Олександр Семенюк,
кандидат юридичних наук,
заступник начальника
Управління Служби безпеки України

УДК 343.2

ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА У СФЕРІ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У статті досліджено систему кримінально-правових норм, які встановлюють відповідальність за несанкціонований витік інформації з обмеженим доступом, проведено аналіз наукових поглядів щодо класифікації таємної інформації та її поділу на види, розроблено пропозицій щодо оптимізації та вдосконалення зазначених кримінально-правових норм.

Ключові слова: *кримінальна відповідальність, інформація з обмеженим доступом, професійна таємниця, державна таємниця, конфіденційна інформація, комерційна таємниця, чужа таємниця.*

Сучасний розвиток інформаційних технологій на основі комп'ютерних і телекомунікаційних технологій, яка стрімко набирає темпів, спричинив новий революційний етап у розвитку країн — інформаційного суспільства.

Під впливом динаміки суспільних відносин в інформаційному суспільстві виникають нові види, форми і прояви суспільно небезпечних діянь, які раніше не могли існувати через відсутність технологій, з використанням яких вони реалізуються. Сьогодні як міжнародною спільнотою, так і нашою державою визнано, що інформаційна безпека, кібернетичний простір, інформація та інформаційно-комунікаційні технології потребують кримінально-правового забезпечення. Натомість, інформаційна безпека та безпека кібернетичного простору на сьогодні вирішується ситуативно шляхом встановлення кримінального захисту певного виду «таємниць», інформації та безпеки діяльності ЗМІ, переважно в частині свободи слова [1, с. 9]

Значною мірою це обумовлено широким колом нових загроз у сфері інформаційних відносин, а також відсутністю глибокого теоретичного аналізу ситуації, що склалася, та пропозицій науковців щодо доцільності та обсягу можливого кримінально-правового втручання в цей процес.

Питання щодо перспектив розвитку кримінального законодавства у сфері охорони інформації з обмеженим досту-

пом постає не вперше. Так, до пошуку шляхів вдосконалення кримінально-правового забезпечення розвитку інформаційного суспільства долучилися такі вітчизняні вчені як Н. Карчевський, І. Корж, В. Мисливий, І. Павленко, Н. Савінова, О. Тугарова, В. Цимбалюк та інші. Однак, незважаючи на актуальність зазначеного питання, здебільшого науковці обмежуються висвітленням існуючих проблем у цій сфері та визначенням подальших напрямів їх дослідження. При цьому розробка конкретних пропозицій щодо змін у Кримінальному кодексі України залишається за межами їх наукових розвідок.

Метою цієї статті є дослідження кримінально-правових норм, які встановлюють відповідальність за несанкціонований витік інформації з обмеженим доступом, та розроблення пропозицій щодо їх оптимізації та вдосконалення.

Потреба в адекватній відповіді на нові виклики з боку злочинного середовища, а також усвідомлення законодавцем не лише необхідності інформаційної свободи як нормального стану суспільства, а й захисту тих чи інших видів інформації, несанкціонований витік якої може завдати шкоду особі, суспільству або державі, викликали появу у Кримінальному кодексі України нових статей, що встановлюють відповідальність за порушення порядку створення, збирання, одержання, пересилання, зберігання чи розповсюдження тієї чи іншої інформації з обмеженим доступом.

Разом зі статтями, що були успадковані від Кримінального кодексу УРСР, всі ці норми утворили інститут кримінально-правової охорони інформації з обмеженим доступом, до якого на даний час відносяться: ст. 111 «Державна зрада», ст. 114 «Шпигунство», ст. 132 «Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби», ст. 145 «Незаконне розголошення лікарської таємниці», ст. 159 «Порушення таємниці голосування», ст. 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер», ст. 168 «Розголошення таємниці усиновлення (удочеріння)», ст. 182 «Порушення недоторканості приватного життя», ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю», ст. 232 «Розголошення комерційної або банківської таємниці», ст. 232[1] «Незаконне використання інсайдерської інформації», ст. 328 «Розголошення державної таємниці, ст. 329 «Втрата документів, що містить державну таємницю», ст. 381 «Розголошення відомостей про заходи безпеки щодо особи, взятої під захист», ст. 387 «Розголошення даних оперативно-розшукової діяльності, досудового розслідування», ст. 397 «Втручання в діяльність захисника чи представника особи», ст. 422 «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості».

Проведений нами аналіз цих норм дозволяє стверджувати, що відсутність загальної концепції кримінально-правової політики у сфері забезпечення інформаційного суспільства в Україні та чітких вихідних критеріїв і реальної оцінки параметрів інформації, що повинна захищатися за допомогою кримінально-правових норм, призвели до надмірної деталізації кримінально караних правопорушень порядку доступу до такої інформації, їх розосередженості по різних розділах Особливої частини КК, неузгодженості між собою за об'єктивною стороною, структурою та санкціями. Старі норми зберегли політичне забарвлення та переваги інформаційних інтересів держави перед інформаційними інтересами окремої особи та суспільства. Крім цього, незважаючи на значну кількість таких норм, частина інформації з обмеженим доступом, конфіденційність якої

гарантована державою в інших законодавчих актах, залишилася за межами кримінально-правової охорони.

