

Висновок. Таким чином, для українського суспільства 90-ті роки ХХ ст. були перехідним періодом до нової інформаційної політики. Хоча Україна і стала незалежною державою, але ще певний час в країні керували пострадянські політичні еліти. Перехід від авторитарного режиму до демократичного не може бути швидкий. Існує певна інерція політичної системи, яка вибудовувалася десятиліттями. Перехід до демократичного суспільства в Україні почався з проголошенням незалежності, та відбувається донині. За четверть століття незалежності Українська держава пережила дві революції («Помаранчеву революцію» 2004 р., та «Революцію гідності» 2013 р.). Весь цей час в країні відбувається модернізація політичної системи, яка проходила не лінійно. Демократизація суспільства залежала від політичного курсу, якого дотримувалася політична еліта, що знаходилася при владі в різні роки.

Модернізація державної інформаційної політики не могла відбуватися окремо від тих політичних процесів, які проходили в Україні. Зміни почали відбуватися ще в часи «перебудови» та «гласності». Це поклато початок реформам в інформаційній сфері. Для подальшої демократизації суспільства вирішальну роль відіграла система комунікації між владними установами та суспільством.

В період «перебудови» та «гласності» відбулася трансформація інформаційного середовища, оскільки саме в цей період встановлюється сучасний принцип створення і поширення політичної інформації. Модернізація політичної системи держави позитивно вплинула на інформаційну політику. В суспільстві зросла роль засобів масової інформації, з'явилися такі ознаки демократії як: свобода слова, плюралізм думок.

Завищені очікування пов'язані з отриманням незалежності України та проведенням реформ, призвели не тільки падіння довіри і до влади, і до ЗМІ. Розірваність в інформаційному просторі держави в свою чергу свідчить про недосконалість інформаційної політики України. Подальшого дослідження потребує питання модернізації державної інформаційної політики України та вивчення досвіду провідних демократичних країн світу в інформаційній сфері.

Список використаних джерел

1. Бондар Ю. В. Становлення та еволюція національного інформаційного простору України в процесі формування демократичної політичної культури українського суспільства [Текст] / Ю. Бондар. – К., 2010.
2. Волковинська В. Реформувати та інформувати! [Електронний ресурс] / В. Волковинська, 2016. – Режим доступу: http://nbuv.gov.ua/index.php?option=com_content&view=article&id=2134:informatsijnij-suprovid-reform&catid=8&Itemid=350 / (дата звернення 16.12.2016) – Назва з екрана.
3. Інформаційна політика України: європейський контекст: Монографія [Текст] / Л. В. Губерський [та ін.]. – К.: Либідь, 2007. – 360 с.
4. Манойло А. В. Государственная информационная политика в особых условиях: Монографія [Текст] / А. В. Манойло. – М.: МИФИ, 2003. – 388 с.
5. Нестеряк Ю. В. Державна інформаційна політика: теоретико-методологічні засади: Монографія [Текст] / Ю. В. Нестеряк. – К.: НАДУ, 2014. – 292 с.
6. Реформи в Україні: громадська думка населення // Фонд «Демократичні ініціативи» ім. Ілька Кучеріва [Електронний ресурс]. – Режим доступу: <http://dif.org.ua/article/reformi-v-ukraini-gromadska-dumka-naselennya/> (дата звернення 16.12.2016) – Назва з екрана.

7. Флах К.–Г. Влада і злиденність преси [Текст] / Ред.–упор. В. Ф. Іванов; [переклад В. Климченка]. – Київ: Академія української преси, Центр вільної преси, 2015. – 186 с.

8. Шайгородський Ю. Політика: взаємодія реальності і міфу [Текст] / Ю. Шайгородський. – К.: Знання України, 2009.

