вопросы методики расследования дел о поджогах. − М.: ВЮЗИ. – 1951 . − 137 с. 10. Шиманова З.Е. Пожарно-техническая экспертиза. − М.: МКХ РСФСР. – 1963 . − 86 с. 12. Пантелеев И.Ф. Расследование и профилактика взрывов, пожаров, крушений и авиапроисшествий. − М.: „Юрид. лит.” – 1975. − 208 с.

МАНЖАЙ О.В., *кандидат юридичних наук, доцент кафедри інформаційної безпеки факультету психології, менеджменту, соціальних та інформаційних технологій*

Харківський національний університет внутрішніх справ

МАНЖАЙ І.А., *інженер-програміст навчального відділу*

Харківський економіко-правовий університет

ОКРЕМІ АСПЕКТИ ЗАХИСТУ СЛУЖБОВОЇ ІНФОРМАЦІЇ В УМОВАХ РОЗБУДОВИ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

8 липня 2009 р. Президент України Указом № 514/2009 затвердив «Доктрину інформаційної безпеки України» [1], в якій відзначається, що за сучасних умов інформаційна складова набуває дедалі більшої ваги і стає *одним із найважливіших елементів забезпечення національної безпеки*. 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.

Проблеми охорони службової інформації в Україні та за межами країн СНД висвітлені у вітчизняній науці недостатньо. Це зумовило написання даної роботи, метою якої є порівняльний аналіз захисту службової інформації в різних країнах.

Для того, щоб визначити місце службової інформації у системі охорони державних інформаційних ресурсів України потрібно навести класифікацію інформації за порядком доступу (рис. 1).

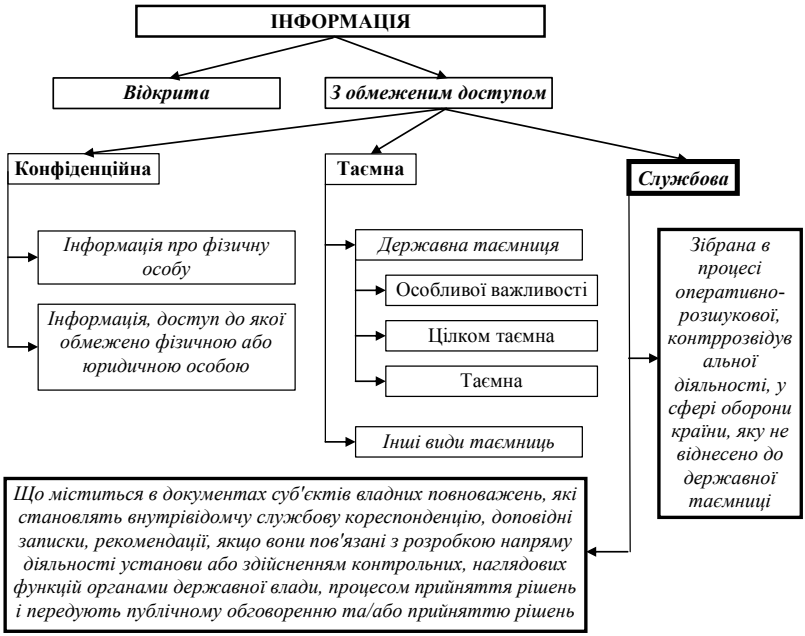


Рис. 1. Законодавча класифікація видів інформації в Україні

В Україні відомостям, які містять службову інформацію, надається гриф **«Для службового користування»** (ДСК).

Організаційно роботу з документами ДСК в конкретному підрозділі можна представити, як показано на рис. 2.



Рис. 2. Організація роботи з інформацією ДСК

Для друкування та розмноження документів ДСК встановлено спеціальну процедуру та перелік об'єктів, де вони можуть бути надруковані (розмножені).

Схематично це можна окреслити так, як на рис. 3.

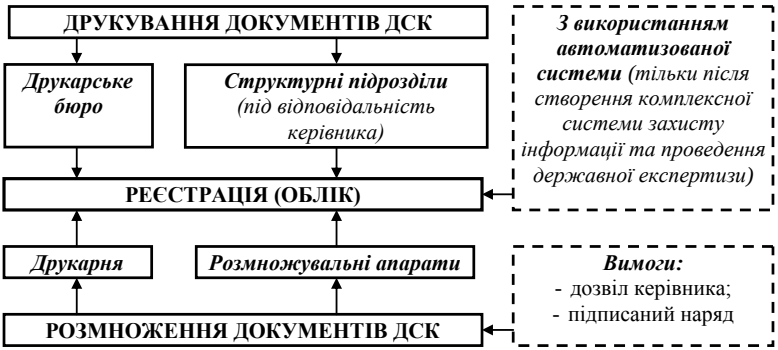


Рис. 3. Друкування (розмноження) документів ДСК

Документи ДСК зберігаються у службових приміщеннях і бібліотеках у шафах (сховищах), як надійно замикаються та опечатуються.

Модель руху документів ДСК зображено на рис. 4.

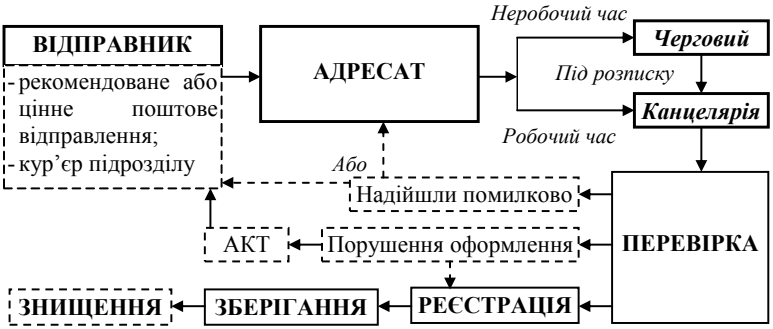


Рис. 4. Приблизна модель руху документів ДСК

Окремі реквізити, які повинні мати документи ДСК, наведено на рис. 5.

