НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ЗАХИСТУ СЛУЖБОВОЇ ІНФОРМАЦІЇ

НАВЧАЛЬНИЙ ПОСІБНИК

Київ – 2017

УДК 35.083.8
ББК 67.9(4Укр)404я73 0-64

Рецензенти:
А. М. Гуз - доктор історичних наук, професор;
О. Б. Розвадовський - доктор юридичних наук

Внесок авторів:
Касперський І. П. - 1.1.; Князев С. О. - вступ; 2.2.; 2.3.;
Матяш О. І. - 2.1.; Солодка О. М. - розділ 4;
Ткачук Т. Ю. - 1.2.; 1.3.; Шлапаченко В. М.,
Мейдич І. М. — розділ 3; Школа В.П. - 2.3.
Рекомендовано до друку Редакційно-видавничою радою
Національної академії СБ України,
протокол N° 4 від 28 жовтня 2015 року

0-64 Організаційно-правові основи захисту службової 0-64 інформації: навч. посіб. /1. П. Касперський, С. 0. Князєв, О. І. Матяш та ін. - Київ : Нац. акад. СБУ, 2017.-120 с.

Розглянуто організаційно-правові основи захисту службової інформації зокрема проблемні питання, пов’язані з відсутністю певної законодавчої бази, недостатнім нормативно-правовим визначенням механізмів реалізації прийнятих законодавчих норм, які стосуються використання цього виду інформації з обмеженим доступом.

Для науково-педагогічних працівників НА СБ України, студентів, курсантів, слухачів, працівників режимно-секретних органів.

УДК 35.083.8
ББК 67.9(4Укр)404я73

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ

ДКУД - Державний класифікатор управлінської діяльності України

ДСК – для службового користування

ЕК – експертна комісія

ЕОМ – електронно-обчислювальна машина

ІзОД = інформація з обмеженим лоступом

КК - Кримінальний кодекс України

КРД – контррозвідувальна діяльність

КПК - Кримінальний процесуальний кодекс України

КСЗІ - криптографічна система захисту інформації

КУпАП - Кодекс України про адміністративні правопорушення

ОРД –оперативно-розшукова діяльність

РСО – режимно-секретний орган

СБ України – Служба безпеки України

Ст. - стаття

ВСТУП

Стан захисту державного інформаційного простору є одним із показників ефективності роботи держави, щодо захисту власних інформаційних ресурсів від протиправних посягань. Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути покладені ефективні організаційно-правові заходи.

Останніми роками в Україні відбулись істотні зміни у процесах державного управління на всіх рівнях, які були зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Проте, швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

Сучасні реалії, пов’язані з проведенням широкомасштабної антитерористичної операції також створили додаткові потужні загрози для існування інформаційної сфери держави. Українське суспільство наочно побачило наскільки уразливою може ставати навіть відкрита інформація, яку можливо неправомірно перекручувати, обмежувати у доступі та використовувати як спосіб маніпулювання свідомістю.

Крім того, у сфері використання службової інформації потребує врахування існуюча низка проблемних питань пов’язаних з відсутністю певної законодавчої бази, недостатнім нормативно-правовим визначенням механізмів реалізації прийнятих законодавчих норм, які стосуються використання даного виду інформації з обмеженим доступом.

У зв’язку із цим, особливого значення набувають можливості реалізації у сучасних умовах організаційно-правових заходів захисту інформації з обмеженим доступом, серед якої важливе місце займає службова інформація.

Зважаючи на визначене, автори представленого навчального посібника зосередили увагу на комплексному розгляді питань пов’язаних з організаційно-правовими основами захисту службової інформації. Виділенні найбільш проблемних питань щодо захисту даного виду інформації з обмеженим доступом та наданні можливих пропозицій щодо їх вирішення.

Структурно видання складається з чотирьох розділів після кожного визначені питання для самоперевірки, використані та рекомендовані джерела. Наприкінці, для більш повного розуміння окремих питань, наводиться ряд додатків.

Посібник може бути використано під час проведення занять з наступних дисциплін: «Забезпечення державної безпеки у сфері охорони державної таємниці», «Організаційно-правові засади охорони державної таємниці», «організація захисту інформації з обмеженим доступом», а також під час проведення курсів підвищення кваліфікації співробітників підрозділів охорони державної таємниці СБ України та режимно-секретних органів установ.

РОЗДІЛ 1
ПРАВОВИЙ ЗАХИСТ СЛУЖБОВОЇ ІНФОРМАЦІЇ

1.1. Поняття та ознаки службової інформації

На виконання своїх функцій держава оперує величезними масивами інформації. Окремі з цих даних не підлягають розголошенню, оскільки це може нанести шкоду інтересам, які захищаються законом. Найважливіші державні дані становлять державну таємницю. Проте, крім державної таємниці, є і інша інформація, розголошення якої, хоча і не зможе нанести шкоду національній безпеці, проте може ускладнити діяльність окремих державних органів, вплинути на їх здатність виконувати свої функції і зобов'язання. Тому держава обмежує доступ до цих даних у окремому режимі, який є менш обтяжливим, ніж режим державної таємниці, проте забезпечує адекватний рівень захисту від розголошення.

Відповідно до статті 21 Закону України «Про інформацію» уся інформація з обмеженим доступом поділяється на таємну, конфіденційну та службову. Як бачимо, законодавством службову інформацію виділено в окремий вид, отже вона має ті ознаки, що дозволяють відрізнити її від інших «закритих» даних.

Ознаки службової інформації наведено у положеннях статті 9 Закону України «Про доступ до публічної інформації», а саме вказано, що до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Цим же законом запроваджено загальні підстави обмеження доступу до інформації (так званий трискладовий тест). Отож обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Також виходячи зі змісту цього Закону варто визнати, що службова інформація належить до категорії публічної інформації, тобто це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень чи інших розпорядників публічної інформації. Відповідно до Закону України «Про інформацію» суб’єкти владних повноважень – це органи державної влади, органи місцевого самоврядування або інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

На основі цього можливо виділити наступні найсуттєвіші ознаки службової інформації:

- це публічна інформація;

- нею володіють суб’єкти владних повноважень на виконання своїх функцій;

- суб’єкти владних повноважень мають право обмежувати доступ до цих даних;

- підставою обмеження такого доступу є можливість нанесення шкоди внаслідок розголошення цієї інформації суттєвим інтересам, що захищаються законом;

- ця інформація не належить до державної таємниці.

Виходячи з викладеного службова інформація – це дані, що не становлять державної таємниці і перебувають у власності суб'єктів владних повноважень, які мають право обмежувати доступ до них у встановленому законом порядку, на підставі того, що їх розголошення може завдати суттєвої шкоди правам та законним інтересам, що перебувають під правовим захистом.

Проте право обмежувати доступ до інформації не безмежне і повинно закінчуватись там, де починається право суспільства і громадян на доступ до необхідної інформації.

Тому законодавством визначено категорії інформації, доступ до якої обмежувати заборонено. Об'єднання відповідних положень законів України «Про інформацію» та «Про доступ до публічної інформації», «Про державну таємницю» дає наступний перелік даних, які не можуть бути обмежені у доступі:

- про стан довкілля, якість харчових продуктів і предметів побуту;

- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

- про факти порушення прав і свобод людини і громадянина;

- про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

- про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі копії відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно;

- відомості, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до Закону України "Про запобігання корупції";

- інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Важливим елементом системи захисту службової інформації є процедура надання відомостям цього статусу.

Названу процедуру закріплено у Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, яку затверджено Постановою Кабінету Міністрів України № 1893 від 27 листопада 1998року.

Отож віднесення інформації до службової відбувається шляхом її включення до відповідних переліків відомостей, які містять службову інформацію. Ці переліки затверджуються міністерствами, іншими центральними органами виконавчої влади, обласними та прирівняними до них міськими державними адміністраціями (далі - органи державної влади) у вигляді наказів цих державних органів.

Формують названі переліки експертні комісії, що утворюються органами державної влади. До складу цих комісій включаються представники режимно-секретного та інших структурних підрозділів з числа найбільш кваліфікованих фахівців. У разі потреби для участі в роботі експертної комісії можуть залучатися фахівці заінтересованих підприємств, установ та організацій (за погодженням з їх керівниками) з метою розгляду питань, що належать до їх компетенції. Працівники режимно-секретного органу хоча і не займаються організацією обігу службової інформації, проте їх участь у комісіях необхідна для виключення випадків внесення у переліки службової інформації даних, що становлять державну таємницю, а також відомостей, які не можуть бути обмежені у доступі. Рішення комісії оформляється протоколом, який затверджується відповідним органом державної влади. На підставі рішення експертної комісії інформація включається до переліку відомостей, які містять службову інформацію, і носіям

якої надається гриф обмеження доступу «для службового користування» (ДСК). На підставі цих переліків визначається необхідність проставлення грифа «Для службового користування» на конкретному документі чи виданні.

У разі потреби на державних підприємствах, в установах і організаціях з урахуванням особливостей їхньої діяльності розробляються та за погодженням з органом державної влади, до сфери управління якого вони належать, вводяться в дію переліки конкретних видів документів у відповідній сфері діяльності.

Відповідно до Закону України «Про доступ до публічної інформації» ці переліки не можуть бути обмежені у доступі. Вимога забезпечення доступу до переліків службової інформації обґрунтовується тим, що за Конституцією кожен має право знати свої права, а переліками фактично обмежується право громадян на доступ до інформації. Тому громадяни повинні знати до яких видів даних доступ обмежено правомірно.

З одного боку, Законом України «Про доступ до публічної інформації» чітко не визначено, чи є складання Переліку обов'язковим для суб'єкта владних повноважень, чи тільки його правом. В той же час, Указом Президента України № 547 від 5 травня 2011 року «Питання забезпечення органами виконавчої влади доступу до публічної інформації» закріплено обов'язок органів виконавчої влади затвердити переліки відомостей, що становлять службову інформацію, та оприлюднити їх в установленому порядку.

На практиці, переважна більшість органів державної влади та органів місцевого самоврядування закріпили такі Переліки. Більше того, органи Прокуратури, проводячи перевірки, відсутність переліку трактували як порушення закону.

Загальний аналіз переліків інформації, яка є службовою, дозволяє зробити наступні висновки щодо груп даних, які туди включають:

- відомості, що є службовою інформацією, згідно з чинним законодавством (такі як журнали обліку вхідних і підготовлених секретних документів, чи відомості про довгострокові та річні програми мобілізаційної підготовки місцевого органу виконавчої влади);

- відомості щодо результатів контрольних заходів (дані з актів перевірок, матеріали службових розслідувань);

- відомості, отримані з інших органів державної влади у статусі службової інформації;

- відомості, що відображають специфіку діяльності конкретного органу державної влади (наприклад у Збройних Силах - відомості про підготовку особового складу авіаційних підрозділів, у Державній службі України з надзвичайних ситуацій - розпорядження по зв'язку при ліквідації надзвичайної ситуації мирного часу).

До названих переліків не може бути включена інформація, доступ до якої заборонено обмежувати відповідно до закону, а також інформація, що становить державну таємницю чи конфіденційну інформацію про особу. Керівники органів державної влади та їхніх структурних підрозділів, державних підприємств, установ і організацій у разі потреби мають право зняти гриф «Для службового користування» з документів, підготовлених цим органом чи його структурним підрозділом, підприємством, установою, організацією, якщо відомості, що містяться у цих документах, не відповідають перелікам. Положення цих переліків можуть бути оскаржені безпосереднім зверненням до органу, який затвердив перелік, або у судовому порядку.

Законом не встановлено вимог щодо строків збереження статусу службової інформації чи термінів перегляду переліків, проте є окремі виключення. Так відповідно до п. 5 Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію з введенням у дію цієї Інструкції тиражовані документи, видані з грифом «Для службового користування» до 1991 року, а також тиражовані документи, випущені у світ у різний час з іншими обмежувальними грифами, крім грифів «Службова таємниця», «Таємно», «Цілком таємно» та «Особливої важливості», можуть розглядатися як відкриті документи за наявності письмової згоди організацій, що їх підготували, або правонаступників цих організацій.

Крім того, є формальні підстави перегляду статусу службової інформації кожного разу, коли запитується дана інформація (документ), бо частиною 4 статті 6 Закону України «Про доступ до публічної інформації» встановлено, що інформація з обмеженим доступом має надаватися розпорядником інформації, якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

1.2. Зміст правових заходів захисту службової інформації

Нормативно-правові акти надають різні визначення поняття «захист інформації», зокрема його визначають як сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією (п. 2.8 Положення про порядок та умови видачі інформації з Єдиного ліцензійного реєстру, затвердженого наказом Ліцензійної палати при Мінекономіки України від 15.11.1996 р. № ЛП-37. Крім того, Законом України «Про державну таємницю» від 21.01.1994 р. № 3855-XII вживається термін «охорона державної таємниці» — як комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню таємної інформації та втратам її матеріальних носіїв. Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР поняття «захист інформації в системі» розглядається як діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Крім того, законодавство не диференціює поняття «охорона» і «захист» інформації. Так, «термін «охорона» у термінологічних словосполученнях Конституції України, вживається для позначення достатньо широкого кола повноважень державних органів, що передбачають, зокрема, запобігання правопорушенням, їх недопущення та відновлення прав і свобод у випадку їх порушення, а також притягнення винних до юридичної відповідальності. Головною особливістю вживання цього терміна у Конституції є його вживання зі

значенням, аналогічним терміну «захист» як обов'язку держави та інших зобов'язаних суб'єктів до дій щодо забезпечення прав і свобод людини». Отже, «терміни «захист» та «охорона» у нормативному контексті вживаються як синоніми чи схожі за значенням поняття щодо мети, завдань, методів та суб'єктів забезпечення прав, тому можуть використовуватись у практиці як ідентичні поняття. Однак в науці інформаційного права вони не розглядаються як тотожні. Охорона інформації - встановлення її загального правового режиму, захист, заходи, які використовуються у тих випадках, коли суб'єктивні права на інформацію порушені або залишаються спірними. Проте в цій частині дослідження термін «захист інформації» доцільно застосовувати в тому широкому значенні, яке йому надає законодавець, воно включає як заходи, спрямовані на відвертання можливості неправомірних дій з службовою інформацією, так і заходи, спрямовані на захист і відновлення вже порушених прав.

Отже, нормативно-правове розуміння правових заходів захисту інформації, в тому числі й службової, зводиться до системи правових, організаційних, інженерних, технічних заходів, що спрямовані на збереження цілісності службової інформації та запобігання її витоку.

Таким чином, правові заходи захисту службової інформації можна визначити як сукупність методів, засобів і прийомів, спрямованих на забезпечення інформаційної безпеки людини, суспільства і держави у всіх сферах їх життєво важливих інтересів. Сутність їх полягає у виявленні, вилученні і нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації, а цілі і методи адміністративно-правового захисту службової інформації здійснюються виходячи з її змісту.

Тому зміст правового захисту службової інформації ототожнюється з процесом забезпечення інформаційної безпеки як необхідності нормального функціонування держави, суспільства, окремої людини.

Дійсно, захист інформації організовує і здійснює власник, користувач інформації або уповноважена ними особа (фізична чи юридична), а також держава в особі компетентних органів, у межах своєї правоохоронної функції. Захистом інформації власник охороняє свої права на володіння і розпорядження

інформацією, намагається запобігти незаконному заволодінню нею і використанню її на шкоду власним інтересам. Система захисту може бути різна, на розсуд власника, а може і не мати такого захисту взагалі. Він здійснюється на основі диспозитивних методів, що входять у сферу цивільно-правового розгляду. Захист інформації стає предметом адміністративно-правового регулювання у випадках, коли обмеження доступу до інформації прямо передбачені законами, коли ці обмеження пов'язані із забезпеченням інформаційних прав і свобод людини, інформаційних аспектів національної, державної, громадської безпеки, моральності, громадського здоров'я тощо і, що дуже важливо, суб'єктом застосування цих обмежень є держава в особі її компетентних органів.

Захист службової інформації можна визначити як комплекс дій власника інформації для забезпечення прав на її володіння і розпорядження, а також сприяння життєдіяльності людини, суспільства і держави на основі створення органами управління безпечних умов, що обмежують розповсюдження і виключають або істотно ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв.

Форми правового захисту службової інформації традиційно можна класифікувати на юрисдикційні і не юрисдикційні. До перших відносяться – захист порушених прав суб'єктів інформаційних правовідносин в судовому та адміністративному порядку. До других – організаційні, технічні, криптографічні адміністративно-правові засоби захисту службової інформації.

Механізм захисту службової інформації є певним поєднанням, організаційних, технічних, криптографічних і юрисдикційних засобів захисту інформації. Усі вони є правовими оскільки встановлюються правовими актами управління, у тому числі нормативно-правовими актами. Таким чином, адміністративно - правовий захист службової інформації – це діяльність щодо застосування юрисдикційних і не юрисдикційних форм її захисту.

Організаційно–правові заходи захисту службової інформації – це комплекс дій і засобів, спрямованих на створення ефективних умов для забезпечення інформаційної безпеки в органах публічної влади. У залежності від фінансових можливостей, статусу суб'єкта, що реалізовує повноваження власника відносно

інформаційних ресурсів, змісту службової інформації цей комплекс заходів може розроблятися посадовцями, які відповідають за забезпечення інформаційної безпеки або підрозділами служби інформаційної безпеки.

Різноманітні моделі і рекомендації щодо створення системи організаційних заходів захисту службової інформації ґрунтуються на універсальному комплексі послідовних заходів:

- формування служби інформаційної безпеки або призначення особи (групи осіб), відповідальних за забезпечення інформаційної безпеки в цій структурі органу виконавчої влади;

- призначення відповідальних осіб у виділених приміщеннях, на конкретних інформаційних об'єктах, а також в приміщеннях, де зберігається службова інформація, у тому числі і на паперових носіях;

- розробка і затвердження плану заходів щодо забезпечення інформаційної безпеки (річного, квартального, місячного тощо);

- конкретизація плану з певною метою, завданнями, місцем і часом здійснення заходів;

- навчання, підвищення кваліфікацій фахівців щодо забезпечення захисту службової інформації, контроль за рівнем їх підготовки з урахуванням можливостей бюджетного фінансування.

Вказані вище плани і заходи щодо організаційного забезпечення безпеки інформації, безумовно, мають свою специфіку відносно окремих видів інформаційних ресурсів і регламентуються підзаконними нормативно-правовими актами, які зважаючи на межі даного видання розглядатися не будуть, адже, як правило, мають гриф обмеження доступу. Проте на рівні законів встановлюються загальні напрями комплексу адміністративно-правових заходів щодо забезпечення захисту службової інформації, у тому числі й організаційних. Комплекс організаційних заходів забезпечення захисту службової інформації створює основу для використання технічного захисту службової інформації – засобів, спрямованих проти несанкціонованого доступу до цієї інформації, проти її спотворення, блокування, знищення.

Діяльність щодо технічного захисту службової інформації, що підлягає ліцензуванню, повинна відповідати наступним вимогам: наявність спеціальної освіти у осіб, що її здійснюють або наявність у них спеціальної підготовки; відповідність виробничих приміщень, виробничого, випробувального і контрольно-вимірювального устаткування технічними нормами і вимогами, встановленими державними стандартами і нормативно-методичними документами щодо технічного захисту службової інформації; використання сертифікованих (атестованих за вимогами безпеки інформації) автоматизованих інформаційних систем і засобів їх захисту; використання третіми особами програм для ЕОМ або баз даних на підставі договору з їх правовласниками.

Криптографічний захист інформації – це захист інформації за допомогою шифрувальних засобів (криптографічні система захисту інформації - КСЗІ). Даний вид заходу здійснюється на підставі спеціальної Інструкції, що визначає порядок організації і забезпечення безпеки зберігання, обробки, передачі по каналах зв'язку з використанням криптографічних засобів захисту інформації обмеженого доступу, державною таємницею. Слід зазначити, що ліцензіати відповідно до цієї інструкції зобов'язані забезпечувати комплексність захисту службової інформації - тобто використовувати інші засоби захисту, окрім криптографічних, в їх оптимальному поєднанні. Так, наприклад, усі співробітники органів криптографічного захисту інформації зобов'язані дотримуватись вимог щодо надійного зберігання експлуатаційної і технічної документації, ключових документів (ключів, шифрів), негайно вживати заходи щодо відвертання та просочування інформації у разі втрати, розкрадання, недостачі КСЗІ, ключів, шифрів посвідчень, пропусків тощо. Порушені права можуть бути відновлені також в результаті розгляду судом заяви громадянина про неправомірність дії посадовця або колегіального органу. До юрисдикційних форм захисту відноситься також застосування кримінальних, адміністративних, а також дисциплінарних санкцій.

Юрисдикційні форми реалізації правових заходів захисту службової інформації у сфері діяльності державної влади реалізуються з метою відновлення

порушених прав суб'єктів інформаційних правовідносин. До таких заходів, у першу чергу, ми відносимо:

- *віднесення* відомостей до службової інформації;

- *організація діловодства у якому використовується* службова інформація, що є основою для *реєстрації* інформаційних ресурсів;

- *облік* всіх без винятку інформаційних ресурсів, що містять службову інформацію;

- *обмеження доступу* до службової інформації, що забезпечується системою їх захисту;

- *правовий захист* службової інформації, що виражається існуванням правових норм, якими передбачено настання юридичної відповідальності за порушення законодавства про службову інформацію.

1.3. Порядок віднесення відомостей до службової інформації органів публічної влади в системі правових заходів

В наш час Україна і вся світова спільнота знаходяться на хвилі інформаційного буму. Як свідчить міжнародна практика та сучасна ситуація в країні, правова неврегульованість процесів обміну інформації призводить до того, що загальнодоступними стають відомості, які мають обмежений доступ. Це завдає серйозного збитку не лише окремим громадянам та організаціям, але і безпеці усієї держави.

Не є таємницею, що діяльність органів публічної влади у значній мірі пов'язана з отриманням і використанням відомостей обмеженого доступу, розголошення яких може спричинити порушення конституційних прав громадян, а також зниження ефективності роботи державних органів.

В процесі здійснення своєї діяльності державні службовці органів державної влади отримують інформацію про режим і характер роботи підприємств, розташованих на певній території, відомості, що стосуються особистого життя громадян, а також іншу інформацію (наприклад, службового характеру). Ця інформація, а також відомості про окремі методи, прийоми і

результати роботи органів державної влади можуть складати зміст інформації з обмеженим доступом. Розголошення таких відомостей, а також витік такої інформації може порушити нормальну їх діяльність і значно знизити її ефективність.

До того ж, актуалізується необхідність дослідження інформаційної відкритості феномену влади, визначення меж ефективності механізму її здійснення в рамках управління потребує поєднання знання про публічну політику та сучасне управління (включаючи навички впровадження інновацій в управлінську сферу та знання про сучасні інформаційні технології управління).

Крім того, на пошук нових теоретико-методологічних підходів до розв'язання зазначених проблем наштовхує потреба подолання перманентного кризового стану публічної влади, при поглибленні негативних тенденцій в державному управлінні. На жаль, основною проблемою трансформаційних процесів в Україні є те, що нові завдання вирішуються в основному старими заходами, оскільки нові демократичні механізми в державних інституціях та суспільстві відсутні. Разом з тим, головним елементом демократичного суспільства, який передбачає узгодження інтересів різних суспільних груп у процесі підготовки та ухвалення рішень органами влади є інформаційна відкритість публічної влади. Глибинна суть публічної політики полягає у залученні до процесу прийняття політичного рішення всіх зацікавлених сторін у вирішенні конкретної проблеми.

Проте, сьогодні можемо констатувати випадки, коли окремі державні органи проводять власну інформаційну політику, нерідко спрямовану на компрометацію інших інститутів влади. А це вже може стосуватися питання гарантування національної інформаційної безпеки.

Водночас, як зазначають фахівці СБ України, аналіз матеріалів практики вказує, що у переважній більшості випадків доступ до інформації обмежується штучно, а дії державних службовців підпадають під категорію корупційних. Причини цього вбачаються, насамперед, у бажанні посадових осіб державних органів та установ, використовуючи своє службове становище, приховати

інформацію про протиправні дії або злочинну бездіяльність і уникнути відповідальності.

Поряд із визначеними проблемами реалізації правових заходів захисту службової інформації органів публічної влади, основною, на нашу думку, залишається відсутність законодавчого її визначення. Адже пунктом 3 ст. 21 Закону «Про інформацію» встановлено, що "порядок віднесення до «… службової інформації, а також порядок доступу до неї регулюються законом». Попри це жодного єдиного порядку віднесення інформації до службової не встановлено ні Законом «Про інформацію», ні Законом «Про доступ до публічної інформації», ні іншим законом. Закон «Про доступ до публічної інформації» лише повторює «відповідно до закону». Дана проблема зумовила і значну кількість проблем правозастосовного характеру, зокрема, органи державної влади часто під грифом службової інформації приховують цілком відкриту інформацію.

Потреба у «втаємниченні» службової інформації пов'язана тим, що органам влади в певних випадках потрібно обговорювати й приймати рішення не публічно (щоб не спричинити ажіотажу, спекуляцій на ринку, приховування доказів чи фактів правопорушень і т.п.), якщо йдеться про інформацію з документів суб'єктів владних повноважень, що становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами публічної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень, а також тим, що окремі масиви інформації правоохоронних органів не потребують складних заходів захисту як у державній таємниці, але їхнє оприлюднення дуже ймовірно зашкодить інтересам держави, суспільства чи окремих суб'єктів, якщо йдеться про інформацію зібрану в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, які не віднесено до державної таємниці.

