УДК 343.1

КОВАЛЬОВ К.Є., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ
ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ

ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТА СЛУЖБОВОЇ ТАЄМНИЦІ У СФЕРІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ЗА ЗАКОНОДАВСТВОМ ОКРЕМИХ ДЕРЖАВ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Анотація. *У статті висвітлена організація охорони оперативно-розшукової інформації в окремих країнах світу.*
Ключові слова: *державна таємниця, оперативно-розшукова діяльність, світовий досвід, інформаційна безпека, законодавство.*

Аннотация. *В статье освещена организация охраны оперативно-розыскной информации в отдельных странах мира.*
Ключевые слова: *государственная тайна, оперативно-розыскная деятельность, мировой опыт, информационная безопасность, законодательство.*

Summary. *The organization of protection of operative and intelligent information in certain countries of the world is highlighted in this article.*
Keuwords: *the state secret, operative and intelligent activity, world experience, information security, legislation.*

Постановка проблеми. У Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.15 р. № 287 [1], зазначається, що одним із пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів є реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС. Водночас, у ст. 7 Закону України “Про основи національної безпеки України” [2] визначено загрози національній безпеці України в інформаційній сфері, однією з яких є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю.

Одним із напрямів правоохоронної діяльності, яка захищена за допомогою інституту таємниць, є оперативно-розшукова діяльність, і це не є випадковістю. Адже держава завжди убезпечувала найбільш чутливі сторони свого існування саме за допомогою обмеження доступу до інформації про них. Тим більш, що в оперативно-розшуковій діяльності особливе місце займає принцип забезпечення конспірації її провадження.

Дослідженням проблем захисту інформації з обмеженим доступом займалися багато вчених, але в контексті охорони державної таємниці слід виділити роботи О.Є. Архіпова, Р.В. Корсуна, В.М. Лопатіна, В.В. Макаренка, І.М. Мейдича, А.С. Пашкова, О.В. Шамсутдінова та М.В. Шлапаченка.

Водночас, охорона державної таємниці потребує удосконалення. Зростає також і роль порівняльного кримінального права. Бажано дослідити проблему охорони інформації з обмеженим доступом і під цим кутом зору.

Метою статті є порівняльний аналіз охорони державної та службової таємниці за законодавством окремих держав для удосконалення законодавства України у цій сфері.

Виклад основного матеріалу. Французький компаративіст Рене Давид, розглядаючи право різних країн, виділяє три основні групи правових систем: романо-германську правову сім’ю, сім’ю загального права і сім’ю соціалістичного права [3, с. 40].

Для порівняння достатньо розглянути відповідне законодавство кількох країн – репрезентантів правових систем, що належать до згаданих сімей права. Перш за все, це законодавство ФРН, (романо-германська правова сім’я), Англії та США (сім’я загального права).

У Німеччині система захисту державних секретів перетинається із загальною системою захисту значущих секретів у сфері промисловості й торгівлі (промислове шпигунство) та регулюється нормами низки законів, до яких відносяться: Кримінальний кодекс, Закон про боротьбу з недобросовісною конкуренцією, Постанова про боротьбу з підкупом не посадових осіб, Федеральний закон про охорону даних тощо. Кримінальний кодекс Німеччини, наприклад, містить положення про те, що державною таємницею є факти, об’єкти й інформація, доступні лише обмеженому колу осіб, які повинні зберігатися в секреті від іноземних держав з метою недопущення спричинення шкоди зовнішній безпеці Федеративної республіки.

Удосконалення захисту державних секретів здійснюється за трьома напрямами: вдосконалення законодавства у сфері захисту державних секретів і секретів фірм; посилення органів контррозвідки та надання їм великих повноважень, у тому числі й у сфері захисту державних секретів; створення організацій “самодопомоги” в промисловості та розгортання їх діяльності.

Важливим у вдосконаленні захисту секретів під час проведення науково-дослідних робіт військового призначення в Німеччині є посилення повноважень органів контррозвідки, і, зокрема, тих її підрозділів, які здійснюють боротьбу зі шпигунством і опікуються захистом державних секретів, у тому числі й у промисловості.

У системі забезпечення захисту державних секретів у питаннях боротьби з “промисловим шпигунством” іноземних держав важлива роль відводиться об’єднанням промисловців, так званим організаціям “самодопомоги”.

До таких організацій відноситься, наприклад, “Координаційний центр по забезпеченню безпеки в промисловості”, створений у Кельні в 1969 році, який вирішує проблеми забезпечення режиму секретності в промисловості держави [11].