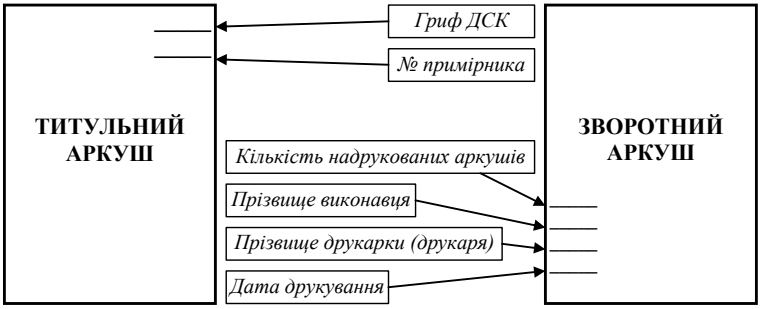


Рис. 5. Титульний та зворотний аркуш документу ДСК

За порушення роботи зі службовою інформацією, передбачена адміністративна (ст. 212-5 КпАП), а в окремих випадках – кримінальна відповідальність (ст. 330 Кримінального кодексу).

Приблизно так само, як і в Україні, врегульовано питання захисту службової інформації обмеженого поширення в Російській Федерації.

Основна нормативно-правова база обмеження доступу до

окремих відомостей службового характеру складається з Положення про порядок поводження зі службовою інформацією обмеженого поширення у федеральних органах виконавчої влади, затверджене Постановою Уряду РФ № 1233 від 03.11.1994 [3]; Указу Президента Російської Федерації № 188 «Про затвердження переліку відомостей конфіденційного характеру» від 06.03.1997 [4].

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»). Аналогом української службової інформації є як раз «конфіденційна», до якої відносяться відомості, несанкціоноване розкриття яких може завдати шкоди національній безпеці [5, Section 1.2].

Згідно з чинним законодавством Великобританії службова інформація має ступінь обмеження доступу «для службового користування» (Restricted).

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, підірвати належний рівень 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 передача інформації не була загальновідомою, покази осіб у справі, розголошення яких може зашкодити розслідуванню тощо.

У ФРН відповідні документи, що містять службову таєм-

ницю, позначають грифом «Для службового користування» (VS nur fur den dienstgebrauch). Відповідальність за порушення службової таємниці встановлена у 28 Розділі Кримінального кодексу ФРН. 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 [6, Section II (1)].

На підставі досліджених матеріалів доходимо висновку, що на відміну від ФРН, а також країн пострадянського простору для США та Великобританії характерними є більш докладні приписи щодо віднесення тієї чи іншої інформації до службової. Дана обставина зумовлена прецедентною системою права, яка тяжіє до якомога більшої конкретизації рішень, що можуть бути прийняті в рамках тих чи інших суспільних відносин.

Підбиваючи підсумки зазначимо, що в усіх країнах для службової інформації передбачено окремий, особливий порядок отримання, обробки, зберігання, захисту та розкриття. Процедурні питання роботи з такою інформацією мають приблизно однаковий характер в усіх розглянутих країнах.

Список літератури: 1. Доктрина інформаційної безпеки України, затверджена указом Президента України від 08.07.2009 № 514/2009 // Офіційний вісник України. – 2009. – № 52 (20.07.2009). – ст. 1783. 2. Про основи національної безпеки України: закон України від 19.06.2003; [із змінами і доповненнями на 01.07.2010] // Офіційний вісник України. – 2003. – № 29 (01.08.2003). – ст. 1433. 3. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвер-

жденное постановлением Правительства РФ № 1233 от 03.11.1994 г. // Собрание законодательства РФ. – 25.07.2005. – № 30 (ч. II). – ст. 3165. 4. Об утверждении перечня сведений конфиденциального характера: указ Президента РФ №188 от 06.03.1997 г.; [с изм. и доп. на 23.09.2005] // Собрание законодательства РФ. – 10.03.1997. – № 10. – ст. 1127. 5. Executive Order 13526 Classified National Security Information, December 29, 2009 [Електронний ресурс]. – Режим доступу: http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf. 6. Instruction sheet on the Handling of Protectively Marked Information Classified VS-NUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED) [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VS-MerkblattEnglisch_pdf.pdf?__blob=publicationFile.

ОГІЄНКО І.В., *кандидат юридичних наук, доцент кафедри трудового, аграрного, екологічного права та соціального захисту населення*

Харківський економіко-правовий університет

ПРАВОВІ АСПЕКТИ ЗАЙНЯТОСТІ НАСЕЛЕННЯ ЯК ВАЖЛИВИЙ ЧИННИК РОЗБУДОВИ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Процес становлення громадянського суспільства, який відбувається протягом тривалого періоду еволюції сучасної цивілізації, складний і суперечливий. Він має багато закономірностей, спільних для багатьох країн. Але кожна держава, розвиваючи громадянське суспільство, вносила щось особливе, характерне саме для неї. Кожна держава має бути зацікавлена в створенні, всебічному розширенні і поглибленні громадянського суспільства, якщо воно прагне до за-