Вочевидь, існуюча на даний час система кримінально-правових норм, що встановлює відповідальність за порушення режиму таємності інформації, повинна бути оптимізована шляхом відмови від надмірної деталізації правопорушень залежно від виду інформації, що охороняється (державна, лікарська, банківська, адвокатська, комерційна, службова таємниці, таємниця усиновлення тощо), та заміни цих норм на такі, що забезпечать кримінальну охорону більш загального об'єкта.

Без чітких вихідних критеріїв та реальної оцінки параметрів інформації, що приховується, неможливо дати об'єктивну характеристику особливостям і конкретним різновидам таємниці, розробити такі заходи охорони, які були б адекватними ймовірній шкоді, нанесеній зацікавленому в її нерозповсюдженні суб'єкту в разі її розголошення або несанкціонованого доступу до неї. Тому для пошуку такого узагальнюючого об'єкта кримінально-правової охорони необхідно розглянути наукові погляди щодо класифікації таємної інформації та її поділу на види.

Насамперед розглянемо позицію прихильників теорії інформаційної революції американців Р. Кохане та Дж. Ная, які поділяють всю інформацію, що обертається в сучасному світі, на три види: вільну, комерційну та стратегічну [2].

Якщо не брати до уваги вільну інформацію, до якої науковці відносять таку, що поширюється безкоштовно, без будь-якої матеріальної компенсації (телебачення, радіомовлення, політична реклама, різного роду інформаційні акції, вільна інформація, розміщена в мережі Інтернет, тощо), то таємна інформація поділяється на комерційну та стратегічну. При цьому під комерційною мається на увазі інформація, що виробляється з метою отримання прибутку у вигляді компенсації за її використання іншими, а під стратегічною розуміється інформація, що безпосередньо пов'язана з діяльністю держави, головною характеристикою якої є специфічний режим її збирання, виробництва, зберігання та використання, а саме — режим таємності, який забезпечується силою державного примусу [3, с. 42—45].

На нашу думку, такий видовий розподіл таємниці не відповідає науковим вимогам поділу понять.

Так, за допомогою визначення поняття розкривається його зміст, а за допомогою поділу — його обсяг. Поділ поняття — це логічна операція, що дозволяє за допомогою вибраної ознаки розподілити обсяг ділимого поняття на ряд членів (підмножин). При поділі поняття його обсяг розкривається шляхом перераховування його видів (складових).

Водночас, у запропонованому цими науковцями поділі залишається за межами таємної інформації такий її вид як таємниця фізичної особи, яка не охоплюється поняттями комерційної та стратегічної інформації. В даному випадку порушено правило співрозмірності поділу, згідно з яким сума обсягів видових понять має дорівнювати обсягу ділимого (родового) поняття.

В. Лопатін пропонує умовно поділити таємниці на наступні групи: комерційну таємницю, банківську таємницю, професійну таємницю, персональні дані та службову таємницю [4, с. 37]. Проте такий поділ поняття таємниці також не можна вважати беззаперечним. За правилом поділу поняття, члени поділу повинні виключати один одного, тобто не повинні мати загальних елементів (перетинатися), оскільки, якщо поділ здійснюється не за однією підставою, то його члени не виключатимуть один одного. Професійна таємниця є більш загальним поняттям та безпосередньо включає в себе комерційну, банківську та службову таємниці. Тобто ці поняття співвідносяться між собою як загальне та конкретне і не можуть бути співставлені в одному ряду як окремі його різновиди.

І. Петрухін в основу всіх видів таємниць покладає особисту таємницю, а інші види таємниць об'єднує під одним поняттям професійної таємниці, до якої відносить: лікарську, адвокатську, банківську, комерційну, нотаріальну, журналістську, релігійну таємниці, таємницю реєстрації актів цивільного стану, таємницю усиновлення [5, с. 15].

У представлених класифікаціях звертає на себе увагу бажання науковців виокремити «професійну» таємницю, під якою ними розуміється таємна інформація, що стала відомою під час виконання професійних або службових обов'язків. Але чужа таємниця, що стала надбанням лікаря, адвоката, нотаріуса та інших осіб внаслідок виконання ними професійних або службових обов'язків, утворює, на наше переконання, конфіденційну інформацію. Зазначена особливість визначає як специфіку суб'єктивного складу і змісту, так і специфіку підстав виникнення правового режиму конфіденційної інформації щодо конкретних відомостей таємного характеру про фізичних або юридичних осіб із метою забезпечення реалізації і захисту їхніх прав і законних інтересів.

Конфіденційна інформація визначається не змістом конкретних відомостей, а їх наявністю у віданні визначених законом суб'єктів інформаційних відносин внаслідок виконання покладених на них функцій (службових або професійних повноважень). Тобто йдеться про підміну понять, оскільки конфіденційна інформація не утворює професійну таємницею. Ці поняття не є тотожними.

