УДК 355.45:343.1

**КОВАЛЬОВ К.Є.**, старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1243-3973.

# ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ

***Анотація.*** *Стаття присвячена питанням обігу інформації з обмеженим доступом. Досліджуються проблеми, пов'язані з обігом інформації з обмеженим доступом в Україні, та аналізується міжнародний досвід у сфері захисту інформаційних ресурсів.*

***Ключові слова:*** *державна таємниця, інформація з обмеженим доступом, міжнародний досвід, інформаційна безпека, законодавство.*

***Summary.*** *The article is devoted to the circulation of restricted information. The problems related to the circulation of restricted information in Ukraine are studied, and the international experience in the field of information resources protection is analyzed.*

***Keywords:*** *state secret, restricted information, international experience, information security, legislation.*

***Аннотация.*** *Статья посвящена вопросам циркуляции информации с ограниченным доступом. Исследуются проблемы, связанные с оборотом информации с ограниченным доступом в Украине, а также анализируется международный опыт в области защиты информационных ресурсов.*

***Ключевые слова:*** *государственная тайна, информация с ограниченным доступом, международный опыт, информационная безопасность, законодательство.*

**Постановка проблеми.** Аналіз наукових та практичних матеріалів, а також нормативно-правових актів стосовно інформації з обмеженнями у доступі та інтелектуальної власності, як її похідної і контррозвідувального забезпечення їх охорони та захисту (протидії конкурентній розвідці, або промисловому шпигунству – отримання недоступної інформації про економічну діяльність конкурентів) є актуальною і полягає у необхідності забезпечення захисту інформаційних ресурсів з обмеженим доступом.

Для вирішення вказаного завдання, контррозвідувальним підрозділам (умовне найменування, яке нами приймається для скорочення терміна і під яким розуміються органи з протидії промисловому шпигунству та конкурентної розвідки), необхідно мати повний перелік інформаційних ресурсів, які мають грифи обмеження і лише на їх основі визначати систему відповідних заходів з їх забезпечення.

При цьому важливим є те, що за радянського періоду та в останнє десятиріччя 20 століття в Україні державою забезпечувався ефективний захист лише таємної інформації, котра завжди була її власністю.

На нашу думку, необхідно більш детально розглянути та обґрунтувати вирішення зазначеної проблеми.

**Результати аналізу наукових публікацій.** Дослідженням проблем захисту інформації з обмеженим доступом займалися такі вчені, як: О.Є. Архіпова, О.Ф. Бантишева, Р.В. Корсун, Б.Д. Леонов [1], В.М. Лопатін, В.В. Макаренка, І.М. Мейдич, А.С. Пашкова, А.В. Савченка, М.І. Хавронюк, О.В. Шамсутдінова, В.М. Шлапаченка та ін.

Проте, як вважаємо, в сучасних умовах захист інформації з обмеженим доступом потребує удосконалення. Тому є необхідність дослідити проблему захисту інформації з обмеженим доступом контррозвідувальними органами.

**Метою статті** є удосконалення захисту інформації з обмеженим доступом на підставі аналізу нормативно-правових актів з охорони інформації з обмеженнями у доступі, зокрема у сфері інтелектуальної власності.

**Виклад основного матеріалу.** Слід зазначити, що безпека будь-якої соціальної одиниці (держави, організації, підприємства) в першу чергу залежить від здатності державного механізму забезпечити керованість економічних перетворень, політичного і суспільного будівництва та багатьох інших факторів. Але, в першу чергу, державний механізм повинен чітко визначити і передбачати внутрішні та зовнішні загрози, які виникають, чи в найближчому майбутньому можуть виникнути на шляху його розвитку. Лише за першої умови додатково може виникнути необхідність додаткової охорони та захисту такого роду інформаційних масивів.