References

1. Bondar Ju. V. Stanovlennja ta evolucija nacional'nogo informacijnogo prostoru Ukrainy v procesi formuvannja demokratychnoi politychnoi kul'tury ukrai'ns'kogo suspil'stva [Текст] / Ju. Bondar. – К., 2010.
2. Volkovyn's'ka V. Reformuvaty ta informuvaty! [Elektronnyj resurs] / V. Volkovyn's'ka, 2016. – Rezhym dostupu: http://nbuv.gov.ua/index.php?option=com_content&view=article&id=2134:informatsijnij-suprovid-reform&catid=8&Itemid=350 / (data zvernennja 16.12.2016) – Nazva z ekrana.
3. Informacijna polityka Ukrainy: jevropejs'kyj kontekst: Monografija [Текст] / L. V. Gubers'kyj [ta in.]. – К.: Lybid', 2007. – 360 s.
4. Manojlo A. V. Gosudarstvennaja informacionnaja politika v osobyh uslovijah: Monografija [Текст] / A. V. Manojlo. – М.: MIFI, 2003. – 388 s.
5. Nesterjak Ju. V. Derzhavna informacijna polityka: teoretyko-metodologichni zasady: Monografija [Текст] / Ju. V. Nesterjak. – К.: NADU, 2014. – 292 s.
6. Reformy v Ukraini: gromads'ka dumka naseleennja // Fond «Demokratychni iniciatyvy» im. Il'ka Kucheriva [Elektronnyj resurs]. – Rezhym dostupu: <http://dif.org.ua/article/reformi-v-ukraini-gromadska-dumka-naselennya/> (data zvernennja 16.12.2016) – Nazva z ekrana.
7. Flah K.–G. Vlada i zlydennist' presy [Текст] / Red.–upor. V. F. Ivanov; [pereklad V. Klymchenka]. – Kyi'v: Akademija ukrai'ns'koi' presy, Centr vil'noi' presy, 2015. – 186 s.
8. Shajgorods'kyj Ju. Polityka: vzajemodija real'nosti i mifu [Текст] / Ju. Shajgorods'kyj. – К.: Znannja Ukrainy, 2009.

Edeleva M. A., aspirant, Zaporizhzhia State National University (Ukraine, Zaporizhzhia), marinys@bk.ru

Modernization of Informational politics in the conditions of transition from authoritarianism to democracy

Modernization of the informational politics of USSR began during the period of «perestroika», when the government targeted democratic course of restructuring of political institutions of Soviet Union and «open» politics was established and social relations were reformed. All of these changes lead to democratic changes in the communicational relations between government and society which had a positive impact on general development and served as a base for further democratic transformations. The process of modernization in modern Ukraine still isn't complete, even though democratic changes in the informational sphere have a positive impact on the political system in total.

Using comparative method of investigation one can reveal peculiarities of informational politics of Ukrainian SSR, its' common traits and specificity in the period of «perestroika» and in conditions of independent Ukraine in order to find optimal forms of political organization of governmental informational politics of Ukraine and ways to resolve questions in the informational sphere. Systemic analysis was used for the investigation and studying of peculiarities of modernization of the governmental informational politics.

Keywords: governmental informational politics, modernization, «perestroika», informational space, political communication, mass media.

УДК 327.7

Задувайло О. К.,
аспірантка відділу інформаційної безпеки та розвитку інформаційного суспільства. Національний інститут стратегічних досліджень (Україна, Київ),
zaduvailo@ukr.net

ПРОБЛЕМА ВИЗНАЧЕННЯ ПОНЯТТЯ «ЧУТЛИВА ІНФОРМАЦІЯ» В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Розглядається поняття «чутлива інформація», аналізується міжнародно-правовий режим доступу до чутливої інформації. Вказується на співвідношення понять «чутлива» та «секретна» інформація.

Ключові слова: державна таємниця, чутлива інформація, секретна інформація, законодавство США, міжнародне законодавство.

7 травня 2009 р. Управління урядового друку (Government Printing Office) США опублікувало 266-сторінковий документ на своєму веб сайті, який представив детальну інформацію про ядерні об'єкти, локацію, і діяльність США. На прохання спікера Палати представників США, було проведено розслідування у зв'язку з оприлюдненням чутливої інформації, яка може завдати шкоди національній безпеці США. Як виявилось в ході розслідування в підготовці даного документа брали участь одночасно декілька урядових установ: Міністерство енергетики, Комісія з ядерного регулювання, Рада національної безпеки, Білий Дім та Палата Представників.