Професійна таємниця — це інформація, за допомогою якої представник тієї чи іншої професії досягає більш швидкого або кращого результату своєї діяльності, що надає йому перевагу перед колегами по «цеху». (Наприклад, професійною таємницею вважався склад лаку, яким Страдиварі покривав свої музичні інструменти.) Тому термін «професійна таємниця» більш близький за своїм змістом до поняття «комерційна таємниця».

Крім пошуку складових поняття таємниці, дослідники пропонують різноманітні підходи та критерії класифікації цього явища.

Так, А. Фатьянов пропонує класифікувати всі таємниці за наступними критеріями:

— за характером, змістом відомостей, що до них відносяться;

— за кількістю суб'єктів, у розпорядженні яких перебувають такі відомості, та від яких вони приховуються;

— за принципом первинності та вторинності систем обмеження доступу до інформації [6, с. 47—48].

На нашу думку, таку класифікацію не можна вважати досконалою, оскільки не зрозуміло, яким чином застосовувати запропоновані критерії та яке практичне значення матиме такий поділ. Наприклад, при класифікації державної таємниці за кількістю суб'єктів, у розпорядженні яких перебувають такі відомості, ще можна підрахувати кількість секретоносіїв у державі і навіть розмежувати їх за формою допуску, але вирахувати кількість суб'єктів, від яких вони приховуються, навряд чи можливо з огляду на те, що допуск та доступ до такої інформації обмежено як всім громадянам України, так і іноземцям, які його не отримали в установленому порядку.

О. Кулініч пропонує класифікувати таємну інформацію за способом її придбання. За цим критерієм вона поділяє таємниці, придбані на підставі цивільно-правового договору та отримані під час здійснення професійної діяльності [7, с. 79]. Такий критерій розподілу підтримують В. Ліпкан та В. Баскаков, але, зважаючи на дискусійність питання щодо виокремлення видів інформації за цим критерієм, пропонують здійснювати поділ таємної інформації на придбану безоплатно та придбану за гроші [8, с. 97].

Як вважається, така класифікація не є універсальною, тобто такою, що може бути застосована для всіх видів таємниць. Якщо поділ таємної інформації на таку, що придбана на підставі цивіль-

но-правового договору або отримана під час здійснення професійної діяльності, а також придбана безоплатно чи за гроші, ще прийнятний при класифікації комерційної таємниці, то для таємниці фізичної особи та державної таємниці він не має жодного сенсу.

Свою класифікацію таємниць пропонує нам і законодавець. Відповідно до Закону України «Про інформацію» будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація (статті 20, 21) [9].

Цей Закон не розкриває змісту понять, які складають інформацію з обмеженим доступом. Їх тлумачення дається у Законі України «Про доступ до публічної інформації», відповідно до якого конфіденційна інформація — це інформація, 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 (ст. 7). Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю (ст. 8). До службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу 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 (ст. 9) [10].

Згідно з наведеним у цьому Законі визначенням, єдиним критерієм віднесення інформації до конфіденційної є можливість її розповсюдження лише за згодою фізичної або юридичної особи та на умовах, що ними визначені. Але такий критерій віднесення інформації до конфіденційної має дуже складне практичне застосування.

Ю. Капіца з цього приводу зазначає, що незрозуміло, як буде визначатися режим конфіденційності інформації (наприклад, інформація про приватне життя), у разі коли така інформація не розповсюджується або у випадку розповсюдження не обумовлюється її конфіденційність [11, с. 119].

З метою вироблення власного уявлення щодо змісту конфіденційної інформації розглянемо декілька визначень таємниць, закріплених у різних законодавчих актах.

Відповідно до ч. 1 ст. 22 Закону України «Про адвокатуру та адвокатську діяльність» адвокатською таємницею є будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладанні договору про надання правової допомоги з передбачених цим Законом підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, зміст порад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, одержані адвокатом під час здійснення адвокатської діяльності» [12].

Згідно з Основами законодавства України про охорону праці лікарською таємницею є інформація про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина (ст. 40) [13].

Банківську таємницю становить інформація щодо діяльності та фінансового стану клієнта, яка стала відомою

банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку [14].

Всі ці таємниці об'єднує те, що таємні відомості, які утворюють їх зміст, є таємницями фізичної або юридичної особи, які стали відомі стороннім особам внаслідок виконання ними службових або професійних обов'язків. Іншими словами — це чужа таємниця.

Саме чужа таємниця, яка перебуває у віданні сторонніх осіб, яким вона стала відомою внаслідок виконання ними службових або професійних обов'язків, становить предмет та зміст конфіденційної інформації. До того часу, поки таємна інформація не стала відомою сторонній особі, вона не може вважатися конфіденційною. Але і після того, як таємна інформація стала надбанням сторонньої особи і набула для неї статусу конфіденційної, для її власника вона залишається таємною інформацією. В такому разі одна й та сама інформація одночасно існує у статусі таємної інформації фізичної особи та статусі конфіденційної інформації.