Однією з найбільш важливих складових діяльності із забезпечення безпеки держави, суспільства та особи є розвідувальна діяльність спецслужб, яка здійснюється безперервно. Практика діяльності СБ України свідчить про те, що "масштаб збитків, які несе Україна внаслідок тільки іноземного шпигунства, не піддається оцінці. Є всі підстави остерігатися, що цей чинник може стати діючим на довгий термін". Як би не відрізнялися точки зору на суть розвідувальної діяльності, а саме на характеристику її основних структурних елементів – мету і об'єкт. Головна мета розвідувальної діяльності – це отримання інформації з обмеженим доступом про сторону, у відношенні якої ведеться розвідка, і саме яку ми маємо всі підстави називати розвідувальною інформацією. Головним завданням, сутністю розвідувальної діяльності є здобування саме "закритої" інформації. Адже використання спеціальних, досить дорогих у матеріальному плані сил та засобів ведення розвідки для здобування інформації, яка слабко охороняється, або недостатньо захищена, є занадто дорогою забаганкою. Не потребує великих зусиль обґрунтування відповіді на питання "а хто ж протидіє розвідці?". Звичайно ж контррозвідка. Тобто спеціалізована структура, головним завданням якої є не допустити витік інформації, на яку ведеться полювання конкурентами. Розвідувальні органи іноземних держав завжди цікавила, цікавить і буде цікавити "секретна" інформація загального характеру про: політичний потенціал України; плани реалізації політичної стратегії; пріоритетні інтереси в сфері політичних відносин; зовнішньоекономічні зв'язки; економічні систему й потенціал України; плани з реалізації економічної стратегії; військовий потенціал України; зовнішні військово-політичні відносини і військово-стратегічні позиції; військово-стратегічні плани вищого військового командування та інші [2].

Перерахована інформація, у залежності від її призначення зосереджується за зазначеними сферами діяльності держави на наступних об'єктах:

- *у політичній сфері:* державні органи; органи управління зовнішньополітичною діяльністю; органи державної безпеки; органи, що здійснюють адміністративно-політичні функції в країні (у тому числі органи правопорядку); суспільно-політичні організації, і насамперед організації, що здійснюють міжнародні зв'язки; міжурядові політичні організації;
- *в економічній сфері:* державні органи, що здійснюють планування і керівництво економікою й окремими її галузями; державні установи, що планують і здійснюють зовнішні економічні зв'язки; міжурядові організації у сфері економічних відносин; головні підприємства промисловості, транспорту і зв'язку; наукові установи, що ведуть дослідження в галузі економіки тощо;

- *у військовій сфері:* центральні управління Міністерства оборони України, Генеральний штаб, штаби видів збройних сил, стратегічних угруповань військ, об'єднань, з'єднань і частин; об'єднані військові організації; військові частини, оснащені новими видами зброї і бойової техніки, арсенали і склади їх зберігання; установи, що займаються науково-дослідними і дослідно-конструкторськими роботами в сфері озброєння і військової техніки, іспитові полігони; засоби закритого оперативного зв'язку Міністерства оборони; підрозділи, що займаються стратегічними військовими перевезеннями тощо;

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

Зазначені відомості секретного змісту викладені у Зводі відомостей, що становлять державну таємницю [3].

Загальну систему завдань контррозвідки в найбільш загальному вигляді можна визначити як виявлення, попередження і припинення розвідувальної діяльності, що проводиться у виді агентурної і технічної розвідки, а також розвідки з використанням легальних можливостей, спрямованої на одержання секретних відомостей, у політичній, економічній, військовій і науково-технічній сферах діяльності України, що знаходяться на фізичних об'єктах зазначених сфер; виявлення, попередження і припинення розвіддіяльності, яка проводиться, в основному, у виді агентурної розвідки, спрямованої на одержання секретної інформації від секретоносіїв, та – технічної розвідки, спрямованої на одержання інформації з каналів зв'язку.

Таким чином, одним із найбільш пріоритетних видів діяльності контррозвідки – це протидія агентурній розвідці, тому що її діяльність спрямована на здобування інформації про стратегічні плани держави, її органів, організацій і окремих осіб у реальному часі, що можуть дати також інші види розвідки, а особливо на перспективу. Це підтверджується розвитком подій у сучасному світі [4 – 13].

Отже, нами підтверджується актуальність захисту "таємниць" контррозвідкою, котра, в сучасних умовах забезпечується комплексом, а не системою заходів на державному рівні.

Цікавими з цього приводу є висновки ряду фахівців стосовно призначення органів контррозвідки закордонних країн у системі захисту засекреченої інформації й діяльності: "Захист секретної інформації й діяльності, витік або розголошення яких може завдати шкоди національній безпеці, покладено на міністерства, відомства й організації, які несуть повну відповідальність за схоронність науково-дослідних і дослідно-конструкторських розробок, передових технологій, зразків пріоритетної промислової продукції, як у цивільній, так і військовій сферах.

У США, зокрема, це завдання покладене на Міністерство юстиції й Управління по нагляду за забезпеченням безпеки інформації. У ФРН відповідальність за організацію й забезпечення режиму таємності на підприємствах і в науково-дослідних установах покладена на Міністерство економіки.

