

ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ЗАХИСТУ ТА ОБМЕЖЕННЯ ОБІГУ ІНФОРМАЦІЇ В ЦІЛЯХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

§ 1 Правове регулювання обігу інформації в суспільстві

Проблеми захисту найбільш важливої інформації та застосування обмежень щодо її обігу можна цілком справедливо вважати найдавнішим напрямком інформаційної безпеки держави. Від самого виникнення такого інституту, як держава, почала поширюватися практика оголошення різного роду відомостей таємними і встановлення відповідних правових норм для захисту цієї таємниці. Не втрачає актуальності ця проблема і нині.

Для чіткого визначення правової природи заборон і обмежень подібного роду потрібно визначитися з основними принципами обігу інформації в суспільстві. Цей обіг відбувається відповідно до цілого ряду факторів. По-перше, це фактори природні. Тобто маються на увазі різного роду фізичні та фізіологічні закони, які впливають на обіг інформації. До таких факторів фізичного характеру можна, наприклад, віднести значення швидкості світла, якою обмежуються передачі даних за допомогою електронних засобів комунікації, фізичні якості фізичних носіїв інформації, які обумовлюють строк зберігання інформації на цих носіях, можливість її зміни тощо. Крім того, діють, як ми вже зазначили, фізіологічні закони, які характеризують властивості індивіда як носія інформації: рівень його інтелекту, який визначає можливості щодо збору і обробки інформації, його здатність до забування, чим окреслюється строк, за який інформація може залишатися точною без збереження її на фізичних носіях, та ряд інших.

Разом з тим велике значення для обігу інформації в суспільстві відіграють саме суспільні закони, до яких належать норми моралі та норми права. Саме ці норми визначають основні характеристики тих процесів, які прийнято називати інформаційними відносинами, що виникають між різними учасниками: фізичними та юридичними особами, державою. Ці інформаційні відносини включають «процеси створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження і споживання інформації».¹

Інформаційні відносини, оскільки суб'єктами передачі інформації в них виступають як індивіди, так і соціальні групи, безумовно, є різновидом суспільних відносин. В даному разі також є актуальним загальне правило стосовно охорони державою найбільш важливих видів суспільних відносин, що набувають підвищеного суспільного значення. Тому держава встановлює відповідні правові норми, якими регламентуються права, обов'язки та правила поведінки їх учасників.

Відповідно ті інформаційні відносини, в яких названі суб'єкти «беруть участь як носії прав і обов'язків, встановлених нормами інформаційного права, називаються інформаційно-правовими відносинами (або інформаційними правовідносинами)»².

Таким чином, певні види інформаційних відносин у суспільстві регулюються правовими нормами. Ці правові норми насамперед регламентують параметри інформаційних процесів, за якими відбувається обіг інформації в людському суспільстві. Безумовно, обіг різних видів інформації (наприклад, виділених нами вільної, комерційної та стратегічної) регулюється різними правовими нормами, які відповідають їхній специфіці. Залежно від виду інформації законодавство передбачає наявність або відсутність тих чи інших обмежень або заборон. Згідно з такими міркуваннями, «аналіз основних видів інформації, що виробляється, дає можливість поділити їх на дві групи: відкриту, яка вільно розповсюджується в інформаційній сфері, і обмеженого доступу, розповсюдження якої можливе лише на умовах конфіденційності або таємності.

До відкритої інформації належать:

- інформація, що створюється в процесі творчості (витвори науки та мистецтва, відкриті патенти та авторські свідоцтва);
- документована інформація, що надається обов'язково;

¹ Копылов В.А. Информационное право. – М.: Юристь, 1997. – С. 171 – 172.

² Рассолов М.М. Информационное право. – М., Юристь, 1999. – С. 41.

- офіційні документи;
- масова інформація, що розповсюджується ЗМІ;
- інша інформація необмеженого доступу.

До інформації обмеженого доступу належить:

- документована інформація про державну та службову таємницю (в порядку захисту інтересів держави);
- документована інформація, що містить відомості про ноу-хау та ноу-ноу (в порядку захисту секретів виробництва і науки);
- персональні дані (в порядку захисту особистої таємниці).¹

Але, на нашу думку, схема «відкритої та закритої інформації» не може до кінця розкрити особливості існуючих її винятків та обмежень. Так, наприклад, подібна схема не робить різниці між інформацією, яка містить державну таємницю і доступ до якої може бути наданий лише обмеженому колу осіб, та інформацією, яка може бути передана будь-яким зацікавленим особам за відповідну винагороду (ті ж самі ноу-хау), причому це може бути як передача копії цієї інформації, так і повна передача усіх прав на подібну інформацію. З другого боку, говорячи про відкриту інформацію, знову ж таки ми можемо стверджувати, що вона може бути закритою для певного кола осіб. Наприклад, це стосується заборони відповідно до положення «Про державне посвідчення на право розповсюдження і демонстрування фільмів»² Національною радою України з питань телебачення і радіомовлення демонстрації по телебаченню фільмів з елементами насильства та еротики до 22.00. Крім того, в рамках такої класифікації абсолютно ігнорується система авторських прав та права власності на інформацію, за яких інформація може бути відкритою для доступу, але мати обмеження щодо розповсюдження або обробки.

На нашу думку, основою класифікації в даному разі мають бути не аморфні поняття «відкритості» або «закритості» інформації, а методи правового регулювання, що застосовуються до регулювання суспільного обігу того чи іншого виду інформації.

Таких методів ми можемо назвати два — диспозитивний та імперативний. За диспозитивного методу умови обігу інформації, її використання, розповсюдження, передачі прав на неї третім особам визнача-

¹ Копылов В.А. Информационное право. — М.: Юрист, 1997. — С. 35 — 36.

² Постанова Кабінету Міністрів України «Про положення про державне посвідчення на право розповсюдження і демонстрування фільмів» від 17 серпня 1998 р. № 1315

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

ються або власником цієї інформації особисто, або на основі договору з іншими зацікавленими особами. Це не означає відсутності нормативно-правового регулювання обігу цієї інформації, але в рамках цього регулювання існує відповідна свобода дії. Як приклад можна навести законодавство про авторські права, про право інтелектуальної власності, законодавство, що охороняє інформацію про особисте життя (адже ці дані також можуть бути оприлюднені за згодою цієї особи), тощо.

З другого боку, існує специфічний обіг інформації, який регулюється імперативним методом, що характеризується наявністю чітких законодавчих приписів і норм поведінки, відміна яких за згодою сторін неможлива. Це стосується, наприклад, встановлених законом прямих обмежень щодо державної, службової, лікарської, адвокатської таємниці, певних видів статистичної інформації, персональних даних тощо.

Таким чином, тип правового регулювання обігу інформації є однією з визначальних юридичних характеристик інформації. На основі початкової приналежності диспозитивного та імперативного методів правового регулювання відповідно до цивільного та адміністративного права ми можемо аналогічно назвати два види правового обігу інформації – цивільний та адміністративний. Причому держава «...вилучає її (інформацію – Б.К.) з цивільного обігу на будь-якому етапі. Ми вводимо поняття цивільного обігу, оскільки інформація, віднесена до державної таємниці, вилучається лише з обігу, що регулюється цивільним законодавством, але продовжує свій обіг відповідно до існуючого правового регулювання питань охорони державної таємниці. Коли значення або цінність інформації знижується, вона випадає з цивільного обігу і потрапляє у вільний обіг».¹

Звісно, до наведеної нами цитати слід зробити кілька зауважень.

По-перше, вилучення або обмеження інформації з обігу ґрунтується не лише на законодавстві про державну таємницю, про що ми писали вище. Одночасно оголошення інформації державною таємницею не виключає існування цивільно-правових відносин щодо неї, наприклад, це стосується результатів наукових розробок, досліджень тощо. «При володінні, використанні і розпорядженні інформаційними ресурсами, що становлять державну таємницю, повноважні державні органи вступають у майнові і зобов'язуючі відносини з іншими суб'єктами цивільно-

¹ Гостев И.М. Информационное право в России. // Конфидент, 2000. – № 1-2, январь – апрель. – С.18.