Саме з цих міркувань хибною є пропозиція В. Ліпкана та В. Баскакова щодо поділу всієї таємної інформації на конфіденційну, до якої вони зараховують будь-яку інформацію з обмеженим доступом, що не має ознак державної таємниці, та таємну — будь-яку інформацію з обмеженим доступом, що має ознаки державної таємниці [8, с. 96]. Адже за межами запропонованого цими науковцями поділу таємної інформації залишається таємниця фізичної або юридичної особи.

Оскільки для сторонньої особи розголошення конфіденційної інформації безпосередньої шкоди не завдає, то збереження цих відомостей у таємниці забезпечується шляхом законодавчого встановлення юридичної відповідальності за її несанкціоноване (без погодження з її власником) розповсюдження. Лише розпорядження власною таємницею у будь-який спосіб не тягне юридичної відповідальності (санкцій). Іншими словами, збереження в таємниці прихованої інформації є правом, а не обов'язком для її власника, який не лише визначає можливі способи її використання, а й може припинити саме існування подібного режиму без будь-яких юридичних наслідків для себе.

Власник таємної інформації має право самостійно визначати спосіб та час її оприлюднення, необхідність її охорони, коло осіб, яким надається доступ до неї, вимагати від таких осіб зберігати її у таємниці. Зі свого боку держава гарантує захист таємниці шляхом законодавчого закріплення права на таємницю, встановлює правила поводження з такою інформацією та застосовує засоби впливу щодо порушників режиму конфіденційності інформації. Отже, якщо факт передачі таємної інформації сторонній особі мав місце, то така особа стає носієм вже не власних, а чужих відомостей, тому встановлення для цієї особи режиму конфіденційності інформації буде не правом, а обов'язком, за порушення якого наступає відповідальність за діючим законодавством.

З точки зору обов'язковості правил поведінки, встановлених правовим режимом конфіденційної інформації, уявляється, що він імперативний для суб'єктів, яким ця інформація була передана або стала відомою (в силу закону, договору), і диспозитивний для суб'єктів, які цю інформацію надають і яких вона стосується.

Щодо терміну дії режиму конфіденційності повинне застосовуватися наступне правило: за терміном дії спеціальні правові режими інформації переважно є безстроковими і тривають, поки існують стосунки, об'єктом яких є режимна інформація.

Таким чином, можна виділити наступні відмінні ознаки конфіденційної інформації:

— це таємна інформація про фізичну або юридичну особу, що перебуває у володінні сторонньої особи внаслідок вико-

нання службових або професійних обов'язків;

— дійсна або потенційна цінність для власника;

— має довірчий характер і не підлягає розголошенню внаслідок можливості заподіяння шкоди її власнику;

— навмисна закритість (обмеженість доступу), регламентована та гарантована законодавством.

Кожна із зазначених ознак знаходиться в тісному зв'язку з іншими. Наявність вищевказаних ознак у сукупності характеризує ту чи іншу інформацію як конфіденційну. Відсутність будь-якої з них свідчить про неможливість надання відповідним відомостями статусу конфіденційних.

Конфіденційність не є чимось невід'ємним, властивим самій інформації в силу її природи, але конфіденційність інформації існує в силу закону або встановлюється вольовим рішенням уповноваженої на те особи на підставі закону.

Виходячи зі сказаного, можна стверджувати, що конфіденційність інформації завжди вторинна, тому суб'єкт, якому передана або стала відомою інформація, зобов'язаний дотримуватися її конфіденційності, має право використати її тільки у встановлених законом цілях, а також передавати її, якщо це прямо передбачено в законі, тільки тим особам, які визначені в законі, або з відома власника інформації.

Якщо таємна інформація про фізичну особу або комерційна таємниця стає відомою стороннім особам внаслідок виконання ними службових або професійних обов'язків, утворюється конфіденційна інформація, яка, залежно від того, кому вона стала відомою, набуває статусу банківської, адвокатської, лікарської таємниць, таємниці сповіді, усиновлення, нотаріальних дій, листування, телефонних розмов, телеграфної та іншої кореспонденції. Крім цього, конфіденційна інформація може також набути статусу слідчої таємниці або службової інформації.

Повертаючись до змісту таємної інформації у трактовці Закону України «Про доступ до публічної інформації», зазначимо, що до такого виду інформації, крім державної, законодавець відносить професійну, банківську таємницю, таємницю слідства та інші передбачені законом таємниці. Законодавець не розкриває змісту поняття «професійна таємниця», тому під цим видом інформації може розумітися як конфіденційна інформація, так і комерційна таємниця. Не розкривається і зміст поняття «інші передбачені законом таємниці», що не виключає повтору вже зазначених видів таємниць.

Віднесення до службової інформації відомостей, що були зібрані в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці, також не виключає, що до таких відомостей може потрапити інформація про приватне життя особи, комерційна таємниця та інша таємна інформація про фізичну або юридичну особу, внаслідок чого вона набуде статусу конфіденційної інформації.