У ФРН інформація з обмеженим доступом може мати три ступені секретності: “цілком таємно” (Streng Geheim); “таємно” (Geheim); “конфіденційно” (VS-Vertraulich). Слід зазначити, що у ФРН до державної таємниці відносяться лише відомості, які необхідно зберігати в секреті від іноземних держав з метою недопущення завдання шкоди зовнішній безпеці Федеративної республіки. В той же час відомості, які містять інформацію про проведення оперативно-розшукових заходів, належать до службової таємниці та охороняються відповідним законодавством. Відповідальність за порушення службової таємниці встановлена у 28 розділі Кримінального кодексу ФРН. Відповідні документи, що містять службову таємницю, позначають грифом “Для службового користування” (VS nur fur den dienstgebrauch).

Якщо документи для службового користування обробляються в автоматизованих системах, то мають бути дотримані певні вимоги безпеки. А саме автоматизовану систему має бути обладнано фаєрволом, у випадку підключення до мережі Інтернет, має бути затверджений перелік осіб, які мають доступ до автоматизованої системи,

використовуватися механізми автентифікації та ідентифікації (ім’я користувача та пароль), обов’язковою є наявність Інструкції з ІТ-безпеки тощо [12, Section II (1)].

Основним джерелом кримінального права ФРН є Кримінальний кодекс, що був прийнятий 15 травня 1871 р., і діє в редакції від 13 листопада 1998 р.

Розділ 2 Особливої частини КК ФРН має назву “Зрада батьківщині та загроза зовнішній безпеці”. Ця глава складається з 13 статей, в яких, зокрема, містяться норми про відповідальність за розголошення державної таємниці (§ 95), зрадницьке або інше вивідування державної таємниці (§ 96), видачу державної таємниці (§ 97), видачу нелегальної таємниці (§ 97-a), розголошення відомостей, помилково прийнятих за державну таємницю (§ 97-b).

Відповідно до абз. 1 § 95 КК ФРН під “розголошенням державної таємниці” розуміється створення неправомочній особі доступу або публічне оголошення охоронюваної державної таємниці, що створює загрозу спричинення тяжкої шкоди зовнішній безпеці Федеративної Республіки [13].

“Неправомочною” визнається будь-яка особа, яка за родом служби чи роботи не має права володіти даними відомостями. Цією особою може буде також визнаний іноземний громадянин, якщо він не відповідає ознакам спеціального адресата (§ 94 КК ФРН), тобто не належить до іноземної розвідки чи іноземного уряду. Слід зазначити, що застосування цієї норми обмежується тими випадками, коли у винного відсутній конспіративний зв’язок із представником іноземного уряду або зрадницький умисел, інакше таке діяння кваліфікується як шпигунство (§ 94 КК ФРН).

Під публічним розголошенням розуміють особливий випадок повідомлення державної таємниці неправомочним особам, коли винний своїми діями робить таку інформацію відомою відразу великій кількості осіб.

Для притягнення до кримінальної відповідальності необхідно, щоб винний усвідомлював, що відомості, які розголошуються, є державною таємницею і що вони повідомляються неправомочній особі. Якщо ця умова відсутня, то особа до кримінальної відповідальності не притягується за відсутністю складу злочину. Необхідною умовою є також розуміння винним того, що відомості передаються саме сторонній особі, а не представникові іноземної держави. Це відповідає пануючому у німецькій доктрині визначенню умислу, сформульованому Верховним Судом ФРН: “Умисел – це воля до здійснення складу злочину при усвідомленні всіх його обставин” [14, с. 212].

Особливістю даної кримінально-правової норми є те, що законодавець не пов’язує відповідальність зі спеціальним суб’єктом. Таким чином, у § 95 КК не проводиться різниці між особами, яким відомості, що становлять державну таємницю, були довірені по службі чи роботі, і приватними особами. Це, на нашу думку, слабкий бік німецького законодавства, яке невиправдано розширює сферу кримінальної репресії за розголошення державної таємниці.

Санкція § 95 КК передбачає покарання у виді позбавлення волі на строк від 6 місяців до 5 років. За наявності обтяжуючих обставин строк зазначеного покарання зростає до 10 років. Таким чином, позбавлення волі є, в даному випадку, єдиним безальтернативним видом покарання.