ного права. Зокрема, при передачі фізичними або юридичними особами інформаційних ресурсів у власність держави у зв'язку з їх засекреченням між ними виникають договірні відносини, а у випадках неправомірних дій державних органів постають питання про відшкодування шкоди, завданої громадянам або організаціям. Договірні відносини виникають між юридичними особами і державними органами, яким передано відомості, документи або дослідні зразки, що становлять державну таємницю при виконанні науково-дослідних і дослідно-конструкторських робіт».¹

По-друге, регулювання інформаційних відносин нормами цивільного права не виключає застосування до них додаткових обмежень. Наприклад, це стосується тих самих обмежень в цілях захисту моральності та здорового способу життя.

Таким чином, два правові методи регулювання створюють три можливі види правового обігу інформації: відкритий, що регулюється виключно цивільно-правовими нормами, закритий, що регулюється адміністративно-правовими нормами, і нарешті обмежений, до якого застосовуються обидва види правового регулювання. До них також долучається вільний обіг інформації, який правом не врегульований взагалі.

Але якщо говорити про інформацію як правову категорію, тобто про «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі» (ст. 1. Закону «Про інформацію»)², то будь-яка інформація, що відповідає цим критеріям, підпадає під дію відповідних правових норм.

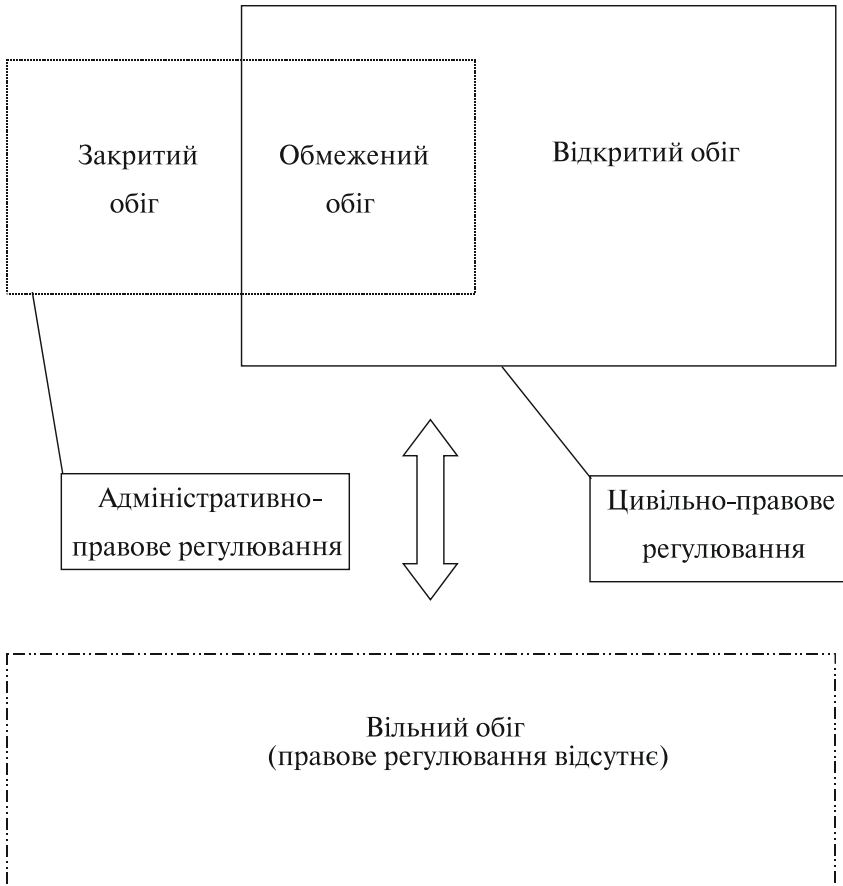
Але чи означає це, що будь-які дані, які визнаються законом інформацією, можуть стати об'єктом захисту в цілях інформаційної безпеки? Однозначно ні. На нашу думку, об'єктом захисту в цілях інформаційної безпеки є лише та інформація, яка згідно із законом знаходиться в закритому або обмеженому обігу, тобто інформація, до якої знову ж таки законом встановлені обмеження імперативного характеру. Як правило, застосування таких обмежень щодо доступу обумовлюється великою суспільною цінністю інформації і можливими суспільно небезпечними наслідками несанкціонованих дій з такою інформацією. Так, нормами ч. 5 ст. 30 Закону «Про інформацію» визначається, що до

¹ Северин В.А. Правовые проблемы информационной безопасности предприятия. // Юрист, 2001. – № 6. – С. 29.

² Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України, 1992. – № 48. – Ст. 650.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.



Мал. 10.4.1. Види суспільного обігу інформації

Водночас інформація, доступ до якої обмежується її власником на власний розсуд, має трохи інші характеристики. «Інформація, що становить комерційну таємницю, визначається суб'єктом підприємницької діяльності і являє для нього справжню або потенційну цінність, доступ до такої інформації обмежується і застосовуються заходи до її

охорони».¹ Таким чином, віднесення інформації до комерційної таємниці «не є грифом таємності, а лише вказує на те, що право власності на дану інформацію охороняється законодавством»².

І тут ми повинні поставити запитання, чи взагалі слід розглядати будь-які заходи щодо захисту інформації частиною національної інформаційної безпеки. Ми вважаємо, що ні. І ось чому.

Згідно із ст. 17 Конституції України³, захист інформаційної безпеки визнається найважливішою функцією держави. Головними критеріями віднесення питань захисту інформації до сфери державної функції захисту інформаційної безпеки, як вже зазначалося, є її велике суспільне значення і можливі суспільно небезпечні наслідки несанкціонованих дій з такою інформацією. Крім того, якщо мова йде про захист інформаційної безпеки як функцію держави, то цей захист здійснюється державними органами на правових засадах.

Такі критерії обумовлюють певні характеристики захисту інформації в цілях інформаційної безпеки:

- по-перше, випадки обмеження доступу інформації прямо передбачені законом;
- по-друге, ці обмеження пов'язані із забезпеченням інформаційних прав і свобод людини, забезпеченням інформаційних аспектів національної, державної, громадської безпеки, моральності, громадського здоров'я тощо. Тобто йдеться про обмеження, які покликані гарантувати визначені законодавством безпечні умови життєдіяльності людини, суспільства і держави;
- і, по-третє, ще однією важливою характеристикою є те, що суб'єктом застосування цих обмежень виступають держава та її компетентні органи.

Таким критеріям відповідає лише інформація, обіг якої регулюється імперативними, адміністративно-правовими методами.

Коли ж ми говоримо про захист інформації, що ґрунтується на праві власності на цю інформацію, наприклад, комерційної таємниці, об'єкта авторського права, інтелектуальної власності тощо, то мова, відповідно, повинна йти не про захист інформаційної безпеки, а про захист

¹ Северин В.А. Правовые проблемы информационной безопасности предприятия // Юристь, 2001. – № 6. – С. 29.

² Ярочкин В.И. Информационная безопасность. – М.: Международные отношения, 2000. – С. 351.

³ Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України, 1996. – №30 – Ст. 141.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

права власності. Зокрема, така думка підтверджується нормами ч. 3. ст. 30 Закону «Про інформацію», якими визначається, що громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною за власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

У цитованій нами нормі ще раз наголошується на диспозитивному характері регулювання доступу до інформації, що знаходиться у приватній власності, в тому числі підкреслюється, що система захисту подібної інформації встановлюється її власником на власний розсуд. Тобто така інформація може мати абсолютно різні ступені захисту, а може не мати такого захисту взагалі, крім того, суб'єктом цього захисту є не держава, а фізичні і юридичні особи. А це вже не відповідає розумінню функції держави як суспільно важливого напрямку її діяльності.

Насправді захист зазначених видів інформації теж здійснюється державою і її компетентними органами, але вже не в рамках функції захисту інформаційної безпеки, а в рамках правоохоронної функції, як захист права власності.

§ 2 Режими доступу до інформації

Ще однією особливістю правового регулювання обігу інформації є те, що залежно від типу інформації існують і відповідні, специфічні правила поведінки при здійсненні інформаційної діяльності, встановлені правовими нормами. Законом «Про інформацію» (ст. 28) такі правила поведінки визначаються як режими доступу до інформації. Згідно з нормами цієї статті, «режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації»¹. За своїм значенням режим доступу є однією з головних юридичних характеристик інформації, адже ним визначаються конкретні групи правових норм, що застосовуються до тієї чи іншої документованої або публічно виголошеної інформації.

