної таємниці в США: протидія економічному шпигунству / Г. Андрощук // Наука та інновації. - 2013. - Т. 9. - № 1. - С. 80-95.

25. Антонюк А. Основи захисту інформації в автоматизованих системах : [навч. посібник] / А. Антонюк. – К. : Академія, 2003. – 244 с.

26. Баскаков В. Ю. Захист інформації з обмеженим доступом у умовах боротьби з організованою злочинністю / В. Ю. Баскаков. [Електронний ресурс]. – Режим доступу: http://goal-int.org/zaxist-informacii-z-obmezhenim-dostupom-u-umovax-borotbi-z-organizovanoyu-zlochinnistyu/

27. Безверхня І. В. Поняття інформаційних правовідносин / І. В. Безверхні, Л. В. Перевалова. [Електронний ресурс]. – Режим доступу:http://webcache.googleusercontent.com/search?q=cache:R_fjWDVudQJ :www.kpi.kharkov .ua/archive/MicroCAD/2011/S25/%25D0%259F% 25D0%259E%25D0%259D%25D0%25AF%25D0%25D0%259E%25D0%25A1%25D0%2598%25D0%259D.pdf+&cd=2&hl=uk&ct=clnk&gl=ua

28. Беляков К. Інформація організаційноправової сфери /К.Беляков // Право України. - 2004. - № 6. - С. 88-92.

29. Василенко Д. П. Законодавство провідних країн світу в сфері захисту інформації / Д. П. Василенко, В. І. Маслак // Вісник КДУ імені Михайла Остроградського. - №2. - 2010 (61). - Частина 1. - С.128-132

30. Глуховеря В. А. Юридична відповідальність у механізмі забезпечення режиму інформації з обмеженим доступом / В. А. Глуховеря // Право і суспільство. – 2015. - №1. – С.123-128

31. Грищенко І. Механізм міжнародного співробітництво у сфері охорони державної таємниці між Україною та ЄС / І. Грищенко // Visegrad journal on human rights. – 2016. - №2-1. – С.33-38

32. Грищенко І. Правова охорона обміну інформацією з обмеженим доступом між Україною та державним Східної Європою / І. Грищенко // Національний юридичний журнал: теорія та практика. – 2016. – С.152-156

33. Дімчогло М. І. Консолідація інформаційного законодавства України : автореферат дисертації на здобуття наукового ступеня кандидат юридичних наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Марина Іванівна Дімчогло. – К., 2012. – 18 с.

34. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі / І. Діордіца // Підприємництво, господарство і право. - 2017. - №4. - С.99-107

35. Єсімов С. Правові режими службової інформації в Україні / С. Єсімов, М. Ковалів, Р. Скриньковський // Traektoria Nauki = Path of Science. - 2018. - №4. - С.7001-7012

36. Інформатизація, право, управління (організаційно-правові питання): Монографія / Р. А. Калюжний, О. Д. Крупчан, В. Д. Гавловський, М. В. Гуцалюк, М. Я. Швець, В. С. Цимбалюк; За заг. ред.: М. Я. Швеця, О. Д. Крупчана. − К.: НДЦ правової інформатики АПрНУ, 2002. – 191 с.

37. Інформаційна безпека України: Глосарій / В.А. Ліпкан, Л.С. Харченко, О.В. Логінов. – К. : Текст, 2004. – 136 с.

38. Інформаційне право України та електронне право високих технологій: (електронний курс лекцій українською мовою) / Автор – доцент кафедри кримінального права та правосуддя ЗНУ, кандидат юридичних наук, доцент Олег Володимирович Синєокий ; Запорізький національний університет ; Національна бібліотека України ім. В. І. Вернадського. – Запоріжжя : ЗНУ, 2010. – 215 с.

39. Інформація в праві: теорія і практика [Текст] : [Моногр.] / К. І. Бєляков; ДНДІ М-ва внутріш. справ України. − К. : КВІЦ, 2006. − 116 с.

40. Климчук С. Загальна характеристика законодавства про інформаційну безпеку ЄС, США та Канади / С.Климчук // Юстініан. - 2006. - №11. [Електронний ресурс] - Режим доступу: http://www.justinian.com.ua/article.php?id=2462

41. Колобов Л. Комерційна таємниця та питання захисту комерційної таємниці / Л. Колобов, І. Колесникова // Підприємництво, господарство і право. - №5. – 2016. – С.8-13.