У разі необережного розголошення державної таємниці дії винного кваліфікуються за § 97 КК ФРН, що має назву “Видача державної таємниці”. В абз. 1 § 97 цього Кодексу йдеться про поєднання умисного розголошення державної таємниці з необережним створенням загрози заподіяння шкоди зовнішній безпеці країни. Розголошуючи державну таємницю, особа повинна діяти умисно, тобто усвідомлювати факт розголошення й характер відомостей, що розголошуються. Щодо

наслідків розголошення її вина полягає в необережності: особа не передбачає можливості настання тяжкої шкоди для зовнішньої безпеки ФРН. Отже, можна дійти висновку, що названий злочин характеризується складною формою вини. Ця форма вини знайшла законодавче відображення в абз. 9 § 11 і сформульована так: “умисним є також діяння, що створює передбачений законом склад злочину, який щодо діяння передбачає умисел, а щодо спричиненого цим діянням спеціального наслідку вважає достатньою необережність” [12 с. 208].

Особа, яка вчинює такий злочин, передбачений абз. 1 § 97 КК, карається штрафом або позбавленням волі на строк до 5 років.

Абз. 2 § 97 КК ФРН встановлює відповідальність осіб, яким державна таємниця була довірена по службі, роботі чи за спеціальним розпорядженням відповідного державного органу [12 с. 208].

Виходячи зі змісту цієї норми, дії винного полягають у тому, що він “легковажно” робить надбанням неправомочної особи відомості, що становлять державну таємницю. Суспільна небезпечність такого злочину виражається в загрозі заподіяння тяжкої шкоди зовнішній безпеці республіки. Санкція цієї норми передбачає покарання у виді штрафу або позбавлення волі на строк до трьох років.

Якщо ж особа, яка має доступ до державної таємниці, одержує секретну інформацію від інших осіб, але не забезпечує її належної охорони, то § 97 КК ФРН не застосовується.

Особи, які вчинили діяння, передбачені § 97 КК ФРН, притягаються до кримінальної відповідальності тільки за вимогою федерального уряду, причому уряд має обґрунтувати необхідність покарання цієї особи. Як правило, потрібно встановити та вказати вид і розмір заподіяної шкоди зовнішній безпеці ФРН.

У Великій Британії існує закон з охорони державної таємниці, який має назву “Про державну таємницю” (Official Secrets Act). Цей Закон був прийнятий у 1989 р. Однак, історія законодавства з охорони державної таємниці у Великобританії сягає своїми коренями у далеке минуле. Вона бере початок з 1889 р, коли було вперше прийнято закон з аналогічною назвою.

Систему охорони державної таємниці викладено в настанові з охорони державної таємниці (Manual of Protective Security), на базі якої міністерства розробляють власні настанови.

Згідно з чинним законодавством Великобританії інформація з обмеженим доступом може мати чотири ступені секретності: “цілком таємно” (Top Secret); “таємно” (Secret); “конфіденційно” (Confidential); “для службового користування” (Restricted).

До інформації зі ступенем “цілком таємно” відносяться відомості, несанкціоноване розголошення яких може створити загрозу внутрішній стабільності Об’єднаного Королівства або дружніх йому країн; призвести до значних людських жертв; може завдати значної шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; заподіяти значну шкоду взаєминам з дружніми урядами або спричинити довгострокові збитки економіці Королівства.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей, є перелік потенційних мішеней терористів, база даних інформаторів та кримінальної розвідки тощо.

До інформації зі ступенем “таємно” відносяться відомості, несанкціоноване розголошення яких може обернутися підвищенням рівня міжнародної напруженості; серйозно зашкодити відносинам з дружніми урядами; безпосередньо загрожувати життю або завдати значної шкоди громадському порядку або безпеці та свободам особистості; завдати значної шкоди ефективності або безпеці британських чи

союзницьких сил або розвідувальним операціям; спричинити істотну матеріальну шкоду національним фінансам чи економіці та комерційним інтересам.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії, є об’єкти спеціальних операцій; інформація, яка розшифровує особу інформатора, оскільки її розголошення може загрожувати його життю.

До інформації зі ступенем “конфіденційно” відносяться відомості, несанкціоноване розголошення яких може завдати матеріальної шкоди дипломатичним стосункам, що матиме наслідком офіційний протест або інші санкції; заподіяти шкоду безпеці та свободам особистості; завдати шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; спричинити шкоду національним фінансам чи економіці та комерційним інтересам; істотно підірвати фінансову спроможність основних (великих) організацій; перешкодити розслідуванню або полегшити вчинення тяжкого злочину тощо.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії, є відомості про інформаторів, які не розкривають їх справжньої особи, проте розголошення яких може загрожувати безпеці інформаторів; відомості про спеціальні операції, розкриття яких може зашкодити розслідуванню тяжких злочинів; відомості про характер злочинної діяльності та можливі методи її припинення.