У той час жодна з вище зазначених установ не несе повну відповідальність за публічне розкриття документу. Федеральні відомства використовують безліч різних маркувань (близько 130), які класифікують інформацію як «чутлива інформація» [1]. І тому досить часто виникають ситуації коли співробітники тих чи інших відомств не володіють інформацією про деякі види маркувань і тому не знають, як правильно захищати таку інформацію. Як результат, основними причинами витоку інформації стали відсутність чітких міжвідомчих інструкцій при передачі документів, що містять чутливу інформацію, різні процедури регулювання та маркування чутливої інформації в кожному відомстві та надмірна кількість маркувань інформації, що відноситься до чутливої. За результатами розслідування інформація, що міститься в проєкті декларації була обмежена цивільною ядерною діяльністю держави, більшість інформації вже знаходилась у відкритому доступі на веб сайтах агентств або інших загальнодоступних документів, тому оприлюднення якої не завдало шкоди національній безпеці. Однак, на думку уряду, федеральні органи, що відповідають за збір цієї інформації та консолідуєть в один документ, повинні дотримуватися режиму чутливості і, таким чином уникнути розголошення даної інформації [1].

В наведеному прикладі відсутність чіткого нормативно-правового регулювання захисту чутливої інформації, відсутності загального і чіткого визначення деяких таємниць призвело до серйозних проблем пов'язаних із використанням інформації в інтересах державної політики. Для України, яка визначає в своїх ключових безпекових документах пріоритет реформування системи захисту державної таємниці, дослідження світових практик в цій сфері (передусім – розвинутих демократичних держав), має стати важливим етапом на шляху вироблення власної оновленої системи захисту державної таємниці.

Потенційна соціальна корисність і небезпека збирання, зберігання, використання і поширення інформації вимагають чіткого механізму правового регулювання інформаційних відносин, розроблення ефективних юридичних засобів реалізації інформаційних прав і свобод людини та громадянина за умови забезпечення інформаційної безпеки. Кожна демократична держава з метою забезпечення інформаційної безпеки формує систему захисту чутливої інформації, надаючи їй певного статусу.

Дослідження чутливої інформації в правовій площині забезпечує розуміння даного поняття, яка правового еквівалента, що формується в системі

законів. Розробка такої концепції бере початок в епоху Просвітництва політичної філософії у вченнях Ж. Ж. Руссо про соціальний договір та Дж. Локка про природні права [2, с. 20]. Це послужило одним з філософських базисів Конституції США, а багато з цих постулатів були задіяні в розробці законодавчих актів, які декларують право людини на інформацію. Деякі з цих досліджень тісно співпрацюють з економічними дослідженнями особливо, коли йде мова про приватні права (недоторканість приватного життя).

Диференційний захист чутливої інформації характеризується складним набором правил, в якому суб'єкт з правами власності на інформацію має право зберігати інформацію від її розголошення або навпаки оприлюднювати за власним бажанням. З цього боку, чутлива інформація, це інформація, що належить власнику (суб'єкт, який має право на інформацію), але не належить іншим суб'єктам і тільки власник встановлює правила доступу до цієї інформації.

Поняття чутлива інформація (sensitive information) частіше зустрічається в економічних словниках, де зазначено, що це інформація, несанкціоноване розкриття, модифікація або укриття якої може призвести до значної шкоди або затратам [3, с. 136]. Також це поняття часто порівнюють з комерційної інформацією і визначають, як інформацію, розголошення якої може завдати шкоди організації або підприємству [4].

В юридичному словнику під чутливою інформацією розуміється, інформація, яка захищається від несанкціонованого розкриття з метою захисту приватного життя або безпеки організації чи держави [5]. Доступ до такої інформації повинен бути захищений відповідним законодавством. Тобто їй надається правовий статус і чітко визначається поле його дії.

Отже, окрім економічної сфери чутлива інформація широко застосовується в законодавстві інформаційної сфери національної безпеки, але змістове навантаження в кожній країні відрізняється. Вперше це поняття як складової національної безпеки було використано урядом США. Закон про національну безпеку 1947 р. [6] та Закон про атомну енергію 1954 р. [7] стали початковим відліком у формуванні державної політики щодо секретної та несекретної інформації. Протягом багатьох років федеральний уряд використовує поняття «чутлива, але не секретна» (sensitive but unclassified) до певного виду інформації. Та лише в Законі про комп'ютерну безпеку 1987 р. [8] було дано офіційне визначення терміну «чутлива інформація», що означає будь-яку інформацію, втрата, неправильне використання або несанкціонований доступ до або зміна якої може негативно впливати на національний інтерес, або проведення федеральних програм або конфіденційність, на яку особа має право відповідно до Закону про недоторканість приватного життя (The Privacy act) 1974 р. [9], але яка не має спеціальних повноважень відповідно до положень, зазначених в урядовому розпорядженні або нормативним актом Конгресу, щоб утримувати в секреті інтереси національної оборони або зовнішньої політики [10, с. 20].