Попри проаналізовані окремі нормативні акти, в яких містяться норми, що визначають зміст та обсяг прав громадян на доступ до публічної інформації, базовим законом в даному аспекті є Закон «Про доступ до публічної інформації» від 13 січня 2011 року. Безумовно, прийняття даного закону стало певним

проривом у розвитку демократичних процесів в нашій державі. Проте, детальний аналіз згаданого закону змушує нас акцентувати увагу на принципових, на наш погляд, його позиціях щодо регулювання окремих аспектів доступу до службової інформації.

Зокрема, Закон «Про доступ до публічної інформації» не містить норми відповідно до якої після прийняття рішення інформація, що була віднесена до службової інформації доступ до якої було обмежено стає відкритою. А це означає, що в разі, якщо інформація все таки буде віднесена до службової інформації для того, щоб журналіст чи скажемо пересічний громадянин отримав доступ до неї необхідно буде звертатися до суду. На нашу думку, доцільно було б закріпити норму, відповідно до якої відкритою з дня прийняття рішення ставала інформація (у т.ч. службова):

1) що міститься у документах суб'єктів владних повноважень і становить внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробленням напрямів діяльності установи, процесом прийняття рішень і передують їх публічному обговоренню та/або прийняттю;

2) зібрана у процесі здійснення контрольних або наглядових функцій органами державної влади.

Крім вже зазначеного, підкреслимо, що Закон «Про доступ до публічної інформації» визначає (п. 2 ст.6) три загальні умови обмеження доступу до інформації:

- виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

- розголошення інформації може завдати істотної шкоди цим інтересам;

- шкода від оприлюднення такої інформаціє переважає суспільний інтерес в її отриманні.

Наявність одночасно всіх цих умов суб'єкт владних повноважень має встановити, приймаючи рішення про обмеження доступу до певної інформації.

Іншими словами, ми вважаємо, що інформацію можна віднести до службової тільки за умови проходження, так званого трискладового тесту. Перша складова полягає в тому, що інформація закривається лише тоді, коли її розповсюдження може загрожувати легітимній меті (захист національної безпеки, територіальної цілісності і т.д.). Але цього недостатньо, для обмеження доступу до інформації треба застосовувати другу складову: з'ясувати чи шкода від розповсюдження конкретної інформації буде суттєвою. Третя складова визначає: а що суттєвіше шкода від оприлюднення такої інформації чи від її втаємничення? Закриваючи доступ до будь-якої інформації орган влади повинен довести усі три складові.

Варто зазначити, що трискладовий тест — це новела, запроваджена Законом «Про доступ до публічної інформації» і органи влади ще не мають досвіду в її застосуванні, що ймовірно призведе до численних суперечок та судових спорів. Одним із таких можна визнати Рішення Львівської міської ради № 737 від 05.08.2011 Про затвердження переліку відомостей, які не містять ознак публічної інформації. Проблема полягає в тому, що Закон України «Про доступ до публічної інформації» не передбачає такого поняття як перелік відомостей, які не містять ознак публічної інформації. Більше того, відомості, зазначені у Переліку, є публічною інформацією. Таким чином, у даному рішенні порушені порядок та умови віднесення публічної інформації до категорії службової інформації.

Визнання інформації суспільно необхідною є безперечним юридичним фактом, котрий дозволяє поставити питання про поширення такої інформацію без згоди її власника. Н. Петрова справедливо стверджує, що «тема суспільної значимості інформації виникає щоразу, коли є легітимні підстави обмеження доступу до певної інформації, і з'являється право громадськості дізнатися про неї».

Незважаючи на той факт, що у Законі України «Про доступ до публічної інформації» терміни «суспільно необхідна інформація», «суспільний інтерес» згадується декілька разів, їх визначення відсутнє. Ми вважаємо, що необхідність визначення цієї правової конструкції є вкрай необхідною, адже доведення у суді факту, що певна інформація з обмеженим доступом є суспільно необхідною, дає

підставою для прийняття рішення про надання такої інформації за запитами (наприклад, інформація про стан здоров'я кандидатів у президенти, або президента чи скажімо народних депутатів). Або такий аргумент: на підставі встановлення факту, що певна інформація з обмеженим доступом є суспільно значимою, особа може бути звільнена від відповідальності за розповсюдження цієї інформації з обмеженим доступом (наприклад у випадку крайньої необхідності розголошення державної таємниці).

Натомість в оновленій редакції Закону України «Про інформацію» з'явилося положення відповідно до якого під суспільно необхідною інформацією розуміється інформація, що є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Разом із тим виникає необхідність з'ясувати, що саме означає категорія «суспільний інтерес». Для цього необхідно відповісти на три запитання.

1. *Коли з'являється потреба апелювати до цієї категорії?*

Це відбувається кожного разу, коли виникає потреба отримати певну публічну інформацію, а вона була неправомірно віднесена до інформації з обмеженим доступом. Тоді необхідно звертатися до суду з вимогою визнати незаконність дій суб'єкту владних повноважень. Відмова в наданні інформації може бути мотивована суб'єктом владних повноважень або юридичною особою приватного права тим, що запитувана інформація є конфіденційною. Тоді слід вимагати судового рішення щодо надання цієї інформації через те, що вона становить суспільний інтерес. Наприклад, стан здоров'я народних депутатів, відомості про доходи і майно вищих посадових осіб тощо. Нарешті, ми згадуємо, що інформація становить суспільний інтерес, коли одночасно доступ до неї обмежений, і за розповсюдження такої інформації притягають до відповідальності.

2. За якими критеріями та за яких умов можна стверджувати, що інформація становить суспільний інтерес?

Звернемося до ст. 29 Закону України «Про внесення змін до Закону України «Про інформацію». Відповідно до цієї статті «Інформація з обмеженим доступом

може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо».

Тобто, відповідно до цієї статті необхідно встановити: 1) яка інформація суспільно необхідною, тобто є предметом суспільного інтересу; 2) чи право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. Труднощі тут полягають в тому, що термін «предмет суспільного інтересу» є також оціночною категорією.

Практична рекомендація, яка ж, власне, інформація становить суспільний інтерес, пропонують автори книги «Свобода інформації: теорія та практика». Зокрема, Р. Карвер, пропонує при вирішенні питання, чи є інформація суспільно необхідною, виходити з того, що суспільний інтерес означає, що громадськість має вигоду від того, що певна інформація стане доступною. Він також звертає увагу на той факт, що важко визначити, яка ця вигода могла б бути, тому що, природно, за його словами, що вона змінюватиметься від справи до справи.

Досить слушними можуть виявитися для практичного застосування наведені Р. Карвером критерії, складені Комітетом з Етики Британського Національного Союзу Журналістів (NUJ):

a) Виявлення чи викриття злочину чи серйозного проступку;

b) Захист суспільного здоров'я чи безпеки;

c) Запобігання введенню в оману громадськості певними твердженнями чи діями з боку особи чи організації;

d) Викриття неналежного використання державних коштів чи інших форм корупції в державних органах;

e) Розкриття потенційних конфліктів інтересів у тих, хто посідає владні і впливові місця;

f) Викриття жадібності корпорацій;

g) Викриття лицемірної поведінки тих, хто займає високі посади.

Із представлених у науковій літературі думок з приводу того, яка інформація становить суспільний інтерес, заслуговує на увагу визначення, запропоноване В. Речицьким, а також критерії, розроблені Н. Петровою.

В.Речицький пропонує до інформації, що становить суспільний інтерес, відносити інформацію, яка свідчить про загрозу державному суверенітету та територіальній цілісності України, порушення інтересів територіальних громад і права власності народу України; дозволяє здійснити обґрунтований політичний вибір; гарантує обізнаність із подіями та фактами, що безпосередньо впливають на стан і характер життя людини; забезпечує реалізацію конституційних прав, основоположних свобод і обов'язків; запобігає правопорушенням, введенню громадськості в оману, а також шкідливим екологічним та іншим наслідкам від діяльності (бездіяльності) суб'єктів господарювання тощо.

Н. Петрова пропонує при вирішенні питання, чи становить інформація суспільний інтерес, брати до уваги:

1) чи суперечить чиясь поведінка посадовому обов'язку;

2) чи йдеться про наявність правопорушення;

3) чи є ознаки зловживання владою;

4) чи йдеться про недбале виконання обов'язків або неналежне управління публічним (державним) органом;

5) чи наявна корупція (невиправдане використання державних/громадських коштів) або шахрайство;

6) чи йдеться про загрозу здоров'ю, безпеці особи, групі осіб, довкіллю;

7) чи посадова особа вводила в оману громадськість публічними заявами;

8) судову помилку;

9) якщо йдеться про інтереси національної безпеки;

10) якщо йдеться про економічний добробут; 11) якщо йдеться про права людини.

Критерії, запропоновані В.Речицьким та Н.Петровою, дають можливість найбільш точно встановити, яку інформацію слід відносити до інформації, що становить суспільний інтерес.

3. Хто має вирішувати, чи становить інформація суспільний інтерес?

Така необхідність з'являється у розпорядника інформації, який отримав запит щодо надання інформації з обмеженим доступом, але запитувана інформація становить суспільний інтерес, і тоді розпорядник інформації має застосувати трискладовий тест. Така необхідність виникає у судді, який розглядає позов з вимогою визнати незаконність дій суб'єкту владних повноважень щодо віднесення певної інформації до інформації з обмеженим доступом, або вирішує питання, чи можна надати у відповіді на запит конфіденційну інформацію, яка становить суспільний інтерес. Визнати, чи є інформація суспільно необхідною, суддя мусить також, коли вирішується питання щодо звільнення від відповідальності за розповсюдження інформації обмеженим доступом через те, що розповсюджена інформація є суспільно необхідною.

Зауважимо, що, оскільки відповідно до ч. 2 ст. 71 Кодексу адміністративного судочинства України «обов'язок доказування в адміністративних справах про протиправність рішень, дій чи бездіяльності суб'єкта владних повноважень покладається на відповідача, якщо він заперечує проти адміністративного позову»**,** то варто вимагати, щоб при розгляді справи суб'єкт владних повноважень довів, що віднесення публічної інформації до інформації з обмеженим доступом відбувалося з дотриманням вимог зафіксованих у ст. 6 Закону «Про доступ до публічної інформації». Тобто представник суб'єкту владних повноважень повинен обґрунтувати в суді, що інформація закривалася для захисту певної легітимної мети, пояснити, яку саме істотну шкоду може завдати розголошення цієї інформації, та чому ця шкода переважає право громадськості мати доступ до цієї інформації.

Підсумовуючи, відмітимо, що відповідно до ст. 9 Закону України "Про доступ до публічної інформації", до службової інформації "може" належати, окрім зібраної в процесі оперативно-розшукової, контррозвідувальної діяльності та у сфері оборони країни, лише інформація "що міститься в документах суб'єктів

владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов’язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами публічної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень”.

Вищенаведений абзац містить обов’язкові і виключні умови, за одночасної наявності яких інформацію лише і може бути віднесено до службової:

1. Інформація має міститься у “внутрівідомчій” службовій кореспонденції, доповідних записках і рекомендаціях.

2. Такі документи мають бути пов’язані з розробкою напрямку діяльності відповідного органу чи зі здійсненням його контрольних чи наглядових функцій.

3. Такі документи мають передувати публічному обговоренню та/або прийняттю рішень.

Іншими словами, фактично на статус службової інформації може претендувати лише внутрішнє листування та обговорення перед прийняттям конкретного рішення, або документи щодо здійснення перевірок до прийняття рішення про результати перевірок. Це означає, що публічна інформація не може бути віднесена до службової, якщо ця інформація вже міститься у рішенні відповідного органу, у тому числі й в актах індивідуальної дії (указ, наказ, рішення, розпорядження, постанова та ін.), за виключенням інформації, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни. Таким чином, рішення органів виконавчої влади не можуть бути віднесені до службової інформації. Для прикладу, не може бути надано гриф «ДСК» Постанові, Розпорядженню Кабінету Міністрів України, Наказу Податкової Адміністрації України та ін.

Відповідно до ст. 5 Закону України “Про оперативно-розшукову діяльність” оперативно-розшукова діяльність здійснюється оперативними підрозділами:

- Міністерства внутрішніх справ України - кримінальною, транспортною та спеціальною міліцією, спеціальними підрозділами по боротьбі з організованою злочинністю, забезпечення безпеки працівників суду, правоохоронних органів і учасників кримінального судочинства;

- Служби безпеки України - розвідкою, контррозвідкою, військовою контррозвідкою, захисту національної державності, спеціальними підрозділами по боротьбі з корупцією та організованою злочинністю, оперативно-технічними, внутрішньої безпеки, оперативного документування, боротьби з тероризмом і захисту учасників кримінального судочинства та працівників правоохоронних органів;

- прикордонних військ - підрозділами по оперативно-розшукової роботи;

- управління державної охорони - підрозділом оперативного забезпечення охорони виключно з метою забезпечення безпеки осіб та об'єктів, щодо яких здійснюється державна охорона;

- органів державної податкової служби - оперативними підрозділами податкової міліції;

- органів і установ Державного департаменту України з питань виконання покарань - оперативними підрозділами.

Проведення оперативно-розшукової діяльності іншими підрозділами зазначених органів, підрозділами інших міністерств, відомств, громадськими, приватними організаціями та особами забороняється.

Щодо контррозвідувальної діяльності, то згідно ст. 5 Закону України «Про контррозвідувальну діяльність» спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності є Служба безпеки України. Окремі контррозвідувальні заходи виключно в інтересах забезпечення охорони державного кордону України, посадових осіб, стосовно яких здійснюється державна охорона, а також забезпечення безпеки своїх сил і засобів, інформаційних систем та оперативних обліків можуть проводити розвідувальні органи України та Управління державної охорони України. Здійснення контррозвідувальних заходів іншими суб'єктами, крім визначених цим Законом, забороняється.

Таким чином, обмеженню в доступі може підлягати лише та службова інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу 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.

Відповідно до вищенаведеного, ми вважаємо, що не може бути віднесено до службової інформації:

1) інформацію котра міститься у міжвідомчій кореспонденції (наприклад, Міністерство А пише Держдепартаменту Б).

2) документи, не пов’язані з розробкою напрямків діяльності державних органів чи здійсненням його контрольних чи наглядових функцій (наприклад, інформацію про фінансову діяльність).

3) інформацію у документах, що не передують публічному обговоренню та/або прийняттю рішень. Зокрема – і це надважливо – власне рішення, тобто нормативно-правові чи індивідуально-правові акти. Іншими словами, відповідно до закону держава (органи влади, посадові особи) та органи місцевого самоврядування взагалі не мають права надавати гриф «для службового користування» і не оприлюднювати абсолютно всі (за винятком тих, що мають гриф таємності за Законом «Про державну таємницю») правові акти.

Крім зазначеного, на нашу думку, не підлягають віднесенню до службової інформації:

- відомості, що становлять державну таємницю;

- відомості, які не відносяться до інформації з обмеженим доступом в силу положень Конституції України, закону «Про інформацію»;

- відомості, що входять до складу інформації про діяльність державних органів та органів місцевого самоврядування, обов'язкову для розміщення в інформаційних системах загального користування;

- відомості, що підлягають поширенню в засобах масової інформації у випадках, встановлених законами;

- відомості про обставини, що створюють безпосередню загрозу для життя і здоров'я людей;

- відомості, що містяться в документах і матеріалах, що безпосередньо зачіпають права і свободи громадянина, за запитом цієї особи, якщо інше не передбачене законами;

- відомості, відносно яких режим обмеженого доступу скасований судовим рішенням;

- відомості, що містяться в судових рішеннях, які набрали чинності, якщо інше не передбачене в самому судовому рішенні або у законах;

- дані про стан здоров'я осіб, що займають державні посади України;

- відомості про привілеї, компенсації і пільги, що надаються державою громадянам, посадовцям, підприємствам, установам та організаціям;

- дані про умови постачання товарів, виконання робіт, надання послуг для державних (муніципальних) потреб, за винятком відомостей, що становлять державну таємницю.

Слід зазначити, що це повністю відповідає п.3 ст.14 Закону «Про інформацію», за якою «з метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття» – тобто всіх актів.

При цьому, зауважимо, що віднесенню до службової інформації в обов'язковому порядку, на нашу думку, підлягають:

а) відомості, що добровільно передаються в установленому порядку в державні органи та органи місцевого самоврядування фізичними особами або організаціями за умови збереження їх конфіденційності, якщо вимога збереження їх конфіденційності є законною й обґрунтованою;

б) відомості, пов'язані з умовами для постачання товарів для державних потреб запропонованими організаціями, допущеними в установленому порядку до участі в конкурсах (тендерах) на постачання товарів для державних потреб;

в) персональні дані фізичних осіб, що знаходяться у розпорядженні державного органу або органів місцевого самоврядування у зв'язку з виконанням своїх повноважень;

г) відомості про діяльність державних органів та органів місцевого самоврядування, віднесені до службової інформації відповідно до закону.

До службової інформації можуть відноситись також і:

а) відомості, пов'язані з підготовкою проектів індивідуальних правових і нормативних правових актів, включаючи тексти проектів таких актів, якщо їх передчасне поширення і (чи) розголошування завдасть шкоди життєво важливим інтересам особи, суспільства і держави або призведе до створення односторонніх переваг для суб'єктів, що отримали доступ до вказаних відомостей;

б) відомості про заплановані перевірки які проводяться за дотриманням законодавства України;

в) відомості про авторство пропозицій і особисті позиції, викладені під час обговорень, консультацій в процесі роботи державного органу, органу місцевого самоврядування, за винятком випадків, коли автор публічно оголошує ці відомості або не заперечує проти розкриття відомостей свого авторства;

г) відомості про внутрішньовідомчі і міжвідомчі обговорення, консультації робочого і підготовчого характеру, включаючи протоколи нарад, службові записки, довідкові та інші матеріали, що мають підготовчий характер, якщо інше не передбачене законами.

Проте, діяльність органів публічної влади з організації роботи по доступу до публічної інформації часто характеризується «втаємничуванням» відкритої інформації. Зокрема, основними порушеннями, що зафіксовано при аналізі окремих підзаконних нормативних актів органів влади, яким встановлено перелік відомостей, які становлять службову інформацію і яким надається гриф «Для службового користування» є наступні:

1. До переліку включено відомості, що відносяться до інших типів обмеження інформації, конфіденційної та таємної, яка не може міститись в цьому списку.
2. Значна частина переліків службової інформації закінчується словами «інші відомості» або «примітки», що суперечить вимогам законодавства і створює передумови для безпідставного обмеження доступу до інформації у майбутньому.
3. В перелік внесено інформацію, що не відноситься до службової і має значний суспільний інтерес. Наприклад, в переліку обласної ради до службової

віднесено інформацію про номерні знаки робочих автомобілів керівництва органу влади.

4. При формуванні переліків інформації з обмеженим доступом, органами влади не дотримано вимоги, що передбачає проведення трискладового аналізу даних перед її обмеженням.

5. Органи влади незаконно обмежують доступ до розпоряджень та інструкцій щодо присвоєння грифів «ДСК».

У зв’язку із наведеним основними принципами віднесення відомостей про діяльність органів публічної влади до службової інформації є:

- законність віднесення відомостей про діяльність органів публічної влади до службової інформації;

- обґрунтованість віднесення відомостей про діяльність органів публічної влади до службової інформації;

- своєчасність віднесення відомостей про діяльність органів публічної влади до службової інформації і зняття режиму обмеженого доступу;

- пріоритет прав і свобод людини та громадянина перед правами інших суб'єктів правовідносин;

- захист прав користувачів (споживачів) інформації на доступ до інформації;

- відкритість і громадський контроль за діяльністю органів публічної влади;

- захист прав громадян на недоторканість приватного життя, таємницю листування, телефонних переговорів, поштових телеграфних та інших повідомлень;

- відповідальність за порушення права користувачів (споживачів) інформації на доступ до інформації про діяльність органів публічної влади у зв'язку з незаконним і (чи) необґрунтованим її віднесенням до службової інформації, або з ненаданням інформації, що не становить службову інформацію, а також за незаконне поширення інформації, що становить службову інформацію.

Віднесення відомостей, що знаходяться в органі публічної влади до службової інформації повинно здійснюватися уповноваженими посадовцями органу публічної влади відповідно до Переліку відомостей, що становлять службову інформацію. Склад посадовців, наділених повноваженнями щодо

віднесення відомостей, які знаходяться в органі публічної влади до службової інформації (далі - уповноважені посадовці), затверджується керівником органу публічної влади. Дані особи при створенні документу самостійно визначають в нім ознаки наявних відомостей, що становлять службову інформацію. Віднесення відомостей, що знаходяться в органі публічної влади до службової інформації, здійснюється відповідно до принципів законності, обґрунтованості, своєчасності.

Принцип законності полягає в забезпеченні відповідності відомостей, відносно яких органами публічної влади застосовується режим обмеженого доступу, Переліку відомостей, що становлять службову інформацію.

Принцип обґрунтованості полягає у встановленні доцільності віднесення конкретних відомостей, що знаходяться в органі публічної влади до службової інформації з урахуванням вірогідних наслідків такого рішення, виходячи з інтересів громадянина, суспільства і держави.

Принцип своєчасності полягає в необхідному встановленні режиму обмеженого доступу на поширення відомостей, що знаходяться в органі публічної влади віднесених до службової інформації, з моменту їх отримання, створення (встановлення) або завчасно, а також необхідності відміни режиму обмеженого доступу негайно при втраті підстав для віднесення відомостей до службової інформації.

У разі, коли на думку відповідальної особи за створення документа у створюваному документі містяться відомості, що становлять службову інформацію, то особа в установленому порядку повинна звернутися до уповноваженого посадовця органу публічної влади з пропозицією про віднесення відомостей, що містяться в документі, до службової інформації.

Уповноважений посадовець органу публічної влади, на нашу думку, має бути наділений такими повноваженнями:

- перевіряє в установленому порядку документи на предмет наявності в них відомостей, які визнаються службовою таємницею відповідно до принципів законності, обґрунтованості і своєчасності;

- періодично, але не рідше, ніж через кожні шість місяців, проводиться перевірка осіб, котрі знаходяться в органах публічної влади документів, що містять відомості, які становлять службову таємницю;

- складає і веде регістр документів, що містять відомості, які становлять службову таємницю;

- приймає рішення про відміну режиму обмеженого доступу до відомостей, що становлять службову таємницю, у зв'язку з втратою або відсутністю можливості настання несприятливих наслідків від передчасного розголошування і (чи) поширення цих відомостей;

- несе в установленому порядку дисциплінарну та іншу відповідальність за законність та обґрунтованість прийнятих ним рішень про встановлення режиму обмеженого доступу до відомостей, що знаходяться в органах публічної влади.

Питання для самоперевірки.

1. Дайте визначення захисту службової інформації;

2. Чим відрізняється захист від охорони службової інформації;

3. Що Ви розумієте під терміном «правові заходи захисту службової інформації»;

4. Перерахуйте основні правові заходи захисту службової інформації;

5. Які Ви можете визначити юридичні форми захисту службової інформації;

6. Розкрийте порядок віднесення інформації до службової;

7. Визначіть умови віднесення інформації до службової;

8. Назвіть основні принципами віднесення відомостей про діяльність органів публічної влади до службової інформації;

9. Розкрийте особливості документування службової інформації;

10. Що передбачає правовий режим службової інформації.

Використані та рекомендовані джерела

1. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства: монографія / В.С. Цимбалюк. – К.: Освіта України, 2011. – 426 с.

2. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності: навч. посібник. — К. : Скіф; КНТ, 2008. — 343с.

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : [уч. пособ.] /Шаньгин В.Ф. – М. : Форум, 2008. – 416 с.

4. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135. – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2135-12

5. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 374. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/374-15

6. Наказ Про затвердження Переліку відомостей, що становлять службову інформації у Головному управлінні юстиції у Львівській області від 21.07.2011 р. № 1180. – [Електронний ресурс]. – Режим доступу: obljust.lviv.ua/files/nakaz3.doc.

7. Перелік відомостей, що містять службову інформацію та яким присвоюється гриф обмеження доступу «Для службового користування» в органах державної податкової служби України : наказ ДПС України від 13.01.2012 № 35. – [Електронний ресурс]. – Режим доступу:http://www.sta.lviv.ua/index.php?id=2137 .

8. Перелік відомостей, що становлять службову інформацію, і яким надається гриф «Для службового користування» : розпорядження голови Буської районної державної адміністрації 24 лютого 2012 року № 59. – [Електронний ресурс]. – Режим доступу:http://busk-rda.gov.ua/articles.php?lng=ua&pg=1396

9. Suski A. Rozwojhistoricznypojeciadocumentuorazprobaichuogolnenia //Akt. probl. inform, i doc. — 1968. — 13, N 4. – C. 22-39

10. Державний стандарт ДСТУ 2732:2004 «Діловодство й архівна справа» : Архівні стандарти і документація. – Нарматівна база – [Електронний ресурс]. – Режим доступу: http://www.archives.gov.ua/Law-base/Standards/

11. ISO 15489-1 - InformationandDocumentation – Recordsmanagement – Part 1: General // ISO – PrintedinSwitzerland. – 2001. – 19 p.

12. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію : Постанова Кабінету Міністрів України від 27 листопада 1998 р. № 1893 (із наступними змінами та доповненнями) [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/1893-98-%D0%BF

13. Про електронний цифровий підпис : Закон України від від 22.05.2003 № 852. – Електронний ресурс. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/852-15

14. Про затвердження Положення про центральний засвідчувальний орган : Постанова Кабінету Міністрів України від 28 жовтня 2004р. № 1451. – Електронний ресурс. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1451-2004-%D0%BF

15. Про авторське право й суміжні права : Закон України від 23.12.1993 № 3792. – Електронний ресурс. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3792-12

16. Колодій І. Поняття та зміст інформації: соціальні та правові аспекти / І. Колодій // Підприємництво, господарство і право. – 2007. – № 1. – С. 83–86

17. Про науково-технічну інформацію : Закон України від 25.06.1993 № 3322. – Електронний ресурс. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/%D0%BF%D1%80%D0%BE%20%D0%BD%D0%B0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE-%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D1%83%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8E

18. Касперський І.П. Зміст службової інформації як нового виду інформації з обмеженим доступом / І.П.Касперський // Актуальні проблеми управління інформаційною безпекою держави : збір. наук.-прак. конф., 22 березня 2011 року, м. Київ. – К. : Наук.-вид. відділ НА СБ України, 2011. – С. 37-43

19. Пастернак М.С. Місце державної таємниці в новій системі класифікації інформації з обмеженим доступом в Україні / М.С.Пастернак //

Актуальні проблеми управління інформацій¬ною безпекою держави : збір. наук.-прак. конф., 22 березня 2011 року, м. Київ. – К. : Наук.-вид. відділ НА СБ України, 2011. – С. 98-102

20. Дідікін А. Механізм реалізації права громадян на доступ до публічної інформації в законодавстві Росії та України / А.Дідікін, М.Кияк // Юридичний журнал. – 2011. - № 4 (106). – С. 49-50

21. Питання забезпечення орга¬нами виконавчої влади доступу до публічної інформації : Указ Президента України від 5 травня 2011 р. № 547/2011 // Урядовий кур'єр. - 2011. - № 84

22. Макаренко В.В. Проблеми інституційного забезпечення контролю за дотриманням законодавства про службову інформацію / ВВ.Макаренко, С.М.Шовкун. – Науково-практичний журнал «Інформаційна безпека людини, суспільства, держави». – № 2. – 2011 р. – С. 111-116

23. Князєв С.О. Несанкціонований витік інформації з обмеженим доступом: сучасні тенденції / С.О.Князєв. – Науково-практичний журнал «Інформаційна безпека людини, суспільства, держави». – № 2. – 2012 р. – С. 105-112

24. УтечкаизPricewaterhouseCoopers: украденыданные 77 тыс. Госслужащих // Информационнаябезопасность. – 2010. – № 3. – С. 77-86.

25. Доля А. Сколькостоитутечкаинформации на самомделе? [Электронный ресурс] / А.Доля // CNEWS. – Режим доступа : http://safe.cnews.ru/

26. Ткачук Т.Ю. Правові засади доступу громадян до публічної інформації у контексті законодавчих змін / Т.Ю.Ткачук. – Науково-практичний журнал «Інформаційна безпека людини, суспільства, держави». – № 2. – 2011 р. – С. 62-69

27. Ткачук Т. Ю. Актуальні теоретичні та практичні проблеми визначення правової природи службової інформації / Т. Ю. Ткачук. – Науково-практичний журнал «Інформаційна безпека людини, суспільства, держави». – № 3. – 2012 р. – С. 51-58.

РОЗДІЛ 2.
ОСОБЛИВОСТІ ПОВОДЖЕННЯ З ДОКУМЕНТАМИ, ЯКІ МІСТЯТЬ СЛУЖБОВУ ІНФОРМАЦІЮ

2.2. Загальні засади реалізація управлінської складової в установах де циркулює службова інформація

Важко переоцінити роль діловодства в забезпеченні управлінської діяльності будь-якої установи чи організації. Не становить винятку й діловодство, яке містить службову інформацію, де поряд із забезпеченням режимних заходів, спрямованих на попередження витоку інформації з обмеженим доступом під час користування документами, повинно обов'язково реалізовувати управлінську складову. Даний аспект, в свою чергу, включає цілу низку заходів, що отримав узагальнюючу назву – документування. Правильна організація документування запорука ефективної управлінської діяльності будь-якої установи в цілому.

За результатами аналітичних досліджень, що проводились в період 2011 – 2013 років на різних установах України, а також порівняння з даними які оприлюднювались іноземними кампаніями було встановлено, що в загальному обсязі управлінської праці, діловодні операції становлять від 25 до 60% в залежності від специфіки діяльності установи.

Документи потрібні всюди, особливо коли мова йде про реалізацію прав людини в суді, органах суспільного захисту, при вирішенні питань власності тощо. Використання писемної документації дозволяє вирішувати цілий ряд завдань:

забезпечити писемну підставу для доказу або обговорення;

передати офіційну або важливу інформацію;

передати офіційне (важливе) повідомлення декільком адресатам;

пояснити складне питання;

зберегти запис повідомлення;

може бути засобом передачі конфіденційного повідомлення.

Документ виступає як основний засіб ділового спілкування, а також можливе юридичне обґрунтування прав та обов'язків різних суб'єктів управління.

Доцільно навести й офіційне визначення поняття «документ» яке подано у Державному стандарті України ДСТУ 2732 - 94 «Діловодство та архівна справа. Терміни та визначення» – це матеріальний об’єкт, що містить у зафіксованому вигляді інформацію, оформлений у зведеному порядку і має відповідно до чинного законодавства юридичну силу.

Створення повноцінного документа включає необхідність детального розуміння питань, що висвітлюються, ознайомлення із супутньою інформацією, уточнення доцільності його виготовлення, кола питань, які підлягають вирішенню, а також врахування нормативно-правових актів діючих в цій сфері.

Таким чином, зрозуміло, що виконання завдань стосовно удосконалення управління в різних сферах діяльності, в тому числі там де використовується службова інформація неможливо без організації на науковій основі її документаційного забезпечення. Це включає застосування новітніх методик, підходів, технологій тощо спрямованих на створення так званої інформаційної бази для реалізації функції управління, в даному випадку організацією, а також забезпечення контрольних заходів.

Потрібно відмітити, що організація діловодства дуже часто сприймається як рутинний процес, звідти й відношення до його важливості і впорядкування персоналом організації, в тому числі керівництвом, набуває значення тільки після появи істотних проблем спричинених суттєвими помилками загального характеру.

Неуважність до організації цієї роботи може призводить до непередбачених витрат, наприклад, оплата штрафних санкцій за результатами перевірок різних інспекцій (податкова, пожежна, сантехнічна, технічна тощо).

Безвідповідальне ставлення до організації діловодства веде до втрат документів на різних етапах документообігу в організації. Зважаючи на наявність в документах службової інформації несанкціонований виток подібних відомостей, при недбалій організації системи спеціального діловодства здатний спричинити організації, най важкі наслідки. В тому числі призвести до її ліквідації.

Потребує окремого пояснення використана дефініція «функція управління». Визначально слово функція є похідним від латинського «function», що означало

виконання, здійснення, пізніше стало розумітись як діяльність. Словосполучення функція управління вже передбачає вид діяльності, який заснований на розподілі управлінської праці. До його ознак відноситься певна складність, відносна стабільність та однорідність стосовно впливу на об'єкт і суб'єкт управління.

Згідно із загальним визначенням «діловодство» – це діяльність, яка охоплює документування та організацію роботи з документами та спрямована на документаційне забезпечення управління.

Обґрунтованість та ефективність управлінського рішення знаходиться у прямій залежності від своєчасності та достатності отриманої інформації. Закон України «Про інформацію» надає наступне визначення поняття «нформація» - документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

При цьому необхідно зважати на постійно зростаючи обсяги інформації. Аналіз тенденції до зростання інформації за останні два десятиліття надав змогу аналітикам впевнено стверджувати, що кожні 4 роки кількість інформації подвоюється і це тільки початок. Звідти збільшується й інформаційна діяльність під якою вищезгаданий Закон України розуміє сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Відповідно, основними видами інформаційної діяльності визначаються одержання, використання, поширення та зберігання інформації.

Одержання інформації - це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою.

Використання інформації - це задоволення інформаційних потреб громадян, юридичних осіб і держави.

Поширення інформації - це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації.

Зберігання інформації - це забезпечення належного стану інформації та її матеріальних носіїв.

Одержання, використання, поширення та зберігання документованої або публічно оголошуваної інформації повинно здійснюватись у порядку, передбаченому Законами України «Про інформацію», «Про доступ до публічної інформації», «Про державну таємницю» та інших законодавчих актів в галузі інформації. Окрім реалізації порядку документування ряд державних стандартів України, закріплює різні визначення та певні процедурні моменти пов'язані з організацією діловодства.

Зразком для організації загального діловодства в країні спочатку стала «Примірна інструкції з діловодства у міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади» введена в дію Постановою Кабінету Міністрів від 17 жовтня 1997 року № 1153.

Пізніше її замінила подібна «Типова інструкція з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади» введена в дію Постановою Кабінету Міністрів від 30 листопада 2011 року № 1242.

Інструкція встановлює загальні правила документування управлінської діяльності міністерств, інших центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих органів виконавчої влади і регламентує порядок роботи з документами з моменту їх створення або надходження до відправлення або передачі в архів установи.

Норми даної інструкції визначають порядок ведення загального діловодства, її положення поширюються на всю службову документацію, в тому числі створювану за допомогою персональних комп'ютерів. Комп'ютерні (автоматизовані) технології обробки документальної інформації повинні відповідати вимогам державних стандартів та цієї Типової інструкції.

Дотримуючись норм Типової інструкції, міністерства та інші центральні органи виконавчої влади та Ради міністрів Автономної Республіки Крим, місцеві органи виконавчої влади повинні розробляти власні інструкції з діловодства.

Управлінська діяльність установ здійснюється шляхом видання розпорядчих документів.

Видання розпорядчих документів установ визначається актами законодавства, положеннями (статутами) про них.

З питань, що становлять взаємний інтерес і належать до компетенції різних установ, можуть прийматися спільні розпорядчі документи.

Підставами для прийняття розпорядчих документів в установах є:

Конституція і закони України, постанови Верховної Ради України, акти Президента України та Кабінету Міністрів України, рішення та постанови Верховної Ради Автономної Республіки Крим, акти Ради міністрів Автономної Республіки Крим;

провадження виконавчої і розпорядчої діяльності з метою виконання установою покладених на неї завдань і функцій;

потреба у правовому регулюванні діяльності.

Суцільний складний текст документа повинен містити граматично і логічно узгоджену інформацію про управлінські дії та використовується під час складання правил, положень, листів, розпорядчих документів.

Як правило, тексти розпорядчих документів і листів складаються з двох частин. У першій зазначається підстава або обґрунтування для складання документа, в другій - висновки, пропозиції, рішення, розпорядження або прохання.

В окремих випадках текст документа може містити лише одну резолютивну частину, наприклад: наказ - розпорядчу частину без констатуючої, лист - прохання без пояснення.

Разом з тим, порядок ведення діловодства, що містить службову інформацію визначається спеціальними нормативно-правовими актами. Але відразу слід зазначити, що акти які регламентують подібне діловодство відрізняються в основному режимними заходами спрямованими на уникнення витоку інформації з обмеженим доступом. Це питання більш детально буде розглянуто в наступних розділах.

Що стосується реалізації питань документування дана Типова інструкція унормовує й питання пов’язані з діловодними процесами в сфері обігу службової інформації.

Так, Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, введена в дію Постановою Кабінету Міністрів України від 27 листопада 1998 року № 1893 у п. 9 визначає, з урахуванням змін 2011 року, що «під час роботи з документами і матеріалами з грифом «Для службового користування» слід також керуватися «Типовою інструкцією з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади» введеною в дію Постановою Кабінету Міністрів від 30 листопада 2011 року № 1242.

Звідти не випадково, що відповідно до п. 6 Інструкції № 1893 – 1998 року функції ведення обліку, зберігання, розмноження та використання документів, які містять службову інформацію покладені на так звані «управління справами», «загальні відділи», «канцелярії» тощо. Слід додати, що дані структури забезпечують ведення загального (без обмеження доступу) діловодства, а зважаючи на обсяги загального діловодства у порівнянні з невеликим «службовим», відкрите діловодство стає пріоритетним в їх діяльності.

Відповідальність за організацію діловодства в установі покладається на керівника установи. Безпосередньо ведення діловодства відповідно до вимог державних стандартів України, та вищезазначеної Типової інструкції та інших інструкцій здійснюється вже згадуваними спеціально утворюваними управліннями справ, загальними відділами, канцеляріями або секретарями.

В установах, їх структурних підрозділах, у яких за штатним розписом не передбачено посади працівника з діловодства, ця робота проводиться спеціально виділеною для цього особою. Загальне керівництво роботою діловодних служб повинен також здійснювати керівник установи. Це включає:

забезпечення дотримання строків виконання завдань, визначених в нормативно-правових актах різного рівня;

застосування необхідних заходів до скорочення службового листування;

забезпечення регулярної перевірки стану діловодства в апараті установи та в організаціях, що належать до сфери її управління;

всебічне сприяння раціоналізації, механізації та автоматизації діловодних процесів, застосування необхідних заходів до оснащення канцелярії сучасним обладнанням та автоматизованими робочими місцями і локальними обчислювальними мережами на базі ПК;

забезпечення організації навчання працівників діловодної служби установи та її структурних підрозділів для підвищення кваліфікації;

здійснення контролю за обов'язковим додержанням в апараті установи та в організаціях, що належать до сфери її управління, вимог щодо складання, оформлення документів і організації діловодних процесів, передбачених державними стандартами на організаційно-розпорядчу документацію тощо.

Документування управлінської діяльності полягає у фіксації за встановленими правилами на паперових або магнітних носіях управлінських дій, тобто у створенні документів.

З 1999 року в країні почав діяти Державний класифікатор управлінської діяльності України ДК 010-98 (ДКУД).

Даний документ є складовою частиною державної системи класифікації і кодування техніко-економічної та соціальної інформації. Підставою для розробки та впровадження ДКУД стали зміни у складі та змісті організаційно-розпорядчої, первинно-облікової, банківської та звітно-статистичної документації внаслідок реорганізації системи державного управління в Україні.

Державний класифікатор фактично є номенклатурним переліком назв уніфікованих форм документів з унікальними кодовими позначеннями. Він використовується під час збирання та оброблення документів за відповідними уніфікованими формами усіма органами державного і господарського управління та підвідомчими підприємствами й організаціями в процесі виконання відповідних управлінських функцій згідно з чинним законодавством.

ДКУД орієнтовано на забезпечення оброблення інформації із застосуванням засобів комп'ютерної техніки та прогресивних інформаційних технологій. Класифікація здійснюється за 15 напрямами:

1) організаційно-розпорядча документація (код 02);

2) первинно-облікова документація (код 03);

3) банківська документація (код 04);

4) фінансова документація (код 05);

5) звітно-статистична документація (код 06);

6) планова документація (код 07);

7) ресурсна документація (код 08);

8) торговельна документація (код 09);

9) зовнішньоторговельна документація (код 10);

10) цінова документація (код 13);

11) документація з праці, соціальних питань і соціального захисту населення (код 15);

12) документація з побутового обслуговування населення (код 17);

13) бухгалтерсько-облікова документація (код 18);

14) документація з Пенсійного фонду (код 20);

15) словниково-довідкова документація (код 21).

Підставою для створення документів в установах є необхідність засвідчення наявності та змісту управлінських дій, передавання, зберігання і використання інформації протягом певного часу або постійно.

Ряд розпорядчих документів, які готує Національний банк України, міністерства, інші центральні органи виконавчої влади, інші органи відповідно до чинного законодавства підлягають державній реєстрації у Міністерстві юстиції України.

Державна реєстрація розпорядчих документів вищезазначених суб'єктів державного управління здійснюється на підставі Указу Президента України від 3 жовтня 1992 року № 493/92 «Про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади» та Постанови Кабінету Міністрів України від 28 грудня 1992 р. № 731 «Про затвердження Положення про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади».

Згідно з цими нормативно-правовими актами було надано право Міністерству юстиції та іншим органам, що здійснюють державну реєстрацію відомчих нормативно-правових актів, перевіряти у міністерствах, інших органах

виконавчої влади додержання законодавства про державну реєстрацію нормативно-правових актів. У разі потреби вимагати подання нормативно-правових актів на державну реєстрацію та вносити пропозиції щодо усунення виявлених порушень і недоліків та притягнення до відповідальності посадових осіб, винних у допущених порушеннях.

Єдиний механізм даної процедури встановлюється наказом Міністерства юстиції України від 12 квітня 2005 року № 34/5 «Про вдосконалення порядку державної реєстрації нормативно-правових актів у Міністерстві юстиції України та скасування рішення про державну реєстрацію нормативно-правових актів»

Державна реєстрація нормативно-правових актів полягає у проведенні правової експертизи на відповідність його Конституції та законодавству України, Конвенції про захист прав людини і основоположних свобод 1950 року і протоколам до неї, міжнародним договорам України, згоду на обов'язковість яких надано Верховною Радою України, а також з урахуванням практики Європейського суду з прав людини, прийнятті рішення про державну реєстрацію цього акта, присвоєнні йому реєстраційного номера та занесенні до Єдиного державного реєстру нормативно-правових актів.

Відповідно до вимог нормопроектувальної техніки нормативно-правовий акт:

повинен розроблятися з урахуванням його галузевої належності, відповідати за обсягом регламентації визначеному в ньому предмету правового регулювання;

повинен бути чітким, конкретним і зрозумілим;

не повинен дублювати приписів інших нормативно-правових актів;

не повинен містити суперечливих нормативних приписів.

При розробці нормативно-правового акта слід виходити з необхідності правового регулювання управлінської діяльності суб'єкта нормотворення, однією з форм реалізації якої є видання розпорядчих документів, вид яких (наказ, постанова, розпорядження, рішення) визначається законодавчими актами та положеннями.

Розпорядчий документ виготовляється на бланку та повинен мати обов’язкові реквізити й стабільний порядок їх розміщення: найменування суб’єкта нормотворення, назву виду документа, дату і номер, місце видання, структурні складові, підпис, візи.

Міністерством юстиції України надається роз’яснення, що слід розуміти під рядом визначень документів, наведемо тільки окремі приклади:

інструкція - нормативно-правовий акт, який детально визначає зміст і методичні питання правового регулювання у певній сфері суспільних відносин;

наказ - вид розпорядчого документа, який видається від імені суб'єкта нормотворення;

нормативно-правовий акт - офіційний письмовий документ, прийнятий уповноваженим на це суб’єктом нормотворення у визначеній законодавством формі та за встановленою законодавством процедурою, спрямований на регулювання суспільних відносин, що містить норми права, має неперсоніфікований характер і розрахований на неодноразове застосування. Прийняття нормативно-правових актів у вигляді листів і телеграм не допускається;

положення - звід нормативних приписів, який визначає організацію та діяльність органів виконавчої влади, органів державного управління, органів господарського управління та контролю, посадових та інших осіб у певних сферах діяльності;

постанова - вид розпорядчого документа, що приймається колегіальним суб'єктом нормотворення;

правила - нормативно-правовий акт, який конкретизує нормативні приписи загального характеру з метою регулювання поведінки суб'єктів правовідносин у певних галузях і вирішує процедурні питання;

рішення - вид розпорядчого документа, що приймається колегіальним суб'єктом нормотворення;

розпорядження - вид розпорядчого документа, що приймається колегіальним суб'єктом нормотворення;

розпорядчий документ - акт, що видається суб'єктом нормотворення у процесі здійснення ним виконавчо-розпорядчої діяльності з метою виконання покладених на нього завдань та здійснення функцій відповідно до наданої компетенції на основі і на виконання Конституції та законів України, спрямування регулювання суспільних відносин у сферах державного управління, віднесених до його відання.

Кожний документ, який створюється установами має, так званий, життєвий цикл. Інформація документується та отримує форму документа, який відображає певні управлінські процеси, виконує ту або іншу функцію. Після чого документ або знищується або зберігається протягом встановленого часу. Існує категорія документів що мають довічне збереження.

В 1998 році наказом Головного архівного управління при Кабінеті Міністрів України № 41 затверджується перелік типових документів, що утворюються в діяльності установ із зазначенням термінів зберігання документів.

Перелік включає документи, що утворюються під час документування однотипних (загальних для всіх) управлінських функцій, виконуваних органами державної влади, місцевого самоврядування та іншими підприємствами, установами та організаціями незалежно від функціонально-цільового призначення, рівня і масштабу діяльності,форми власності, а також документацію, що утворюється в результаті виробничої і науково-технічної діяльності організацій.

Цей документ став основним нормативом для визначення термінів зберігання документів та їх відбору для включення до складу Національного архівного фонду України або для знищення документів.

Склад документів і строки їх зберігання визначались в результаті безпосереднього вивчення документів із врахуванням рекомендацій фахівців відповідних галузей народного господарства і соціально-культурної сфери, положень відомчих (галузевих) переліків зі строками зберігання, примірних і типових номенклатур справ, рішень Центральної експертно-перевірної комісії Державної архівної служби України про встановлення або зміну строків зберігання окремих видів документів.

Перелік використовується під час формування справ, при підготовці різних видів номенклатури справ, розробці схем класифікації документів та відомчих (галузевих) переліків документів із зазначенням строків їх зберігання, а також у практиці роботи комісій з проведення експертизи цінності документів.

Даний нормативний акт фактично є основним, призначеним для використання всіма організаціями під час відбору на зберігання і для знищення типових документів, тобто загальних для всіх або більшості організацій. Для полегшення роботи з визначення строків зберігання документів до Переліку включено також окремі види документів нетипового характеру.

Як зрозуміло, організація діловодства в установі включає вирішення значної кількості різних питань.

Окремо слід звернути увагу й на важливість підготовки організаціями власної інструкції з питань діловодства. Якщо для державних установ подібна інструкція є обов'язковою, то для інших установ недооцінка її важливості може суттєво вплинути на ефективність реалізації, в тому числі, й управлінської діяльності.

Зрозуміло, що її створення не повинно носити формальний характер. Структура інструкції з діловодства як правило містить наступні розділи: загальні положення; підготовка та оформлення документів; організація документообігу; контроль за виконанням документів; формування справ і збереження документів тощо. Окрім питань, які враховують специфіку діяльності організації потрібно зважати на те, що подібний документ є частиною заходів з поліпшення діловодства й слід дотримуватись наступних напрямів:

створення власної нормативно-правової бази з питань діловодства;

впорядкування складу та форм документів, технологій їх підготовки та оформлення;

використання раціональної організаційної структури, що включає визначення оптимальної кількості працівників служб діловодства та налагодження ефективного взаємозв'язку даної служби з іншими структурами організації;

застосування виправданого порядку проходження й обробки документів;

закріплення процедури підвищення кваліфікації працівників служб діловодства та організації методичної допомоги з цих питань.

Розглянувши певні особливості реалізації управлінської складової в діловодстві та визначивши окремі переваги писемних документів, не слід забувати й про їх недоліки.

Як свідчить світова практика кількість створених установами документів постійно зростає великими темпами. Наприклад, за узагальненими статистичним даними окремих провідних країн світу, щорічний обсяг документів у діяльності тільки органів управління становить 250 млрд. аркушів щорічно. При цьому щорічний приріст знаходиться в межах 8-15% в залежності від конкретної державної структури. Вартість опрацювання одного документа в середньому складає 1,2 $. Проте зменшення видового складу документів тільки за рахунок їх уніфікації та стандартизації, за прогнозами аналітиків дозволить вже виграти понад 10%.

Порівняно із можливостями сучасних технічних засобів комунікації паперові документи мають дуже багато обмежень, зокрема:

неможливість швидкого (порівняно з телефоном, електронною поштою) надання пояснень або додаткової інформації. Звідти писемний документ повинен бути чітким та вичерпним, враховувати можливі питання;

відносно значні витрати на підготовку з врахуванням нормативних вимог, потреби чітко й грамотно сформулювати зміст та оформити паперовий документ, а також витрати на папір, бланки (типографські послуги), поштові послуги тощо;

відповідальність, в тому числі юридична, за зміст, особливо офіційних, паперових документів.

Існує й інший перелік проблемних питання пов’язаних з використанням паперових документів, що не притаманний електронному документообігу ось тільки окремі:

старіння та зношеність при використанні та зберіганні;

витратне тиражування та розсилка;

забезпечення місця для збереження масивів паперових документів;

трудомісткість для проведення систематизації та класифікації;

недостатня швидкість пошуку необхідних паперових документів взагалі або за необхідними параметрами зокрема;

обмеженість технічних можливостей при використанні графічного матеріалу при оформленні паперових документів.

Разом з тим, перехід на електронну форму документообігу далеко не завжди можливий, але й такий перехід сам по собі достатньо складний і потребує значних витрат.

2.2. Організація та вимоги до діловодства, яке містить службову інформацію

Документи відіграють важливе значення в діяльності підприємств, установ та органів влади. Вони фіксують інформацію для її передачі у просторі та часі, забезпечують комунікації між людьми, установами та організаціями.

Документи можуть містити інформацію із різним режимом доступу, частина яких складають документи, що містять службову інформацію.

Вимоги щодо поводження з документами, що містять службову інформацію, у всіх центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади, органах місцевого самоврядування, підприємствах, установах і організаціях незалежно від форм власності (далі – організації) встановлено Інструкцією про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, затверджена постановою Кабінету Міністрів України від 27.11.1998 № 1893 (далі Інструкція).

При поводження із документами з грифом «Для службового користування» співробітники (виконавці) організацій окрім Інструкції керуються також загальнодержавними інструкціями з діловодства, державними стандартами, що регламентують правила складання та оформлення документів, методичними рекомендаціями, індивідуальними інструкціями з діловодства, що розробляються в залежності від особливостей діяльності конкретного підприємства, установи, організації.

Загальні правила поводження з документами в Україні встановлює Типова інструкція з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади, затверджена постановою Кабінету Міністрів України від 30 листопада 2011 р. № 1242.

Реквізити документів та порядок їх розміщення встановлено ДСТУ 4163-2003 «Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів».

Для організації роботи із службовими документами також використовують і інші нормативно-правові акти та стандарти, які складають єдину державну систему діловодства.