До інформації зі ступенем “для службового користування” відносяться відомості, несанкціоноване розголошення яких може зашкодити міжнародним стосункам, ускладнити забезпечення ефективності або безпеки британських чи союзницьких сил; завдати шкоди розслідуванню або полегшити скоєння злочину; завдати фінансової шкоди фізичним або юридичним особам, ускладнити управління державним сектором тощо.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії, може бути інформація, отримана від поліції іншої країни, якщо така інформація не була загальновідомою, покази (свідчення) осіб у справі, розголошення яких може зашкодити розслідуванню тощо.

Існуюча в Англії система захисту державних секретів базується на Законі “Про державну таємницю” (Official Secrets Act), що був розроблений у 1988 р., а набув чинності з 1 березня 1990 р. Цей законодавчий акт замінив раніше діючий закон про державну таємницю, прийнятий ще в 1911 р.

У новому законі конкретизовані формулювання складів злочинів, пов’язаних із розголошенням інформації, що охороняється, більш чітко подане визначення відомостей, які становлять державну таємницю, уточнені поняття збитків, що завдаються державі внаслідок розголошення тих чи інших відомостей.

Чинне кримінальне законодавство Англії розрізняє випадки розголошення державної таємниці особами, які володіють нею за своїм службовим становищем, а також особами, які не мають прямого доступу до такої таємниці.

Перші чотири статті нового закону про державну таємницю передбачають відповідальність спеціального суб’єкта (державного службовця чи підрядчика державної установи) за вчинення злочину, що розглядається. Першочергового значення набувають кримінально-правові заходи, спрямовані на захист від розголошення відомостей про всі аспекти діяльності розвідувальних і контррозвідувальних органів Великобританії.

Злочином вважається розголошення співробітниками спецслужб (у тому числі й колишніми) будь-яких відомостей про їх діяльність. Mens rea (“винна воля”) даного злочину полягає лише у намірі вчинити заборонені законом дії, оскільки для настання відповідальності за передачу секретної інформації не має значення факт спричинення шкоди безпеці та інтересам держави. Отже, владі немає потреби доводити наявність

шкоди чи збитків, завданих таким розголошенням. До кримінальної відповідальності притягується й технічний персонал спецслужб, а також службовці організацій, що виконують замовлення спецслужб, якщо вони розголошують інформацію, отриману в результаті виконання своїх обов’язків. Лише одна обставина при цьому звільняє від відповідальності – незнання, що розголошена інформація стосується діяльності спецслужб і її розголос може завдати шкоди їх діяльності (ст. 1) [15, с. 188].

З цих же підстав притягається до відповідальності особа, яка маючи у своєму розпорядженні або під своїм контролем секретні шифр, пароль, предмет, запис та інші документи, отримані у порушення законів про державні секрети або в результаті доступу до них, пов’язаного з її посадою, передала зазначені секретні матеріали тому, хто не уповноважений їх отримувати.

Розголошення відомостей щодо оборони або міжнародних відносин переслідується в кримінальному порядку, однак обвинувач (держава в особі органів прокуратури) повинен довести наявність реальних збитків (статті 2 і 3). Наприклад, при розгляді справи про розголошення інформації щодо національної оборони обвинувач зобов’язаний навести конкретні факти ослаблення бойової могутності збройних сил.

Злочином вважається також розголошення інформації, яка може бути використана злочинцями, якщо в результаті цієї дії виникає чи може виникнути будь-який з наступних наслідків: здійснюється злочин чи втеча з-під варти, ускладнюється запобігання вчиненню злочинів чи їх розслідування, виникають перешкоди в затримці чи кримінальному переслідуванні злочинців (ст. 4).

У законі встановлена кримінальна відповідальність і за дії, що сприяють розголошенню секретної інформації: недбале зберігання документів і розголошення відомостей, які полегшують несанкціонований доступ до державної таємниці, а також порушення офіційних розпоряджень, що регламентують зберігання та роботу із секретними документами (ст. 8). До кримінальної відповідальності можуть притягатися також особи, які не є державними службовцями чи підрядчиками державних установ. Насамперед це стосується працівників засобів масової інформації, зокрема журналістів, які різними шляхами прагнуть отримати секретну інформацію. Щоб домогтися засудження, сторона обвинувачення має довести, що в особи були достатні підстави вважати, що розголошена нею інформація захищена законом і що її розголошення завдасть шкоди національним інтересам країни (ст. 5). Тобто для судового переслідування необхідна наявність mens rea – прямого умислу [15, с. 388].