42. Колодюк А. В. Інформаційне суспільство: сучасний стан та перспективи розвитку в Україні : Дис... канд. політ. наук: 23.00.03 / А. В. Колодюк // Київський національний ун-т ім. Тараса Шевченка; Інститут журналістики. – К., 2004. – 234 с.

43. Коломоєць Т.О. Штрафи за законодавством про адміністративні правопорушення: автореф. дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Т.О. Коломоєць ; Ун-т внутр. справ. - Х., 1999. - 16 с.

44. Коренюк О. Інформація з обмеженим доступом: об’єкт господарських відносин / О. Коренюк // Зовнішня торгівля: економіка, фінанси, право. - 2018. - № 2. - С.91-100

45. Кримінальний кодекс України: Науково-практичний коментар: У 2 т. – Т. 2: Особлива частина / Ю.В. Баулін, В.І. Борисов, В.І. Тютюгін та ін.; за заг. ред. В.Я. Тація, В.П. Пшонки, В.І. Борисова, В.І. Тютюгіна. – Х. : Право, 2013. – 1040 с.

46. Кулініч О. О. Інформація з обмеженим доступом як об’єкт цивільних прав : автореф. дис. … канд. юрид. наук : спец. 12.00.03 – цивільне право і цивільний процес; сімейне право; міжнародне приватне право. Київ, 2006. - 20 с.

47. Кулініч О.О. Інформація з обмеженим доступом як об’єкт цивільних прав : дис… канд. юрид. наук : 12.00.03 / Ольга Олексіївна Кулініч. - О., 2006. - 200 с.

48. Луценко С. Генезис інформаційно-комунікаційних теорій сучасного суспільства/С.Луценко, О.Кучабський//Інформаційна політика. – 2012. – №2. – С.60-67

49. Марутян Р. Інформаційні ресурси: нові підходи до визначення поняття/Р.Марутян// Сучасна українська політика: Політики і політологи про неї / гол. ред.: М. І. Михальченко ; Українська акад. політ. наук, Поліщук. – Київ : Укр. центр політ. менеджменту. - №18 : . – 2009 . – С. 93-104.

50. Марущак А. І. Свобода слова та інформація з обмеженим доступом: співвідношення понять // Бюлетень Мін’юсту України. – К., 2005. – №.6 (44) – С. 44 – 49

51. Марущак А. Інформаційне право: доступ до інформації : [навч. посібник] / А. Марущак. – К. : КНТ, 2007. – 532 с.

52. Мєзєнцева Н. Б. Деякі аспекти захисту інформації з обмеженим доступом / Н. Б. Мєзєнцева // Економіка та держава. - № 2. - 2013. - С.141-144

53. Мороз Н. Поняття інформації обмеженого доступу / Н. Мороз // Вісник Національного ун-ту «Львівська політехніка». Серія «Юридичні науки». – 2017. - С.284-289.

54. Нашинець-Наумова А. Організація системи захисту інформації субєктів господарювання / А. Нашинець-Наумова // Підприємництво, господарство і право. – 2016. - №2. – С.110-116

55. Олефір А. О. До проблеми використання комерційної таємниці у господарських відносин / А. О. Олефір // Проблеми законності: зб. наук. ін – Харків, 2015. – №129. – С. 104-114.

56. Паєнко О. А. Міжнародно-правове регулювання охорони та захисту комерційної таємниці / О. А. Паєнко // Молодий вчений. – квітень 2015 року. - №4. – С.136-139.

57. Пекар П. В. Окремі питання відповідальності юридичних осіб за пропаганду війни / П. В. Пекар // Верховенство права. – 2017. [Електронний ресурс]. – Режим доступу: http://sd-vp.info/2017/okremi-pitannya-vidpovidalnosti-yuridichnih-osib-za-propagandu-vijni

58. Перов Д. А. Зміст та структура інформаційних правовідносин / Д. А. Перов, А. П. Климентьєв // Науковий вісник Міжнародного гуманітарного університету. - 2013. - №6-3. Том 1. – С.81-84

59. Петров Є. В. Інформація як об'єкт цивільно-правових відносин: Автореф. дис. канд. юрид. наук: 12.00.03. – Х., 2003. – 19 с.

60. Поліщук О. В. Види юридичної відповідальності за правопорушення у сфері інформаційних правовідносин / О. В. Поліщук // Молодий вчений. – 29-30 червня 2017 року. – С.68-71

61. Право інтелектуальної власності. Підручник для студентів вищих навч. закладів / За ред. О. А. Підопригори, О. Д. СвятоцЬкого. – К.: Видавничій Дім «Ін Юре», 2002. – 624 с.