Для забезпечення єдиного порядку обліку, зберігання і використання документів, які містять службову інформацію Інструкцією розкриваються питання:

– основних вимог до організації роботи з документами,

– допуску громадян до роботи з документами,

– системи діловодства,

– формування номенклатури справ,

– життєвого циклу документу,

– облікових форм,

– завдань режимно-секретного органу.

За необхідності організаціям надано право затверджувати відомчі інструкції з питань обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію. Такі інструкції розробляються організаціями з урахуванням особливостей своєї діяльності відповідно до вимог Інструкції та погоджуються із Службою безпеки України та Державною архівною службою України.

В організаціях повноваження щодо організації роботи із документами, що містять службову інформацію, розподіляється наступним чином:

– керівники організацій разом з режимно-секретними органами здійснюють забезпечення контролю за виконанням вимог щодо поводження із службовою інформацією;

– режимно-секретні підрозділи організацій здійснюють заходи із запобігання розголошенню відомостей, що містяться в документах з грифом «Для службового користування», та випадкам втрат таких документів;

– управління справами, загальні відділи, канцелярії організації (далі - канцелярії) здійснюють безпосередньо ведення обліку, зберігання, розмноження, використання, а також контроль документів, що містять службову інформацію (рис 1).

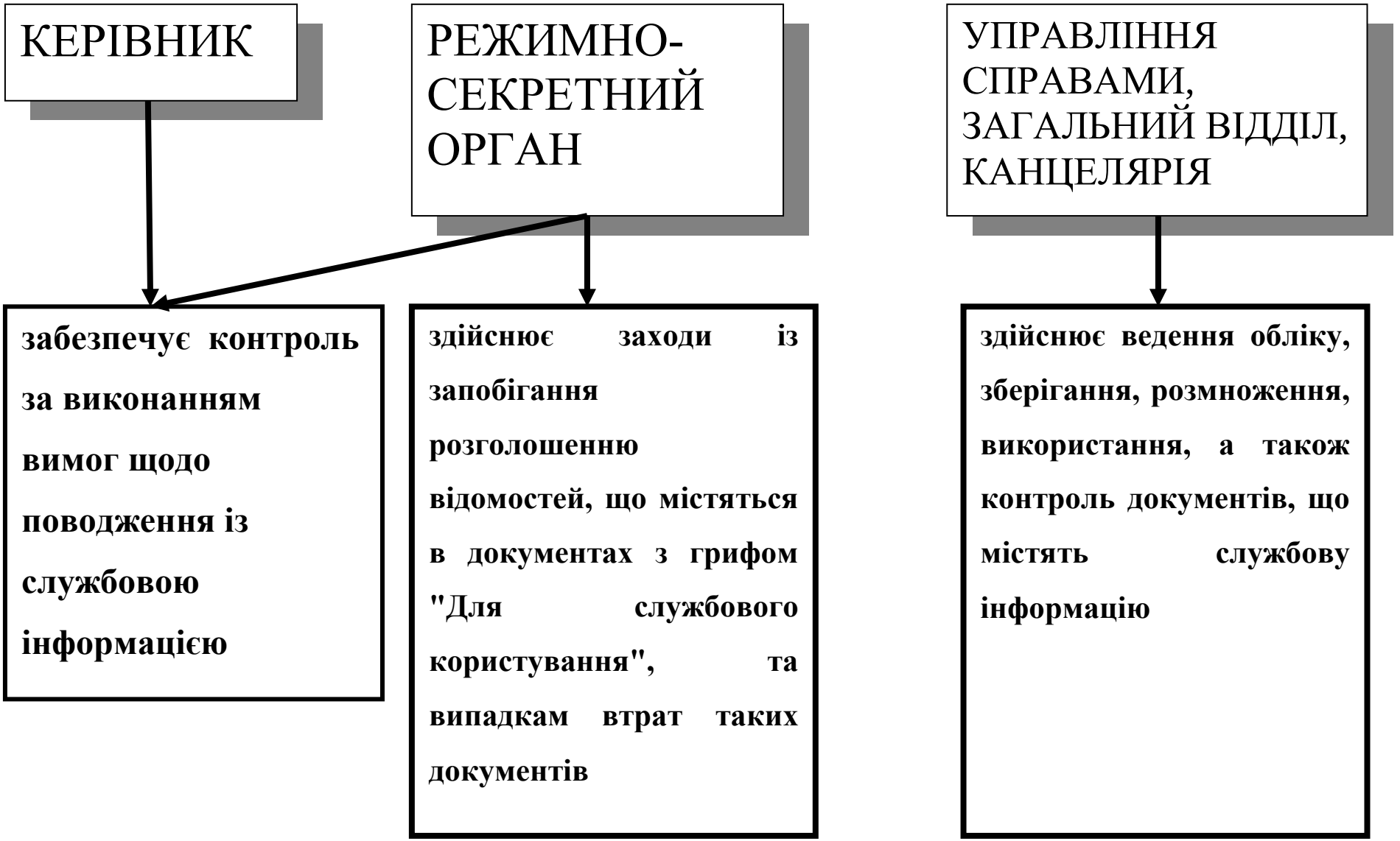

Рис 1. Повноваження щодо організації роботи із документами, що містять службову інформацію,

Питання пов’язані з контролем за обігом документів, що містять службову інформацію покладається на СБ України.

Таким чином основний обсяг робіт із службовими документами припадає на канцелярію. Від її злагодженої роботи та вміння організувати діяльність виконавців залежить зручність роботи із службовою інформацією, а також недопущення її втрати та розголошення.

Початок організації роботи із службовою інформацією починається з визначення того що відноситься до службової інформації.

Віднесення інформації до службової здійснюється міністерствами та іншим центральними органами виконавчої влади, Радою міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською міськими державними адміністраціями. У межах своїх повноважень вони розробляють та вводять в дію переліки службової інформації (далі – Переліки).

Переліки використовуються виконавцями документів як підстава для обмеження доступу до створюваних ними конкретних документів.

Виконання вимог, що встановлені нормативно-правовими актами до поводження із службовим документами, залежить від створених умов роботи виконавцям та знання ними правил роботи.

Ознайомлення співробітників з правилами роботи із службовими документами покладається на канцелярії організацій.

Канцелярії в обов'язковому порядку організують навчання співробітників з нормативно-правовими актами, які визначають вимоги до поводження з службовою інформацією та відповідними відомчими інструкціями, про що складаються списки та підтверджуються розписками співробітників.

Категорії працівників, які допускаються до роботи з виданнями з грифом «ДСК», визначаються керівниками організацій. Рішення про допуск до конкретного службового документа здійснюється згідно з вказівками, викладеними у резолюціях керівника організації (структурних підрозділів). До справами з грифом «ДСК» допускаються посадові особи, які мають досвід роботи та безпосереднє відношення до цих справ, згідно із списками, погодженими з канцелярією.

Представники інших організацій допускаються до ознайомлення і роботи з документами з грифом «ДСК» з дозволу керівників організацій (структурних підрозділів), у володінні та розпорядженні яких перебувають ці документи, за наявності письмового запиту організацій, в яких вони працюють, із зазначенням характеру завдання, що виконується.

Виконавці, допущені до роботи з документами з грифом «ДСК», використовують та можуть поширювати цю інформацію тільки за службовою потребою.

Службова інформація, що стала відома під час роботи, не може бути повідомлена будь-кому усно або письмово. Також виконавцям забороняється користуватися відомостями з документів з грифом «ДСК» для відкритих виступів або опублікування у засобах масової інформації, експонувати такі документи на відкритих виставках, демонструвати їх на стендах, у вітринах або інших громадських місцях.

У разі потреби опублікування або передання для опублікування відомостей, що містять службову інформацію, це може бути здійснено тільки з письмового дозволу керівника організації, якщо такі відомості не суперечать Перелікам.

У відомчих бібліотеках закритого типу видання з грифом «ДСК» видаються:

1) співробітникам цієї організації - за списками, затвердженими керівником організації (структурного підрозділу), або за його письмовим дозволом;

2) співробітникам інших організацій - за письмовими зверненнями цих організацій та з письмового дозволу керівника організації (структурного підрозділу), що зберігає ці видання.

Ознайомлення громадянами України з виданнями з грифом «ДСК» у масових бібліотеках здійснюється за письмовими клопотаннями керівників організацій, в яких вони працюють. У клопотаннях повинні міститися теми роботи. Дозволи на роботу з виданнями дійсні протягом року. Видання з грифом «ДСК» з письмового дозволу керівника організації можуть видаватися по міжбібліотечному абонементу на підставі письмових запитів керівників організацій, яким ці видання потрібні.

Виконавці документів з грифом «ДСК» працюють з цими документи в межах службових приміщень організації. У разі потреби керівник організації (структурного підрозділу) може дозволити виконавцям або співробітникам канцелярії винести за межі службового приміщення організації документи з грифом «ДСК» для їх погодження, підписання тощо в організаціях, що знаходяться у межах одного населеного пункту. В окремих випадках з дозволу керівника організації дозволяється перевезення документів з грифом «ДСК» до іншого населеного пункту за умови, що такі документи перевозяться групою у складі не менше двох працівників (або одного озброєного працівника), що мають виконувати роботу з ними в іншому населеному пункті. Особам, які відряджені до інших населених пунктів, забороняється мати при собі матеріали з грифом «ДСК». Ці матеріали повинні бути заздалегідь надіслані на адресу організації за місцем відрядження співробітника.

Виписки з документів і видань з грифом «ДСК», робляться у зошитах, що мають аналогічний гриф, які після закінчення роботи надсилаються на адресу організації, яка давала дозвіл на ознайомлення і роботу з документами з грифом «ДСК».

Зняття копій, а також здійснення виписок з документів з грифом «ДСК» співробітниками організації, де перебувають документи, проводиться з дозволу керівника організації (структурного підрозділу). Розмноження документів з грифом «ДСК» у друкарні або на розмножувальних апаратах здійснюється з дозволу керівника організації (структурного підрозділу) за підписаними ним нарядами під контролем канцелярії. Облік розмножених документів здійснюється за кількістю їх примірників.

Документи з грифом «ДСК» в залежності від того яким чином вони отримані установою поділяють на вхідні, вихідні та внутрішні. Усі вони підлягають обліку на всіх етапах опрацювання.

Облік службових документів відбувається шляхом реєстрування, яке полягає у внесенні у облікові форми короткої інформації про службовий документ із зазначенням реєстраційного індексу та дати реєстрування.

Реєстраційний індекс службового документу це позначка, яка може бути цифровою або абетково-цифровою.

Облік службових документів здійснюється за кількістю сторінок, а видань (книги, журнали, брошури) - за кількістю примірників.

Для реєстрації використовують журнали за формою 2 або картки за формою 3 (додаток 1, 2).

Журнали для обліку службових документів як правило виготовляють друкарським способом. Вони повинні відповідати вимогам Інструкції, для чого їх прошивають, сторінки нумерують та опечатують, а на останній сторінці, яка пронумерована, робиться запис про кількість сторінок у журналі.

Підготовку журналів здійснює працівник канцелярії, який завіряє записи у журналі підписом та печаткою «Для пакетів».

Для зручності у роботі при значному обсязі документообігу коли реєстрування документів відбувається на різних ділянках канцелярії дозволяється використання окремих журналів для:

- вхідних документів;
- вихідних документів;
- видань з грифом «Для службового користування».

Використання окремих журналів дозволяє краще аналізувати потоки документів, знаходити потрібні документи.

Носіями службової інформації також можуть бути оптичні диски, флеш накопичувачі, пристрої, прилади, речовини. У такому випадку якщо гриф обмеження доступу неможливо нанести безпосередньо на матеріальній носій службової інформації, він має бути зазначений у супровідному документі.

Облік машинних носіїв службової інформації здійснюється окремо від обліку паперових носіїв такої інформації у журналах за формою 4 або на картках за формою 5 (додаток 3,4).

Видання з грифом «Для службового користування», реєструється за одним вхідним номером у журналі обліку за формою 6 (додаток 5).

Додатково розмножені примірники видання обліковуються за номером цього видання, про що робиться позначка на розмноженому виданні та у формах

обліку. Нумерація додатково розмножених примірників продовжується від останнього номера примірників, що були розмножені раніше.

Якщо в установах незначний обсяг документів з грифом «Для службового користування», дозволяється вести їх реєстрацію разом з іншою несекретною документацією. При цьому на картці (у журналі) до реєстраційного номера документа або видання додається позначка «ДСК».

Реєстрації підлягають всі документи, що надходять до установи. На кожному з них, а також на супровідному листі до видання з грифом «Для службового користування» проставляється реквізит – відмітка про надходження документа до організації. Цей реквізит розміщується у нижньому полі документу праворуч, він, як правило, проставляється штампом, у якому зазначаються найменування організації, реєстраційний індекс документа та дата його надходження.

Друкування документів з грифом «Для службового користування» може здійснюється у різних структурних підрозділах, наприклад, друкарнях, відділах розмножувальної техніки та друкарському бюро організації. Видання з грифом «Для службового користування» включаються тільки у службові каталоги. Забороняється включати такі видання у відкриті каталоги та бібліографічні покажчики.

У друкарнях та у відділах розмножувальної техніки облік документів з грифом «Для службового користування», що тиражуються в незначному обсязі, може здійснюватися в одному журналі разом з іншими несекретними документами. При цьому до реєстраційного номера чи назви документа додається позначка «ДСК».

Також допускається друкування службових документів у структурних підрозділах під відповідальність їх керівників.

Використання комп’ютерних систем для друкування документів з грифом «Для службового користування» може здійснюватися тільки після створення комплексної системи захисту інформації та підтвердження її відповідності вимогам нормативних документів з питань технічного захисту інформації в порядку, встановленому законодавством. Дозвіл на використання комп’ютерної

системи із зазначеною метою надається згідно з наказом керівника організації за наявності атестата відповідності комплексної системи захисту інформації.

Службові документи повинні мати всі необхідні реквізити, вимоги до розміщення яких встановлено ДСТУ4163-2003. Для їх ідентифікації та виділення того, що вони містять службову інформацію, у відповідності до Переліків, поставляють гриф обмеження доступу – «ДСК». Розміщується він у верхньому полі першої сторінки праворуч на відстані 104 мм від лівого поля (рис 1). Для видань гриф обмеження доступу розміщується на обкладинці та на титульній сторінці. Також обов’язково проставляється номер примірника.

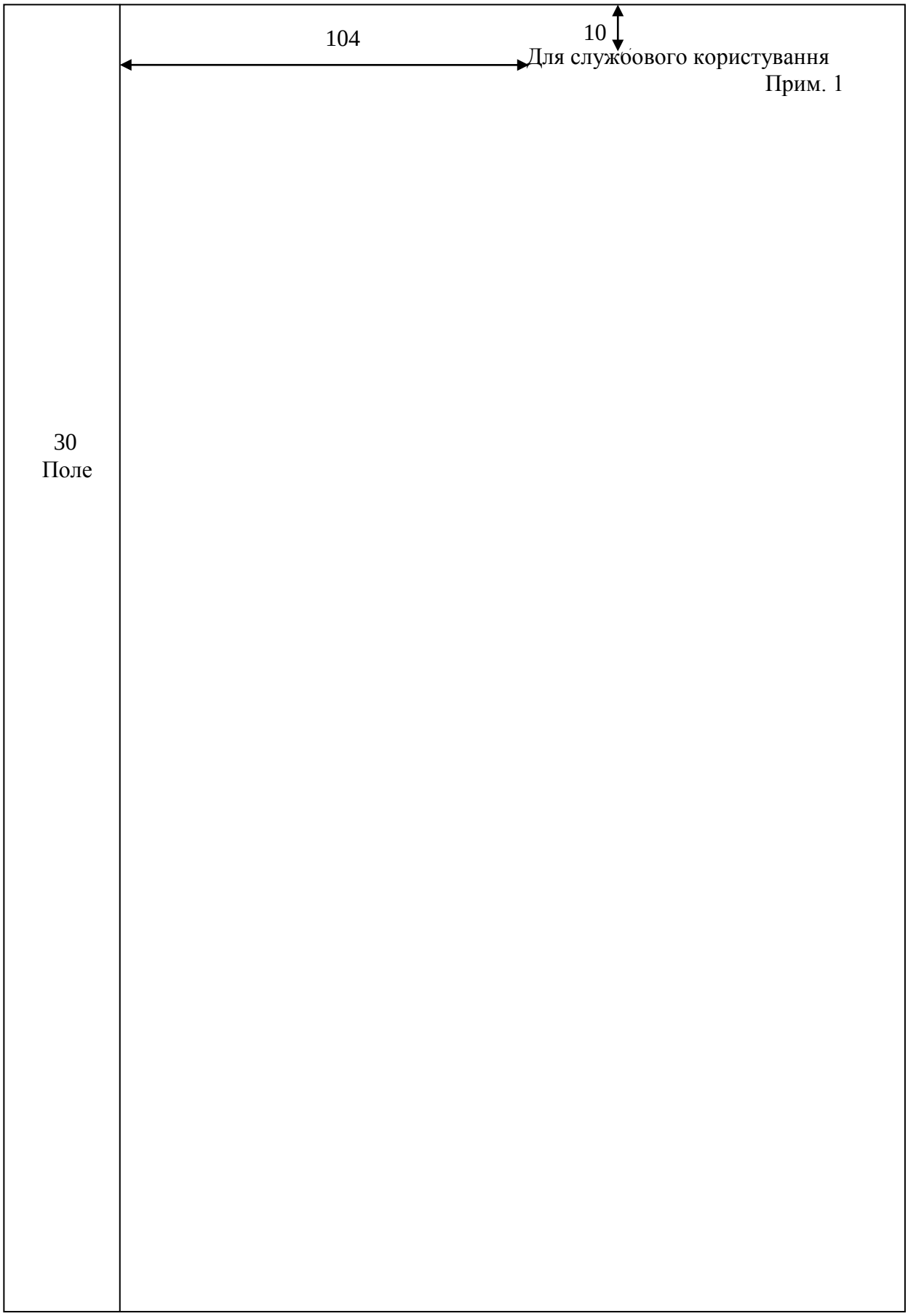

Рис.1 Зразок розміщення реквізиту гриф обмеження доступу документу формату А4, що містить службову інформацію

Надруковано 2 прим.
Прим. 1- на адресу
Прим. 2 - до справи
Вик. Шевченко О.П
Друк. Тарасюк С.М.
Гриф «ДСК» п.1.1.Переліку
ПЕОМ № 234
ЖМД № 1234
01.01.2015

Рис.2 Зразок розміщення зворотного боку останньої сторінки документу формату А4, що містить службову інформацію

На звороті останньої сторінки кожного примірника документа друкарка (або виконавець, який друкував документ) повинна зазначити кількість надрукованих примірників, прізвище виконавця, власне прізвище і дату друкування документа. До вказаних обов'язкових реквізитів в організаціях де використовують ПЕОМ для підготовки службових документів додатково вказують інформацію про ці засоби, а також для зручності подальшої роботи вказують пункт Переліку у відповідності до якого здійснюється обмеження доступу до документу (рис.2).

Надруковані і підписані документи з грифом «Для службового користування» разом з їх чернетками та варіантами передаються для реєстрації співробітнику канцелярії, який здійснює їх облік. Чернетки і варіанти знищуються виконавцем та співробітником канцелярії, про що на копії вихідного документа робиться запис: «Чернетки і варіанти знищені. Дата. Підписи».

В структурних підрозділах організації призначають відповідальних за облік і зберігання документів (справ) з грифом «ДСК».

Документи з грифом «ДСК» повинні зберігатися у службових приміщеннях і спеціальних бібліотеках у шафах (сховищах), які надійно замикаються та опечатуються. Забороняється зберігати документи з грифом «ДСК» у бібліотеках загального користування та у їх підсобних фондах.

У разі зміни працівників відповідальних за облік і зберігання службових документів, вони зобов'язані передати всі службові документи новим працівникам. Після перевірки наявності всіх документів, справ та інших матеріальних носіїв службової інформації, що знаходяться на обліку, складається за довільною формою акт прийому-передачі цих документів (справ), що затверджується керівником організації (структурного підрозділу).

Для накопичення та зберігання документи з грифом «ДСК» після їх виконання формуються у справи. Порядок формування цих справ передбачається номенклатурами справ несекретного діловодства. Документи з грифом «ДСК» залежно від виробничої та інформаційної потреби дозволяється формувати у

справи окремо або разом з іншими несекретними документами з одного й того ж питання. У номенклатуру справ в обов'язковому порядку включаються всі довідкові та реєстраційні картотеки і журнали на документи з грифом «ДСК». Справи з документами з грифом «ДСК» повинні мати внутрішні описи.

У випадку коли до справи з несекретними документами, є необхідність долучати окремі документи з грифом «Для службового користування», та такі справи повинні бути віднесені до категорії обмеженого розповсюдження і використання. На обкладинках і титульних сторінках цих справ також проставляється гриф «ДСК», а в номенклатуру справ вносяться відповідні уточнення.

Якщо в організації створюється велика кількість однакових видів документів (наказів, інструкцій, планів тощо) з грифом «ДСК» та без цього грифа, доцільно формувати їх в окремі справи. При цьому в графі номенклатури справ «Індекс справи» до номера справи з документами з грифом «Для службового користування» додається позначка «ДСК».

В організаціях, у діяльності яких створюється незначна кількість документів з грифом «Для службового користування», номенклатурою справ може бути передбачене запровадження однієї справи із заголовком «Документи з грифом «Для службового користування». Термін зберігання такої справи не встановлюється, а у відповідній графі номенклатури справ проставляється позначка «ЕК» (експертна комісія).

Якщо у справі «Документи з грифом «Для службового користування» містяться тільки документи тимчасового зберігання, вона може не переформовуватися. Термін зберігання такої справи встановлюється відповідно до найбільшого терміну зберігання документів, що містяться в цій справі. Позначка «ЕК» у графі номенклатури справ «Термін зберігання» закреслюється і зазначається уточнений термін зберігання.

Після закінчення діловодного року справа «Документи з грифом «Для службового користування» переглядається посторінково членами експертної комісії організації та у разі потреби приймається рішення про переформування документів. Документи постійного зберігання, що містяться у цій справі,

формуються в окрему справу, якій надається окремий заголовок і яка додатково включається до номенклатури справ. Документи тимчасового зберігання залишаються у цій справі згідно із затвердженою номенклатурою справ.

Якщо члени експертної комісії за результатами перегляду наявних у справі документів дійдуть висновку, що вони за сукупністю містять відомості, які становлять державну таємницю, про це складається відповідний акт. Цій справі надається гриф обмеження доступу згідно із законодавством про державну таємницю. Зберігання її здійснюється відповідно до вимог секретного діловодства.

Організація роботи із справами з грифом «Для службового користування», здійснюється таким чином, щоб видані для роботи справи поверталися у канцелярію або архівний підрозділ у той же день.

Видача та приймання справ та видань з грифом «ДСК» виконавцям здійснюється під розписку в картці обліку справ і видань, що видаються за формою 7 (додаток 6). Окремі справи з грифом «ДСК» з дозволу керівника канцелярії або архівного підрозділу організації можуть перебувати у виконавця протягом терміну, необхідного для виконання завдання, за умови повного забезпечення їх схоронності і додержання правил зберігання.

Виконавцям забороняється вилучення із справ або переміщення документів з грифом «ДСК» з однієї справи до іншої без дозволу канцелярії. В разі особливої потреби за погодженням з канцелярією документи можуть бути вилучені або переміщення, про що робляться відмітки в облікових формах, включаючи внутрішні описи.

Передача документів з грифом «ДСК» між співробітникам здійснюється тільки через канцелярію, архівний підрозділ або бібліотеку.

Справи з грифом «ДСК», передані організаціями до державних архівних установ, використовуються на правах документів обмеженого користування відповідно до вимог Інструкції. Видача таких справ дослідникам здійснюється з письмового дозволу керівника державної архівної установи. Організація-фондоутворювач під час передачі справ до державної архівної установи може обумовити вимогу щодо погодження з нею видачі таких справ. В такому випадку

видача таких справ дослідникам здійснюється з письмового дозволу керівника організації-фондоутворювача.

Пересилання документів з грифом «ДСК» до інших організацій у межах України здійснюється рекомендованими або цінними поштовими відправленнями, а також з кур'єрами організацій. Доставка документів з грифом «ДСК» представниками інших організацій здійснюється на підставі письмового доручення. Документи, справи і видання з грифом «Для службового користування», що розсилаються, повинні бути вкладені у конверти або упаковані таким чином, щоб виключалася можливість доступу до них. На упаковці або конверті зазначаються адреси і найменування одержувача та відправника, номери вкладених документів з проставленням позначки «ДСК». На конвертах (упаковках) документів з грифом «ДСК» забороняється зазначати прізвища і посади керівників організацій (структурних підрозділів) і виконавців документів, а також найменування структурних підрозділів.

Розсилання (відправлення) тиражу документів з грифом №ДСК» здійснюється на підставі рознарядок, підписаних керівником організації (його заступником) та керівником канцелярії, із зазначенням облікових номерів примірників, що розсилаються (відправляються).

Видання з грифом «ДСК» не можуть бути надіслані за кордон у порядку книгообміну або експонування на виставках, презентаціях тощо.

При наявності технічних можливостей може відбуватися передача службової інформації каналами зв'язку, в яких застосовується засоби технічного та (або) криптографічного захисту інформації.

Копіювання для сторонніх організацій документів з грифом «ДСК», одержаних від інших організацій, здійснюється за погодженням з організаціями-авторами цих документів. Відповідальність за випуск документів з грифом «ДСК», що тиражуються, несуть керівники організацій (структурних підрозділів), у яких вони тиражуються.

Під час розмноження документів з грифом «ДСК» з використанням засобів копіювально-розмножувальної техніки заходи технічного захисту інформації здійснюються відповідно до законодавства.