У законі також передбачена кримінальна відповідальність за несанкціоноване розголошення секретної інформації, якщо вона раніше була передана урядом Великобританії іншій державі чи міжнародній організації та була вперше розголошена за кордоном (ст. 6). Сторона обвинувачення має довести, що розголошена (найчастіше у журналістській публікації) інформація є державною таємницею, а її витік завдав чи міг завдати шкоди. Крім того, тут теж необхідно спиратися на наявність mens rea: обвинувачуваний повинен був знати про характер інформації, що ним розголошується, та про можливу шкоду. Недоведеність будь-якого з перерахованих фактів призводить до виправдання обвинуваченого.

Обставинами, що звільняють від кримінальної відповідальності, не можуть бути твердження обвинуваченого, що розголошення інформації не може завдати шкоди, оскільки вона вже опублікована за кордоном [14, с. 190].

Отже, при розголошенні державної таємниці сторона обвинувачення в більшості випадків має доводити наявність шкоди, завданої цим розголошенням, причому з різними категоріями інформації пов’язані різні категорії шкоди.

За розголошення відомостей, що становлять державну таємницю, передбачається покарання у вигляді тюремного ув’язнення строком до 2 років, штрафу до 2 тис. фунтів стерлінгів чи два покарання одночасно. За вчинення дій, що сприяють такому розголошенню, винний карається позбавленням волі строком до 3 місяців, штрафом до 2 тис. фунтів стерлінгів чи двома покараннями (ст. 10).

Кабінет міністрів Великобританії вживає активних заходів щодо запобігання витоку секретних відомостей через засоби масової інформації, керуючись при цьому положеннями закону про державну таємницю, а також адміністративного закону про конфіденційність. Відповідно до положень останнього уряд має право вимагати через суд першої інстанції заборони публікації певних матеріалів шляхом внесення окремої ухвали судді без зазначення осіб, щодо яких застосовується заборона. Внаслідок цього автору і видавцям можуть заборонити публікування матеріалів за кордоном. Суд має право зобов’язати ініціаторів публікації забрати рукопис з будь-якого іноземного видавництва. Уряд може вимагати від видавців і автора подати на розгляд зміст публікації і перелік використаних джерел, якщо вони бажають, аби заборона була знята.

У США система обмеження доступу до певних відомостей регулюється Указом Президента “Секретна інформація в сфері національної безпеки”, відповідно до якого в США існують три ступені секретності: “цілком таємно” (Top Secret), “таємно” (Secret) та “конфіденційно” (Confidential).

Причому, до інформації зі ступенем секретності “цілком таємно” відносяться відомості, несанкціоноване розкриття яких може завдати значної шкоди національній безпеці, до інформації зі ступенем секретності “таємно” – відомості, несанкціоноване розкриття яких може завдати значної шкоди національній безпеці, а до інформації зі ступенем секретності “конфіденційно” – відомості, несанкціоноване розкриття яких може завдати шкоди національній безпеці (Section 1.2 [16]).

До категорій інформації, яка може бути засекречена, відносяться відомості про військові плани, озброєння або операції; інформація іноземних урядів; відомості про розвідувальні заходи (включаючи спеціальні заходи), розвідувальні джерела чи методи або криптологію; іноземні відносини або закордонні заходи США, включаючи конфіденційні джерела; наукову, технологічну або економічну діяльність щодо забезпечення національної безпеки, яка забезпечує захист від міжнародного тероризму; програми США щодо безпеки ядерних матеріалів та обладнання; вразливості та можливості систем, установок, інфраструктур, проектів, планів або захисних служб національної безпеки, які забезпечують захист від міжнародного тероризму або зброї масового знищення.

Інші категорії інформації засекречувати забороняється.

Відповідно до згаданого Указу Президента США державні органи розробляють власні інструкції щодо роботи з державною таємницею.

Як правило, окремі відомості щодо проведення оперативно-розшукових заходів відносять до державної таємниці на підставі їх належності до відомостей про розвідувальні заходи (включаючи спеціальні заходи), розвідувальні джерела чи методи отримання розвідувальної інформації.

При розгляді в суді кримінальних справ може виникнути необхідність у розкритті окремих секретних аспектів оперативно-розшукової діяльності. В такому разі суди США користуються Законом “Про процедури з секретною інформацію” (Classified Information Procedures Act) (18 U.S.C. App. IV) 1980 р. Відповідно до цього закону в разі, якщо суддя вважатиме, що розкриття секретних відомостей є необхідним для вирішення питання про невинність підсудного, він має право вимагати розкриття таких відомостей.

Якщо в розкритті таких відомостей буде відмовлено відповідним державним органом, то судове переслідування припиняється. Як показує судова практика, в більшості випадків, коли виникали подібні ситуації, судове переслідування припинялося.