Тобто, інакше кажучи, інформація, яка називається «чутливою» в даному законі є несекретною. Проте, закон чітко говорить, що організації несуть відповідальність за захист таких даних. Очевидно, що

інформація, яка є «секретною» (classified) не підпадає під дію законів про чутливу інформацію, адже секретна інформація класифікується на «цілком таємну» (top secret), «таємну» (secret), конфіденційну (confidential) відповідно до інструкції Міністерства оборони 5200.1-R [11].

Разом з тим суспільство, чи-то журналіст чи-то просто небайдужий громадянин прагне мати вільний і необмежений доступ до інформації, яка є не секретна або не захищена законодавством. Проте деякі несекретні дані, які містять чутливу інформацію потребують чіткого контролю та захисту від небажаного розголошення, адже це може завдати шкоди інтересам держави, організації або особи.

До «чутливої інформації» в законодавстві США відноситься широка категорія інформації, яка містить у собі дані, які знаходяться в документообігу федеральних органів (FOUO) [11], правоохоронних органів (LES) [12], критична програмна інформація (CPI) [13], інформація розповсюдження якої обмежено (LIMDIS) [11] та інформація, яка стосується питань безпеки (SSI) [14]. Остання є категорією чутливої, але несекретної інформації, яка обробляється в рамках правил урядового обміну інформації і контролю. SSI є інформація, отримана під час проведення заходів по забезпеченню безпеки, публічне розкриття якої, на думку державних установ, може завдати шкоди транспортній безпеці, невиправданим вторгненням в приватне життя, або розкриття комерційної таємниці чи конфіденційної інформації [14].

В пояснювальній записці Організації економічного співробітництва і розвитку до документу «Guidelines on the Protection of Privacy and Transborder Flows of Personal Data» (Загальні принципи щодо захисту недоторканності приватного життя та транскордонних потоків особистих даних), висловлюється думка, що «це, ймовірно, не представляється можливим визначити набір даних, які підпадають під категорію «чутлива інформація» тому що будь-яка інформація може бути чутливою в залежності від контексту» [15].

Однак, стаття 8 Директиви ЄС, що стосується «особливих категорій даних» (Data Protection Directive), останні визначаються як «персональні данні, які розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, профспілкове членство, правопорушень, що стосуються судимостей або заходів безпеки, а також обробку даних про здоров'я чи усиновлення» [16]. Ця стаття забороняє обробку такого роду інформації без згоди, за винятком зазначених обставин і дозволяє державам – членам заборонити обробку таких даних навіть за згодою суб'єкта даних. Всі данні, які зазначені в даній директиві також можна віднести до «чутливої інформації», але офіційного визначення даного поняття немає.

На міжнародному рівні проблематика визначення «чутливої інформації» опрацьовувалась, зокрема, на рівні Організації Об'єднаних націй. Важливим в цьому сенсі міжнародно-правовим документом, який чітко регламентує правовий захист чутливої інформації, є бюлетень Генерального секретаря ООН з питань інформаційної чутливості, класифікації та обробки (ST /SGB/ 2007/6) [17]. В бюлетені зазначено, що всі документи, створені або отримані ООН повинні

перевірятися на наявність чутливої інформації, тому що неналежне розкриття чутливої інформації може завдати шкоду діяльності ООН, чи піддати небезпеці її персонал. Для того щоб пом'якшити ці ризики, ООН розробила формальну процедуру класифікації для ідентифікації документів, які повинні бути захищені у відповідності до маркування чутлива інформація:

– документи, створені ООН, отримані від або передані третім особам, відповідно до маркування чутлива інформація;

– документи, розкриття яких може поставити під загрозу безпеку будь-якої людини, порушити її права або уторгуються в її особисте життя;