Справи постійного та тривалого (понад 10 років) зберігання з грифом «ДСК» періодично переглядаються з метою можливого зняття цього грифа. Перегляд здійснюється під час передачі справ із структурних підрозділів до архівного підрозділу організації, у процесі зберігання справ в архівному підрозділі (як правило не менш як один раз на 5 - 10 років), а також під час підготовки справ постійного зберігання для передачі до державної архівної установи. Комісії створюються з працівників канцелярії, режимно-секретного та інших структурних підрозділів організації.

Рішення про зняття грифа «ДСК» приймається експертною комісією організації-автора документа (видання) чи правонаступника. Результати роботи комісії оформлюються актом, що складається за довільною формою та затверджується керівником організації. В акті перелічуються заголовки та номери за описом справ, з яких знімається гриф «ДСК».

У відповідності до прийнятого рішення проводяться робота із зняття грифу обмеження доступу. Це відбувається шляхом нанесення на обкладинки справ гриф «ДСК» штампа або запису від руки із зазначенням дати і номера акта, що став підставою для зняття грифа. Аналогічні відмітки вносяться до опису і номенклатури справ.

Знищення та передача до архіву документів,що містять службову інформацію здійснюється після проведення експертизи наукової, історико-культурної цінності документів і справ, розгляду і затвердження її результатів. Експертиза документів здійснюється відповідно до порядку утворення та діяльності комісій з проведення експертизи цінності документів, затвердженого постановою Кабінету Міністрів України від 08 серпня 2007 р. N 1004.

Справи із структурних підрозділів до архівного підрозділу організації передаються в упорядкованому стані. При цьому, справи постійного зберігання, що містять документи з грифом «ДСК», включаються в опис за формою 8 (додаток 7) разом з іншими справами, що містять нетаємні документи постійного зберігання.

На справи з документами з грифом «ДСК» з терміном зберігання до 10 років включно описи можуть не складатися. Їх передача до архівного підрозділу здійснюється за номенклатурами справ.

Справи з грифом «ДСК» постійного зберігання передаються до державних архівних установ у встановленому Мін'юстом порядку з обов'язковою посторінковою перевіркою документів, включених до них. Підготовка справ для архівного зберігання (оформлення, опис справ на обкладинках і складання описів справ) здійснюється згідно з правилами, встановленими Мін'юстом.

Відібрані для знищення справи з грифом «ДСК», що не мають наукової, історико-культурної цінності та втратили практичне значення, можуть оформлятися окремим актом або включатися у загальний акт за формою 9 (додаток 8) разом з іншими несекретними справами, відібраними до знищення. При цьому у графі "Заголовки справ" після номерів цих справ проставляється відмітка «ДСК».

Відібрані для знищення документи, справи і видання з грифом «ДСК» перед здачею на переробку як макулатура повинні в обов'язковому порядку подрібнюватися до стану, що виключає можливість прочитання їх.

Після знищення матеріалів з грифом «ДСК» в облікових документах (картках, журналах, номенклатурах справ, описах справ тимчасового зберігання) робиться відмітка «Знищено. Акт N ____ від (дата)».

Інформаційні бюлетені, реферативні інформаційні видання, телефонні та адресні довідники, а також копії документів, стенографічні записи і друкарський брак знищуються без акта, але з відміткою в облікових формах, що засвідчується підписами виконавця і працівника, відповідального за їх облік і зберігання.

Для здійснення контролю за станом руху службових документів здійснюють перевірку їх наявності. Така перевірка здійснюється щорічно комісією, що призначається наказом керівника організації. До складу цієї комісії обов'язково включаються особи, яким доручено облік і зберігання цих документів, а також працівники режимно-секретних підрозділів.

У бібліотеках та архівних підрозділах, де зосереджена значна кількість документів з грифом «Для службового користування», перевірка їх наявності може здійснюватися один раз на п'ять років.

Результати перевірки наявності оформляються актом за формою 10 (додаток 9).

У випадку втрати або розголошення службових документів проводять службові розслідування.

Про факти втрати документів з грифом «Для службового користування» або розголошення відомостей, що містяться в них, терміново доводиться до відома керівника організації а також керівників режимно-секретного підрозділу та канцелярії, а також письмово повідомляються органи СБУ із зазначенням обставин втрати документів чи розголошення відомостей та вжитих заходів. Для розслідування факту втрати документів з грифом «Для службового користування» або встановлення факту розголошення відомостей, що містяться в них, наказом керівника організації призначається комісія, висновок якої затверджується керівником організації.

Відповідні записи про втрачені документи вносяться в облікові форми на підставі акта комісії, затвердженого керівником організації. Акти комісії про втрачені справи постійного зберігання після затвердження їх керівником організації передаються до архівного підрозділу для включення у справу фонду.

За порушення, що призвели до розголошення інформації «Для службового користування», втрати або незаконного знищення документів з грифом «Для службового користування», а також інших вимог Інструкції винні особи несуть дисциплінарну або адміністративну відповідальність згідно із законодавством.

3.3 Контроль за станом використання службової інформації

Багато людей сприймають контроль як певні обмеження, примушення, відсутність самостійності і т.п. – словом все те, що прямо протилежне нашим уявленням про свободу особи. Саме через це трактування контролю як функції управління, розуміється іноді невірно.

Державний контроль – це процес забезпечення досягнень державою своїх цілей. Цей процес складається з встановлення стандартів, вимірів фактично досягнутих результатів і проведення коректувань в тому випадку, якщо досягнуті результати істотно відрізняються від встановлених стандартів.

В нашому випадку, стосовно використання службової інформації, контроль напряму пов'язаний з існуванням, самозбереженням і прогресивним розвитком України як суверенної держави, здійсненні цілеспрямованої політики забезпечення, в тому числі, її національної безпеки.

Національна безпека України повинна слугувати корінним (базовим) інтересам народу України і відтак спрямовуватися на усунення або подолання деструктивної дії внутрішніх, регіональних і глобальних факторів, що перешкоджають або гальмують досягнення національно-значимих цілей.

Закон України «Про основи національної безпеки України» (N 964-IV, 19.06.2003) визначив основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Зокрема, *національна безпека* - 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 у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості та сільського господарства, транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр,

земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам.

Суб'єктами забезпечення національної безпеки є:

Президент України;

Верховна Рада України;

Кабінет Міністрів України;

Рада національної безпеки і оборони України;

міністерства та інші центральні органи виконавчої влади;

Національний банк України;

суди загальної юрисдикції;

прокуратура України;

місцеві державні адміністрації та органи місцевого самоврядування;

Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України;

органи і підрозділи цивільного захисту;

громадяни України, об'єднання громадян.

Контроль за реалізацією заходів у сфері національної безпеки здійснюється відповідно Президентом України, Верховною Радою України, Кабінетом Міністрів України, Радою національної безпеки і оборони України в межах їх повноважень, визначених Конституцією і законами України.

До сфери національної безпеки відноситься інформаційна безпека.

Порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, та інформації, що становить суспільний інтерес визначено положеннями законів України «Про доступ до публічної інформації» (N 2939-VI, 13.01.2011) та «Про інформацію» (N 2657-XII, 02.10.1992).

Контроль за забезпеченням доступу до публічної інформації, до якої також відноситься службова інформація, здійснюється наступним чином:

1. Парламентський контроль за дотриманням права людини на доступ до інформації здійснюється Уповноваженим Верховної Ради України з прав людини, тимчасовими слідчими комісіями Верховної Ради України, народними депутатами України.

2. Громадський контроль за забезпеченням розпорядниками інформації доступу до публічної інформації здійснюється депутатами місцевих рад, громадськими організаціями, громадськими радами, громадянами особисто шляхом проведення відповідних громадських слухань, громадської експертизи тощо.

3. Державний контроль за забезпеченням розпорядниками інформації доступу до інформації.

Завданням такого контролю є недопущення віднесення до інформації з обмеженим доступом відомостей зазначених у статті 21 Закону України «Про інформацію» та статті 6 Закону України «Про доступ до публічної інформації».

Крім цього, контролюється порядок віднесення до службової інформації.

Обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

Як зазначалось раніше, з метою забезпечення єдиного порядку обліку, зберігання і використання матеріалів, які містять службову інформацію, Кабінет Міністрів України затвердив своєю Постановою від 27 листопада 1998 року № 1893 Інструкцію про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію. Міністерства, інші центральні органи виконавчої влади відповідно до вимог зазначеної Інструкції та з урахуванням особливостей своєї діяльності можуть за погодженням з СБ та Державною архівною службою затверджувати відомчі інструкції з питань обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію.

Також, Кабінет Міністрів України зобов’язав керівників міністерств, інших центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності разом з режимно-секретними органами забезпечити контроль за виконанням вимог вищезазначеної Інструкції. При цьому, СБ України уповноважена здійснювати контроль за обігом документів, які містять службову інформацію.

Діяльність СБ України здійснюється в межах повноважень визначених Законом України «Про Службу безпеки України» (N 2229-XII, 25.03.1992).

Статтею 24 цього Закону СБ України зобов'язано вживати заходів щодо забезпечення охорони державної таємниці та здійснення контролю за додержанням порядку обліку, зберігання і використання документів та інших матеріальних носіїв, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

При виконанні цих завдань співробітникам СБ України надається право:

1) вимагати від громадян та посадових осіб припинення правопорушень і дій, що перешкоджають здійсненню повноважень СБ України, перевіряти у зв'язку з цим документи, які посвідчують їх особу, а також проводити огляд осіб, їх речей і транспортних засобів, якщо є загроза втечі підозрюваного або знищення чи приховання речових доказів злочинної діяльності;

2) подавати органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям усіх форм власності обов'язкові для розгляду пропозиції з питань національної безпеки, у тому числі із забезпечення охорони державної таємниці;

3) складати протоколи про адміністративні правопорушення, віднесені законом до компетенції СБ України, проводити особистий огляд, огляд речей, вилучення речей і документів, застосовувати інші передбачені законом заходи забезпечення провадження у справах про адміністративні правопорушення;

4) виключно при безпосередньому припиненні злочинів, розслідування яких віднесено законодавством до компетенції СБ України, переслідуванні осіб, що підозрюються у їх вчиненні, заходити в жилі, службові, виробничі та інші

приміщення, на території і земельні ділянки та оглядати їх в порядку, передбаченому КПК України.

Співробітники СБ України самостійно приймають рішення в межах своїх повноважень. Вони повинні відмовитись від виконання будь-яких наказів, розпоряджень або вказівок, які суперечать чинному законодавству. За протиправні дії та бездіяльність вони несуть дисциплінарну, адміністративну та кримінальну відповідальність.

Законні вимоги співробітників СБ України при виконанні ними службових обов'язків є обов'язковими для громадян і посадових осіб. Непокора або опір законним вимогам співробітників СБ України, неправомірне втручання в їх законну діяльність тягнуть за собою відповідальність, передбачену законодавством.

Таким чином, можна констатувати, що контроль за службовою інформацією поділяється на три напрями:

- громадськістю, через органи влади та управління;
- безпосередньо керівниками установ та організацій, де циркулює службова інформація;
- уповноваженими співробітниками СБ України.

До недавнього часу функція контролю в нашій державі зводилася до перевірки дотримання інструкцій, законів і виявлення порушників, реєстрації в актах недоліків, тобто негативних сторін діяльності організацій. Ніхто не цікавився тим, щоб розвивати ініціативу працівників щодо вдосконалення роботи, розвивати розуміння спільних інтересів. В умовах ринкової економіки такий підхід є анархізмом. Самоконтроль стимулює у співробітників почуття власної відповідальності за результати, потребує менше часу і витрат, ніж інші види контролю.

Зокрема в процедурі контролю фахівці виділяють три чітко виражених етапи:

1. Розробка стандартів і критеріїв (попередній контроль) .
2. Співставлення з ними реальних результатів (поточний контроль).
3. Прийняття необхідних корегувальних дій (заключний контроль).

Попередній контроль реалізується через правила, процедури тощо. Його основні важелі закладені в процесі реалізації таких функцій управління, як планування та організація.

Попереднім він називається тому, що здійснюється до фактичного початку робіт. Основними засобами здійснення попереднього контролю є реалізація (не створення, а саме реалізація) певних правил, процедур і ліній поведінки.

Оскільки ці правила і лінії поведінки виробляються для забезпечення виконання планів, то їх сурове дотримання – це спосіб переконатися, що робота розвивається в потрібному напрямку.

В організаціях попередній контроль використовується в трьох головних напрямках – по відношенню до людських, матеріальних і фінансових ресурсів.

Попередній контроль в області людських ресурсів досягається за рахунок ретельного аналізу тих ділових і професійних знань, які необхідні для виконання тих чи інших посадових обов‘язків.

Попередній контроль матеріальних ресурсів здійснюється шляхом розробки мінімально допустимих рівнів якості і проведення фізичних перевірок відповідності матеріалів, що відповідають цим вимогам.

Поточний контроль втілює в собі таку його рису, як безперервність здійснення, і полягає у корекції виникаючих відхилень в процесі виконання прийнятих рішень.

На цьому етапі проводиться «Співставлення досягнутих результатів з встановленими стандартами». На цьому етапі керівник (менеджер) повинен визначити, наскільки досягнуті результати відповідають тому, чого він очікував. При цьому менеджер приймає ще одне важливе рішення: наскільки допустимі відхилення від стандартів.

Поточний контроль здійснюється безпосередньо в ході проведених робіт. Частіше всього об‘єктом є підлеглі співробітники, а сам він традиційно є прерогативою їх безпосереднього керівника. Регулярна перевірка роботи підлеглих, обговорення виникаючих проблем і пропозиції щодо удосконалення роботи дозволять виключити відхилення від намічених планів. Поточний контроль не проводиться буквально одночасно з виконанням самої роботи.

Швидше він базується на вимірах фактичних результатів, одержаних після проведення роботи.

Заключний контроль відповідає завершальним етапам здійснення певних робіт і дає результати для їх прогнозування.

Разом з тим, заключний контроль здійснюється надто пізно, щоб відреагувати на проблеми в момент їх виконання, проте він має дві важливі функції. Перша дає керівництву організації інформацію, необхідну для планування, у випадку, якщо аналогічні роботи передбачається проводити в майбутньому. Порівнюючи фактичні і потрібні результати, керівництво має можливість краще оцінити, наскільки реально були складені плани.

Друга полягає в тому, щоб сприяти мотивації. Якщо мотиваційні винагороди залежать від результатів, то виміряти треба їх точно і об‘єктивно.

За ступенем охоплення проблем, контроль може бути вибірковим та суцільним залежно від того, який їх обсяг підлягатиме контролю. Крім цього, контроль може здійснюватися у відкритій формі, коли про нього заздалегідь повідомляється або негласно, наприклад, співробітниками СБ України.

Система контролю, яка не дозволяє усунути серйозні відхилення, перш ніж вони переростуть у крупні проблеми, беззмістовна і непотрібна. Природно, що проведене коригування повинно концентруватися на усуненні справжньої причини відхилення. Це повинно бути обов‘язковою програмою дій, щоб повернути організацію до правильних дій.

Контроль - важлива функція управління, застосування якої дає керівнику можливість слідкувати за виконанням управлінських рішень і вносити необхідні корективи. За своїм положенням функція контролю стоїть на другому місці після функції планування (постановки цілей). І це зрозуміло, адже якщо до підлеглих не доведена мета їхньої діяльності, то нічого буде контролювати. Незважаючи на те, що контроль не надто подобається працівникам, він все-таки є об'єднувальним чинником діяльності контролюючих та контрольованих.

Основне завдання контролю - забезпечити досягнення цілей і місії організації. Потреба контролю є об'єктивною і визначається дією таких чинників:

- зміною законів, політики, структури організації тощо;

- небезпекою виникнення кризових ситуацій;
- потребою забезпечення інформаційної безпеки;
- інші.

Тобто функція контролю спрямована на виявлення відхилень у процесі забезпечення інформаційної безпеки держави і полягає у своєчасній їх ліквідації. Контроль повинен:

- орієнтуватися на досягнення конкретних результатів;
- забезпечувати своєчасність, мобільність, надійність та гнучкість застосування контрольних операцій;
- відзначатися простотою;
- бути економічним, тобто базуватися на порівнянні витрат на його організацію з його результатами.

Для підвищення ефективності контролю потрібно:

- забезпечувати двостороннє спілкування між працівниками органів контролю та людьми, діяльність яких контролюється;
- уникати надто пильного (прискіпливого) контролю;
- застосовувати методи жорсткого, але справедливого контролю;
- використовувати методи матеріального стимулювання за результатами контролю;
- впроваджувати інформаційно-управлінську систему контролю з використанням комп'ютерної техніки.

Контроль за усіма стадіями діяльності підприємства повинен давати його керівництву інформацію щодо ухвалення відповідних рішень.

В системі СБ України, на виконання завдань покладених на неї Законом України «Про Службу безпеки України» реалізовано два способи контролю за службовою інформацією, що циркулює в країні.

Перший – офіційний контроль, який реалізований шляхом проведення планових та позапланових перевірок стану обігу документів, які містять службову інформацію. Порядок здійснення СБ України контролю за обігом документів, які містять службову інформацію, визначений наказом СБ України від 17 серпня 2006

року № 550 «Про затвердження Інструкції про порядок здійснення Службою безпеки України контролю за обігом документів, які містять службову інформацію».

При проведенні перевірок вивчаються:

- акти попередніх перевірок, матеріали службових розслідувань за фактами розголошення службової інформації, втрати її матеріальних носіїв (якщо мали місце такі факти), стан виконання викладених у них рекомендацій;
- умови зберігання документів та роботи з ними;
- порядок складання, оформлення, друкування, обліку, приймання, розсилання (відправлення), розмноження, використання, знищення, передачі документів на архівне зберігання;
- особливості оброблення, зберігання, друкування документів з використанням автоматизованих систем;
- порядок формування документів у справи, складання номенклатури справ, їх обліку та зберігання;
- порядок поводження з мобілізаційними документами, яким надано гриф "Для службового користування";
- порядок передачі документів за кордон;
- фактична наявність матеріальних носіїв службової інформації;
- порядок охорони службової інформації, під час прийому іноземних делегацій, груп та окремих іноземців.

Перевірка починається зі співбесід з керівником організації або вповноваженою ним особою, керівником канцелярії, начальником РСО, під час яких уточнюються особливості діяльності організації, пов'язаної з конфіденційною інформацією, що є власністю держави, місця, де обробляється та зберігається така інформація, визначається порядок організації перевірки. За результатами співбесід, у разі потреби, головою комісії корегується завдання кожному члену комісії.

Перевірка проводиться в присутності керівника канцелярії та начальника РСО організації чи їх заступників, а на окремих дільницях - працівників

канцелярії та РСО. Під час проведення перевірки можуть бути присутніми керівники структурних підрозділів організації або їх заступники.

За результатами перевірки складається Акт перевірки. Інформація, яка викладається в ньому, має бути достовірною, конкретною та повною з посиланням на відповідні норми актів законодавства, що були порушені. Включення до акта перевірки даних, висновків та пропозицій, які не підтверджені документально, а також надання морально-етичних оцінок діям працівників організацій не допускається.

Якщо під час перевірки буде виявлено ознаки злочину чи адміністративного правопорушення, голова комісії невідкладно доповідає про це особі, яка надала припис на проведення перевірки, для прийняття рішення відповідно до чинного законодавства України.

Статтею 255 Кодексу України про адміністративні правопорушення (N 8073-X, 07.12.1984) передбачено, що уповноважені на те посадові особи органів Служби безпеки України мають право складати протоколи про адміністративні правопорушення у справах про адміністративні правопорушення, зазначеними в 212-5.

Стаття 212-5. Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію

Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, -

тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб - від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, -

тягне за собою накладення штрафу на громадян від сорока до ста сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб - від ста

шістдесяти до двохсот шістдесяти неоподатковуваних мінімумів доходів громадян.

Другий – здійснення оперативно-розшукових заходів з метою попередження, виявлення, припинення і розкриття будь-яких форм розвідувально-підривної діяльності проти України.

Координація дій щодо реалізації прав підрозділів, які проводять оперативно-розшукову діяльність з метою боротьби з тероризмом, здійснюється Службою безпеки України.

Слідчі органів безпеки здійснюють досудове розслідування злочинів, передбачених статтею 330 Кримінального кодексу України.

Питання для самоперевірки.

1. Які нормативно-правові акти регламентують поводження із службовими документами?
2. Як розподіляються повноваження посадових осіб в організаціях?
3. Хто може бути допущений до роботи із службовими документами та справами, та які обмеження інформаційної діяльності на них накладаються?
4. Яким чином здійснюється облік службових документів?
5. Де відбувається друкування службових документів, які реквізити ідентифікують службові документи, та які вимоги до їх розміщення?
6. Які службові документи формуються у справи?
7. Порядок передачі службових документів до архівних установ.
8. Порядок знищення службових документів.
9. Що включає в себе поняття державного контролю?
10. Назвіть суб’єктів які здійснюють контроль за забезпеченням доступу до публічної інформації, до якої також відноситься службова інформація?
11. Що включає в себе поняття офіційного контролю стану обігу документів, що місять відомості які становлять службову інформацію?
12. Які заходи необхідно впроваджувати для підвищення ефективності функції контролю за службовою інформацією?

Використані та рекомендовані джерела

1. Про інформацію: Закон України від 02.10.1992 // Відомості Верховної Ради України, 1992. - № 48. - ст. 650.

2. Про основи національної безпеки України: Закон України від 19.06.2003 // Відомості Верховної Ради України, 2003. - № 39. - ст. 351.

3. Про доступ до публічної інформації: Закон України від 13.01.2011 // Відомості Верховної Ради України (ВВР), 2011. - № 32. - ст. 314.

4. Про контррозвідувальну діяльність: Закон України // Відомості Верховної Ради України (ВВР), 2003. - № 12. - ст. 89.

5. Про оперативно-розшукову діяльність: Закон України //ВВР, 1992. - № 22. - ст. 303.

6. Про державну таємницю: Закон України від 21 вересня 1999 р., № 1079-XIV // Відомості Верховної Ради України (ВВР). – 1999. - № 49. - ст. 428.

7. Про Службу безпеки України: Закону України // Відомості Верховної Ради України (ВВР), 1992. - № 27. - ст. 382.

8. Кримінальний кодекс України // Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131

9. Кримінальний процесуальний кодекс України // Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст. 88.

10. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст.1122

11. Постанова Кабінету Міністрів України від 27.11.1998 N 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» [Електронний ресурс]. // Режим доступу: http://zakon3.rada.gov.ua/laws/show/1893-98-п".

12. Типова інструкція з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади, затверджена постановою Кабінету Міністрів України від 30.11.2011 р. N 1242. / Офіційний вісник України від 12.12.2011. 2011 р., № 94, стор. 206, стаття 3433, код акту 59442/2011.

13. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів: ДСТУ 4163-2003. [Чинний від 2003-09-01]. - К.: Держспоживстандарт України, 2003. - 23с.

14. Наказ Служби безпеки України від 17.08.2006 N 550 «Про затвердження Інструкції про порядок здійснення Службою безпеки України контролю за обігом документів, які містять конфіденційну інформацію, що є власністю держави» (Зареєстровано в Міністерстві юстиції України 11 вересня 2006 р. за N 1046/12920)

3. ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ ПОВ'ЯЗАНІ З ВИКОРИСТАННЯМ СЛУЖБОВОЇ ІНФОРМАЦІЇ

3.1. Кримінальна відповідальність за передачу або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

3.1.1. Поняття кримінальної відповідальності

Кримінальна відповідальність – це особливий правовий інститут, у межах якого здійснюється реагування держави на вчинений особою злочин. Офіційну оцінку поведінки особи як злочинної, а її самої як злочинця, згідно з ч. 1 ст. 62 Конституції та ч. 2. ст. 3 КК України, може давати лише суд в обвинувальному вироку.

Основною відмінністю кримінального права від інших галузей права є те, що його завдання полягає не в регуляції найбільш важливих суспільних відносин, а в їх охороні. Ця специфіка обумовлює і специфіку відповідальності за порушення встановлених норм. Відповідальність особи за вчинення діянь, які чинне кримінальне законодавство визнає злочинними, має назву «кримінальної відповідальності».

Відповідно до ч. 1 ст. 2 КК України підставою кримінальної відповідальності є наявність у вчиненому діянні складу злочину, передбаченого відповідною нормою Особливої частини Кримінального кодексу.

Під складом злочину розуміється сукупність закріплених у законі про кримінальну відповідальність об'єктивних та суб'єктивних ознак, за наявності яких реально вчинене суспільно небезпечне діяння визнається злочином.

Об'єктивні та суб'єктивні ознаки у складі злочину об'єднуються в чотири групи (об'єкт злочину, об'єктивна сторона злочину, суб'єкт злочину, суб'єктивна сторона злочину), кожна з яких має свій юридичний зміст. Теорія кримінального права називає ці групи елементами складу злочину.

Усі елементи складу злочину та передбачені законодавцем їх ознаки становлять одне ціле, вони існують лише в єдності, в сукупності. Відсутність хоча

б однієї з них означає і відсутність складу злочину, а отже, й підстав для притягнення особи до кримінальної відповідальності.

Як і будь-який акт вольової поведінки людини, злочин становить єдність його зовнішніх (об'єктивних) та внутрішніх (суб'єктивних) ознак, що утворюють, відповідно, його об'єктивну й суб'єктивну сторони.

Суспільно-небезпечне діяння (дія чи бездіяльність), описане та криміналізоване в КК України, є основною характеристикою зовнішніх ознак злочину (його первинним об'єктивним проявом), розкриває його сутність, виступає фундаментом всієї конструкції складу злочину та кримінальної відповідальності.