Крім цього, в даному контексті слід також відзначити Указ Президента США “Про структурну реформу щодо підтримання безпеки секретних мереж та обґрунтованого поширення та убезпечення секретної інформації” (Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information) від 07.10.11 р. № 13587, який присвячено захисту секретної інформації, що циркулює в комп’ютерних мережах.

Кримінальне право США, яке запозичило положення англійського кримінального права, відрізняється своєрідністю. Норми кримінально-правового характеру зібрані головним чином у розділі 18 Зводу законів США, реформованого ще в 1948 р. (це так званий Федеральний кримінальний кодекс США) [17]. В окремих штатах діють свої кодекси: КК штату Нью-Йорк 1965 р., що являє собою главу 40 Зводу законів цього штату, КК Аляски 1978 р. тощо.

У США немає єдиного підходу до законодавчого встановлення кримінально-правової охорони державних секретів. В структурі правових джерел і в класифікації норм федерального законодавства та окремих штатів спостерігається помітне розмаїття.

З одного боку, діє закон про покарання за розголошення офіційної інформації (1985), який за дане діяння передбачає покарання у вигляді штрафу в розмірі 15 тис. доларів чи трьох років тюремного ув’язнення, або обидва види покарання одночасно. З іншого боку, існує директива міністерства оборони США “Про нерозголошення важливої технічної інформації” (1984 р.), відповідно до якої винному загрожує тюремне ув’язнення або штраф – 1 млн. доларів чи на суму, що вп’ятеро перевищує вартість збитків, завданих розголошенням [18, с. 26].

Активно ведеться боротьба і з витоком офіційної інформації про діяльність американських розвідувальних служб, про їх співробітників і агентуру. Так, закон про захист особового складу розвідки (1982 р.) за розголошення зазначених відомостей передбачає штраф у розмірі до 50 тис. доларів чи тюремне ув’язнення строком до 10 років, або обидві міри покарання одночасно.

Крім зазначених нормативно-правових актів, норми федерального законодавства, що регулюють кримінальну відповідальність за злочини, пов’язані з розголошенням офіційної інформації, містяться також у розділі 18 Зводу законів США (“Кримінальне право та процес”), у розділі 50 (“Війна і національна безпека”) та в інших розділах Зводу законів. Ці норми відрізняються надзвичайною казуїстичністю, особливо при перерахуванні секретних об’єктів або способів злочинних посягань на державну таємницю.

Так, федеральний Звід законів у § 793 передбачає кримінальну відповідальність за умисне повідомлення, передачу, надіслання матеріалів чи інформації щодо національної оборони “якій-небудь особі, не уповноваженій на її одержання”, або спробу чи сприяння вчиненню таких дій, якщо особа “має підстави вважати, що це завдасть шкоди Сполученим Штатам чи стане на користь іноземній державі” [19, с. 40].

Для цього складу злочину характерним є спеціальний суб’єкт: особа, яка на законних підставах має доступ, контролює чи володіє довіреними їй відповідними матеріалами чи інформацією.

Для притягнення до кримінальної відповідальності за розголошення інформації щодо національної оборони, намір завдати шкоди не потрібний. Достатньо того, що обвинувачений усвідомлював важливість інформації, оскільки в даному випадку, як заявив

юридичний комітет Сенату, “йдеться про профілактичні заходи, щоб секретний матеріал не міг потрапити до ворога, а не про боротьбу з активним шпигунством” [20, с. 224].

Крім того, у федеральному законодавстві встановлена кримінальна відповідальність за необережне (“через грубу недбалість”) видалення з місць зберігання чи передачу будь-якій неуповноваженій особі зазначених у § 793 d матеріалів чи інформації або неповідомлення вищестоящій посадовій особі про таке видалення чи передачу при вказаних вище суб’єктивних ознаках, тобто маючи підстави вважати, що це завдасть шкоди Сполученим Штатам чи стане у нагоді іноземній державі. Суб’єктом у даному випадку виступає як особа, якій довірена або котра володіє чи контролює таку інформацію, тобто спеціальний суб’єкт (§ 793 f Зводу законів США), так і особа, яка незаконно володіє, має доступ чи контролює інформацію оборонного характеру, тобто загальний суб’єкт (§ 793 e) Зводу законів США).

Кожне з названих діянь тягне за собою покарання у вигляді штрафу в розмірі до 10 тис. доларів чи тюремного ув’язнення на строк до 10 років, або обидва покарання одночасно.

Федеральне законодавство передбачає кримінальну відповідальність також за незаконне фотографування або зарисовку важливих оборонних об’єктів, за публікацію або продаж таких фотографій, малюнків тощо. Згідно з §§ 795-797 Зводу законів США порушники цих правил, незалежно від їх суб’єктивних намірів чи “підстав вважати”, можуть бути позбавлені волі на строк до 1 року або оштрафовані на 1 тис. доларів.