– документи, розкриття яких може поставити під загрозу безпеку держав-членів або завдати шкоди безпеці або належному проведенні будь-якої операції або діяльності ООН, включаючи будь-яку з її операцій з підтримання миру;

– документи, що пов'язані з внутрішнім дослідженням ООН;

– документи, в тому числі проекти документів, розкриття яких може підірвати вільний і незалежний процес прийняття рішень ООН;

– документи, що містять комерційну інформацію, у разі розкриття такої інформації може завдати шкоди фінансовим інтересам ООН або інших сторін-учасниць;

– інші види інформації, які через їх зміст або обставини їх створення або обробку повинні бути закритому доступі.

Маркування «чутлива інформація» повинні використовуватися розумно і тільки в тих випадках, коли розкриття інформації може бути шкідливим для належного функціонування ООН або добробуту і безпеки своїх співробітників або третіх осіб, або порушення правових зобов'язань організації. У таких випадках режим доступу повинен гарантувати, що така інформація не буде навмисно чи ненавмисно оприлюднена.

Також в цьому документі запропоновано основні правила, яких потрібно дотримуватися, для захисту конфіденційних документів, як у паперовому, так і електронному вигляді:

– не можна скасувати будь-яке рішення про класифікацію чутливості документа. Завдання розсекречення документа присвоюється конкретних старшим офіцерам в кожному відділі ООН;

– якщо документ, який ідентифікований як конфіденційний або строго конфіденційний, повинен бути позначений належним чином і в коротший термін після його створення;

– якщо документ, який був отриманий від третьої особи повинен бути ідентифікований як конфіденційний або суворо конфіденційний, він повинен бути позначений належним чином і в коротший термін після його створення;

– зберігатися всі документи повинні надійно і під чітким контролем в установленому порядку і в будь-який час [17].

Узагальнюючи нормативно-правові практики США та ЄС щодо визначення поняття «чутлива інформація», можна виділити наступні характерні риси нормативного розуміння чутливої інформації:

– це будь-яка інформація незалежно від її форми, природи та способу передачі; інформація у будь-якій

Таблиця

Види даних, які відносяться до чутливої інформації в різних країнах світу

	Види даних	Кількість країн, які відносять їх до «чутливої»
1	За рішенням суду або побічно, через інші закони, із-за можливої дискримінації	11
2	Інформація, яка стосується питань безпеки	17
3	Політичні переконання або приналежності	27
4	Національність, раса/етнічність	25
5	Професійна/торгова асоціація	2
6	Персонал/профспілки	22
7	Релігійні переконання або приналежність	29
8	Філософські або моральні переконання	25
9	Сексуальні нетрадиційні погляди або практики	26
10	Відомості про судимість/розслідування або досудовий розгляд	14
11	Інформація про стан здоров'я/генетичні дані	34
12	Соціальне страхування	2
13	Домашнє насилля	1
14	Штрафи	3
15	Сімейний стан	3
16	Усиновлення	1
17	Фінансування/доходи/рахунки/дебет/кредит/платіжні карти	5
18	Паролі	1
19	Персональні дані	1
20	Біометричні дані	4
21	Соціальний статус	1
22	Адреса проживання	1
23	Вік	1
24	Освіта	1
25	Державні ліцензії/страхування	4
26	Психічні відхилення	1

формі та будь-які документи, матеріали, вироби, речовини або фізичні поля, на/в яких представлена інформація; будь-які дані незалежно від їхньої форми представлення, виду та умов відтворення; будь-який документ, рисунок, план, карта, фотографія, звуковий запис чи відеоплівка або інший документ чи інший носій інформації, що містять інформацію; інформація, відображена в будь-якій формі;

– охорона такої інформації здійснюється з метою забезпечення недоторканності приватного життя, комерційної таємниці, національної безпеки та інтересів кожної з країн;

– основною загрозою чутливої інформації визначається несанкціонований доступ та витік, що призводить до її розголошення;

– зміст та перелік такої інформації, а також способи контролю та методи обмеження доступу визначаються кожною країною самостійно відповідно до національного законодавства [18].