62. Правова охорона як складова інформаційної безпеки цивільної авіації: автореф. дис. канд. юрид. наук : 12.00.07 / О. О. Золотар ; Держ. НДІ МВС України. – К., 2010. – 20 с.

63. Притула А. М. Пропаганда – компонент гібридної війни: шляхи протидії засобами кримінального права / А. М. Притула // Юридична наука. – 2015. - №3. – С.99-104

64. Проблемні питання правового регулювання обігу інформації з обмеженим доступом (державна таємниця та службова інформація) / О.О. Федоренко, С.О. Керсіцький, А.І. Курбатов. [Електронний ресурс]. – Режим доступу: http://ndipzir.org.ua/wp-content/uploads/2013/04/Fedorenko Kersitsky yKurbatov.pdf

65. Селезньова О. М. Структура інформаційних правовідносин / О. М. Селезньова //Науковий вісник Ужгородського національного університету. - 2014. - №27. – Том 2. – С.183-186

66. Сидоренко В. В. Адміністративна відповідальність в інформаційній сфері / В. В. Сидоренко // Науковий вісник Херсонського державного ун-ту. – 2013. - №3. – С.55-57

67. Синєокий О. В. Інформаційне право України та електронне право високих технологій: [електронний ресурс] (електронний курс лекцій українською мовою) / Запорізький національний університет; Національна бібліотека України ім. В. І. Вернадського. – Запоріжжя : ЗНУ, 2010. – 215 с.

68. Сідак В. Організація системи захисту інформації в Німеччині: еволюція та сучасний стан / В. Сідак // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (13), 2006. С.7-11.

69. Скок П. В. Поняття інформації з обмеженим доступом / П. В. Скок // Науковий вісник Херсонського державного ун-ту. – 2015. – №3-2. – Том 2. – С.165-168

70. Службова інформація: порядок віднесення та доступу. Практичний посібник / За редакцією Д. М. Слизьконіс. Автори-укладачі: О.Л. Огданська, В.В. Таран, В.В. Щербаченко – К.: Центр політичних студій та аналітики, 2014. - 76 с.

71. Тихомиров О. О. Юридична відповідальність за правопорушення в інформаційній сфері : навч. посіб. / О. О. Тихомиров, О. К. Тугарова. − К. : Нац. акад. СБУ, 2015. – 172 с.

72. Тугарова О. К. Забезпечення охорони інформації з обмеженим доступом при тимчасовому доступі до речей і документів / О.К. Тугарова // Юридичний науковий електронний журнал. – 2015. - №5. – С.223-226

73. Тугарова О. К. Кримінально-правове забезпечення охорони інформаційних правовідносин / О. К. Тугарова // Науковий вісник Херсонського державного ун-ту. – 2015. - №4. – С.61-66

74. Харенко О.В. Поняття «інформація» в юридичній науці та законодавстві України/О.В.Харенко//Часопис Київського ун-ту права. – 2014. - №3. – С.119-124

75. Чайков М. Коллизии секрета производства (ноу-хау) / М. Чайков, А. Майкова // [Електронний ресурс].-Режим доступу: http://www.avtonews.net/005 /kollizii-sekreta-proizvodstva-noukhau?page=0,1

76. Шевчук О. М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки : автореф. дис. на здобуття наук. ступеня канд. юрид. наук за спец. : 12.00.07 «адміністративне право і процес ; фінансове право ; інформаційне право» /О. М. Шевчук. – Запоріжжя, 2011. – 23 с.

77. Шпенов Д. Ю. Інформаційні правовідносини : автореф. дис. на здобуття наук. ступеня канд. юрид. наук за спец. : 12.00.07 «адміністративне право і процес ; фінансове право ; інформаційне право» / Д. Ю. Шпенов. – Київ, 2012. – 19 с.

78. Яременко О.І. Інформаційні відносини як предмет правового регулювання: теоретичний аспект / О.І. Яременко // Вісник Хмельницького інституту регіонального управління та права. – 2004.– № 1-2. – С. 158

79. Ясечко С.В. Цивільно-правова відповідальність за порушення права на інформацію : автореф. дис. ... канд. юрид. наук : «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / С.В. Ясечко. -Х., 2011. - 21 с.

80. Shannon C. E. Collected Papers, edited by N. J. A. Sloane and A. D. Wyner. – New York: IEEE Press. – 1993. – 924 p.