Завдання контррозвідувальних органів закордонних країн із захисту засекреченої інформації й діяльності від витоку або несанкціонованого розголошення визначається: розробкою загальних рекомендацій із забезпечення таємності діяльності відомчих служб безпеки; перевіркою осіб з метою оформлення допуску до секретної інформації й виробництв; організацією підбору, підготовки й навчання співробітників служб безпеки промислових підприємств і державних установ; співробітництвом з адміністрацією й службами безпеки відомств, корпорацій і фірм по запобіганню витоку промислових і інших секретів; перевіркою ефективності задіяних систем забезпечення безпеки інформації й діяльності від витоку або несанкціонованого розголошення; наданням допомоги в

проведенні технічних заходів, спрямованих на забезпечення безпеки секретної інформації й матеріалів; інформуванням адміністрації відомчих служб безпеки, громадськості про форми й методи роботи спеціальних служб; обміном інформацією із зацікавленими організаціями з питань поліпшення захисту секретів і підготовки пропозицій в органи виконавчої влади для прийняття управлінських рішень; розслідуванням випадків розголошення або витоків засекреченої інформації або діяльності, що призведе до збитків інтересам національної безпеки".

Достатньо важливим елементом у протидії розвідувальним спрямуванням виступає сфера так званого військово-технічного співробітництва, яка включає до свого складу обмін та торгівлю військовими технологіями та технологіями подвійного використання.

Таким чином, у сучасному процесі розвитку міжнародного науково-технічного співробітництва із промислово розвиненими країнами питання, пов'язані з купівлею-продажем технології, що включає передачу знань, науково-технічного, комерційного й управлінського досвіду ("ноу-хау"), набувають особливої актуальності і вимагають комплексного врегулювання, насамперед на національному рівні.

У зв'язку з переходом до ринкової економіки в Україні прийнято пакет важливих законів (про власність, підприємництво, інвестиції, валютне регулювання, банківську діяльність, спільні підприємства тощо). На цьому фоні також необхідно налагодити ефективний захист майнових інтересів власників "ноу-хау" не тільки в процесі співробітництва із закордонними країнами, але й в Україні.

Промислово розвиненими країнами, зокрема ФРН, США, Великобританією, Канадою, Японією та Швейцарією, накопичений великий законодавчий досвід у регламентуванні відносин в області захисту комерційної таємниці. Тому вивчення й аналіз форм правового забезпечення майнових інтересів власників торговельних секретів, "ноу-хау" в цих країнах дозволяє більш цілеспрямовано й продуктивно підійти до моделювання спеціального законодавства, відсутнього на даний час в Україні. У США діє спеціальне законодавство, що поєднує правила поведінки зацікавлених осіб в галузі використання торговельних або ділових секретів. У Великобританії та США для рішення спорів сторін залучаються прецедентні судові й адміністративні рішення. У ФРН (країна з кодифікованим правом) відносини регулюються правилами, включеними в закони, що ставляться до різних законодавчих галузей [14, с. 18-48].

У сучасних умовах Україна потребує удосконалення заходів із взаємодії зазначених органів щодо координації їх зусиль у сфері економічних секретів, а також у формуванні системи комплексного захисту державної й комерційної таємниці. Вона має 4 групи об'єктів: особливо важливі оборонні об'єкти з державною формою матеріальної й інтелектуальної власності, на яких зосереджують державні секрети; оборонні об'єкти, що підлягають конверсії; підприємства недержавного сектора, на яких розміщуються оборонні замовлення; недержавні підприємства із приватною формою власності, на яких охороняються відомості, що становлять комерційну таємницю (інтелектуальну власність підприємства).

Участь контррозвідки як спецслужби в захисті комерційної таємниці на таких підприємствах у випадку протиправних зазіхань на цінну конфіденційну інформацію з боку іноземних розвідок і промислових шпигунів повинна ефективно регулюватися нормативно-правовими актами на відміну від сучасності [15, с. 49-50].

З цього приводу показовим є аналіз сучасного стану нормативно-правового закріплення захисту інформації та інтелектуальної власності у нормах державних та недержавних структур України на основі якого можливе удосконалення їх нормативно-правового регулювання за визначеними вище напрямками.