Один з провідних світових експертів в області приватної інформації та права Д. Солов (Daniel J. Solove), дослідивши законодавства понад 30 країн світу, він склав таблицю де відобразив, які категорії інформації відносяться до категорії «чутлива» (див. табл.) [19].

Спектр даних, які відносяться до чутливої інформації та методи її захисту в кожній країні різні. Та в більшості країн інформація, яка може стосуватися заходів безпеки, або інформація, яка циркулює в органах державної влади підпадає під категорію «чутлива» і потребує чіткого контролю.

На нашу думку, спираючись на дослідження Д. Солова доречно класифікувати інформацію відповідно до її чутливості:

– Приватна інформація, яка містить дані про особу, розголошення якої може завдати їй шкоди. До такої інформації можна віднести біометричні дані, медичну інформацію, особисту фінансову інформацію, релігійні і політичні переконання, унікальні індикатори, такі як паспорт або номер соціального страхування. До загроз можна віднести не лише такі злочини, як крадіжка особистих даних, а й розкриття персональної інформації, яку особа воліла б залишити приватною.

– Бізнес інформація включає в себе все, що створює ризик для підприємства чи організації у разі отримання такої чутливої інформації конкурентами або широким загалом. Плани придбання, фінансові дані, постачальники, інформація про клієнтів, про персонал тощо. У зв'язку з постійно зростаючим обсягом даних, що генеруються підприємствами чи організаціями, методи захисту корпоративної інформації від несанкціонованого доступу стають невід'ємною складовою корпоративної безпеки, в–першу чергу ці методи включають в себе управління метаданими.

– Інформація, яка стосується питань безпеки – це інформація, певні відомості, несанкціонований доступ до яких може заподіяти шкоду національним інтересам держави. Наприклад інформація про програми безпеки і плани дій в надзвичайних ситуаціях, директиви з безпеки, заходи безпеки, безпека маскуванню інформації, критична авіація або інформаційна інфраструктура морських активів, тощо. Але дана інформація, не підпадає під втаємничення і надання грифу секретності.

Ми вважаємо, що така класифікація чутливої інформації дає чітке уявлення, про види даних, які відносяться до неї. В порівнянні з державною таємницею при розголошенні, якої вона не на носить суттєвої шкоди національній безпеці держави та може завдати шкоди при виконанні службових обов'язків в сфері національної безпеки. В міжнародному законодавстві secret information (секретна інформація) визначається як інформації в військовій, економічній, зовнішнь-політичній сфері, розвідувальній та контррозвідувальній діяльності, доступ до якої обмежується в інтересах безпеки держави, існує на рівні закону, і закон встановлюється зміст перелік даних, котрі відносяться до державної таємниці [20]. В українському законодавстві державна таємниця ототожнюється з секретною і визначається, як вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та, які визнані Законом України і підлягають охороні державою [21, с. 7].

Узагальнюючи вище зазначене, варто сказати, що правовий режим чутливої інформації використовується для високого ступеня безпеки практично усіма урядами світу, він покликаний охороняти відомості, вільний обіг, яких може порушити права та інтереси держави, суспільства і окремої особи, забезпечити інформаційну незалежність суб'єктів приватного права у відносинах із державою і між собою, узгодити публічну потребу у свободі інформації та право кожного на збереження таємниці. Саме тому характерною рисою для більшості розвинених країн є наявність відповідних законодавчих актів, що встановлюють принципи, критерії, механізми класифікації чутливої інформації, а також процедуру її охорони з боку держави чи власника.