¹ Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України, 1992. – № 48. – Ст. 650.

За своєю суттю режим доступу до інформації є різновидом спеціальних правових режимів, які являють собою «сукупність правил, закріплених в юридичних нормах, які регулюють певну діяльність людей».¹ Правові режими існують у рамках багатьох галузей права, але оскільки ми вже визначили, що захист інформації в цілях інформаційної безпеки відбувається на основі імперативного методу правового регулювання, то відповідні режими доступу до інформації за своїми характеристиками є найбільш близькими до адміністративно-правових режимів.

Особливими ознаками режиму доступу до інформації виступає специфіка його об'єкта – правові відносини, що виникають з приводу документованої або публічно виголошеної інформації. Головними характеристиками, які кваліфікують вид режиму доступу до інформації, є суб'єкт визначення доступності цієї інформації, коло суб'єктів, які мають доступ до цієї інформації, особливі вимоги та правила зберігання і поширення цієї інформації, строк дії режиму тощо.

Але в літературі існують і деякі інші погляди на режими інформації. Так, наприклад, іноді говорять про правовий режим інформаційних ресурсів як умову правового регулювання інформаційних відносин щодо нього. Зазначається, що «правові норми в даному разі встановлюють чотири обов'язкові вимоги, без яких інформаційний ресурс не може бути включено до системи правових відносин і отримати повноцінні гарантії в процесі взаємодії суб'єктів з приводу конкретних об'єктів даного ресурсу. Зміст правового режиму в даному разі визначають норми, які встановлюють:

- порядок документування інформації;
- право власності на окремі документи й окремі масиви документів, документи і масиви в їх інформаційних системах;
- категорію інформації за доступом до неї;
- порядок правового захисту інформації».²

Таким чином, режим доступу до інформації може також розглядатися в рамках більш складного правового режиму, що визначає цілий ряд інших аспектів існування інформації в системі правових відносин. Але разом з тим саме режим доступу є універсальною характеристикою інформації. Адже режим доступу до інформації не залежить від

¹ Бахрах Д. Н. Административное право: Учебник для вузов. – Москва: БЕК, 1999. – С. 202

² Бачило И.Л. Информационное право. Основы практической информатики. – М., 2001. – С. 99.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

порядку її документування. Більше того, режимом доступу визначається можливість знаходження інформації у приватній власності і порядок її правового захисту.

Так ми підходимо до розгляду окремих, передбачених законом режимів доступу до інформації в цілях забезпечення інформаційної безпеки України.

Основою правового регулювання захисту та обмеження доступу до інформації є норми ч. 2. ст. 32 Конституції України¹, згідно з якими не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Та норми ч. 3 ст. 34 Конституції України, якими передбачено можливість обмеження свободи інформації на основі закону 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.

Ці конституційні норми, з одного боку, надають фізичним особам право вимагати захисту особистої інформації та обмежують втручання державних органів і третіх осіб в цю сферу, а з другого – передбачають компетенцію держави та її органів щодо регулювання і обмеження обігу інформації та застосування заходів щодо примусового виконання цих обмежень.

Згідно із Законом «Про інформацію» (ст. 28) за режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Доступ до відкритої інформації надається будь-яким зацікавленим особам, а обмеження права на одержання відкритої інформації забороняється. Тим же законом (ст. 29) передбачено ряд шляхів забезпечення доступу до відкритої інформації:

- систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках);
- поширення її засобами масової комунікації;
- безпосереднього надання її зацікавленим громадянам, державним органам та юридичним особам.

¹ Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України, 1996. – №30 – Ст. 141.

Інформація з обмеженим доступом за своїм правовим режимом, в свою чергу, поділяється на конфіденційну і таємну (ст. 30 Закону «Про інформацію»).

§ 3 Державна таємниця

Найважливішою і, відповідно, максимально захищеною вважається інформація, оголошена державною таємницею. Її правовий режим встановлюється законами «Про державну таємницю»,¹ «Про інформацію» та рядом інших нормативно-правових актів. Закон України «Про державну таємницю» регулює суспільні відносини, що виникають з приводу віднесення певних відомостей до державної таємниці, їх розсекреченням та захистом в інтересах національної безпеки України.

Цей закон, зокрема, визначає:

- основні терміни і поняття, пов'язані з державною таємницею;
- компетенцію органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці;
- здійснення права власності на секретну інформацію та її матеріальні носії;
- фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею;
- порядок віднесення інформації до державної таємниці;
- порядок засекречення і розсекречення матеріальних носіїв інформації;
- порядок охорони державної таємниці;
- контроль за забезпеченням охорони державної таємниці;
- відповідальність за порушення законодавства про державну таємницю.

Так, відповідно до ст. 1 Закону «Про державну таємницю», «державна таємниця (далі також — секретна інформація) — вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці

¹ Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-ХІІ // Відомості Верховної Ради України, 1994. — № 16. — Ст. 93. (В редакції Закону № 1079-ХІV від 21.09.99)

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

України та які визнані у порядку, встановленому цим законом, державною таємницею і підлягають охороні державою»¹.

Той факт, що правові відносини щодо інформації, оголошеної державною таємницею, можуть регулюватися нормами цивільного законодавства, підкреслюється в ст. 6 Закону «Про державну таємницю». Згідно з її нормами, власник секретної інформації або її матеріальних носіїв здійснює своє право власності з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до Закону «Про державну таємницю».

У випадку, якщо обмеження права власності на секретну інформацію або її матеріальні носії завдають шкоди їх власнику, відшкодування здійснюється за рахунок держави у порядку та розмірах, що визначаються у договорі між власником такої інформації або її матеріальних носіїв і компетентним органом державної влади. Таким договором також визначаються:

- порядок та умови охорони державної таємниці, включаючи режим секретності під час користування і розпорядження секретною інформацією та її матеріальними носіями;
- обумовлюється згода власника цієї інформації та її матеріальних носіїв на здійснення права власності з урахуванням обмежень, встановлених відповідно до закону;
- взяття власником на себе зобов'язання щодо збереження державної таємниці та ознайомлення його з мірою відповідальності за порушення законодавства про державну таємницю.

У випадку відмови власника засекреченої інформації від укладення договору чи його порушення, за рішенням суду відповідна інформація або її матеріальні носії можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості.

Питання віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречення покладено на державних експертів з питань державної таємниці. Експерти з питань державної таємниці у Верховній Раді України призначаються Головою Верховної Ради, в інших органах державної влади – Президентом України за поданням керівника відповідного державного органу.

¹ Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-ХІІ // Відомості Верховної Ради України, 1994. – № 16. – Ст. 93. (В редакції Закону № 1079-ХІV від 21.09.99)

Рішення про засекречення інформації або її розсекречення приймається державним експертом з питань державної таємниці за власною ініціативою або за зверненням керівника відповідного органу державної влади, виключно на підставах, передбачених в ст. 8 Закону «Про державну таємницю». У рішенні державного експерта з питань державної таємниці щодо засекречення інформації визначається:

- інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим ст. 8 Закону «Про державну таємницю»;
- підстави для віднесення інформації до державної таємниці та обґрунтування шкоди національній безпеці України у разі її розголошення;
- ступінь секретності зазначеної інформації;
- обсяг фінансування заходів, необхідних для охорони такої інформації;
- орган державної влади, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та орган державної влади (органи), якому надається право визначати коло суб'єктів, що матимуть доступ до цієї інформації;
- строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Строк дії режиму таємності безпосередньо залежить від того, до якого ступеня таємності віднесено інформацію. Так, згідно зі ст. 13 Закону «Про державну таємницю», строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для інформації із ступенем секретності «особливої важливості» – 30 років, для інформації «цілком таємно» – 10 років, для інформації «таємно» – 5 років.

Висновок державного експерта з питань таємниць про засекречення або розсекречення інформації приймається в місячний термін після відповідного звернення керівника органу державної влади і набирає чинності з моменту внесення Службою безпеки України змін до Зводу відомостей, що становлять державну таємницю.