У федеральному законодавстві США встановлена також кримінальна відповідальність за розголошення службової необоронної інформації, про яку йшлося вище. Особливому захисту підлягають коди, шифри, криптографічні системи, різні апарати та пристрої, що використовуються для забезпечення секретності інформаційних зв’язків США чи інших держав. “Свідоме і добровільне” розкриття відповідних відомостей не уповноваженій на ознайомлення з ними особі, а також їх публікація чи будь-яке використання на шкоду інтересам США караються позбавленням волі на строк до 10 років чи штрафом (§ 796 Зводу законів США). Такому ж покаранню підлягає винна особа за публікацію або розкриття будь-якій особі кодів чи змісту дипломатичного листування (§ 952 Зводу законів США). Окремо регулюється охорона секретів, пов’язаних з дослідженнями в галузі атомної енергії (§§ 2271-2281 розділу 42 Зводу законів США).

Федеральне законодавство і КК штатів містять також загальні і спеціальні норми про різного роду зловживання службовим становищем і незаконне поширення та використання інформації. При цьому суб’єктами посадових злочинів можуть бути не тільки так звані публічні посадові особи, але й звичайні службовці та наймані робітники органів публічної адміністрації, публічних корпорацій і державних банків. Суб’єктами посадових злочинів можуть бути також і будь-які інші особи.

У главі 93 розділу 18 Зводу законів США особливу групу зловживань становить діяльність чиновників у сфері використання службової інформації.

Так, вчиняє злочин, передбачений § 1902, посадова особа, службовець чи будь-яка особа, яка діє від імені США, департаментів або представництв, якщо вона в силу свого службового становища чи посади, володіючи якою-небудь інформацією, що має значення для торгівлі США та ринкової діяльності, свідомо й неуповноважено передає її особі, яка відповідно до закону або посадової інструкції не повинна отримувати таку інформацію. Цей злочин карається штрафом до 10 тис. доларів або (і) позбавленням волі на строк до 10 років. До цієї ж групи посадових злочинів належить і поширення інформації щодо діяльності Корпорації фінансової реконструкції (§ 1904). За такий злочин передбачене покарання у вигляді штрафу до 10 тис. доларів або (і) позбавлення волі на строк до 5 років.

Крім зазначених вище випадків розголошення спеціальної інформації, глава 93 (§ 1905) містить норму про відповідальність за розголошення секретних відомостей загального характеру. Відповідно до цієї норми, якщо посадова особа чи службовець державних установ США, що за родом своєї служби володіє секретною інформацією, пов’язаною з проваджуваним розслідуванням, даними анкет або секретами торгівлі, управління, стилю роботи, даними про персонал, устаткування, статистичними даними, сумами чи джерелами доходів, прибутками чи витратами будь-якої особи, фірми, компанії, корпорації, неуповноважено опубліковує, розкриває, розголошує чи будь-яким іншим способом поширює таку інформацію, то вона карається штрафом у розмірі до 1000 дол. або позбавленням волі строком до 1 року. Особа, засуджена за вчинення цього злочину, повинна бути звільнена з посади чи з місця роботи.

Очевидно, що система нормативних актів США в галузі охорони секретної інформації надто розгалужена, складна і громіздка, що, однак, пояснюється особливостями системи загального права, до якої належить і американське право. У законодавстві США існує не одна, як в Україні, а досить велика кількість кримінально-правових норм, які передбачають відповідальність за розголошення державної таємниці. Причому критерієм диференціації даних норм виступає, насамперед, предмет злочину. Інакше кажучи, кожній категорії офіційної інформації відповідає окрема норма федерального кримінального законодавства. Автори вважають, що дані положення американського законодавства неприйнятні для вітчизняної правової системи, особливо, якщо враховувати, що санкції аналізованих кримінально-правових норм США, котрі передбачають винятково великі розміри покарань, практично ідентичні [21].

Висновки.

Незважаючи на різницю в правовому регулюванні захисту інформації, яка є державною таємницею у Великобританії, США, ФРН, інформація про проведення конкретних оперативно-розшукових заходів та залучення осіб до конфіденційного співробітництва має обмежений доступ за законодавством цих країн. Для зазначеної інформації передбачено особливий порядок отримання, обробки, зберігання, захисту та розсекречування. В законодавстві цих країн процедурні питання роботи з такою інформацією схожі.