Якщо підсумувати проведений нами аналіз класифікації інформації обмеженого доступу, визначеної Законом України «Про доступ до публічної інформації», то можна стверджувати, що дана класифікація містить порушення правил як поділу понять, так і вибору підстав для класифікації.

Як вже зазначалось, за правилом логіки щодо співрозмірності поділу понять, сума обсягів його складових (видових понять) має дорівнювати обсягу ділимого (родового) поняття. В той самий час, у представленій в цьому Законі класифікації інформації з обмеженим доступом всі її складові (таємна, конфіденційна та службова інформація) містять одні й ті самі види таємниць — конфіденційну інформацію, що призводить до появи зайвих членів поділу.

При класифікації дуже важливий вибір її підстав, оскільки різні підстави да-

ють різні класифікації одного і того самого поняття. Як відомо, класифікація може здійснюватися за суттєвими та несуттєвими ознаками. Розподіл предмета по групах (класах) на підставі його суттєвих ознак дає уявлення про його якості на підставі приналежності до тієї чи іншої групи класифікації. Допоміжна класифікація на підставі несуттєвих ознак не дозволяє судити про якість предмета (терміна), а лише слугує для більш легкого його пошуку.

Допущене законодавцем порушення логічного взаємозв'язку при визначенні критеріїв, які слугують для розподілу різних систематизованих рядів інформації з обмеженим доступом, призвело до одночасної присутності окремих явищ цього поняття, зокрема конфіденційної інформації, у різних систематизованих рядах.

Ми вважаємо, що підґрунтям класифікації слід обирати основу, яка не просто вказує на відмінність одного виду таємниць від іншого, а дозволяє за несхожістю характеру засобів і методів, що застосовуються, а також мети кінцевого результату звести всю різноманітність підстав систематизації до необхідних і достатніх, які дадуть можливість розмежувати однопорядкові структурні утворення та дозволять побудувати ефективну роботу з охорони різних видів таємної інформації. При цьому в основу класифікації таємної інформації має бути покладений суб'єкт, якому безпосередньо буде завдано шкоду внаслідок її несанкціонованого витоку (розголошення або втрати матеріальних носіїв такої інформації). Виходячи з цих критеріїв, ми пропонуємо поділяти всю таємну інформацію на *таємницю фізичної особи, комерційну* та *державну таємниці*.

Будь-якій таємній інформації властива персоніфікованість, тобто приналежність інформації конкретному суб'єктові права, поєднана з наявністю його інтересу або обов'язку в збереженні таємниці. Вона обумовлена тим, що збереження в таємниці конкретних відомостей здійснюється з метою унеможливлення настання потенційної шкоди, яка може бути завдана власнику таємної інформації від її поширення.

Шкода може виражатися у нанесенні як матеріальних, так і моральних, у тому числі політичних, збитків. Крім цього, метою обмеження доступу до інформації є не лише намагання запобігти шкоді, а й бажання отримати певні переваги (виграш у бою, можливість отримати певний зиск від володіння секретами вироблення конкурентоспроможної продукції). Втрата таких переваг внаслідок несанкціонованого витоку прихованої інформації також розглядається як завдання збитків (упущення вигоди). Розмір збитків залежить від цінності такої інформації, під якою слід розуміти рівень її значущості для інтересів конкретного суб'єкта інформаційних відносин.

Оскільки власниками таємної інформації можуть виступати окремі фізичні особи, певні соціальні групи (сім'я, корпорація людей, що об'єдналися для досягнення значущих для них цілей) або держава, то цінність такої інформації для різних суб'єктів соціальних відносин є різною.

Уявлення щодо цінності інформації та змістовні критерії обмеження доступу до окремих її відомостей безпосередньо формує суспільство.

Укорінені в суспільній свідомості на конкретному історичному етапі уявлення щодо пристойності тих чи інших вчинків безпосередньо впливають на зміст таємниці приватного життя, сімейних відносин та більшості форм соціально-побутового спілкування. Предметом інформації, що приховується від сторонніх осіб, є такі дійсні чи вигадані дані про осіб, їх дії або дії щодо них, які фізична особа бажає зберегти в таємниці і розголошення яких, на її думку, скомпрометує або принизить честь і гідність її чи близьких їй осіб. До таких відомостей, зокрема, можуть належати дані про інтимні сторони життя, захворювання, неблаговидні вчинки, злочинну

діяльність тощо. Цінність таємниці тут полягає у можливості збереження поваги оточення до громадянина на тому самому рівні, що і до розголошення цих відомостей.

Цінність комерційної таємниці виражається в тих можливих прибутках або збитках, що можуть бути отримані внаслідок її використання іншими, оскільки у цій сфері цінність інформації безпосередньо обчислюється у грошових одиницях.