Звід відомостей, що становлять державну таємницю, формує та публікує в офіційних виданнях Служба безпеки України на підставі

рішень державних експертів з питань таємниць. Зміни до Зводу відомостей, що становлять державну таємницю, публікуються не пізніше трьох місяців з дня одержання відповідного рішення чи висновку.

Інформація, що може бути віднесена до державної таємниці визначається відповідно до норм ст. 8 Закону «Про державну таємницю» і викладена у Зводі відомостей, що становлять державну таємницю України (ЗВДТ), «який є єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування ЗВДТ держава забезпечує захист і правову охорону відомостей, які зареєстровані в ньому¹.

Сам ЗВДТ являє собою систематизований перелік відомостей, що становлять державну таємницю. Цей перелік складається зі статей, пунктів та підпунктів. Відомості систематизуються за чотирма великими групами (статті) відповідно до сфери державної діяльності:

- сфера оборони,
- сфера економіки,
- сфера зовнішніх відносин,
- сфера державної безпеки і охорони правопорядку.

Відомості, що належать до кожної з цих груп, класифікуються на окремі пункти та підпункти за основними характеристиками:

- змісту відомостей, що становлять державну таємницю;
- ступеня секретності («особливої важливості», «цілком таємно», «таємно»);

- строку дії рішення про віднесення інформації у роках (30 років, 10 років, 5 років).

Реєстрація відомостей у ЗВДТ є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифу секретності, який відповідає ступеню секретності, встановленому для них у ЗВДТ. Самі ж записи у ЗВДТ не повинні містити державних секретів.

Перелік відомостей, що становлять державну таємницю, в рамках визначених Законом «Про державну таємницю» та ЗВДТ чотирьох основних сфер можна також умовно класифікувати за деякими напрямками та видами інформації. Так, у військовій сфері можна виділити інформацію, що стосуються безпосередньо Збройних сил України, до якої, зокрема, віднесено відомості:

- про зміст оперативних планів та документів бойового управління директив, бойових наказів, донесень та зведень;

¹ Наказ Голови Служби безпеки України «Про затвердження Зводу відомостей, що становлять державну таємницю» від 1 березня 2001 № 52.

- про підготовку військ до виконання оперативних (бойових) завдань;
- про систему бойового чергування;
- про стратегічне розгортання та зміст мобілізаційних завдань, оперативно-мобілізаційних заходів;
- про зміст закритих навчальних програм у вищих військових навчальних закладах Збройних сил України.

Іншу групу можна кваліфікувати як інформацію військово-технічного характеру. Зокрема, це відомості:

- про військові об'єкти, зразки озброєння і військової техніки, органи державної влади і режимні об'єкти, підприємства, установи та організації, що підлягають захисту від засобів технічних розвідок;
- про норми технічного захисту інформації, віднесеної до державної таємниці;
- про нові зразки озброєння та військової техніки, нові технології створення та модернізації зразків озброєння та військової техніки;
- про досягнення науки і техніки, які можуть бути використані для потреб оборони і мають принципове значення для розробки нових видів озброєння та військової техніки;
- про систему фізичного захисту ядерних установок, ядерних матеріалів.

Також приділяється увага захисту інформації, яка стосується заходів щодо захисту населення в умовах можливих військових конфліктів. Так, у ЗВДТ включено інформацію:

- про управління системою Цивільної оборони України в умовах воєнного часу;
- про схеми та джерела водозабезпечення, заходи їх охорони;
- про особливо важливі та важливі об'єкти, які беруться під військову і воєнізовану пожежну охорону в умовах воєнного стану.

І, нарешті, до державної таємниці у військовій сфері віднесено ряд відомостей географічно-топографічного характеру, які мають важливе значення для бойового застосування військ, зокрема:

- про результати роботи щодо створення й уточнення державної системи координат і геодезичних параметрів, розробку і застосування національних космічних топогеодезичних засобів для забезпечення Збройних сил України;
- геодезичні дані, топографічні і картографічні матеріали з певними характеристиками, оприлюднення яких можливе лише після узгодження відповідно до законодавства.

Наступною сферою класифікації відомостей, що становлять державну таємницю, є сфера економіки. Серед інформації економічного характеру, що її внесено до ЗВДТ, також можна виділити кілька основних груп.

По-перше, це інформація військово-економічного характеру, захист якої є одним із заходів щодо забезпечення функціонування економіки України в умовах воєнного стану, матеріально-технічного забезпечення Збройних сил та підприємств оборонного призначення. Наприклад, до ЗВДТ внесено відомості, які характеризують:

- виробничі потужності мобілізаційного призначення галузей національної економіки щодо виробництва оборонної продукції;
- заходи, передбачені для забезпечення сталості функціонування галузей економіки України в умовах воєнного стану;
- кількість, вартість, строки постачання озброєння і військової техніки в Збройних силах України та військових формуваннях;
- номенклатуру, кількість, строки постачання військових формувань основними видами пального і мастильних матеріалів, речового та медичного майна, продовольства тощо.

Іншу групу можна охарактеризувати як стратегічно-економічну інформацію, що розкриває характеристики забезпеченості економіки України стратегічними або критично-необхідними сировиною і матеріалами. Згідно з ЗВДТ, це, наприклад, відомості:

- про розміри і розміщення стратегічних запасів та резервів нафти, газу і нафтопродуктів України;
- про балансові запаси корисних копалин у надрах та обсяги їх видобутку (виробництва) в Україні;
- про балансові запаси урану в надрах України;
- оперативно-статистичні дані митних органів про експортно-імпортні операції з окремими стратегічними видами сировини й продукції;
- про магістральні або внутрішньозонові лінії зв'язку, мереж зв'язку загального користування із зазначенням трас проходження через об'єкти зв'язку, що належать до мобілізаційних потужностей господарства України.

І, нарешті, останню групу складають відомості, захист яких здійснюється в інтересах забезпечення нормального функціонування кредитно-фінансової системи України. В цю групу входять такі відомості:

- про номенклатуру та обсяги матеріальних цінностей державного резерву;

- про кількість надходження до Державного фонду дорогоцінних металів і дорогоцінного каміння України, про відпуск їх на потреби народного господарства за період від одного року і більше, про планові обсяги реалізації золота за вільно конвертовану валюту або кількість золота, яке видане на закупівлю за кордоном товарів, за період від одного року і більше;

- про розроблені монетним двором Національного банку України банкноти і монети України нових зразків;

- про засоби захисту від підробки банкнот, бланків державних цінних паперів і документів суворого обліку України (крім відомостей про загальновідомі засоби захисту);

- про технології виготовлення та застосування спеціальних складових захисних голографічних елементів, які створюються на замовлення органів державної влади, у тому числі для захисту від підробки банкнот, цінних паперів, документів суворого обліку.

У сфері зовнішніх відносин визначено два основні види інформації, що становить державну таємницю і підлягає охороні.

По-перше, це інформація, розголошення якої може завдати шкоди зовнішньополітичній діяльності України, в тому числі відомості, що містяться в директивах, планах та вказівках делегаціям і посадовим особам, які представляють Україну, розголошення яких розкриває стратегію і тактику зовнішньої політики України.

По-друге, це інформація щодо деяких аспектів міждержавного військово-економічного співробітництва, яка згідно з законодавством України або її міжнародно-правовими зобов'язаннями є таємною. Це, зокрема, стосується відомостей про номенклатуру, обсяги та фінансування операцій з експорту, імпорту озброєння, військової техніки, окремих стратегічних видів сировини і продукції, а також відомості про військово-технічне та науково-технічне співробітництво з іноземними державами тощо.

І, нарешті, ще однією сферою інформації, яка становить державну таємницю, що її виділяє національне законодавство, є сфера державної безпеки і охорони правопорядку. Серед переліку відповідних відомостей, наведених у ЗВДТ, також можна виділити кілька характерних напрямків.

Так, по-перше, це інформація про деякі аспекти негласної та правоохоронної діяльності, яка впроваджується правоохоронними органами та військовими підрозділами України. А також про особовий склад і підготовку відповідних підрозділів і осіб, що здійснюють подібну діяльність. Ця група включає відомості:

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

- про зміст, плани, організацію і результати оперативно-розшукової та розвідувальної діяльності, її конкретні засоби, форми і методи;
- про отримані результати ведення агентурної та спеціальної розвідки, радіоелектронної розвідки, контролю безпеки інформації та зв'язку тощо;
- про штат, штатну розстановку, стан, зміст і організацію бойової і спеціальної підготовки особового складу Служби безпеки України, Головного управління розвідки Міністерства оборони України, Управління державної охорони.