Визначений Декларацією про незалежність, Конституцією та Законом України "Про основи національної безпеки України" курс на відродження української державності, побудови соціальної та демократичної держави покладає на СБ України забезпечення політичної, економічної, науково-технологічної, соціальної, воєнної, інформаційної та екологічної безпеки. Вказане акцентується рішеннями СБ України, що закріплені в низці основних, базових нормативних документів.

Тому визначення завдань контррозвідки із забезпечення інформаційної безпеки держави та захисту інтелектуальної власності в Україні в межах своєї компетенції у сучасних умовах набули крайньої актуальності.

Досить актуальною для України на цей час визначається проблема захисту власного інформаційного простору та національних інформаційних ресурсів.

Однак, як і в попередні роки повторюються помилки, що були закладені раніше, але визначається необхідність сприяння державних органів керівникам відповідних структур у охороні державної таємниці, а також іншої інформації з обмеженим доступом, що є власністю держави.

У Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.15 р. № 287 [16], 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, ст. 7 Закону України "Про основи національної безпеки України" [17], визначено загрози національній безпеці України в інформаційній сфері, однією з яких є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю.

Сучасний стан правової регламентації захисту інформації з обмеженим доступом в Україні визначається прийняттям останнім часом Законів України "Про інформацію", "Про доступ інформації" та "Про державну таємницю".

Схематично поділ інформації за режимом доступу відповідно до цих законів включає в себе три такі категорії: конфіденційна, таємна і службова інформація.

*Конфіденційна інформація.* Згідно ст. 7 Закону України "Про доступ до публічної інформації" – 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" [*].

*Таємною є інформація з обмеженим доступом*, яка має вищий, порівняно з іншими категоріями утаємниченої інформації, ступінь захисту, оскільки її розголошення однозначно спричинить завдання шкоди певній особі, суспільству, державі. До таємної інформації належить державна таємниця, професійні таємниці (адвокатська, лікарська тощо), таємниця слідства та інші види таємної інформації, які визначені спеціальними законами.

*Службова інформація* запроваджена як нова категорія інформації з обмеженим доступом, згідно ст. 9 Закону України "Про доступ до публічної інформації". До такої інформації належать відомості:

---

[*] *Прим. від ред.* Згідно чинного Державного стандарту України "Технічний захист інформації. Терміни та визначення" від 1997 р. (ДСТУ 3396.2-97): *"**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"* (див. [19]). Тобто мова йде про тріаду повноважень права власності окремих осіб. При цьому, будь-який Державний стандарт України є нормативно-правовим, законодавчим актом.

1) що містяться 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) зібрані в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять службову інформацію, присвоюється гриф "для службового користування". Доступ до таких документів надається відповідно до ч. 2 ст. 6 Закону України "Про доступ до публічної інформації".

Головною метою діяльності СБ України визначаються організація та забезпечення захисту інтересів України і її громадян від розвідувально-підривної діяльності спецслужб іноземних держав, організацій, груп та окремих осіб, сприяння вищим органам влади України в реалізації курсу держави на зміцнення її оборонного та економічного потенціалу.

До основних, пріоритетних завдань контррозвідки у захисті національних інтересів традиційно відноситься захист науково-технологічного потенціалу України; захист інтелектуального та наукового потенціалу від витоку за межі України (висококваліфікованих фахівців оборонного комплексу); захист від несанкціонованої передачі за кордон інформації, що становить державну таємницю, та конфіденційної інформації, яка є власністю держави, і витік якої може завдати шкоди інтересам України.

Виходячи з викладеного, цілком обґрунтованим є висновок, що захист інформаційної сфери України є пріоритетним для СБ України, тобто захист національного інформаційного простору є одним із пріоритетних національних інтересів України, як і проведення наукових досліджень, підготовка навчально-методичних видань стосовно оперативних та законодавчих засад захисту держави в інформаційній сфері, з питань забезпечення ефективних і оптимальних шляхів його організації.

Основними напрямами діяльності СБ України у сфері захисту економічного, науково-технічного та оборонно-промислового потенціалу України, традиційно вважається здійснення заходів щодо протидії спрямуванням спецслужб іноземних держав до пріоритетних науково-технічних програм та розробок у сфері створення новітніх систем і зразків озброєння та військової техніки, недопущення фактів витоку інформації, яка становить державну таємницю та передбачену законом конфіденційну інформацію; здійснення заходів з нейтралізації загроз національній безпеці в інформаційній сфері.

Невід'ємною складовою економічної безпеки є надійність захисту державної таємниці та службової інформації.