В Кримінальному Кодексі України протиправні посягання щодо службової таємниці передбачені у ст. 330.

Стаття 330. Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни

1. Передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства, -

караються обмеженням волі на строк до трьох років або позбавленням волі на строк від двох до п'яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

2. Ті самі дії, вчинені з корисливих мотивів, або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб, -

караються позбавленням волі на строк від чотирьох до восьми років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

3.1.2. Об’єктивні ознаки складу злочину, передбаченого ст. 330 КК України.

Об’єктивна сторона складу злочину – це сукупність передбачених законом ознак, які характеризують зовнішній прояв суспільно небезпечного діяння, яке посягає на об’єкти кримінально-правової охорони, а також об’єктивні умови, пов’язані з цим посяганням.

Описуючи те чи інше злочинне діяння в диспозиціях норм Особливої частини КК України, законодавець здійснює це шляхом визначення саме об’єктивної сторони складу злочину.

Об’єктивна сторона визначає: а) в чому полягає злочин, б) яким чином він скоюється, в) у яких умовах місця, часу, обстановки він відбувається, г) за допомогою яких засобів і знарядь вчинюється.

Виконання саме об’єктивної сторони складу злочину є підставою для застосування кримінального закону, для притягнення винуватого до кримінальної відповідальності. Крім того, саме об’єктивна сторона є головним критерієм розмежування окремих злочинів, оскільки при властивій багатьом злочинам тотожності об’єкта посягання, форми вини та ознак суб’єкта, лише об’єктивна сторона завжди є різною. Відтак, це чи не найважливіший для практичної діяльності елемент складу злочину. Її аналіз дає можливість встановити інші елементи й ознаки складу злочину: об’єкт, якому заподіюється шкода даним злочином, відповідну форму вини, мотив, мету злочину, які не завжди вказуються в диспозиціях статей Особливої частини КК, і, таким чином, правильно кваліфікувати вчинене.

Таким чином, саме об’єктивна сторона злочину, передбаченого ст. 330 КК дає можливість усвідомити сутність злочинного посягання та уникнути помилок в характеристиці інших елементів складу злочину. Відтак, розгляд досліджуваного виду злочинної діяльності доцільно почати саме з об’єктивної сторони.

У диспозиції ст. 330 КК України альтернативно названо два діяння:

- передача іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службову інформацію, зібрану у

процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни;

- збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

Під передачею розуміється повідомлення будь-яким способом вказаних у законі відомостей адресатам передачі – іноземним підприємствам, установам, організаціям або їх представникам.

Зрозуміло, що передача певних відомостей іноземним адресатам передбачає наявність у суб'єкта їх матеріальних носіїв (доступ до них) або володіння змістом такої інформації.

Враховуючи особливості вчинення злочину, способами передачі можуть бути усне чи письмове інформування, або вручення інформаційних носіїв (паперових, електронних, зразків матеріалів, виробів тощо), здійснені безпосередньо, через посередників, або з використанням будь-яких технічних приладів, засобів зв'язку, комп'ютерів та мережі «Інтернет», або тайників.

Передачу може бути здійснено як шляхом дії так і шляхом бездіяльності. Так, наприклад, особа, яка на законних підставах опрацьовує у себе в кабінеті документи з грифом «ДСК», приймає представника іноземного підприємства, (установи, організації) та при проявленні ним інтересу до цих документів, умисно не обмежує йому доступ до них. Або коли особа, зафіксувавши стороннє втручання в закриту електронну мережу, умисно (за завданням іноземних представників, або з власної ініціативи) утримується від своєчасного запровадження заходів протидії. Тобто, своєю пасивною поведінкою (бездіяльністю) особа свідомо не перешкоджає незаконному заволодінню (ознайомленню, викраденню) секретними відомостями, що перебувають у її володінні, користуванні чи розпорядженні, представниками іноземної держави чи іноземної організації. Фактично передає їх.

Передачу секретних відомостей у формі бездіяльності слід відрізняти від пособництва як виду співучасті при вчиненні передачі службової таємниці. У п. 6

ст. 27 КК законодавець передбачає пособництво, вчинене, зокрема, у формі усунення перешкод. Відтак, усунення перешкод можна розглядати як ліквідацію перепон, що заважають (ускладнюють, унеможливлюють) реалізації злочинного наміру співучасників, яке може виражатися в залишенні незачиненим приміщення, куди має проникнути виконавець, відключенні сигналізації (або її умисного не увімкнення) тощо. Зауважимо, що при пособництві особа лише усуває перешкоди (можливо, лише окремі, не всі), що в подальшому полегшує доступ до службової інформації при спробах її отримання. До речі, ці спроби, з різних причин, можуть і не відбутися, а пособницькі дії виявитись недостатніми.

Зауважимо також, що на сьогодні передача службової таємниці іноземним адресатам не може трактуватись як однозначно протиправне діяння. На відміну від радянських часів, у наш час обмін інформацією з обмеженим доступом є звичайним і досить поширеним явищем у міжнародних стосунках, а його умови регламентовані законодавством. Таким чином, якщо зазначена інформація збирається з метою передачі або передається іноземному підприємству, установі, організації або їх представникам у порядку, передбаченому чинним законодавством України, це не може мати кримінально-правового значення. Відтак, кримінальній відповідальності підлягає лише незаконна передача іноземним адресатам службової інформації.

Збирання відомостей, що становлять службову таємницю - передбачає їх пошук та добування будь-яким способом з наступним зосередженням в одному або декількох місцях. При цьому, способами пошуку можуть бути розпитування, відстеження, спостереження, а способами добування – копіювання, фотографування, зняття інформації з каналів зв’язку, проникнення до комп’ютерних систем, придбання інформаційних носіїв шляхом купівлі, отримання в результаті шантажу або обміну, таємне чи відкрите викрадення, насильницьке заволодіння тощо.

Такі способи збирання обумовлюють широке застосування спеціальних технічних засобів (акустичних пристроїв (направлених або вмонтованих мікрофонів, лазерних пристроїв зняття аудіо інформації), пристроїв зняття інформації з комунікацій, засобів перехоплення побічних випромінювань,

оптичних приладів, електронних пристроїв для фіксування та передавання інформації тощо).

Разом з тим, при вчиненні збирання, передбаченого ст. 330 КК слід розмежовувати законні та незаконні способи збирання. Кримінально-правовій забороні можуть підлягати лише незаконні способи збирання, оскільки право не порушуючи закону вільно збирати будь-яку інформацію проголошується Конституцією України (ст. 34). Крім того, «з'ясування всіма законними засобами умов і подій в державі перебування і повідомлення про них уряду акредитуючої держави», відповідно до положень Віденської конвенції про дипломатичні зносини 1961 р. (підпункт «d» п. 1 ст. 3), є однією з офіційних функцій дипломатичного працівника. Подібними є і обов'язки консульських співробітників, викладені у Віденській конвенції про консульські зносини 1963 р. (п. «c» ст. 5).

Логічно припустити, що належно зберігаючи свою службову інформацію, держава на законодавчому та організаційно-виконавчому рівні має виключити можливість правомірного отримання цих відомостей не уповноваженими особами. У протилежному випадку інформація з обмеженим доступом фактично перестає нею бути, а дії держави щодо кримінального переслідування осіб за отримання цієїінформації без порушення закону нагадують провокацію. Наприклад, не може бути визнано незаконним збирання будь-якої інформації шляхом аналізу відкритих засобів масової інформації, або шляхом підслуховування розмов у міському транспорті, оскільки державою передбачені певні правила нерозповсюдження секретної інформації і порушення цих правил однією особою (наприклад, розголошення) не може автоматично утворювати винуватість іншої особи за їх сприйняття (збирання). Такий підхід узгоджується і з положенням п. 5 ст. 42 Закону України «Про друковані засоби масової інформації (пресу) в Україні» відповідно до якого журналісти не несуть відповідальності за публікацію відомостей, якщо в них розголошується таємниця, яка спеціально охороняється законом, проте ці відомості не було отримано журналістом незаконним шляхом.

Відтак, криміналізації підлягає лише незаконне збирання, під яким слід розуміти добування чи отримання відомостей, що становлять службову інформацію, протиправним способом або без належних правових підстав. Протиправними слід визнавати способи, що передбачають вчинення дій, прямо заборонених законами або підзаконними актами України. Ними, наприклад, можуть бути таємне чи відкрите викрадення матеріальних носіїв (в т.ч. за умов правомірного доступу), неправомірне ознайомлення з документами чи предметами в будь-який спосіб, організація витоку мовної інформації шляхом протиправного використання спеціальних технічних пристроїв, отримання секретних відомостей від фізичних або юридичних осіб, які ними володіють, за підробленими документами, або шляхом обману, шантажу, шахрайства, вимагання, підкупу чи шляхом застосування насильства тощо.

Проте, зауважимо, що при вчиненні передачі (незаконного передавання) іноземному підприємству, установі, організації або їх представникам відомостей «ДСК» законність чи незаконність способів їх збирання на кваліфікацію злочину не впливатиме.

Адресатами передачі, відповідно диспозиції ст. 330 КК, є іноземні підприємства, установи та організації (їх представники). Під ними слід розуміти підприємства, установи та організації, що належать іноземній державі чи приватним особам з числа іноземних громадян чи осіб без громадянства (їх обєднанням).

Іноземна держава – це держава, розташована за межами України, на яку не поширюється її суверенітет, незалежно від того, чи визнає Україна її незалежність, чи має з нею дипломатичні відносини, та в яких стосунках із нею перебуває.

Отже, в контексті ст. 330 КК України до іноземних установ та організацій можна віднести науково-дослідні об’єднання, політичні партії, промислові та релігійні організації, а також міжнародні організації, в тому числі неофіційні, нелегітимні чи злочинні («тіньові» уряди у вигнанні, міжнародні терористичні чи злочинні організації, тощо), крім офіційних міжнародних організації, членом яких є Україна.

Представник іноземного підприємства установи чи організації – це особа, яка уповноважена виражати їх інтереси та діє від її імені або представляє її за спеціальним повноваженням, у тому числі таємним (неофіційним).

Слід також зазначити, що на сьогодні представником іноземного підприємства, установи чи організації може бути і громадянин України, який, наприклад, представляє в Україні іноземну компанію, фірму, банк, науково-дослідний інститут, волонтерську організацію, фонд тощо. З огляду на це правильне встановлення адресата є визначальним аргументом при кваліфікації дій передбачених у ст.330 КК України.

За чинним КК України протиправною визнається передача або збирання з метою передачі відомостей, що становлять службову інформацію, лише іноземним підприємствам, установам та організаціям (їх представникам). Ті ж самі дії, вчинені особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, де адресатом передачі службової інформації є інше (не іноземне) підприємство установа чи організація або особа, що їх представляє, на сьогодні взагалі не передбачають кримінальної відповідальності.

Предметом злочину, передбаченого у ст. 330 КК є відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

Як вже зазначалося, службову інформацію, як новий вид інформації з обмеженим доступом, було запроваджено у 2011 р . Законом України «Про доступ до публічної інформації». В законодавстві вона, по суті, замінила «конфіденційну інформацію, що є власністю держави», залишивши незмінним ступінь обмеження доступу та відповідний гриф - «Для службового користування».

У визначенні службової інформації, наведеному у ст. 9 цього Закону міститься вичерпний перелік форм документів, які можуть містити службову інформацію. Зокрема, вона може міститися 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. Разом з тим певна некоректність формулювання переліку не дозволяє визнавати службовою інформацією листування між відомствами (а лише «внутрішньовідомча службова кореспонденція»), або документи, не пов'язані з розробкою напрямків діяльності державних органів чи здійсненням їх контрольних функцій (наприклад, інформація про фінансову діяльність), чи інформація у документах, що не передують публічному обговоренню та/або прийняттю рішень, тощо.

Крім того, приймаючи рішення про обмеження доступу до службової інформації відповідно до Закону України «Про доступ до публічної інформації» треба встановити одночасну наявність визначених в ньому умов (трискладовий тест). Втім, зробити це на підставі існуючого законодавчого визначення службової інформації вкрай проблематично, оскільки в ньому не зазначено чи завдає розголошення цих відомостей істотної шкоди і яким (чиїм) інтересам, а відтак, - чи підлягають ці відомості охороні державою, чи ні. Зауважимо, що згадані критерії у визначені іншого виду інформації з обмеженим доступом – державної таємниці, законодавцем враховані.

Зовнішньою ознакою того, що документ містить вказану інформацію, є наявність грифа обмеження доступу «Для службового користування» і номера примірника у правому верхньому кутку першої сторінки, для видань - на обкладинці та на титулі, а якщо документ міститься на магнітному носієві інформації - безпосередньо на ньому або у супровідному документі. Гриф проставляється виконавцем та особою, яка підписує документ, а на виданні - автором (укладачем) і керівником, який підписав видання до друку.

Проте на сьогодні гриф обмеження доступу «для службового користування» не завжди є орієнтиром у визначенні відомостей як предмета злочину, передбаченого ст. 330 КК, оскільки, порівняно з критеріями віднесення інформації до «конфіденційної інформації, що є власністю держави», які визначались у додатку 13 (на сьогодні втратив чинність) до Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є

власністю держави, затвердженої Постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893 (інформація повинна створюватись за кошти державного бюджету або перебувати у володінні, користуванні чи розпорядженні організації; використовуватися з метою забезпечення національних інтересів держави; не належати до державної таємниці; унаслідок розголошення такої інформації можливе: порушення конституційних прав і свобод людини та громадянина; настання негативних наслідків у внутрішньополітичній, зовнішньополітичній, економічній, військовій соціальній, гуманітарній, науково-технологічній, екологічній, інформаційній сферах та у сферах державної безпеки і безпеки державного кордону; створення перешкод у роботі державних органів), критерії віднесення до службової інформації, запроваджені Законом України «Про доступ до публічної інформації», виходячи з її визначення, значно звужені, що, відповідно, звужує і коло інформації, яка може бути віднесена до службової, залишаючи при цьому для неї той самий гриф – «для службового користування». Таким чином, не вся інформація з грифом «ДСК» може на сьогодні становити службову інформацію.

Зокрема, визначаючи сфери обігу службової інформації, законодавець визначає лише оперативно-розшукову та контррозвідувальну діяльності, та сферу оборони країни, не припускаючи можливість наявності відомостей «ДСК» у зовнішньополітичній, внутрішньополітичній, економічній, військовій, соціальній, гуманітарній, науково-технологічній, екологічній, інформаційній сферах та у сферах державної безпеки і безпеки державного кордону, визначених у ст. 6 Закону України «Про основи національної безпеки України» як такі, що містять реальні та потенційні загрози національній безпеці України та стабільності в суспільстві.

У ст. 330 КК законодавець визначає предметом злочину «відомості, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни», тобто наводить другу частину законодавчого визначення службової інформації – «до службової може належати така інформація: … 2) зібрана у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до

державної таємниці». Проте, у диспозиції цієї статті нічого не зазначається щодо першої частини законодавчого визначення службової інформації – відомостей які «міститься в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень», відтак можна стверджувати, що ці відомості не становлять предмет злочину, передбаченого ст. 330 КК, хоча й можуть мати гриф «для службового користування».

Варто зауважити, що відповідно до п. 31 Постанови Кабінету Міністрів України № 1893 від 27 листопада 1998 р. «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» службова інформація (як раніше і «конфіденційна інформація, що є власністю держави»), за сукупністю може становити державну таємницю, а отже, за певних умов, може бути предметом злочину передбаченого не лише ст. 330 КК але й ст. 111 (114) КК - при вчиненні шпигунства.

Отже, доповнюючи зроблений раніше висновок, можемо констатувати, що на сьогодні не кожна інформація з грифом «ДСК» є службовою інформацією і не всяка службова інформація підлягає кримінально-правовій охороні, навіть попри те, що її сукупність може становити державну таємницю.

Зазначимо також, що предметом злочину, передбаченого ст. 330 слід визначати відомості у будь-якій формі фіксації (матеріальній чи нематеріальній) та достатньому для усвідомлення обсязі і якості відтворення, які становлять службову інформацію.

Об'єктом злочину в кримінальному праві є суспільні відносини, блага та інтереси, які прийняті під кримінально-правову охорону і яким внаслідок вчинення злочину спричиняється або може бути спричинена шкода.

У кримінально-правовій науці поширена триступенева класифікація об'єктів «по вертикалі»: загальний, родовий і безпосередній. На ній побудована

система Особливої частини КК України: – Особлива частина – глава Особливої частини – склад злочину. Триступеневому поділу застосовується і щодо об'єкта кримінально-правової охорони: загальний об'єкт – родовий об'єкт – безпосередній об'єкт. Запропонована система класифікації відповідає потребам практики, є логічною, оскільки вона заснована на співвідношенні філософських категорій загального, особливого й окремого.

За класичним підходом загальним об'єктом вважається вся сукупність суспільних відносин, благ, цінностей, що охороняється законодавством про кримінальну відповідальність (відповідно до ст. 1 КК України це: права і свободи людини і громадянина, власність, громадський порядок та громадська безпека, довкілля, конституційний устрій України, а також мир та безпека людства.).

Під родовим об'єктом злочину слід розуміти взаємопов'язані та однорідні соціальні цінності, або ж суспільні відносини, блага та інтереси, що охороняються законом про кримінальну відповідальність, на які посягає певна група злочинів. Саме родовий об'єкт складу злочину визначає місце кримінальної норми в системі Особливої частини Кримінального кодексу, суттєво впливає на кваліфікацію злочинного посягання.

Злочинні посягання, передбачені ст. 330 розташовані законодавцем у Розділі XIV «Злочини у сфері охорони державної таємниці, недоторканості державних кордонів, забезпечення призову та мобілізації», проте до жодної з зазначених сфер дії, зазначені у ст. 330 безпосереднього стосунку не мають.

При розгляді об'єкту злочину протиправних посягань на інформацію з обмеженим доступом необхідно враховувати у чиєму володінні (розпорядженні) знаходиться інформація та чиїм інтересам (особи, суспільства, держави) завдається шкода від її витоку. З огляду на взаємопов'язаність цих критеріїв очевидно, що основним з них виступає право володіння (розпорядження) яке зазнає обмеження та призводить до несприятливих наслідків.

Те, що предметом цього злочину є відомості, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (тобто у сфері державної безпеки), свідчить про спрямованість злочину саме проти держави.

Таким чином, родовим об’єктом передачі або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни є безпека держави (державна безпека).

Якщо родовий об’єкт злочину дає можливість встановити групову належність конкретного діяння, то індивідуальні його ознаки визначаються безпосереднім об’єктом посягання. Безпосереднім об’єктом злочину є те конкретне суспільне відношення, благо або інтерес, на який посягає конкретний злочин. Безпосередній об’єкт злочину перебуває в колі елементів, що характеризують конкретний склад злочину, передбачений нормою Особливої частини КК України.

Безпосередній об’єкт є обов’язковою ознакою будь-якого складу злочину, відтак при кваліфікації протиправного діяння його точне встановлення обов’язкове. Це дає змогу визначити суспільні відносини, цінності, блага чи інтереси, на які безпосередньо спрямоване протиправне посягання, оцінити характер його суспільної небезпеки та вирішити, яку саме норму права застосовувати, – тобто правильно кваліфікувати злочин і відмежувати його від подібних суспільно небезпечних діянь.

Безпосереднім об’єктом злочину, передбаченого ст. 330 КК України, в залежності від галузевого характеру службової інформації, що виступає предметом посягань, слід визнавати інтереси держави (державні інтереси) у визначених сферах її діяльності (у сфері оборони, у сфері охорони правопорядку (ОРД, КРД) тощо), де зосереджені відомості, що становлять службову інформацію.

Про спрямованість протиправних посягань на службову інформацію саме проти інтересів держави прямо вказується і у ч.2 ст. 330 КК, (дії, що спричинили тяжкі наслідки для інтересів держави). Зауважимо також, що злочинні посяганя на відомості «ДСК» як у чинному так і в попередніх Кримінальних кодексах України традиційно відносяться до підслідності органів державної безпеки (ч. 2 ст. 216 КПК).

3.1.3. Суб’єктивні ознаки злочину, передбаченого ст. 330 КК України

Відповідно до ст. 18 КК України суб’єктом злочину є фізична осудна особа, яка вчинила злочин у віці, з якого відповідно до цього Кодексу може наставати кримінальна відповідальність. Спеціальним суб'єктом злочину є фізична осудна особа, яка вчинила у віці, з якого може наставати кримінальна відповідальність, злочин, суб'єктом якого може бути лише певна особа.

У теорії та практиці застосування кримінального законодавства панує точка зору, згідно з якою кримінальній відповідальності підлягають лише люди, тобто фізичні особи.

Осудність у кримінальному праві розглядається як сукупність двох критеріїв – медичного (психологічного) та юридичного (психологічного).

Медичний критерій характеризує стан психічного здоров’я особи під час вчинення нею злочину. Він свідчить про такий стан психіки, який характеризується як перебування у здоровому розумі, що дає можливість усвідомлювати власну поведінку. При цьому не виключені можливості наявності в особи незначних відхилень у психіці в межах осудності .

Юридичний критерій полягає у здатності особи усвідомлювати характер своїх суспільно небезпечних дій (бездіяльності) та керувати ними.

Кримінальний кодекс України у ч. 2 ст. 19, базуючись на загальному вченні про осудність, дає нормативне визначення неосудності як умови, за якої особа не підлягає кримінальній відповідальності: «Не підлягає кримінальній відповідальності особа, яка під час вчинення суспільно небезпечного діяння, передбаченого цим Кодексом, перебувала в стані неосудності, тобто не могла усвідомлювати свої дії (бездіяльність) або керувати ними внаслідок хронічного психічного захворювання, тимчасового розладу психічної діяльності, недоумства або іншого хворобливого стану психіки. До такої особи за рішенням суду можуть бути застосовані примусові заходи медичного характеру».

Неосудність – це поняття, протилежне за змістом поняттю осудності. Особа в стані неосудності не може визнаватись суб’єктом злочину, а отже і притягуватись до кримінальної відповідальності.

Відповідно до загальних положень КК України відповідальність за злочини, передбачені ст. 330 КК України настає з 16-річного віку. Встановлення певного мінімального віку кримінальної відповідальності пов’язане насамперед із фізіологічними процесами поступового формування здатності особи, з моменту досягнення певного віку, усвідомлювати свої дії і керувати ними. Особи у віці до 14 років, а також особи у віці від 14 до 16 років, що вчинили шпигунські дії, не підлягають кримінальній відповідальності, оскільки злочини, передбачені ст. 111 та ст. 114 КК, не входять до переліку суспільно небезпечних діянь, вказаних в ч. 2 ст. 22 КК України.

Суб'єктом злочину, передбаченого ст. 330 КК України законодавець визначає «особу, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків», отже окрім загальних ознак, суб’єкт повинен мати одну із зазначених у законі спеціальних ознак, тобто для даного складу злочину характерним є спеціальний суб’єкт.

Категорії працівників, які допускаються до роботи з виданнями з грифом «Для службового користування», визначаються керівниками організацій. Іншим особам (наприклад, журналістам) доступ до службової інформації може бути надано у відповідному порядку (зокрема за письмовим клопотанням керівників відповідних організацій, в яких вони працюють з урахуванням значного суспільного інтересу та з письмового дозволу керівника організації, якому надано право затверджувати переліки відомостей, які містять службову інформацію).

Факт надання допуску означає, що вказані відомості довірені їм у зв'язку з виконанням службових обов'язків.

В диспозиції статті 330 КК законодавець прямо вказує дві альтернативні ознаки спеціального суб’єкта:

1) особа, якій відомості, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, особою, якій ці відомості були довірені у зв'язку з виконанням службових обов'язків;

2) особа, якій відомості, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, стали відомі у зв'язку з виконанням службових обов'язків.

Під особами, яким відомості, що становлять державної таємницю, були довірені у зв’язку з виконанням службовим обов’язків, необхідно розуміти осіб, які допущені до службової інформації відповідно до рішення керівника установи, які мають відповідний досвід роботи з такою інформацією та яка потрібна їм для виконання службових обов’язків.

Цю групу, як правило, складають особи, діяльність (робота, служба чи навчання) яких безпосередньо пов’язана з володінням, добуванням, розробкою чи обробкою службової інформації. До них відносяться наукові та практичні працівники, відповідні посадові та інші особи, які безпосередньо працюють з такою інформацією.

Під особами, яким відомості, що становлять службову інформацію, спеціально не довірялися, але стали відомі у зв’язку з виконанням службових обов’язків, необхідно розуміти осіб, допущенних до роботи зі службовою таємницею, але не мали доступу до конкретних відомостей «ДСК».

Йдеться про осіб, які працюють із службовою інформацією іншого роду чи безпосередньо не працюють зі службовою інформацією, але в результаті їх роботи чи служби такі відомості можуть стати їм відомі (охоронці, шофери, експедитори, кур’єри та інші працівники і службовці, які мають непряме, опосередковане відношення до роботи з матеріалами, документами, виробами, відомості про які становлять службову інформацію).

Виконання службових обов’язків у значенні ст. 330 КК означає здійснення особою діяльності у межах і на підставі оформленого в установленому порядку трудового договору, контракту і т.д. між цією особою і керівником підприємства, установи чи організації, де працює, перебуває на службі чи навчається громадянин.

Слід зазначити, що для осіб, які мають доступ до службової таємниці (ці відомості їм довірені або вже стали відомі) характерною є лише передача (передавання) цих відомостей зарубіжним адресатам, оскільки потреби у їх

збиранні фактично немає, відтак, відповідно існуючого формулювання диспозиції ст. 330 КК законодавець передбачає збирання особами, що мають доступ до певної службової інформації, іншої службової інформації, яка їм не відома, оскільки до неї вони доступу не мають.