Наступну групу складає інформація щодо заходів по охороні різного роду режимних об'єктів, осіб та матеріальних цінностей, які взято під державну охорону. До неї, зокрема, належать відомості:

- про технічні системи забезпечення діяльності, охорони, зв'язку, зміст заходів пропускнуго і внутрішньооб'єктового режиму об'єкта СБУ, Управління державної охорони та Прикордонних військ, на якому впроваджено особливий режим;
- про організацію, стан і способи охорони установ кримінально-виконавчої системи;
- про заходи щодо охорони органів державної влади, осіб та об'єктів, щодо яких здійснюється державна охорона;
- про організацію та порядок забезпечення безпеки пересування територією України вищих посадових осіб України та урядових делегацій іноземних держав;
- про строки, маршрути та організацію охорони перевезення баннот і монет та інших цінностей у системі Національного банку України.

До останньої групи можна віднести інформацію щодо безпосереднього здійснення заходів по захисту інформації та державної таємниці. Зокрема, це відомості:

- про забезпечення безпеки систем урядового та спеціального зв'язку, про зміст заходів щодо комплексного технічного захисту інформації у цих системах від технічних засобів розвідки;
- про організацію та фактичний стан охорони державної таємниці тощо.

Слід зазначити, що рівень таємності відомостей, внесених до ЗВДТ, як правило, залежить не лише від змісту цих відомостей, а й від конкретного об'єкта, інформацію щодо якого ці відомості розкривають. Так, наприклад, відомості про зміст оперативних планів щодо Збройних сил України носять гриф «особливої важливості» і мають строк секретності 30 років, щодо корпусу – «цілком таємно» зі строком секретності 10

років, а щодо дивізії — «таємно» зі строком секретності 5 років.

Але, на нашу думку, існуюча в ЗВДТ класифікація інформації, що є державною таємницею, лише за чотирма сферами є недостатньою. Виходячи зі зробленого нами вище аналізу, постає необхідність запровадження додаткової класифікації в рамках ЗВДТ, що сприяло б більш ефективному і раціональному виконанню законодавства про державну таємницю.

Також є доцільним визначення кола державних органів, до компетенції яких входить розпорядження (передача, допуск) тим чи іншим видом відомостей, що становлять державну таємницю, як це, наприклад, має місце у відповідних нормативно-правових актах Росії¹. Це допомогло б упорядкувати процеси допуску до секретної інформації, визначило органи, що відповідають за надання того чи іншого виду секретної інформації тощо.

До того ж державну таємницю можуть також становити відомості, які не перелічено у ЗВДТ. Маються на увазі випадки міжнародної передачі секретної інформації. Так, згідно зі ст. 3 Закону «Про державну таємницю», передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим законом. Крім того, міжнародним договором України можуть встановлюватися інші, ніж передбачені національним законодавством, правила охорони таємниці іноземної держави чи міжнародної організації.

Режим секретної інформації в даному разі визначається конкретним міжнародним договором, і відповідно ці режими відрізняються, залежно від країни чи міжнародної організації, від якої надійшла інформація, що охороняється. Тобто можливе застосування правових режимів захисту інформації інших, ніж ті, що передбачені національним законодавством.

Можна сказати, що навіть самі визначення таємної інформації при цьому відрізняються. Так, згідно з угодою між Україною і Французькою Республікою (ст. 1)² застосовуються терміни «таємна інформація та матеріали», під якими розуміється інформація та матеріали будь-якого ха-

¹ Указ Президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. № 1203 // Собрание законодательства РФ, 1995, № 49, ст. 4775 (В редакции Указа от 24.01.98 № 61).

² Угода між Урядом України та Урядом Французької Республіки про взаємну охорону таємної інформації та матеріалів від 7 грудня 1999 року. (Схвалено і подано на ратифікацію Постановою Кабінету Міністрів № 468 від 06.05.2001).

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

рактеру, яким був присвоєний ступінь секретності, зазначений у цій угоді, і які в інтересах національної безпеки відповідно до національного законодавства сторін підлягають охороні від одного з таких випадків:

- компрометації, знищення, нецільового використання, викрадення, розголошення або втрати таємної інформації та матеріалів;
- доступу до такої таємної інформації та матеріалів будь-якої особи, що не має допуску.

Причому, на відміну від українського законодавства в цій сфері, яке оперує поняттям «відомості, що становлять державну таємницю», згідно з цією угодою окремо розглядаються такі поняття, як «таємна інформація», що визначається як «будь-яка інформація, зміст якої є таємним, незалежно від форми, в якій вона подана, та способу її передачі»; та поняття «таємні матеріали», що визначені як «будь-які носії інформації, незалежно від їх виду, зокрема, будь-який документ або виріб, на/в яких таємна інформація записана чи розміщена, не порушуючи їх фізичних ознак». Таким чином, даною угодою регулюється не лише правовий режим самої таємної інформації, а й окремо режим фізичних носіїв цієї інформації.

А от, наприклад, згідно з відповідною угодою між Україною та Німеччиною, поняття таємної інформації розглядається в комплексі і зазначається (ст. 1), що: «Таємною інформацією у розумінні цієї Угоди є факти, об'єкти або відомості незалежно від форми їх представлення, які в державних інтересах підлягають збереженню в таємниці. Зокрема, це інформація у будь-якій формі, а також будь-які документи, вироби, речовини або фізичні поля, на/в яких інформація міститься або може бути записана, і які в інтересах національної безпеки Сторін, згідно з їх чинним законодавством, підлягають захисту від несанкціонованого доступу і засекречені відповідним чином. Таємній інформації державним органом або за його розпорядженням надається ступінь секретності, що відповідає необхідному рівню захисту. Сюди також включається таємна інформація, створена організаціями сторін у рамках співробітництва та засекречена на основі чинного законодавства сторін та відповідно до критеріїв цієї Угоди».¹³

Щодо визначення режиму захисту таємної інформації, то тут можна визначити два основні підходи. Згідно з першим з них, міжнарод-

¹³ Угода між Кабінетом Міністрів України та Урядом Федеративної Республіки Німеччини про взаємний захист таємної інформації від 29 травня 1998 р. (Затверджено Постановою Кабінету Міністрів України № 1433 від 14.09.98).

ною угодою запроваджується класифікація таємної інформації, згідно з якою інформація з певним грифом таємності однієї сторони відповідає певному грифу таємності іншої сторони, і сторони угоди забезпечують стосовно такої таємної інформації щонайменше такий самий захист, який передбачається при поводженні з власною таємною інформацією з відповідним ступенем секретності.

Другий підхід полягає в запровадженні на території однієї держави специфічного режиму захисту інформації, який застосовується щодо отриманої інформації іншою державою, з якої цю інформацію було отримано.

Наприклад, у згаданій нами угоді між Україною та Німеччиною застосовуються обидва підходи. Так, згідно із ст. 2 цієї угоди, запроваджено зіставлення режимів таємної інформації. Українському грифу «цілком таємно» відповідає німецький гриф *GEHEIM*, а грифу «таємно» – *VS-VERTRAULICH*. Одночасно в Україні щодо таємної інформації, отриманої з Німеччини, яка носить гриф «*VS-NUR FUR DEN DIENSTGEBRAUCH*» (*VS-NfD*), застосовується специфічний режим, який встановлено додатком до цієї угоди.

Зокрема, основними характеристиками режиму секретності щодо цієї інформації є те, що доступ до таємної інформації з грифом *VS-NfD* дозволяється надавати тільки особам, для яких він необхідний (принцип: знання тільки тоді, коли воно необхідне). Зміст таємної інформації з грифом *VS-NfD* повинен зберігатися в таємниці. Ця інформація зберігається у замкнених приміщеннях, шафах або столах, її передача здійснюється кур'єром або надісланням у запечатаній упаковці. Якщо така інформація обробляється або передається далі за допомогою інформаційної техніки, вона обов'язково повинна бути зашифрованою. Всі фізичні та юридичні особи, яким передається така інформація, повинні бути ознайомлені з додатком, що регулює правила поводження з цією інформацією.