Однією з головних загроз економічній безпеці держави є можлива втрата технологічної незалежності України, наукових шкіл, надбань та пріоритетів внаслідок комерціалізації і переорієнтації вітчизняних наукових центрів на іноземного замовника, витоку перспективних технологій і інтелектуальної власності тощо.

Захист економічного, науково-технічного і оборонно-промислового потенціалу держави забезпечується: захистом державної таємниці, пріоритетних оборонно-промислових та науково-технічних розробок, сприянням збереженню науково-технічного потенціалу держави, сприянням у порядку, передбаченому чинним законодавством, підприємствам, установам, організаціям у збереженні комерційної та іншої визначеної законом таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України, організацією і проведенням на цій основі заходів щодо виявлення спрямувань та

обмеженням доступу спецслужб, організацій та окремих представників іноземних держав до них тощо.

Аналіз стану реалізації положень щодо діяльності СБ України за період з проголошення незалежності до теперішнього часу засвідчив, що потреба у концептуальній оцінці адекватності роботи контррозвідки загрозам державній безпеці в інформаційній сфері вимагає вжиття невідкладних заходів організаційного та оперативного характеру з метою створення єдиного механізму, який дозволяв би цілеспрямовано впливати на них специфічними засобами.

Потребують врегулювання питання забезпечення оборонно-промислового комплексу, захисту конфіденційної інформації, що є власністю держави, надійного захисту відомостей, що становлять державну таємницю (своєчасне виявлення, попередження і припинення фактів витоку секретних відомостей та усунення причин, що створюють передумови до цього).

Все зазначене вище є вкрай важливим для подальшого удосконалення забезпечення охорони та захисту інформації з різними обмеженнями у доступі.

Отже, для удосконалення характеристик системи захисту інформаційної сфери України та її складової – системи захисту інтелектуальної власності необхідно систематизувати та упорядковувати за змістом. Це також підтверджується рядом проблем у забезпеченні охорони та захисту інформації з відповідними грифами.

Детальний аналіз положень доступних для загального доступу джерел, як наукового, так і нормативного змісту дає нам підстави говорити про необхідність забезпечення захисту контррозвідкою всього переліку “таємниць” (інформації з обмеженим доступом), а саме: “службової таємниці”, “комерційної таємниці”, “ноу-хау”, “банківської таємниці”, “інформації про громадян” (персональних даних), “адвокатської таємниці”, “професійної таємниці”, “нерозкритої інформації” тощо, інформація у яких не є державною таємницею.

Тобто на даному етапі гостро постало питання стосовно проблем оцінки захищеності секретної інформації.

З метою оцінки захищеності інформації необхідно оцінити комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню інформації та втратам її матеріальних носіїв. Відпрацьовані критерії захищеності інформації дозволять забезпечити законність та об’єктивність оцінки стану захищеності інформаційних ресурсів. Це дасть змогу отримати “орієнтири” для планування роботи із підвищення рівня захищеності інформації. А для цього потрібен механізм визначення стану захищеності інформації з обмеженим доступом на підприємствах та установах.

Безперечно, це сприятиме ефективному вирішенню проблем профілактики адміністративних порушень законодавства про державну та інші види таємниць. Тобто, основними причинами вчинення адміністративних порушень законодавства про державну таємницю є елементарне незнання секретоносіями норм чинного законодавства про державну таємницю, що зумовлюється відсутністю належної та доступної системи професійного навчання секретоносіїв [18, с. 152].

Кримінальний Кодекс України встановлює відповідальність за значну кількість злочинів, які порушують цілісність, достовірність, законну приналежність, конфіденційність та (або) доступність інформації.

**Висновки.**

З метою попередження адміністративних правопорушень у сфері охорони державної таємниці необхідно поліпшити фінансування витрат на здійснення діяльності, пов’язаної з державною таємницею; удосконалити регіональну систему підготовки та

перепідготовки працівників режимно-секретних органів; посилити вимоги до перевірки рівня знання секретоносіями законодавства про державну таємницю та правил секретного діловодства, а також збільшити суми штрафів, що накладаються за порушення законодавства про державну таємницю.

Значна кількість нормативних актів розглядає інформаційну безпеку в контексті більш загального поняття – національної безпеки (захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам).

Отже, чим активніше розвивається інформаційна сфера, тим більше політична, економічна, оборонна та інші складові національної безпеки будь-якої держави залежать від інформаційної безпеки, причому в ході розвитку технічного прогресу ця залежність дедалі більше зростатиме.