Якщо службова інформація стала відома особі не у зв'язку з виконанням службових обов'язків, а за будь-яких інших обставин (підслухала телефонну розмову, почула від спів службовця, знайшла на вулиці документи з такими відомостями тощо) і надалі вона її передає іноземним адресатам, то така особа не є суб'єктом злочину, що розглядається, і відповідно не підлягає відповідальності за ст. 330 КК України.

Аналіз суб'єктів злочину, передбаченого у ст. 330 КК показує, що положення цієї норми не можуть бути застосовані до громадян України, іноземців, або осіб без громадянства, які вчинили дії, передбачені об'єктивною стороною цього злочину, але відомості, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни не були їм довірені (не стали відомі) у зв'язку з виконанням службових обов'язків, оскільки вони не є суб'єктами цього злочину. За певних обставин такі дії громадян України можуть бути кваліфіковані як державна зрада у формі надання іноземній організації допомоги в проведенні підривної діяльності проти України (ст. 111 КК), тоді як аналогічні дії іноземців та осіб без громадянства за чинним КК не передбачають кримінальної відповідальності.

Суб'єктивна сторона злочину – це внутрішня сторона злочину, що характеризує психічне ставлення особи до вчиненого суспільно небезпечного діяння та його наслідків. Юридичними ознаками що характеризують зміст суб'єктивної сторони, є вина, мотив та мета злочину, а в окремих випадках також емоційний стан, у якому перебувала особа під час його вчинення.

Кожен злочин – це єдність об'єктивного й суб'єктивного. Якщо об'єктивна сторона злочину – це зовнішня характеристика злочину, то суб'єктивна є його внутрішньою характеристикою. Вони настільки пов'язані між собою, що вчинки викривають думки, наміри, а про наміри, думки судять по вчинку». Вирішення питання щодо суб'єктивної сторони злочину теоретично й практично виступає як

найбільш складний та відповідальний момент у встановленні об'єктивної істини в конкретному кримінальному проваджені, як завершальний етап у дослідженні конкретного злочину. В юридичній літературі неодноразово зазначалось, що найбільші труднощі виникають при аналізі конкретних складів злочинів у зв'язку із встановленням суб'єктивної сторони, доказування якої у будь-якому випадку не так і не настільки надійне, як встановлення об'єктивних якостей та характеристик злочину, та породжує більшу частину помилок, які допускаються працівниками слідства та суду.

Розглядаючи суб'єктивну сторону злочину слід зважати на те, що вона не тільки відображає об'єктивні обставини та умови кожного конкретного правопорушення, але й пізнається саме через об'єктивні ознаки. Тому правильне визначення суб'єктивної сторони злочину багато в чому залежить від того, наскільки точно й повно досліджені усі обставини вчиненого діяння та характеристики особи, яка його вчинила.

Вина є обов'язковою та основною ознакою суб'єктивної сторони. Концепція вітчизняного кримінального права передбачає можливість притягнення до кримінальної відповідальності лише за винне суспільно небезпечне діяння (дію або бездіяльність). Саме через вину реалізується демократичний підхід до змісту кримінальної відповідальності, яка передбачає можливість її настання лише у випадках наявності суб'єктивних підстав. Надзвичайна важливість цього положення зумовила необхідність його закріплення в Конституції України (ст. 62), де зазначається: «Особа вважається невинуватою у вчиненні злочину і не може бути піддана кримінальному покаранню, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду».

Відповідно до ст. 23 КК України виною є психічне ставлення особи до вчинюваної дії чи бездіяльності, передбаченої цим Кодексом, та її наслідків, виражене у формі умислу або необережності.

Вина є основною ознакою складу злочину, яка відмежовує злочинне діяння від незлочинного. Вітчизняне кримінальне право передбачає відповідальність лише за принципом винуватості, заперечуючи можливість притягнення до кримінальної відповідальності тільки за факт вчинення суспільно небезпечного

діяння. Отже, злочином може бути лише діяння, яке вчинене умисно або з необережності. Невинувате діяння (casus) не може передбачати кримінальну відповідальність. Отже відповідальність може бути тільки винуватою. Реалізація її без вини робить непотрібним саме існування кримінального права».

Суб'єктивна сторона злочину, передбаченого ст. 330 КК, характеризується виною у формі прямого умислу: особа усвідомлює, що передає відомості з обмеженим доступом, а саме – службову інформацію іноземним підприємствам, установам, організаціям або їх представникам та бажати передати саме ці відомості саме цим адресатам.

Якщо особа (суб'єкт злочину) не усвідомлює своїх дій (наприклад, інша особа використовує її «втемну», або вона вважає відомості, що передаються, такими, що не становлять службову інформацію), то відповідальність за ст. 330 КК виключається. Також, не можна однозначно підходити до кваліфікації дій особи, яка усвідомлювала свої дії, але не бажала їх вчинення (наприклад, повідомлення іноземним представникам службової інформації після застосування тортур або погрози вбивством).

Вчинення злочину у формі збирання відомостей, що становлять службову інформацію, обов'язково передбачає наявність мети передачі цих відомостей іноземним адресатам. Отже, злочин у цій формі завжди вчиняється лише з прямим умислом. Оскільки мета виступає обов'язковою ознакою її відсутність (чи не встановлення) виключає можливість кваліфікації подібних дій за ст. 330 КК України.

Мотиви злочину, передбаченого ст. 330 КК, можуть бути найрізноманітнішими і на кваліфікацію не впливають. Найпоширенішими мотивами є корисливість, страх у результаті погроз або шантажу з боку спецслужб, спонукання громадянина України допомогти підприємству, установі чи організації іноземної країни, до етнічної групи якої він належить, тощо. Події на Сході України виявили і такі мотиви цього злочину, як ненависть до української держави, заперечення державності України, сприяння імперській політиці Росії.

Описуючи діяння, криміналізовані у диспозиції ст. 330 законодавець вдається до уточнення: – «за відсутності ознак державної зради або шпигунства». Ознаками державної зради (ч.1 ст. 111 КК) може бути передача громадянином України службової інформації іноземцям в рамках надання допомоги у проведенні підривної діяльності проти України. Як правило, це передбачає надання згоди на співпрацю з іноземною організацією у проведенні підривної діяльності (як правило – спецслужбою) та виконання певної складової загального плану підривного заходу (акції).

Розмежування «Передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни» (ст. 330 КК України) від шпигунських посягань, передбачених ч.1 ст. 111 КК (для громадян України) та ст. 114 КК (для іноземців та осіб без громадянства) відбувається, перш за все, за предметом посягання.

Відповідно до ст.9 Закону України «Про доступ до публічної інформації» до службової може належати інформація, лише у певних сферах діяльності держави та така, яку не віднесено до державної таємниці.

Разом з тим, виходячи з того, що відповідно до п. 31 Постанови Кабінету Міністрів України № 1893 від 27 листопада 1998 р. «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» службова інформація за сукупністю може становити державну таємницю, а отже, за певних умов, може бути предметом злочину при вчиненні державної зради у формі шпигунства чи шпигунства.

З огляду на те, що предметом злочину виступає інформація, що знаходиться у володінні (розпорядженні) держави, а спрямоване на неї протиправне посягання здатне «спричинити тяжкі наслідки для інтересів держави» (ч. 2 ст. 330 КК), можна стверджувати, що і родовий і безпосередній об’єкти «Шпигунства» та «Передачі або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері

оборони країни» співпадають, проте суспільна небезпечність останнього злочину, виходячи з характеристик предмету посягання, значно нижча.

Що ж до об'єктивної сторони, то дії, криміналізовані у ст. 330 КК України практично аналогічні тим, що вчиняються при шпигунстві. Зміст понять «іноземна організація» та «представник іноземної організації» у статтях 114 та 330 також майже однаковий, за тим винятком, що у ст. 114 під іноземною організацією розуміється будь-яка недержавна організація, а у ст. 330 під «іноземною організацією» розуміється як держана, так і недержавна організація. Слід зауважити, що у цій нормі, на відміну від ст. 114 КК, поняття «іноземна організація» не охоплює собою поняття «іноземне підприємство» та «іноземна установа», які в переліку адресатів зазначаються окремо.

Суб'єктом злочину, передбаченого ст. 330 КК, є особа, якій ці відомості були довірені, або стали відомі у зв'язку з виконанням службових обов'язків.

Категорії працівників, які допускаються до роботи з виданнями з грифом «Для службового користування», визначаються керівниками організацій. Інші особи (наприклад, журналісти) можуть бути допущені до службової інформації з грифом «Для службового користування», у відповідному порядку (зокрема, за письмовим клопотанням керівників відповідних організацій, в яких вони працюють), і факт надання допуску означає, що вказані відомості довірені їм у зв'язку з виконанням службових обов'язків.

З огляду на те, що іноземці можуть мати доступ до державної таємниці, та враховуючи порядок надання доступу до службової інформації, логічно припустити, що представники іноземної держави чи організації можуть бути на законних підставах допущені і до цієї інформації. Отже, ймовірно можуть бути суб'єктами злочину, передбаченого ст. 330 КК.

З суб'єктивної сторони обидва злочини, що розглядаються, можуть бути вчинені тільки з прямим умислом: особа усвідомлює, що передає відповідні відомості іноземним підприємству, установі, організації або їхнім представникам, або що збирає ці ж відомості для передачі їм, і бажає це зробити. Також, в обох складах злочинів мета передачі іноземним адресатам відомостей, що виступають предметом злочину, є обов'язковою ознакою їх збирання.

Кваліфікуючими ознаками злочину, передбаченого у ч.2. ст. 330 КК, є вчинення його:

1) з корисливих мотивів;

2) повторно;

3) за попередньою змовою групою осіб;

4) спричинення ним тяжких наслідків для інтересів держави.

Корисливі мотиви мають місце у разі коли винуватий, вчиняючи злочин, бажав одержати у зв'язку з цим гроші або інші матеріальні блага для себе або інших осіб.

Відповідно до ст. 32 КК України повторністю злочинів визнається вчинення двох або більше злочинів передбачених тією самою статтею, або частиною статті. Повторність відсутня при вчиненні продовжуваного злочину, який складається з двох або більше тотожних діянь, об'єднаних єдиним злочинним наміром. Повторність також відсутня, якщо за раніше вчинений злочин особу було звільнено від кримінальної відповідальності на законних підставах або якщо судимість за цей злочин було погашено чи знято.

Відповідно до ч. 2 ст. 28 КК вчинення злочинів за попередньою змовою групою осіб означає спільне вчинення цього злочину декількома (двома і більше) суб'єктами злочину, які заздалегідь домовилися про спільне його вчинення. Такі особи діють як співвиконавці, при цьому можливий розподіл функцій, за якого кожен співучасник виконує певну роль.

На відміну від злочинів, передбачених статтями 328 і 329, у злочині, передбаченому ст. 330, йдеться не загалом про тяжкі наслідки, а про тяжкі наслідки для інтересів держави.

Тяжкими наслідками для інтересів держави слід визнавати випадки, коли в результаті передачі іноземцям відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, державі було заподіяно значної фінансово-економічної, політичної чи іншої шкоди. Так, зокрема до тяжких наслідків слід відносити випадки, коли в результаті зазначених дій відповідні державні органи змушені були істотно змінювати зміст стратегічних, оперативних, мобілізаційних та інших

важливих планів, організацію охорони певних об'єктів, напрями науково-дослідних робіт, особливо якщо це було пов'язано із заподіянням державі великої майнової шкоди. Тяжкими наслідками розголошення відомостей, що стосуються осіб, які здійснюють оперативно-розшукову діяльність, мають визнаватися, зокрема, відповідні посягання на їхнє життя, здоров'я чи волю.

Питання чи є ті або інші наслідки тяжкими має вирішуватися залежно від сукупності обставин, що характеризують якість і кількість відповідних відомостей, до кого саме вони потрапили, чи були фактично використані на шкоду інтересам України тощо.

Виходячи з цього, залежно від шкоди, яка може бути заподіяна інтересам України при передачі іноземцям зазначеної службової інформації, можливими є такі види тяжких наслідків:

1. Шкода у сфері зовнішніх відносин України (розрив дипломатичних відносин, відкликання посла з будь-якої країни; оголошення персоною нон грата дипломата України; зрив укладання міжнародної угоди України тощо).

2. Шкода у сфері оборони України (зрив воєнної (бойової) операції; необхідність розробки нових оперативно-стратегічних планів, підвищення вразливості об'єктів і систем озброєння та необхідність додаткових витрат на їх передислокацію або відновлення їх бойової ефективності; відмова від застосування від систем озброєння, що стали неефективними в результаті витоку відомостей тощо).

3. Шкода в економічній і науково-технічній сферах (економічні санкції проти України; втрата пріоритету в наукових дослідженнях і можливості патентування та продажу ліцензій на науково-технічні досягнення, зрив програми чи напрямку досліджень; зрив важливої зовнішньоторговельної операції тощо).

4. Шкода у сфері державної безпеки та охорони правопорядку (провал розвідувальної чи контррозвідувальної операції, зрив оперативно-розшукових заходів щодо осіб, у діях яких є ознаки вчинення особливо тяжких або тяжких злочинів проти основ національної безпеки України, проти миру, безпеки людства та інших особливо небезпечних злочинів тощо).

Тяжкі наслідки можуть полягати також у фізичній шкоді: смерть однієї чи більше осіб (загибель людей), а також інші нещасні випадки з людьми за умови, якщо психічне ставлення винної особи до таких наслідків виражене у формі необережності.

3.2. Адміністративна відповідальність за порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію.

3.2.1. Поняття адміністративної відповідальності

Адміністративну відповідальність прийнято визначати як сукупність адміністративних правовідносин, які виникають у зв'язку із застосуванням уповноваженими органами (посадовими особами) до осіб , що вчинили адміністративне правопорушення, передбачених нормами адміністративного права санкцій – адміністративних стягнень.

Адміністративна відповідальність (поряд із кримінальною, дисциплінарною та цивільно-правовою) є особливим видом юридичної відповідальності, якій з одного боку притаманні загальні ознаки – відповідальність настає за наявності вини особи у скоєнні протиправного діяння, конкретизується юрисдикційним актом компетентних органів, пов'язана з державним примусом тощо, з іншого – вона має особливості та специфічні ознаки, зокрема такі:

1) настає за вчинення адміністративного правопорушення (проступку), який є самостійним видом юридичних правопорушень , перелік яких міститься в КУпАП та інших адміністративних актах України;

2) результатом притягнення особи до адміністративної відповідальності є накладення на неї адміністративного стягнення – особливого виду юридичних санкцій, перелік яких установлено в ст. 24 КУпАП;

3) за вчинення проступків суддями притягується до адміністративної відповідальності особа, яка організаційно їм не підпорядковується (на відміну від дисциплінарної відповідальності, де стягнення накладаються у порядку підлеглості керівником);

4) адміністративна відповідальність характеризується особливим процесуальним порядком її реалізації – провадженням у справах про адміністративні порушення, яке передбачено КУпАП. від кримінального та цивільного процесів це провадження відрізняється відносною простотою (меншою кількістю передбачених законодавством процесуальних дій), оперативністю (меншою тривалістю провадження за часом0 й економічністю (меншими матеріальними витратами на здійснення провадження);

5) притягнення до адміністративної відповідальності та накладення адміністративного стягнення не передбачає для правопорушника судимості (як при кримінальній відповідальності);

6) адміністративна відповідальність – цевідповідальність правопорушника перед державою та суспільством. Водночас, ініціатива притягнення правопорушника до відповідальності та обов'язок доведення його провини лежить на державі. Адміністративна відповідальність має попереджувальний характер – не допустити подальших протиправних дій особи, зокрема злочинних;

7) Адміністративна відповідальність за правопорушення настає у випадку, коли воно за своїм характером не передбачає кримінальної відповідальності.

Таким чином, відповідно ст. 9 КУпАП адміністративним правопорушенням (проступком) визнається протиправна, винна (умисна або необережна) дія чи бездіяльність. Яка посягає на громадський порядок , власність, права і свободи громадян, на встановлений порядок управління й за яку законом передбачено адміністративну відповідальність.

3.2.2. Склад правопорушення «Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію».

Порядок обліку зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію визначається відповідною Інструкцією, затверджено Постанова Кабінету Міністрів України від 27 листопада 1998 р. (зі змінами та доповненнями) № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання

документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію».

Адміністративну відповідальність за «Порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави» було встановлено Законом України «Про внесення змін до деяких законодавчих актів України» від 11.05.2004 р. шляхом доповнення Кодексу України про адміністративні правопорушення статтею 212-5, до якої згодом було внесено зміни (Законами № 3775-VI від 22.09.2011 р, який збільшив покарання за вчинення проступків та № 1170-VII від 27.03.2014 р. який визначив предметом проступку службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни - тобто привів у відповідність до Закону України «Про доступ до публічної інформації» 2011 р.)

Стаття 212-5. Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію

Порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, -

тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб - від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, -

тягне за собою накладення штрафу на громадян від сорока до ста сорока неоподатковуваних мінімумів доходів громадян і на посадових осіб - від ста шістдесяти до двохсот шістдесяти неоподатковуваних мінімумів доходів громадян.

Об’єктом правопорушення, передбаченого ст.212-5 КУпАП є інтереси держави у сферах її діяльності де здійснюється обіг службової інформації,

зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності та у сфері оборони країни. Зокрема, забезпечення права держави на володіння (розпорядження) цією інформацією.

Предметом зазначеного правопорушення виступають документи та інші носії службової інформації (видання, справи, магнітні носії інформації тощо).

Зауважимо, що зазначені носії службової інформації мають містити відомості зібрані у процесі оперативно-розшукової, контррозвідувальної діяльності та у сфері оборони країни.

Таким чином, інша службова інформація, та, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу 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, не може бути предметом правопорушення, передбаченого ст.212-5 КУпАП.

Для кваліфікації правопорушення за статтею ст.212-5 КУпАП встановлення предмета є обов'язковим.

Обєктивна сторона зазначеного правопорушення формується за допомогою конструкції «порушення порядку обліку, зберігання і використання» носіїв певної службової інформації. Причому, обовязковою ознакою об'єктивної сторони цього правопорушення є розголошення службової інформації, яке відбулося внаслідок порушення порядку обліку, зберігання і використання її матеріальних носіїв.

Під розголошенням службової інформації слід розуміти сприйняття її змісту особою, якій право на ознайомлення з нею не надано у порядку, встановленому чинним законодавством.

Сприйняття як одна з форм пізнання є відображення у свідомості людини предмета чи явища в цілому в сукупності його властивостей при їх безпосередньому впливові на органи почуттів людини. Водночас у сприйнятті завжди проявляються особливості особистості сприймаючого суб'єкта, тобто в його свідомості інформація, що розголошується, може відбитися лише частково або трансформуватися, спотворитися.

Для визнання розголошення службової інформації правопорушенням не має значення, сприйняла стороння особа секретну інформацію як інформацію з обмеженим доступом чи ні. Центральним моментом у даному випадку є обсяг сприйнятої сторонньою особою інформації та якість такого сприйняття.

Якщо особа усвідомила зміст відомостей, що були їй розголошені, та може її відтворити в обсязі, який свідчить про перехід службової інформації у володіння такої особи, то це слід кваліфікувати як розголошення, а отже як правопорушення, передбачене ст. 212-5 КУпАП.

Якщо ж стороння особа не сприйняла надану інформацію нічого не запам’ятала або ж володіє розголошеними відомостями у настільки незначному обсязі, який в цілому свідчить про необізнаність даної особи з певною службовою інформацією, то об’єктивна сторона правопорушення відсутня.

Причому, несприйняття сторонньою особою наданої їй інформації може статися і з причин, що не залежать від волі особи, що цю інформацію розголошувала, наприклад внаслідок незнання мови, глухоти, сильного сп’яніння та інших причин) або якщо інформація сторонньою особою була сприйнята, але не не зафіксувалися у свідомості.

Розголошення службової інформації (як шляхом дії, так і шляхом бездіяльності) може розглядатися проступком тільки за умов порушенні встановлених правил(порядку) обліку, зберігання і використання документів та інших матеріальних носіїв інформації. Якщо розголошення сталося з інших причин(стихійні лиха, форс-мажорні обставини, військове захоплення об’єкта тощо), кваліфікація цих дій за ст. 212-5 КУпАП. неможлива.

Іншими словами, обов’язковим є встановлення причинно-наслідкового зв’язку між розголошенням службової інформації і порушенням конкретною особою порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни.

Термін «порядок» (правило) передбачає наявність певних нормативно-правових актів, зіставлення з якими дає можливість визначити, чи мають місце

його порушення. Тому для того, щоб зрозуміти, чи було не дотримання певних правил поводження з відомостями, що становлять службову інформацію, необхідно встановити, чи був покладений конкретними нормативно-правовими актами на особу обов'язок діяти відповідним чином, або, навпаки, утриматися від певної поведінки, тобто діяти саме так, а не інакше. Керівним документом у даному випадку є Постанова Кабінету Міністрів України № 1893 від 27 листопада 1998 р. «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» та затверджений відомчий Перелік відомостей, що становлять службову інформацію.

Адміністративну відповідальність за правопорушення, передбачені ст. 212-5 КУпАП може нести лише спеціальний суб'єкт, - особа, яка досягла на момент вчинення правопорушення 16-річного віку і на яку згідно з законодавством України покладено обов'язки щодо обліку, зберігання і використання матеріальних носіїв службової інформації.

Субєктивну сторону вказаного правопорушення характеризує вина як у формі необережності (переважно), так і у формі умислу.

Питання для самоперевірки.

1. Що таке кримінальна відповідальність;
2. Що є об'єктом злочину, передбаченому ст.330 КК України;
3. Дайте характеристику суб'єкту злочина, передбаченого ст.330 КК України;
4. Дайте характеристику суб'єктивної сторони злочина, передбаченого ст.330 КК України;
5. Чим злочин, передбачений у ст.330 КК України відрізняється від державної зради та шпигунства.
6. Дайте характеристику кваліфікуючих ознак злочина, передбачених у ч.2 ст.330 КК України;

Використані та рекомендовані джерела

1. Закон України від 13 січня 2011 р. «Про доступ до публічної інформації» // Голос України. – 2011. – № 24.

2. Закон України від 1992 р. «Про друковані засоби масової інформації (пресу) в Україні», у редакції Закону від 11 травня 2004 р. [Електронний ресурс]. Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.

3. Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8037-10

4. Постанова Кабінету Міністрів України від 27 листопада 1998 р. № 1893 «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» // Урядовий кур'єр. – 1998. – 10 грудня

5. Адміністративне право України : підручник [Ю.П. Бітяк, В.М. Гаращук, О.В. Дьяченко та ін.]. – К.: Юрінком Інтер, 2005. – 544с.

6. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 3-є вид., переробл. та доповн.˜ К. : Атіка, 2003.˜ 1056 с.

7. Уголовный кодекс Украины : научн.-практ. комментарий / отв.ред. : В. И. Шакун, С. С. Яценко. – 5-е изд., доп. – К. : А.С.К., 1999. – 1088 с.

8. Благодарний А.М. Правове регулювання адміністративної відповідальності за правопорушення у сфері державної безпеки: навч. посіб. / А.М. Благодарний. – К. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 88 с.

9. Матишевський П.С. Кримінальне право України: Загальна частина : підруч. для студ. юрид. вузів і фак. / П. С. Матишевський. – К. : А.С.К., 2001. – 352 с.

10. Фріс П.Л. Кримінальне право України: Загальна частина : підруч. для студ. вищ. навч. закладів / П. Л. Фріс.˜ К. : Атіка, 2004.˜ 488 с.

11. Кузнєцов В.О. Кримінальне право України: Загальна та Особлива частини : навч. посіб. / В. О. Кузнєцов, М. П. Стрельбицький, В. К. Гіжевський. – К. : Істина, 2005. – 380 с.

12.Кримінальне право в запитаннях і відповідях: Загальна частина : посіб. для підготовки до іспитів / за заг. ред. В. А. Клименка. – К. : Атіка, 2003. – 288 с.

13. Кримінальне право України: Загальна частина : підруч. для студ. юрид. спец. вищ. закладів освіти / [М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.] ; за ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. – К.-Х. : Юрінком Інтер – Право, 2002. – 416 с.

14. Навроцький В.О. Кримінальне право України: Особлива частина : курс лекцій / В.О.Навроцький. – К. : Т-во «Знання», КОО, 2000. – 771 с.

15. Кримінальне право України: Особлива частина : підруч. / [М. І. Бажанов, В. Я. Тацій, В. В. Сташис, І. О. Зінченко та ін.] ; за ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. – К. : Юрінком Інтер ; Х. : Право, 2002. – 496 с.

16.Бантишев О.Ф. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації) : моногр. / О. Ф. Бантишев – К. : Вид-во НА СБ України, 2004. – 122 с.˜ Бібліогр. : с. 113-120.

17.Введение в психологию / Под ред. А.В.Петровского. – М.: Издательский центр “Академия”, 1995. – С. 137; Філософія: Навч. посібник / Надольний І.Ф., Андрущенко В.П., Бойченко І.В. та ін. / За ред. І.Ф.Надольного.˜ К.: Вікар, 1997.˜ С. 275.

18. Международное право в документах : учеб. пос. / сост. Н. Т. Блатова. – М. : Юрид. лит., 1982. – 856 с.

19.Тацій В.Я. Об’єкт і предмет злочину в кримінальному праві України : навч. посіб. / В. Я. Тацій. – Х. : Укр. юрид. академія, 1994. – 76 с.

20.Коржанський М.Й. Кримінальне право України. Частина загальна : курс лекцій / М. Й. Коржанський. – К. : Наук. думка та Укр. видав. група, 1996. – 336 с.