Враховуючи значне розширення міжнародного співробітництва України, в тому числі в сферах оборони, боротьби зі злочинністю, військово-технічного співробітництва, питання міжнародно-правового регулювання захисту таємної інформації набуватимуть дедалі більшого значення. У зв'язку з тим, можливо, доцільним було б створення національного переліку, в якому б консолідувалися окремі режими захисту таємної інформації, що встановлюється міжнародно-правовими актами.

Ще одним аспектом, на який варто звернути увагу, є те, що останніми роками було зроблено ряд змін у національному законодавстві з

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

метою впорядкування та попередження зловживань у засекреченні інформації.

Так, згідно з нормами ст. 8 Закону «Про державну таємницю», належить до державної таємниці інформація:

- про стан довкілля, про якість харчових продуктів і предметів побуту;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- 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 порушень прав і свобод людини і громадянина;
- про незаконні дії органів державної влади, органів місцевого самоврядування та їхніх посадових осіб;
- інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких дана Верховною Радою України, не може бути засекречена.¹

Також було посилено відповідальність посадових осіб, до компетенції яких входить встановлення, скасування та підтримання режиму секретності. Так, в 1999 р. Кодекс про адміністративні правопорушення було доповнено статтею 212-2 «Порушення законодавства про державну таємницю», яка передбачає відповідальність за засекречення інформації, яка, згідно із Законом «Про державну таємницю», не може бути засекречена, за безпідставне засекречення інформації, порушення порядку засекречення та розсекречення інформації, допуску до такої інформації, режиму секретності та недодержання правил її захисту. Було внесено відповідні зміни до інших статей КпАП.²

¹ Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-ХІІ // Відомості Верховної Ради України, 1994. – № 16. – Ст. 93. (В редакції Закону № 1079-ХІV від 21.09.99)

² Закон України «Про внесення змін до Кодексу України про адміністративні правопорушення щодо встановлення відповідальності за порушення законодавства про державну таємницю» від 21 вересня 1999 року № 1080-ХІV // Відомості Верховної Ради України, 1999. – № 49. – Ст. 429.

§ 4 Таємниця приватного життя

Інформація, що становить державну таємницю, є лише однією зі складових інформації з обмеженим доступом. У національному законодавстві існує ще ціла група правових норм, якими встановлюються обмеження щодо тих або інших видів інформації. Але ця інформація, згідно із ст. 30 Закону «Про інформацію», вже має назву не таємної, а конфіденційної. На відміну від питань захисту таємної інформації, в якій було застосовано правові напрацювання ще радянських часів, правове регулювання захисту конфіденційної інформації в Україні розвинуте слабко і перебуває ще на початкових стадіях формування.

Так, наприклад, в українському законодавстві немає єдиного законодавчого акта, який би систематизував та визначав перелік інформації, яка є конфіденційною. На сьогоднішній день окремі питання обмеження щодо обігу і розповсюдження конфіденційної інформації регулюються нормами Конституції України і багатьох галузей та інститутів права.

Спробу класифікації конфіденційної інформації було зроблено в Російській Федерації, коли указом президента було затверджено перелік відомостей «конфіденційного характеру», в якому було шість видів інформації:

1) персональні дані – відомості про факти, випадки та обставини приватного життя громадянина, що дозволяють розшифрувати його особу, за винятком відомостей, які підлягають розповсюдженню в засобах масової інформації у випадках, передбачених законами;

2) таємниця слідства і судочинства;

3) службова таємниця – службові відомості, доступ до яких обмежено органами державної влади відповідно до Цивільного кодексу та законів;

4) професійна таємниця – відомості, пов'язані з професійною діяльністю, доступ до яких обмежено відповідно до Конституції і законів (лікарська, нотаріальна, адвокатська таємниця, таємниця листування, телефонних переговорів, поштових відправлень, телеграфних та інших повідомлень тощо);

5) комерційна таємниця – відомості, пов'язані з комерційною діяльністю, доступ до яких обмежено відповідно до Цивільного кодексу та законів;

б) відомості про сутність винаходу, корисної моделі або промислового зразка до офіційної публікації інформації про них.¹

Звісно, таку класифікацію не можна вважати досконалою. І насамперед тому, що не досить зрозуміло, на основі чого вона здійснювалася. Так, наприклад, у Росії таємниця листування, телефонних розмов, поштових, телеграфних та інших відправлень встановлюється п. 2 ст. 17 Конституції РФ² як невід'ємне право людини і громадянина. Тобто вона не може розглядатися як суто професійна таємниця працівників систем зв'язку. В той же час такі види таємниць, як адвокатська, лікарська тощо, встановлюються відповідними законодавчими актами, що регламентують той чи інший вид діяльності. Більше того, п. 1 тієї ж ст. 17 Конституції РФ встановлюється право на недоторканність приватного життя, особисту та сімейну таємницю. Таким чином, таємниця листування пов'язана насамперед із захистом особистих даних, а вже потім із виконанням певного роду діяльності щодо надання послуг зв'язку.

Але головне, що прийняття такого акта свідчить про актуальність запровадження класифікації конфіденційної інформації в єдиному нормативно-правовому акті, що дає можливість ефективного застосування її правового захисту.

Як ми вже зазначали, характеризуючи правове регулювання обігу інформації, в основу класифікації має бути покладений насамперед метод правового регулювання, а також специфіка правових норм — природних чи позитивних, на яких ґрунтується те чи інше обмеження обігу інформації.

Перша група такої класифікації, на нашу думку, має бути пов'язана із виконанням державою та її органами своїх конституційних обов'язків (відповідно до ст. 3 Конституції України) щодо забезпечення прав людини. Цей вид конфіденційної інформації можна визначити як **таємницю приватного життя**, яка складається з конфіденційної інформації про особу (ст. 32 Конституції України), таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31 Конституції України).

Основні правові засади забезпечення інформаційних прав і свобод людини та захисту особистої інформації було докладно розглянуто в

¹ Див.: Указ Президента Российской Федерации «Об утверждении сведений конфиденциального характера» от 6 марта 1997 г. № 188.

² Конституції нових держав Європи та Азії / Упоряд. С. Головатий. — К.: Українська правничка фундація. Видавництво «Право», 1996. — С. 405 — 445.

розділі, присвяченому інформаційній безпеці людини та суспільства. Ми зупинимось лише на деяких аспектах, пов'язаних безпосередньо із захистом відповідної інформації, яка обробляється в процесі діяльності органів державної влади та місцевого самоврядування. Насамперед це стосується збирання, обробки та зберігання персональних даних. На жаль, на сьогоднішній день це питання в Україні залишається на рівні конституційної декларації, оскільки спеціальні нормативно-правові акти, які б регламентували подібну діяльність, відсутні.

Законом «Про інформацію»¹ (ст. 23) визначено, що інформація про особу являє собою сукупність документованих або публічно оголошених відомостей про особу. Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

Серед правових гарантій конфіденційності інформації про особу, встановлених Законом «Про інформацію» (ст. 23), можна назвати такі:

- забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом;
- кожна особа має право на ознайомлення з інформацією, зібраною про неї;
- інформація про особу охороняється законом.

Велике значення для правового регулювання захисту особистих даних має рішення Конституційного суду України у «справі К.Г. Устименка»², яким, зокрема, конкретизується тлумачення правових гарантій ст. 23 Закону «Про інформацію». Так, згідно з рішенням Конституційного суду, частину четверту статті 23 Закону України «Про інформацію» треба розуміти так, що забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини.

Крім того, цим рішенням розширюється і конкретизується перелік персональних даних. Згідно із ст. 23 Закону «Про інформацію», основними даними про особу (персональними даними) є: національність,

¹ Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України, 1992. – № 48. – Ст. 650.

² Рішення Конституційного суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) № 5-зп від 30 жовтня 1997 року.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Конституційний же суд визначає, що до конфіденційної інформації, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані). Важливим є те, що, на відміну від Закону «Про інформацію», перелік персональних даних, згідно з рішенням Конституційного суду, не є вичерпним, підкреслюючи можливість віднесення до конфіденційної інформації й інших персональних даних. Тим самим створюються широкі можливості для розвитку відповідного законодавства та підвищення ефективності захисту таємниці приватного життя.