На підставі аналізу законодавства Великобританії та США слід дійти висновку, що для сім’ї загального права (Великобританії та США) характерним є більш докладні приписи щодо віднесення тієї чи іншої правоохоронної інформації до державної таємниці. Дана обставина зумовлена прецедентом англо-саксонської системи права, яка тяжіє до конкретизації судових рішень (з питань охорони оперативно-розшукової інформації), що можуть бути прийняті в рамках тих чи інших суспільних відносин. Законодавчий захист державної таємниці в США близький до британського в плані диференціації відповідальності залежно від категорії розголошеної інформації. Подібність полягає також у тому, що суб’єктами розголошення державної таємниці можуть бути особи, які не мають доступу до таких відомостей, тобто так звані приватні особи. При цьому американське законодавство розмежовує умисне й необережне розголошення державної таємниці та розглядає їх у рамках окремих правових норм.

Кримінальне законодавство ФРН не пов’язує відповідальність за розголошення державної таємниці зі спеціальним суб’єктом.

Таким чином, вважаємо, що виявлені у результаті порівняння особливості законодавства досліджених країн можуть бути враховані під час удосконалення законодавства України у сфері охорони інформації з обмеженим доступом.

Використана література

1. Стратегія національної безпеки України : Указ Президента України від 26.05.15 р. № 287/2015 // Офіційний вісник України. – 2015. – № 43. – Ст. 1353.

2. Про основи національної безпеки України : Закон України від 19.06.03 р. // Офіційний вісник України. – 2003. – № 29. – Ст. 1433.

3. Давид Р. Основные правовые системы современности / Р. Давид. – М., 1988. – С. 40.

4. О государственной тайне : Федеральный закон РФ от 21.07.93 г. / Российская газета. – № 182. – 21.09.93 г.

5. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти : Постановление Правительства РФ от 03.11.94 г. № 1233 / Собрание законодательства РФ. – 2005. – № 30 (ч. II). – Ст. 3165.

6. Об утверждении перечня сведений конфиденциального характера : Указ Президента РФ от 06.03.97 г. № 188 / Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

7. Перечень сведений, отнесенных к государственной тайне : Указ Президента РФ от 30.11.95 г. № 1203 / Российская газета. – № 246. – 27.12.95 г.

8. Комментарий к Уголовному кодексу Российской Федерации ; отв. ред. В.И. Радченко ; науч. ред. А.С. Михлин. – М. : Спарк, 1999. – 862 с.

9. Уголовный кодекс Российской Федерации : постатейный комментарий. – М. : Зерцало, Теис, 1997. – 792 с.

10. Шамсутдінов О.В. Відповідальність за розголошення державної таємниці за новим кримінальним законодавством України // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – № 2. – С. 22-26.

11. Executive Order 13526 Classified National Security Information, December 29, 2009. – Режим доступу : http://edocket.access.gpo.gov/2010/pdf/E931418.pdf

12. Instruction sheet on the Handling of Protectively Marked Information Classified VSNUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED). – Режим доступу : https://www.bsi.bund.de/ SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSMerkblattEnglisch_pdf.pdf?__blob=publicationFile

13. Уголовный кодекс ФРГ. – М. : Изд-во “Зерцало”, 2001. – 208 с.

14. Хавронюк М.І. Кримінальне законодавство України та інших держав континентальної Європи : порівняльний аналіз, проблеми гармонізації / М.І. Хавронюк : монографія. – К. : Юрисконсульт, 2006. – 1048 с.

15. Лейленд П. Кримінальне право : злочин, покарання, судочинство. – (Англ. підхід) / П. Лейленд . – К. : Основи, 1996. – 207 с.

16. Кримінальне право України. Загальна частина ; за ред. М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – К.-Харків : Юрінком Інтер-Право, 2002. – 416 с.

17. Federal Criminal Code and Rules as amended to February 1, 1991. – St. Paul., 1991. – P. 953-1044.

18. Бантишев О.Ф. Як довести, що ти – не шпигун? / Політика і час. – 1994. – № 8. – С. 24-28.

19. Уголовное право Соединенных Штатов Америки : сб. нормативных актов ; сост., отв. ред. И.Д. Козочкин. – М. : Изд-во Ун-та дружбы народов, 1986. – 160 с.

20. Никифоров Б.С. Современное американское уголовное право / Б.С. Никифоров, Ф.М. Решетников. – М. : Наука, 1990. – 256 с.

21. Леонов Б.Д. Особливості відповідальності за злочини у сфері охорони державної таємниці за кримінальним правом деяких зарубіжних держав : порівняльно-правова характеристика : навч. посібник / Б.Д. Леонов, О.В. Шамсутдінов. – К. : Наук.-вид. відділ НА СБУ, 2009 – 92 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~