Список використаних джерел

1. Managing sensitive information [Електронний ресурс] // United States Government Accountability Office. – 2009. – Режим доступу: <http://www.gao.gov/assets/300/299487.pdf>.
2. Thompson D. Sensitive information: An inquiry into the interpretation of information in the workplace from an individual's perspective using qualitative methods: dissertation PHD / Thompson – USA, 2008. – 242 p.
3. Sussman S. Dictionary of Health Information Technology and Security / Sussman. – NY: Springer Publishing company, 2007. – 212 p.
4. Sensitive information [Електронний ресурс] // Business Dictionary. – 2016. – Режим доступу: <http://www.businessdictionary.com/definition/sensitive-information.html>.
5. What is sensitive information? [Електронний ресурс] // The Law Dictionary – 1996. – Режим доступу: <http://thelawdictionary.org/sensitive-information/>.
6. The National Security Act of 1947 [Електронний ресурс] // Office of the Historian, Bureau of Public Affairs United States Department of State. – Режим доступу: <https://history.state.gov/historicaldocuments/frus1945-50Intel/ch6>.
7. Atomic Energy Act of 1954 [Електронний ресурс] // House Office of the Legislative Counsel. – Режим доступу: <https://legcounsel.house.gov/Comps/Atomic%20Energy%20Act%20Of%201954.pdf>.
8. The Computer Security Law of 1987 [Електронний ресурс] // NIST Computer Security Resource. – Режим доступу: http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt.
9. The Privacy act of 1974 [Електронний ресурс] // U.S. Department of justice. – Режим доступу: <https://www.justice.gov/ocpl/privacy-act-1974>.

10. Helyer A. Sensitive But Unclassified / A. Helyer, SANS Institute, Security Essentials GSEC Practical, Version 1.3, 2002. – 20 p.

11. Department of Defense DoD 5200.1-R of 2012 [Електронний ресурс] // Defense technical information center. – Режим доступу: http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf.

12. Department of Homeland Security Management Directive System MD Number: 11042.1 of 2005 [Електронний ресурс] // Department of Homeland Security. – Режим доступу: https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf.

13. Instruction Department of Defense №5200.39 of 2015 [Електронний ресурс] // Defense technical information center. – Режим доступу: <http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf>.

14. U.S. House of Representative Committee on Oversight & Government Reform of 2014 [Електронний ресурс] // Oversight and government reform. – Режим доступу: <https://oversight.house.gov/wp-content/uploads/2014/05/Staff-Report-Operation-Choke-Point1.pdf>.

15. Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum of 1980, [Електронний ресурс] // OECD. – Режим доступу: <https://www.oecd.org/sti/economy/oecdguidelinesontheprotectionofprivacyandtransborderflows/opsionaldata.htm>.

16. European Parliament, Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Directive 95/46/EC, arts 34, 70. [Електронний ресурс] // The European Commission. – Режим доступу: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

17. UN Secretary-General's Bulletin on information sensitivity, classification and handling (ST/ SGB/2007/6) [Електронний ресурс] // United nations archives and records management section. – Режим доступу: <https://archives.un.org/sites/archives.un.org/files/uploads/files/Guidance%20Sensitive%20Information.pdf>

18. Баскаков В. Інформація з обмеженим доступом: аналіз термінологічно-понятійного апарату [Електронний ресурс] / В. Баскаков // Baskakov V. Інформація з обмеженим доступом: analiz terminologichno-ponyatijnogo aparatu / V. Baskakov // GOAL. – 2011. – Режим доступу: <http://goal-int.org/informaciya-z-obmezhenim-dostupom-analiz-terminologichno-ponyatijnogo-aparatu/>.

19. Solove D. What Is Sensitive Data? Different Definitions in Privacy Law [Електронний ресурс] / Solove. – 2004. – Режим доступу: <https://www.teachprivacy.com/sensitive-data-different-definitions-privacy-law/>.

20. Закон України «Про державну таємницю» від 21.01.1994 р. [Електронний ресурс] // Сайт Верховної ради України // Zakon Ukrainy «Pro derzhavnu tajemnytsju» vid 21.01.1994 r. // Sajt Verhovnoi rady Ukrainy. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/3855-12>.

21. Адабаш А. Охрана государственной тайны: законодательство Украины и международный опыт / А. Адабаш // Legea si viata. – 2014. – №9. – С.4–7. // Adabash A. Ohrana gosudarstvennoj tajny: zakonodatel'stvo Ukrainy i mezhdunarodnyj opyt / A. Adabash // Legea si viata. – 2014. – №9. – С.4–7.

Zaduvailo O. K., graduate student of the department of information security and the development of the information society, The National Institute for Strategic Studies (Ukraine, Kyiv), zaduvailo@ukr.net

The problem of the definition of «sensitive information» in the context of information security

The concept «Sensitive information» is considered in the article, analyses the international legal regime for access to sensitive information. Indicate the ratio of the concepts of «sensitive» and «classified» information.

Keywords: state secret, sensitive information, classified information, U.S. legislation, international legislation.

* * *