Потреба держави у засекречуванні певних відомостей обґрунтовується необхідністю забезпечення національної безпеки, територіальної цілісності, незалежної внутрішньої та зовнішньої політики, обстоювання власних інтересів шляхом впливу на поведінку інших суб'єктів міжнародних відносин у бажаному для національних інтересів напрямі, громадського порядку або охорони здоров'я населення. При цьому обсяг відомостей, які приховуються державою, знаходиться у прямій залежності від стану політичної системи та збалансованості інтересів у суспільстві, здатності своєчасно реагувати на зміни, що відбуваються у політичній, економічній і соціальній сферах під впливом історично обумовлених закономірностей.

На наше переконання, спроба окремих науковців [15, с. 20—21] обґрунтувати найбільшу суспільну цінність державної таємниці — це намагання виправдати ситуацію, за якої держава безконтрольна в питаннях засекречування інформації, а ця сфера державно-владних повноважень не тільки виконує функцію охорони певних категорій відомостей від поширення, а й набуває політичного відтінку, перетворюючись на один із істотних елементів у механізмі державного управління.

Ми повністю поділяємо думку В. Ліпкана та В. Баскакова, що доречніше говорити не про соціальну цінність інформації, а про цінність для її власника, оскільки така інформація може не мати жодної соціальної цінності для суспільства, а для її власника має значну цінність через невідомість іншим [8, с. 97].

Поступове усвідомлення того, що будь-яка таємниця має значну цінність для її власника, призводить до того, що застосовані до охорони державної таємниці заходи безпеки беруться сьогодні за зразок при запровадженні механізмів охорони банківської таємниці, захисту персональних даних, інших інформаційних масивів. При підборі кандидатів на роботу у комерційні структури, де циркулює конфіденційна інформація, активно використовуються детектори брехні, здійснюються тривалі перевірки благонадійності майбутніх працівників таких компаній, вживаються безпрецедентні заходи із забезпечення безпеки інформації.

На цьому тлі вражає безвідповідальне ставлення держави до збереження у таємниці історій хвороб або інших матеріальних носіїв інформації, в яких відображаються відомості щодо стану здоров'я, про факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при медичному обстеженні фізичної особи. Жахливий стан фінансування закладів охорони здоров'я зводить нанівець спроби забезпечити надійну охорону такої інформації, а наміри уряду перевести історії хвороб в електронний документообіг ставлять під пряму загрозу несанкціонованого витоку цієї інформації у мережу Інтернет, знижують рівень її захищеності від стороннього втручання. В українській дійсності є чимало прикладів, коли особу, про яку стає відомим факт її тяжкої хвороби, піддавали приниженням, змушували залишити постійне місце проживання та шукати собі притулку в іншій місцевості. Оприлюднення такої інформації може призвести до звільнення особи з роботи та поставити за межу виживання.

Конституція України 1996 р. визнала людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю (ст. 3) [16]. Проте стан захищеності таємної інфор-

мації про фізичну особу та реальні можливості правового захисту у випадку її несанкціонованого розголошення свідчать про суттєве відставання правового регулювання цих суспільних відносин від задекларованої у Конституції їх значущості.

Виходом із цієї ситуації є найскоріше законодавче вироблення єдиного для всіх видів таємниць комплексу правових, організаційних, режимно-секретних, адміністративних та кримінально-правових заходів охорони секретної інформації. Держава зобов'язана взяти на себе формування єдиного механізму захисту різних видів таємної інформації, що ґрунтується на гарантуванні державою безпеки особистості, суспільства, держави. Саме у цьому напрямі повинен розвиватися правовий інститут таємниці, а науковці мають спрямувати свої дослідження на пошук аргументів для обґрунтування єдиної природи таємниці та рівноправності всіх її видів.

Підтвердженням того, що держава має однаково охороняти всі види таємниць незалежно від того, кому може бути завдано шкоду внаслідок несанкціонованого витоку інформації, є кримінальне законодавство Норвегії, де предмет шпигунства набагато ширший, ніж у вітчизняному законодавстві. Так, згідно з § 91а КК Норвегії, предметом посягання є не лише відомості, передача яких іншій державі завдасть або може завдати шкоди інтересам Норвегії, а й відомості, які становлять або можуть становити небезпеку для життя окремої людини, її здоров'я, свободи або власності [17].

Оголошення магістральною проблемою сьогодення прав людини, визнання інтересів особистості більш вагомими порівняно з інтересами суспільства і держави вимагає посилення ролі держави у захисті та охороні особи, оскільки особа не в змозі вирішувати проблему власної безпеки та поновлення прав, які порушені скоєнням злочину. Це — прерогатива держави. Зі зростанням злочинності держава повинна посилювати свої функції у сфері контролю над нею. Тільки та держава, яка здатна максимальною мірою реалізувати завдання захисту прав людини і зробити це своєю основною функцією, може називатися правовою.

У ст. 3 КК зазначено, що законодавство України про кримінальну відповідальність становить виключно Кримінальний кодекс, який ґрунтується на Конституції України та загальновизнаних принципах і нормах міжнародного права. Кримінальний кодекс виходить із принципу відповідності кримінального законодавства Конституції України та її міжнародно-правовим зобов'язанням, а тому не може як у цілому, так і в частині його окремих норм та інститутів суперечити Конституції. Таким чином, КК повинен бути максимально узгодженим з положеннями Конституції України, які мають пріоритетне значення для розвитку кримінального законодавства.