На відміну від України, інститут захисту особистих даних набув розвитку в багатьох країнах світу. Багато країн вже давно прийняли закони в галузі захисту прав суб'єктів персональних даних і створили на їх основі незалежні від уряду державні органи по захисту таких прав. Ці органи, як правило, колегіальні, зазвичай мають назви Комісії по захисту даних. Вперше такий орган було запроваджено в 1919 р. у Швеції, їй почали слідувати інші країни. На сьогодні такі органи діють в Австралії, Австрії, Англії, Бельгії, Болгарії, Греції, Ізраїлі, Іспанії, Канаді, Кіпрі, Гаяні, Маврикії, Нідерландах, Угорщині, Філіппінах, Фінляндії, Франції, ФРН, Швейцарії, Японії тощо.¹

Значну увагу захисту персональних даних приділено і світовим співтовариством. Так, одним з основних міжнародно-правових стандартів у цій галузі вважається прийнята в рамках Ради Європи Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру².

Зокрема, згідно з цією конвенцією (ст. 2), «дані особистого характеру» означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною («суб'єкт даних»). А «автоматизована обробка» включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних і/або арифметичних операцій з цими даними, змінення, знищення, вибірка або поширення даних.

¹ Копылов В.А. Информационное право. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – С. 394.

² Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 року.

Нормами ст. 5 конвенції встановлюються основні принципи автоматизованої обробки персональних даних, згідно з якими дані особистого характеру, що піддаються автоматизованій обробці:

- отримуються та обробляються сумлінно і законно;
- зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями;
- мають бути адекватними, відповідними і ненадмірними з точки зору цілей, заради яких вони зберігаються;
- мають бути точними та у разі необхідності мають поновлюватися;
- зберігаються у форматі, який дозволяє ідентифікувати суб'єктів даних не довше, ніж це потрібно для мети, заради якої такі дані зберігаються.

У випадках, якщо внутрішнє право не забезпечує відповідних гарантій, забороняється піддавати автоматизованій обробці дані особистого характеру, що свідчать про расову приналежність, політичні або релігійні чи інші переконання, а також дані особистого характеру, що стосуються здоров'я або статевого життя, а також дані особистого характеру, що стосуються засудження у кримінальному порядку (ст. 6 конвенції).

Також передбачається, що для захисту даних особистого характеру, які зберігаються у файлах даних для автоматизованої обробки, вживаються відповідні заходи захисту, спрямовані на запобігання випадковому чи несанкціонованому знищенню або випадковій втраті, а також на запобігання несанкціонованому доступу, змінненню або поширенню (ст. 7 конвенції).

Також у конвенції приділяється увага питанню регулювання транскордонних потоків даних особистого характеру та застосування національним законодавством обмежень щодо таких передач даних. Зокрема, забороняється лише з метою захисту недоторканності особистого життя забороняти або зумовлювати спеціальними дозволами транскордонні потоки даних особистого характеру на територію іншої держави – учасниці конвенції, крім випадків, прямо передбачених національним законодавством.

Причини особливої уваги саме автоматизованій обробці персональних даних полягають у тому, що будь-яка автоматизована система обробляє дані «без будь-якого розуміння того, що ці дані собою являють».¹ Таким чином, автоматизована система сама по собі не може виз-

¹ Гостев И.М. Информационное право в России. // Конфидент, 2000. – № 1-2, январь – апрель. – С.17.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

начати законність або незаконність своїх дій і одночасно здатна здійснювати величезну кількість операцій щодо обробки великого масиву даних. Це робить таку автоматизовану систему дуже потужним інструментом, протиправне використання якого може призвести до небезпечних наслідків.

Ще одним аспектом державної діяльності щодо захисту особистої інформації є забезпечення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції. Окрім конституційних гарантій, відповідні норми включено і до галузевого законодавства.

Так, Закон «Про зв'язок»¹ встановлює загальний термін «охорони таємниці інформації, що передається каналами зв'язку», створюючи і підкреслюючи однорідність правових відносин щодо захисту такої інформації незалежно від способу її передачі або форми власності підприємства, що надає послуги зв'язку. Стаття 27 Закону «Про зв'язок» встановлює конкретні правові гарантії захисту цієї таємниці. Зокрема, передбачено обов'язок підприємств зв'язку всіх форм власності вживати організаційно-технічних заходів щодо захисту інформації. Забороняється, крім випадків, передбачених чинним законодавством, виймання і огляд поштової кореспонденції та документальних повідомлень, одержання необхідних довідок про них, здійснення контролю за технічними каналами зв'язку, в тому числі прослуховування телефонних розмов на підприємствах зв'язку всіх форм власності. Підприємства і об'єднання зв'язку мають право вилучати у встановленому порядку заборонені до пересилання вкладання у поштові відправлення (зброя, отруйні, легкозаймисті речовини тощо) тільки у присутності відправника.

Безпосередньо порядок здійснення передачі інформації каналами зв'язку, її захисту від розголошення або перекручення регламентується підзаконними нормативно-правовими актами.

Підсумовуючи аналіз правового регулювання захисту інформації щодо приватного життя, слід ще раз наголосити на наявності значних прогалин у правовому регулюванні і слабкому розвитку механізмів правозастосування.

¹ Закон України «Про зв'язок» від 16 травня 1995 року № 160/95-ВР // Відомості Верховної Ради України, 1995. – № 20. – Ст.143.

§ 5 Обмеження доступу до інформації в інтересах слідства та судочинства

У згаданій нами класифікації конфіденційної інформації окремим різновидом такої інформації називається «таємниця слідства і судочинства». Однак, на нашу думку, ці два поняття слід чітко розрізняти з огляду на їхні специфічні відмінності. Крім того, з точки зору українського законодавства, як саме визначення, так і класифікація взагалі викликає багато запитань.

По-перше, сама назва «таємниця судочинства» є досить суперечливою. Згідно із ст. 129 Конституції України, однією з головних засад судочинства є «гласність судового процесу та його повне фіксування технічними засобами»¹. Вимоги гласності судового процесу ставляться також всіма міжнародно-правовими актами з прав людини і є однією з важливих гарантій цих прав. Таким чином будь-які згадки про «таємницю судочинства» є абсолютно некоректними як з точки зору букви, так і духу закону.

Те обмеження доступу до інформації, яке мається на увазі, визначається трохи по-іншому. Так, наприклад, згідно із ст. 10 Конвенції про захист прав і основних свобод людини 1950 року, передбачається встановлення законодавчого обмеження доступу до інформації, яке необхідне «для підтримання авторитету і неупередженості правосуддя»².

Основним міжнародно-правовим актом, що встановлює стандарти діяльності судових органів та закріплює цей вид таємної інформації, є «Основні принципи незалежності судових органів», які було схвалено ООН³. Згідно з цими принципами (п. 15), судді зобов'язані зберігати професійну таємницю щодо своєї роботи та конфіденційної інформації, отриманої в ході виконання ними своїх обов'язків, за винятком відкритих судових розглядів, і їх не можна примушувати давати свідчення з таких питань.

Таке положення має на меті одразу два завдання. По-перше, це забезпечення незалежності і виключення впливу на судові органи при

¹ Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України, 1996. – №30 – Ст. 141.

² Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4.XI.1950) / «European Treaty Series» – № 5.

³ Основні принципи незалежності судових органів. Схвалені резолюціями 40/32 та 40/146 Генеральної Асамблеї ООН від 29 листопада та 13 грудня 1985 р.

прийнятті ними рішень. А по-друге, забезпечується захист інформації особистого характеру, що може стати відомою під час проведення судового розгляду справи.

Одразу слід зазначити, що цей вид конфіденційної інформації розглядається саме як «професійна таємниця» судді.

Але знову ж таки, визначення «професійна таємниця» не зовсім відповідає нормам Конституції України. Адже, згідно з нормами ст. 127 Конституції, правосуддя здійснюють професійні судді та у визначених законом випадках народні засідателі і присяжні. Таким чином, подібний обов'язок поширюється не лише на осіб, які є професійними суддями. Але для чіткого визначення даного поняття потрібно насамперед розібратися у його конкретному змісті.

В українському законодавстві існує цілий ряд процесуальних норм, якими регулюється питання конфіденційності інформації з метою неупередженості судочинства.