При цьому мова йде про необхідність забезпечення безпеки не лише інформації з обмеженим доступом, але й іншої інформації, оскільки в умовах інформаційного суспільства надається правова охорона інформації як об'єкта права власності, і має бути не лише відвернена загроза несанкціонованого доступу до інформації (порушення конфіденційності), але й загроза порушення її цілісності, достовірності та доступності інформації.

## Використана література

1. Ковальов К.Є., Леонов Б.Д. Забезпечення охорони державної таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняльний аналіз. *Інформація і право*. № 1(20)/2017. С. 82-92.

2. Гордієнко С.Г. Феномен інформації та забезпечення її охорони і захисту при веденні бізнесу: курс лекцій. – (НТУУ "КПІ"). URL: http://ipp.kpi.ua/wp-content/uploads/2016/04/%D0%9A%D1%83%D1%80%D1%81-%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9-%D0%A4%D0%B5%D0%BD%D0%BE%D0%BC%D0%B5%D0%BD-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-docx (дата звернення: 08.05.2021).

3. Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Служби безпеки України від 23.12.20 р. № 383.

4. ЦРУ меняет технику на агентов. URL: http://www.agentura.ru/dossier/usa/cia/gossreforms (дата звернення: 08.05.2021).

5. Андрій Євтушенко. Шпигуноманія-2. *Дзеркало тижня.* № 38 (463). – (4-10 жовтня 2003 року). URL: http://www.dt.ua/1000/1050/42776 (дата звернення: 09.05.2021).

6. Юлія Янчар. У США шпигуноманія. *Львівська газета.* № 166 (236). – (19 вересня 2007 року). URL: http://www.gazeta.lviv.ua/articles/2007/09/19/26355 (дата звернення: 09.05.2021).

7. Джемаль О., Сотников И., Тульский М., Маякова Е. Топ-8 ученых-шпионов. Кого и как можно обвинить в шпионаже. Тайный сбор информации сменили законные методы покупки секретных научных данных. URL: http://compromat.ru/main/nauka/shpieny.htm (дата звернення: 09.05.2021).

8. Использование легальных методов промышленного шпионажа в сетевой разведке. URL: http://www.warning.dp.ua/comp10.htm (дата звернення: 10.05.2021).

9. Лучшая российская шпионка за 30 лет. URL: http://inosmi.ru/europe/20101213/164884915.html (дата звернення: 10.05.2021).

10. Промышленный шпионаж – реальность в СНГ. URL: http://dere.com.ua/library/other/prom_spion.shtml (дата звернення: 10.05.2021).

11. Промышленный шпионаж или бизнес-разведка. *Goodwin.* – (08.15.2011). URL: http://z-filez.info/story/promyshlennyy-shpionazh-ili-biznes-razvedka (дата звернення: 11.05.2021).

12. Промышленный шпионаж, конкурентная разведка, бенч-маркетинг и этика цивилизованного бизнеса. URL: http://www.marketing-ua.com/articles.php?articleid=1499 (дата звернення: 11.05.2021).

13. Чехи запуганы байками о российских шпионах. URL: http://inosmi.ru/europe/20101226 /165208963.html (дата звернення: 12.05.2021).

14. Андрощук Г.А., Крайнев П.П. Правовое регулирование защиты коммерческой тайны за рубежом. *Экономическая безопасность, разведка и контрразведка*. 2002. № 1(1). С. 18-48.

15. Белая книга российских спецслужб. 2-е изд. перераб. Москва: Информ.-издат. агенство “Обозреватель”, 1996. С. 49-50.

16. Стратегія національної безпеки України: Указ Президента України від 26.05.15 р. № 287/2015. *Офіційний вісник України*. 2015. № 43. С. 1353.

17. Про основи національної безпеки України: Закон України № 964-IV від 19.06.03 р. *Офіційний вісник України*. 2003. № 29. Ст. 1433.

18. Адміністративне право України: підручник для юридичних вузів і факультетів / Ю.П. Битяк, В.В. Богуцький, В.М. Паращук та ін. Харків: Право, 2001. 152 с.

19. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*: зб. наук. праць. № 3(90)/2017. С. 36-50; Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право*. № 1(32)/2020. С. 33-46; Брижко В.М., Пилипчук В.Г. Безпека персональних даних: правові стандарти Європейського Союзу та сучасні прикладні проблеми. *Інформація і право.* № 1(36)/2021. С. 17-28.

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