Як справедливо зазначає з цього приводу Н. Савінова, в умовах трансформації суспільних відносин, притаманних інформаційному суспільству, закон про кримінальну відповідальність у частині невідповідності Конституції України, у тому числі міжнародним договорам, ратифікованим Україною, які відповідно до вимог Конституції є частиною національного законодавства України, має бути визнаним неконституційним і скасований. Він має увібрати в себе необхідні для належного кримінально-правового забезпечення поняття і явища, якими регламентуватиметься кримінальна відповідальність за безпеку комунікації, свідомості населення та індивіда, безпеку інформації в широкому розумінні — безпеку впливів на інформацію та убезпечення від негативного впливу інформації [1, с. 269].

З урахуванням конституційного гарантування державою безпеки особистості, суспільства та держави, а також з метою формування єдиного механізму кримінально-правового захисту різних видів таємної інформації, нами пропо-

нується обрати в якості узагальнюючого об'єкта кримінально-правової охорони таке поняття, як «***чужа таємниця***», що охоплює таємницю фізичної особи, комерційну та державну таємниці. Всі інші види таємниць — це лише похідні від зазначених.

За цих умов кримінальна відповідальність за порушення порядку поводження з інформацією, несанкціонований витік якої може завдати шкоди особі, суспільству або державі, має наставати за вчинення таких злочинів.

Протиправне заволодіння чужою таємницею

1. Протиправне заволодіння чужою таємницею шляхом таємного або відкритого викрадення, підкупу, шантажу, вимагання, застосування технічних засобів негласного отримання інформації та в інший протиправний спосіб із метою оприлюднення або незаконного використання цих відомостей —

карається позбавленням волі на строк від трьох до семи років.

2. Ті самі дії, вчинені за попередньою змовою групою осіб або поєднані з проникненням до житла, іншого приміщення чи сховища, заподіянням тяжких тілесних ушкоджень —

карається позбавленням волі на строк від п'яти до восьми років.

3. Умисне розголошення або оприлюднення з використанням засобів масової інформації або мережі Інтернету незаконно отриманих відомостей, що становлять чужу таємницю, а також зберігання або використання таких відомостей, якщо такі дії заподіяли велику шкоду чи спричинили інші тяжкі наслідки —

карається позбавленням волі на строк від п'яти до десяти років.

Розголошення чужої таємниці

1. Умисне розголошення відомостей, що становлять чужу таємницю, особою, якій ці відомості були довірені або стали відомі в порядку, передбаченому законодавством, якщо такі дії заподіяли велику шкоду чи спричинили інші тяжкі наслідки —

карається позбавленням волі на строк від трьох до восьми років.

2. Ті самі дії, вчинені з корисливих мотивів, або з використанням засобів масової інформації чи мережі Інтернет —

карається позбавленням волі на строк від п'яти до десяти років.

3. Необережне розголошення відомостей, що становлять чужу таємницю особою, якій ці відомості були довірені або стали відомі в порядку, передбаченому законодавством, або особою, яка стала обізнаною з такою інформацією випадково чи в інший протиправний спосіб, та усвідомлювала, що такі відомості становлять чужу таємницю, якщо такі дії заподіяли велику шкоду чи спричинили інші тяжкі наслідки —

карається позбавленням волі на строк від двох до п'яти років.

Втрата матеріальних носіїв інформації, що містять чужу таємницю

1. Втрата матеріальних носіїв інформації, що містять чужу таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого порядку поводження із зазначеними матеріальними носіями, якщо такі дії заподіяли велику шкоду чи спричинили інші тяжкі наслідки —

карається позбавленням волі на строк від трьох до п'яти років.

2. Втрата матеріальних носіїв інформації, що містять чужу таємницю, особою, до якої зазначені матеріальні носії потрапили випадково або в інший протиправний спосіб, якщо втрата стала результатом порушення встановленого порядку поводження із зазначеними матеріальними носіями, якщо такі дії заподіяли велику шкоду чи спричинили інші тяжкі наслідки —

карається позбавленням волі на строк від двох до п'яти років.

За відсутності злочинних наслідків у

вигляді завданої розголошенням чужої таємниці чи втрати її матеріальних носіїв шкоди та відсутності умислу щодо таких наслідків, ці дії повинні вважатися кримінальним проступком і кваліфікуватися як умисне або необережне порушення правил поводження з чужою таємницею, яке призвело до витоку такої інформації.

Якщо порушення правил поводження з чужою таємницею не призвело до витоку такої інформації, ці дії мають утворювати склад адміністративного правопорушення.

Список використаних джерел

1. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти: монографія. — Київ: ТОВ «ДКС», 2011. — 342 с.

2. Johnston C. B. Global news access. The impact of new communications technologies. — Westport: Praeger publishers, 1998. — P. 85.

3. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. — Київ: Кондор, 2008. — 384 с.

4. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство. — М.: Фонд «Университет», 2000. — 428 с.

5. Петрухин И. Л. Личные тайны (человек и власть). — М.: Изд-во ИГП РАН, 1998. — 230 с.

6. Фатьянов А. А. Правовое обеспечение безопасности информации в РФ: учеб. пособ. — М.: Юрист, 2001. — 412 с.

7. Кулініч О. О. Інформація з обмеженим доступом як об'єкт цивільних відносин: дис. ... канд. юрид. наук: 12.00.03. — О., 2006. — 200 с.

8. Ліпкан В. А., Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом в Україні: монографія / за заг. ред. В. А. Ліпкана. — Київ: ФОП О. С. Ліпкан, 2013. — 344 с.

9. Закон України «Про інформацію» // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.

10. Закон України «Про доступ до публічної інформації» // Відомості Верховної Ради України. — 2011. — № 32. — Ст. 314.

11. Капіца Ю. М. Проблеми правової охорони комерційної таємниці, ноу-хау та конфіденційної інформації в праві України: реферативний огляд чинного законодавства України та практика його застосування / за ред. В. В. Цвєткова, Є. Б. Кубка. — Київ: Салком, 2000. — 296 с.

12. Закон України «Про адвокатуру та адвокатську діяльність» // Голос України. — 2012. — № 148—149.

13. Основи законодавства України про охорону праці // Відомості Верховної Ради України. — 1992. — № 49. — Ст. 668.

14. Закон України «Про банки і банківську діяльність» // Відомості Верховної Ради України. — 2001. — № 5—6. — Ст. 30.

15. Слободанюк И. А. Развитие уголовного законодательства об ответственности военнослужащих за посягательства на режим сохранности государственной и военной тайны: монография в авторской редакции. — М.: Военный университет, 2005. — 182 с.

16. Конституція України // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.

17. Уголовный кодекс Норвегии / науч. ред. и вступ. ст. д-ра юрид. наук, проф. Ю. В. Голика; пер. с норвеж. А. В. Жмени. — Санкт-Петербург: Юридический центр Пресс, 2003. — 188 с.

Семенюк Александр. Перспективы развития уголовного законодательства в сфере охраны информации с ограниченным доступом.

В статье исследуется система криминально-правовых норм, устанавливающих уголовную ответственность за несанкционированную утечку информации с ограниченным

доступом, проведен анализ научных взглядов на классификацию секретной информации и ее деления на виды, разработаны предложения по оптимизации и совершенствованию указанных уголовно-правовых норм.
Ключевые слова: *уголовная ответственность, информация с ограниченным доступом, профессиональная тайна, государственная тайна, конфиденциальная информация, коммерческая тайна, чужая тайна.*

Semenyuk Oleksandr. Prospects of criminal and law development in the sphere of protection of secret information.

The necessity of adequate answers to the new challenges of the criminal environment and legislator's awareness not only of necessity of informational freedom as a normal society, but also the protection of certain types of information, unauthorized leakage of which may cause harm to the person, society or state, ring up new articles in the Criminal Code of Ukraine which establish responsibility for violation of creating, collecting, receiving, shipping, storage or distribution of any secret information.

Along with articles that were inherited from The Criminal Code of the former USSR and Ukrainian SSR, these rules formed the institution of criminal and law protection of secret information, which currently include articles 111, 114, 132, 145, 159, 163, 168, 182, 231, 232, 232[1], 328, 329, 381 387, 397, 422.

Our analysis of these rules suggests that the absence of general concept of criminal and law policy in the field of providing informational society in Ukraine and clear opening criteria and sober estimate parameters of a realistic assessment of the information should be protected by means of criminal law, led to excessive specification of criminally punishable offenses of arrangements for access to such information, their dispersion on different sections of the Criminal Code, a mismatch between each other by objective side, structure and sanctions. Old rules saved the political overtones and advantsges of informational interests of the state over informational interests of the individual and society. In addition, despite the significant number of such rules, a part of secret information, the confidentiality of which is guaranteed by the state and other legislative acts, was left outside the criminal protection.

Obviously, present system of criminal and law principles which establish liability for violation of secrecy of information, unauthorized leakage of which may cause harm to the person, society or state, should be optimized by avoiding excessive specification of the offenses depending on the type of protected information and replacement of these standards to those that provide criminal protection of more common object.

Considering the constitutional guarantee of the security of the individual, society and state, as well as with the purpose of formation of a unified mechanism of legal protection of various types of secret information, author offers to choose as synthesis object of criminal protection such thing as «excluded secret» which covers the secret of individual, commercial and state secrets. All other kinds of secret are only derived from given ones.

In the article the system of criminal and law principles, which establish liability for unauthorized leak of secret information, is analysed, the analysis of scientific views regarding the classification of secret information and its division into different kinds is undertaken, proposals for optimization and improvement of given criminal and law principles are developed.
Keywords: *criminal liability, secret information, professional secret, state secrets, confidential information, trade secret, excluded secret.*