21.Макаренко В.В. Проблема інституційного забезпечення контролю за дотриманням законодавства про службову інформацію / В. В. Макаренко, С. М. Шовкун // Інформаційна безпека людини, суспільства, держави. – 2011. № 2 (6). – С 111-116.

22.Шлапаченко В.М. Шляхи удосконалення кримінальної відповідальності за шпигунство у формі збирання (ст. 114 КК України) / В. М. Шлапаченко // Інформаційна безпека людини, суспільства, держави. – 2014. № 1(14). – С. 84-95.

4. СЛУЖБОВА ТАЄМНИЦЯ В ЗАКОНОДАВСТВІ ІНОЗЕМНИХ ДЕРЖАВ, ЄС, НАТО

4.1. Загальні критерії обмеження доступу до інформації в законодавстві іноземних держав, НАТО та ЄС

В інформаційному суспільстві одним із фундаментальних прав людини і громадянина визнано право на доступ до інформації, що відображено у відповідних документах міжнародної спільноти, передусім у Загальній декларації з прав людини, Міжнародному пакті про громадянські та політичні права, Європейській конвенції про захист прав людини та основоположних свобод. Так, у статті 10 Європейської конвенції йдеться про те, що кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Питання транскордонності є вкрай важливим в умовах розвитку сучасних інформаційних комунікацій, зокрема мережі Інтернет.

Зважаючи на вище викладене, інформаційне законодавство повинно забезпечувати досягнення балансу інтересів людини, суспільства та держави, а в основу правомірного обмеження доступу до інформації повинні бути покладені принципи свободи доступу до інформації, а саме:

1. Максимальне розкриття. Принцип максимального розкриття полягає у тому, що вся інформація, яка знаходиться в розпорядженні державних органів, підлягає оприлюдненню. Підстави обмеження доступу до інформації повинні бути чітко визначені у законі. Кожен, хто перебуває на території країни, повинен користуватися правом доступу до інформації. Реалізація цього права не вимагає додаткового підтвердження необхідності отримання інформації. У разі відмови надати інформацію державний орган повинен мотивувати своє рішення.

2. Обов’язок публікувати. Свобода інформації передбачає не тільки те, що державні органи зобов’язані відповідати на інформаційні запити, а й те, що вони зобов’язані самостійно оприлюднювати інформацію, яка становить суспільний інтерес. Закон повинен встановлювати загальне зобов’язання щодо категорій інформації, яка повинна бути опублікована.

3. Відкритий уряд. Діяльність державних установ повинна бути відкритою для громадськості.

4. Вичерпний перелік винятків. Усі запити на інформацію до державних органів повинні бути задоволені. Відмова в наданні інформації вважається безпідставною, якщо державний орган не може довести, що інформація, чітко відповідає критеріям трискладового тесту (див. нижче). Цей принцип поширюється на всі державні установи і навіть ті, які виконують функції охорони правопорядку та безпеки.

5. Сприяння доступу. Процедура прийняття рішення за запитами про надання інформації повинна передбачати наявність трьох рівнів уповноважених структур: державний орган, незалежний адміністративний орган, суд. Усі державні органи повинні створити відкриті, доступні внутрішні системи, що забезпечують право суспільства на отримання інформації. Закон повинен передбачати суворі терміни опрацювання запитів і вимагати, щоб відмова була обов'язково письмово вмотивованою.

6. Прийнятний рівень витрат. Оплата за надання інформації за запитами громадян має бути адекватною та не бути перешкодою для звернення громадян із запитами.

7. Відкритість для громадськості засідань державних органів. Засідання органів державної влади мають бути відкритими для громадськості (повідомляється завчасно), що пов'язано із правом громадськості брати участь у процесі прийняття рішень. Засідання може бути закритими тільки за достатніх підстав та відповідно до встановленого законом порядку.

Підставами для проведення закритого засідання за певних обставин може бути розгляд питань національної безпеки, охорони здоров'я населення, громадської безпеки, законності та правопорядку, таємниці слідства, особистої таємниці, комерційної таємниці. Це стосується органів державної влади, що приймають рішення обов'язкового, а не рекомендаційного характеру.

8. Першочергове значення відкритості інформації передбачає, що закони, які не відповідають принципу максимальної відкритості, підлягають змінам або скасуванню. Цей принцип заснований на тому, що з часом закони, які прямо або

опосередковано регламентують питання доступу до інформації, обов'язково мають відповідати принципам, на яких ґрунтується законодавство про доступ до інформації.

9. Захист інформаторів. Особи, які повідомляють інформацію про правопорушення (інформатори), повинні бути захищеними. Якщо особи всупереч закону та виконанню своїх службових обов’язків розкрили певну інформацію, але вчинили так з метою розкриття чи запобіганню вчиненню правопорушень чи злочинів органами влади, то такі особи звільняються від відповідальності.

Крім цього, для того, щоб інформація правомірно обмежувалась у доступі, вона, згідно із запропонованим міжнародною неурядовою організацією Article 19 трискладовим тестом, повинна відповідати трьом вимогам, а саме:

- повинна стосуватися легітимної мети, визначеної законом;
- розголошення такої інформації повинно загрожувати завданням суттєвої шкоди визначеній законом меті;
- шкода, яка може бути заподіяною цій меті повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації.

Легітимна мета повинна бути виправдана визначеним в законі вичерпним переліком правових підстав для обмеження доступу до інформації. Ці підстави, як правило, зумовлені інтересами національної безпеки, територіальної цілісності або громадського порядку, необхідністю запобігання заворушенням чи злочинам, охорони здоров'я населення, захисту репутації або прав інших людей, запобігання розголошенню інформації, одержаної конфіденційно, підтримання авторитету і неупередженості правосуддя.

При розгляді питання шкоди слід звертати увагу на такі аспекти, як переваги відкритого використання відомостей, що підлягають віднесенню до таємниці, а також витрати на захист таких відомостей у порівнянні із збитками, що можуть бути завдані, у разі їх розголошення.

Тема суспільної значущості інформації актуалізується тоді, коли є легітимні підстави обмеження доступу до певної інформації та з'являється потреба застосування права громадськості дізнатися про неї. Визнання інформації

суспільно необхідною має бути безперечним юридичним фактом, що дозволяв би ставити питання про поширення такої інформацію без згоди її власника.

Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо. Тобто у кожному конкретному випадку необхідно встановити, яка інформація є суспільно необхідною, тобто предметом суспільного інтересу.

Отже, питання про суспільну значущість інформації виникає у таких випадках:

- певна публічна інформація була неправомірно віднесена до інформації з обмеженим доступом і є потреба отримати її;
- хоча певна інформація за своєю природою є конфіденційною, разом із тим, ця інформація є суспільно необхідною (відомості про приватне життя вищих посадових осіб), то ця інформація в разі її наявності в органів публічної влади може бути надана за запитом, або бути оприлюднена засобами масової інформації;
- особу притягають до відповідальності за розповсюдження інформації з обмеженим доступом.

4.2. Особливості законодавства у сфері службової інформації європейських держав, ЄС, НАТО

Політикою безпеки інформації європейських держав, ЄС та НАТО передбачено, що стандарти та процедури безпеки застосовуються до всієї інформації, доступ до якої обмежується. У даному випадку мова йде про поняття “класифікована інформація”, аналог якого відсутній у національному законодавстві України, оскільки воно є ширшим, аніж поняття “інформація з обмеженим доступом”.

Загалом, класифікована інформація – інформація, дані, документи, які становлять інтерес для національної безпеки, мають бути захищені, що обумовлено рівнями важливості та наслідками, які випливають із розкриття або несанкціонованого розповсюдження. До класифікованої інформації відноситься інформація, яка становить державну або службову таємниці, та будь-яка іноземна класифікована інформація.

Класифікована інформація іноземних країн – це вид інформації, до якої відносять класифіковану інформацію, надану іноземною країною чи її структурами, міжнародною організацією чи її структурами, за умови збереження її секретності, а також інформацію, отриману в результаті співпраці між однією державою чи її структурами з іншою державою чи її структурами, міжнародною організацією чи її структурами, яка набуває статусу секретної інформації на основі взаємного погодження.

Отже, в законодавстві іноземних держав службова інформація є частиною секретного законодавства і на відміну від нашого законодавства визначена як службова таємниця.

Так, у законодавстві *Литви,* службова таємниця – це політична, економічна, військова, правоохоронна, наукова й технічна інформація, розповсюдження якої має бути обмежено в інтересах держави або установ, що намагаються захистити конституційні права осіб, є одним з видів класифікованої інформації.

Службову таємницю може становити:

- розгорнута інформація про захист інформації, що складає державну або службову таємницю, облік та використання такої інформації;

- розгорнута інформація про порядок перевірки кандидатур осіб, види діяльності яких пов’язані з використанням і захистом секретної інформації, а також інформація про особу, яка накопичується в процесі перевірки правильності первинної інформації;

- інформація про організацію пошуку і затримання злочинців, інші комплексні заходи, що здійснюються та оперативно організовані поліцією, а також інформація про докладно складені плани;

- організація охорони захищених об’єктів та осіб державними установами і їх підрозділами, а також документація на проект, конструкцію й ремонтні роботи на таких об’єктах;

- інформація про взаємодію підрозділів державних і муніципальних установ, підприємств, утворень і організацій із суб’єктами оперативної діяльності;

- докладна інформація про штатне розташування, штатну структуру, матеріально-технічне забезпечення Збройних сил Литви, а також оперативних, спеціальних підрозділів Міністерства Національної оборони, міністерства Внутрішніх справ, Департаменту державної безпеки, Служби спеціальних розслідувань та Митного Управління Литви, які здійснюють оперативну діяльність;

- інформація про облікові дані, вклади на соціальне страхування службовців, які забезпечуються державним соціальним страхуванням і проходять службу в оперативних, спеціальних підрозділах Міністерства Національної оборони, міністерства Внутрішніх справ, Департаменту державної безпеки, Служби спеціальних розслідувань та Митного Управління Литви, які здійснюють оперативну діяльність;

- зведена інформація про державний резерв матеріальних ресурсів і т.п.

У *Республіці Болгарія* службова таємниця – інформація, отримана в результаті діяльності уряду чи органів місцевого самоврядування або така, що зберігається ними – не державна таємниця, і несанкціонований доступ до якої міг би несприятливо вплинути на інтереси держави або спричинити збитки іншому законодавчо визначеному інтересу. Така інформація, відповідно до законодавства, повинна бути предметом класифікації як службова таємниця і позначатися “Тільки для службового використання”.

В *Угорщині* службовою таємницею вважається будь-яка інформація, яка відповідає класифікаційним характеристикам (офіційним категоріям службової таємниці), які визначені посадовою особою, уповноваженою класифікувати інформацію згідно з переліком посадових осіб, уповноважених здійснювати класифікацію інформації відповідно до їх обов’язків та повноважень.

Підставами віднесення інформації до службової таємниці є можливість завдання безпосередньої шкоди належному функціонуванню державних органів або громадських організацій, створення перешкод здійсненню ними своїх функцій або можливість неналежного впливу на сферу їх повноважень, внаслідок чого інтересам Республіки Угорщина буде завдано непрямої шкоди у випадках, якщо до закінчення терміну засекречування цю інформацію буде розголошено публічно або до неї буде здійснено несанкціонований доступ або у випадку її несанкціонованого використання, однаково як і передачі особі, яка не має до неї доступу або утаювання її від особи, яка таке право має.

У *Румунії* службову таємницю становить інформація, розкриття якої може завдати шкоди державній або приватній юридичній особі. Однак, така інформація, на відміну від державної таємниці, не має своїх рівнів класифікації. Законом заборонено відносити до службової таємниці інформацію, яка за своєю природою або змістом призначена забезпечувати інформацією громадян з деяких проблем, які становлять суспільний інтерес, для ухвалення чи запобігання анулюванню закону або перешкоди правосуддю.

Керівники органів державної влади та інституцій, компаній, які повністю або частково знаходяться в державній власності та інших юридичних приватних або державних осіб повинні встановити інформацію, яка є службовою таємницею та правила її захисту, координувати діяльність та заходи контролю для збереження службової таємниці згідно з їх компетенцією та відповідно до норм, які встановлені урядовими рішеннями.

Загалом, головним є те, що класифікованою інформація визначається відповідно до ймовірної *шкоди*, яка може бути нанесена у разі її несанкціонованого витоку чи розголошення. Це важливо тому, що дозволяє прозоро встановити зв’язок між рівнем класифікації інформації та відповідальністю за її розголошення та втрату.

Таблиця 1

Ступені обмеження доступу НАТО	**Ступені обмеження доступу ЄС**	**Українській еквівалент**

TOP SECRET	TRES SECRET UE/ EU TOP SECRET	"Особливої важливості"
SECRET	SECRET UE	"Цілком таємно"
CONFIDENTIAL	CONFIDENTIEL UE	"Таємно"
RESTRICTED	RESTREINT UE	"Для службового користування"

1. **TRES SECRET UE/EU TOP SECRET**: цей ступінь обмеження доступу застосовується лише до інформації і матеріалу, розголошення яких може заподіяти **надзвичайно серйозну шкоду** важливим інтересам Європейського Союзу або одної чи більш держав-учасниць.

2. **SECRET UE**: цей ступінь обмеження доступу застосовується лише до інформації і матеріалу, розголошення яких може заподіяти серйозну шкоду важливим інтересам Європейського Союзу або одної чи більш держав-учасниць.

3. **CONFIDENTIEL UE**: цей ступінь обмеження доступу застосовується до інформації і матеріалу, розголошення яких може заподіяти шкоду важливим інтересам Європейського Союзу або одної чи більш держав-учасниць.

4. **RESTREINT UE**: цей ступінь обмеження доступу застосовується до інформації і матеріалу, розголошення яких є **небажаним для інтересів** Європейського Союзу або одної чи більш держав-учасниць.

Слід зазначити, що в окремих країнах спеціальна перевірка проводиться і щодо тих осіб, які мають намір оформлення допуску на доступ до інформації із ступенем RESTRICTED в Естонії, Чехії та Словаччині здійснюються за місцем роботи, але в Словаччині допуск такого рівня не оформлюється. В Литві й Болгарії перевірка та оформлення допуску на доступ до службових секретів не проводиться.

Доступ до класифікованої інформації надається особам лише за принципом “необхідності”, який передбачає обмеження доступу до класифікованої інформації колом таких осіб, чиї службові обов’язки або спеціальне призначення його вимагають.

Доступ до некласифікованої інформації в документі, який містить класифіковану інформацію, або доступ до тих частин документа, які можуть бути опрацьовані окремо, не може бути обмежений за умови, що технічно

можливо відокремити некласифіковану інформацію чи частини документа від класифікованої інформації, не наражаючи її на небезпеку розкриття, та за умови, що опрацювання некласифікованої інформації складатиме розумний обсяг роботи.

Вимоги НАТО передбачають врахування при вирішенні питань допуску громадян до класифікованої інформації критеріїв благонадійності, ступеня довіри до особи та її надійності, а також її близьких родичів і оточення. Відповідно до вимог НАТО вивчення особи повинно мати за мету також виявлення:

- намірів та фактів вчинення громадянином актів шпигунства, тероризму, саботажу, державної зради;
- контактів громадянина з особами, які мають або мали відношення до шпигунської, терористичної або іншої протиправної діяльності, чи підозрюються у цьому;
- інформації щодо можливої участі або контактів громадянина з членами організацій, які шляхом насилля або іншими незаконними методами ставлять (ставили) за мету зміну державного устрою;
- інформації стосовно фінансових складнощів або непоясненого достатку;
- обставин, що можуть бути предметом шантажу або тиску, в тому числі зі сторони родичів або близьких осіб;
- ознак нечесності, неблагонадійності, ненадійності, нетактовності особи, які проявляються у її поведінці або висловленнях.

Згідно з вимогами стандартів безпеки НАТО та розроблених на їх основі правил безпеки ЄС у державах-учасницях створюються **Національні органи безпеки (НОБ),** основною функцією яких є впровадження стандартів безпеки інформації та здійснення загального контролю за дотриманням вимог національного законодавства в сфері охорони класифікованої інформації. До основних функцій НОБ належить захист класифікованої інформації усіх ступенів, включаючи інформацію з грифом "Для службового захисту інформації".

Такі органи створюються:

- на правах окремих **самостійних державних органів** (Чехія (НОБ), Словаччина (НОБ), Румунія (Бюро національного регістру державної секретної

інформації), Болгарія (Державна комісія безпеки інформації), які є відповідальними за однакове застосування стандартів захисту класифікованої інформація;

- як окремі **структурні підрозділи** при центральних органах державної влади, Польща (Агенція внутрішньої безпеки при МВС), Угорщина (функції НОБ здійснюються підрозділами МВС), Естонія (Департамент поліції безпеки).

Захист класифікованої інформації охоплює:

- юридичний захист – всі конституційні норми та інші юридичні умови, які забезпечують захист класифікованої інформації;
- процедурний захист – всі інструкції, на основі яких власники класифікованої інформації повинні організовувати внутрішню роботу, і всі внутрішні заходи порядку, що гарантують захист класифікованої інформації;
- фізичний захист – всі дії, пов’язані з гарантуванням безпеки та захисту класифікованої інформації, виконувані фізичними заходами та пристроями контролю, а також через технічні засоби;
- захист персоналу, що має доступ до класифікованої інформації або призначений, щоб гарантувати її безпеку – всі процедури перевірки і заходи, що застосовуються до осіб, які виконують завдання, пов’язані із класифікованою інформацією, щоб запобігати та усувати ризики розкриття класифікованої інформації.

Інформація, що становить службову таємницю, засекречується на підставі окремих переліків, що встановлюються державними органами чи уповноваженими на це особами.

Засекречування здійснюється шляхом проставлення на матеріальному носії інформації грифу обмеження доступу, дати засекречування, терміну засекречування, який обчисляється з дати засекречування інформації.

В законодавстві Естонії містяться норми, які зобов'язують власників класифікованої інформації раз на рік здійснювати перегляд носіїв такої інформації на предмет її можливого зниження грифу обмеження доступу чи розсекречування.

Згідно з законодавством Угорщини особа, що засекретила інформацію, зобов'язана не рідше ніж раз на 3 роки для державних секретів та 5 років для службових секретів робити перегляд такої інформації для прийняття можливого рішення про зниження грифу обмеження доступу чи розсекречування.

4.3 Організаційно-правові засади обміну службовою інформацією України з іноземними державами, НАТО та ЄС

Важливим аспектом інформаційної діяльності на сучасному етапі є участь в інформаційному обміні. Характерна для початкового часу епізодичність з часом була змінена на стійкі і тривалі відносини, що створило умови для виокремлення обміну інформацією в самостійну сферу та серед іншого, обумовило необхідність формування системи захисту ІзОД, в тому числі службової інформації.

Позитивний вплив на стан міжнародного співробітництва України мало створення правової бази для обміну ІзОД з іноземними партнерами, а саме підписання угод про взаємний захист інформації, які визначають:

– порядок взаємної охорони ІзОД (відповідно до національного законодавства сторін, актів міжнародних організацій, узгоджених правил);

– зобов’язання сторін щодо забезпечення охорони одержаної інформації, в тому числі недопущення доступу до неї третьої сторони, а також недопущення використання ІзОД інформації з метою, що не відповідає цілям передачі такої інформації;

– порядок надання доступу до ІзОД представникам сторін;

– порядок передачі ІзОД;

– зобов’язання щодо взаємного інформування в разі порушення вимог стосовно охорони ІзОД та вжиття заходів щодо притягнення до відповідальності винних у цьому осіб;

– терміни, протягом яких зобов’язуються забезпечувати взаємну охорону ІзОД;

– вимоги до виконавчих договорів, що укладаються між уповноваженими суб’єктами сторін, про передачу ІзОД (матеріальних носіїв такої інформації);

– порядок вирішення спірних питань;

– визначення органів сторін, на які покладається здійснення співробітництва за договором.

Загалом Україною укладено з іноземними державами та організаціями близько 47 угод про взаємний захист ІзОД, які визначають правові основи обміну такою інформацією та передбачають відповідне організаційне забезпечення зазначеної діяльності.

Однією з таких угод є *Угода Про безпеку між Урядом України та Організацією Північноатлантичного Договору*, яка укладена з метою забезпечення міжнародних зобов'язань Україна-НАТО щодо обігу ІзОД.

Уповноваженими органами, відповідальними за імплементацію заходів у галузі безпеки та процедур, згідно з Угодою про безпеку є СБ України та Офіс безпеки НАТО. Забезпечення охорони інформації НАТО в державних органах та установах покладається на їх керівників.

З метою розроблення та здійснення заходів із забезпечення режиму обмеження доступу в роботі з інформацією НАТО, постійного контролю за його дотриманням, у структурі РСО державних органів, що провадять діяльність з державною таємницею та інформацією НАТО створюються окремі функціональні ланки – Центри реєстрації документів НАТО. У МЗС функціонує Головний центр реєстрації документів НАТО.

Зобов'язання щодо захисту ІзОД між Україною та ЄС визначено в *Угоді України та ЄС про процедури безпеки, які стосуються обміну інформацією з обмеженим доступом*, в *Домовленостях про безпеку між Службою безпеки України (СБУ) ТА Управлінням безпеки Генерального секретаріату Ради ЄС (УБГСР ЄС) і Департаментом безпеки Європейської комісії (ДБЄК)*. СБУ та УБГСР, ДБЄК відповідають за виконання та нагляд за цими стандартами.

Згідно з детальними положеннями, обидві Сторони забезпечують захист інформації з обмеженим доступом на рівні, який щонайменше еквівалентний відповідним мінімальним стандартам, встановленим правилами та інструкціями з питань безпеки Сторони, яка надає інформацію.

Обидві Сторони зобов’язуються забезпечити, щоб заходи безпеки, які виконуються ними:

a) застосовувались до всіх осіб, які мають доступ до інформації з обмеженим доступом, носіїв інформації з обмеженим доступом, усіх приміщень, в яких знаходиться така інформація;

b) були розроблені таким чином, щоб виявляти осіб, які можуть становити небезпеку для інформації з обмеженим доступом, та забезпечувати унеможливлення їхнього доступу до такої інформації;

c) запобігали будь-якому несанкціонованому доступу сторонніх осіб до інформації з обмеженим доступом, зокрема матеріалів, що ті містять, та об’єктів, де вона знаходиться;

d) забезпечували, щоб інформація з обмеженим доступом надавалася лише за принципом необхідності за умовами службової діяльності, який є основним, а у випадках, коли інформація має гриф обмеження доступу ТАЄМНО/CONFIDENTIEL UE або ЦІЛКОМ ТАЄМНО/SECRET UE, лише особам, які мають допуск;

e) забезпечували цілісність та конфіденційність усієї інформації з обмеженим доступом та особливо такої інформації, що зберігається, обробляється або передається в електронному вигляді.

Перед наданням доступу до інформації з обмеженим доступом усі особи, які його потребують, повинні бути проінструктовані стосовно правил захисту інформації з обмеженим доступом відповідного ступеня, до якої вони матимуть доступ. Особи, які мають доступ до ІзОД, повинні бути поінформовані, що порушення цих правил призведе до дисциплінарної відповідальності та (або) кримінальної відповідальності.

Для одержання, відправлення, контролю і збереження ІзОД в Україні, Генеральному Секретаріаті Ради та Європейській Комісії створюється реєстраційна система. Центральна реєстратура документів ЄС у Міністерстві закордонних справ України є центральною реєстратурою для ІзОД ЄС, яка передається до України. Генеральний Секретаріат Ради ЄС є центральною реєстратурою для ІзОД України.

Питання для самоперевірки

1. Які загальні критерії обмеження доступу до інформації в законодавстві іноземних держав, НАТО та ЄС?
2. Які правові ознаки, характерні для службової таємниці в законодавстві іноземних держав, НАТО та ЄС?
3. Які складові захисту службової таємниці, передбачені у законодавстві європейських держав, НАТО та ЄС?
4. Дайте визначення класифікованій інформації та визначте місце службової таємниці у ній.
5. У чому різниця між службовою таємницею та службовою інформацією?
6. Визначте організаційно-праві засади обміну службовою інформацією між Україною, іноземними державами, ЄС і НАТО?

Використані та рекомендовані джерела

1. Principles of freedom of information legislation. ARTICLE 19. – London. – 1999.
2. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу / Курс лекцій. – Вид-во НА СБ України – 2006. – 208 с.
3. Європейська інтеграція України : підруч. / Є.Д. Скулиш, О.Д. Довгань, О.М. Солодка; за заг. ред. Є.Д. Скулиша. – К. : Наук.-вид. центр НА СБ України, 2012. – 384 с.
4. Артемов В. Ю. Порівняння організаційно-правових норм захисту інформації з обмеженим доступом країн-членів НАТО. Навч.-метод. посібник. – К.: КНТ, 2007. – 172 с.
5. Угода про безпеку між Урядом України і Організацією Північноатлантичного Договору / Офіційний Вісник України 2002. – № 40. – ст. 1852.
6. Угода між Україною та Європейським Союзом про процедури безпеки, які стосуються обміну інформацією з обмеженим доступом від 13.06.2005 / Офіційний вісник України від 07.03.2007 р. – № 15. – стор. 163. – стаття 582.

Навчальне видання

ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ЗАХИСТУ СЛУЖБОВОЇ ІНФОРМАЦІЇ

Навчальний посібник

Редактор С. В. Ангедуца
Коректор С. В. Ангедуца
Комп’ютерне макетування Т. О. Коркач
Формат 60х84/16. Ум. друк. арк. 7,02. Обл.-вид. арк. 5,86.
Тираж 10 прим. Зам. № 101

Реєстр. № 29/3/32-4168 від 6 квітня 2017 р.

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. М. Максимовича, 22, Київ, 03022
Свідоцтво суб’єкта видавничої справи ДК № 99 від 23.06.2000