Так, ст. 321 Кримінально-процесуального кодексу України¹ встановлюється «таємниця наради суддів». Згідно з нормами цієї статті, вирок виноситься в окремому приміщенні – нарадчій кімнаті. Під час наради і постанови вироку у нарадчій кімнаті можуть бути лише судді, що входять до складу суду по даній справі. Присутність у нарадчій кімнаті запасних суддів або секретаря судового засідання та інших осіб не допускається. З настанням нічного часу суд вправі перервати нараду для відпочинку.

Важливою є також вимога, згідно з якою судді не мають права розголошувати судження, висловлені у нарадчій кімнаті.

Аналогічні вимоги містяться і у Цивільному процесуальному кодексі України², згідно із ст. 210 якого також встановлюється «таємниця нарадчої кімнати». Її зміст, згідно з нормами вказаної статті, полягає в тому, що при винесенні судового рішення ніхто не має права бути присутнім у нарадчій кімнаті, крім складу суду в даній справі. Також встановлюється, що судді не мають права розголошувати міркувань, що були висловлені в нарадчій кімнаті.

На відміну від норм кримінально-процесуального та цивільного процесуального права, у господарському процесі таємниці наради

¹ Кримінально-процесуальний кодекс України (зі змінами і доповненнями станом на 15 вересня 2001 р.) – Харків. – 2001.

² Цивільний процесуальний кодекс України (станом на 1 серпня 2001 р.) – Харків. – 2001.

суддів не встановлено. Більше того, згідно з ч. 3 ст. 82 Господарського процесуального кодексу України¹, у разі розгляду справи трьома судьями суддя, не згодний з рішенням, зобов'язаний викласти у письмовій формі свою окрему думку, що долучається до справи. Таким чином, існує явна невідповідність принципам вищезгаданих міжнародно-правових актів.

Звісно, ситуація має своє логічне пояснення, оскільки господарсько-процесуальне законодавство значною мірою залишилося незмінним з часів, коли цей вид діяльності був арбітражем, а не судочинством. Але так чи інакше варто підкреслити існуючі відмінності щодо захисту конфіденційної інформації між галузями процесуального права.

Таким чином, на нашу думку, слід користуватися саме поняттям «таємниця наради суддів», тим самим чітко відмежовуючи його від принципу гласності правосуддя. Це поняття є унікальним за своїм змістом і повинно класифікуватися окремо. По-перше, воно значно відрізняється від загальних ознак режиму доступу до інформації. В даному випадку не існує порядку засекречення та розсекречення відомостей, вимог щодо порядку їх зберігання, передачі, допуску тощо. По-друге, вимога щодо конфіденційності інформації є абсолютною. Існують дві абсолютно визначені законодавством вимоги.

1. Ніхто, крім суддів, що ведуть дану справу, не може бути присутнім у нарадчій кімнаті під час наради і винесення вироку або рішення. Це означає, що жоден орган або посадова особа за будь-яких міркувань не може надати допуску для присутності при здійсненні цієї процесуальної дії. Навіть ті посадові особи, які за своєю посадою мають допуск до інформації будь-якого ступеня секретності.

2. Будь-які міркування або судження, висловлені судьями в нарадчій кімнаті, не можуть бути розголошені. Знову ж таки відомості про це є таємними без будь-якого додаткового рішення про їх засекречення і до того ж не мають терміну засекречення. Вони просто не повинні ніколи розголошуватися.

Єдиною інформацією, яка оприлюднюється за результатами наради суддів, є рішення, постанова, ухвала або вирок суду.

Можливо, доцільним було б включення до Закону «Про державну таємницю» норм, які б регулювали питання таємниці наради суддів і визначали її як специфічний вид державної таємниці.

¹ Господарський процесуальний кодекс України (станом на 1 серпня 2001 р.) – Харків. – 2001.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

Крім того, ще одним випадком обмеження доступу до інформації є призначення закритого судового слухання. Так, згідно із ст. 20 КПК України, розгляд справ у всіх судах відкритий, за винятком випадків, коли це суперечить інтересам охорони державної таємниці. Згідно із ЗВДТ¹ (пункт 4.46) відомості про зміст кримінальних справ, розголошення яких може завдати шкоди національній безпеці України, мають гриф «таємно» зі строком засекречення до 5 років.

Крім того, закритий судовий розгляд допускається за мотивованою ухвалою суду:

- у справах про злочини осіб, які не досягли шістнадцятирічного віку;
- у справах про статеві злочини;
- в інших справах з метою запобігання розголошенню відомостей про інтимні сторони життя осіб, які беруть участь у справі;
- в інших справах коли цього потребують інтереси безпеки осіб, взятих під захист.

Але вироки судів у всіх випадках виголошуються публічно.

Таким чином, у першому випадку питання призначення закритого розгляду регулюється законодавством про державну таємницю і в безумовному порядку, а в наступних — кримінально-процесуальним законодавством на основі міркувань суду.

На відміну від кримінального законодавства, цивільне і господарське трохи інакше тлумачать принцип гласності судочинства, надаючи учасникам процесу широкі права щодо відходу від названого принципу з метою захисту особистої або конфіденційної інформації.

Так, ст. 10 Цивільно-процесуального кодексу України визначає, що розгляд справ у всіх судах відкритий, за винятком випадків, коли це суперечить інтересам охорони державної таємниці.

Крім того, закритий судовий розгляд може призначатися за мотивованою ухвалою суду з метою:

- запобігання розголошенню відомостей про інтимні сторони життя осіб, які беруть участь у справі;
- забезпечення таємниці усиновлення.

У таких випадках до залу засідань допускаються лише особи, які беруть участь у справі, а також у разі необхідності свідки, експерти та перекладачі. Більше того, у справах про усиновлення дозволяється не оголошувати прилюдно рішення суду.

¹ Наказ Голови Служби безпеки України «Про затвердження Зводу відомостей, що становлять державну таємницю» від 1 березня 2001 р. № 52.

Окреме положення стосується того, що не допускаються громадяни молодші 16 років, які не беруть участі у справі або не є свідками.

Знову ж таки ми повинні констатувати наявність зовсім інших критеріїв гласності розгляду справ у господарському процесі. Так, згідно із ст. 4-4 Господарського процесуального кодексу України, розгляд справ у господарських судах відкритий, за винятком випадків, коли це суперечить вимогам щодо охорони державної, комерційної або банківської таємниці, або коли сторони чи одна із сторін обгрунтовано вимагають конфіденційного розгляду справи і подають відповідне клопотання до початку розгляду справи по суті. Про розгляд справи у закритому засіданні або про відхилення клопотання з цього приводу виноситься ухвала.

Таким чином, господарське процесуальне законодавство надає значно більше підстав для обмеження розповсюдження інформації щодо суті справи, в тому числі крім прямо зазначених у законі випадків, передбачає наявність і інших причин, які оцінюються на розсуд суду.

Дещо інакшою є ситуація з іншим типом конфіденційної інформації, що об'єднана в даному пункті класифікації – таємницею слідства.

Так, згідно з нормами ст. 52-3 Кримінально-процесуального кодексу України встановлено вимогу щодо нерозголошення відомостей про особу, щодо якої здійснюються заходи безпеки.

Нерозголошення відомостей про особу, взяту під захист, може забезпечуватися шляхом обмеження відомостей про неї в матеріалах перевірки (заявах, поясненнях тощо), а також протоколах слідчих дій та судових засідань. Орган дізнання, слідчий, прокурор, суд (суддя), прийнявши рішення про застосування заходів безпеки, виносить мотивовану постанову, ухвалу про заміну прізвища, імені, по батькові особи, взятої під захист, на псевдонім. Надалі у процесуальних документах зазначається лише псевдонім.

У випадку застосування подібних заходів безпеки заборонено розголошувати особисту інформацію, за допомогою якої можна ідентифікувати особу, щодо якої застосовано заходи безпеки. Згідно з ч. 1 ст. 52-3 КПК, до такої інформації віднесено:

- справжнє прізвище, ім'я, по батькові,
- рік, місяць і місце народження,
- сімейний стан,
- місце роботи,
- рід занять або посада,
- місце проживання,

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

- інші анкетні дані, що містять інформацію про особу, яка перебуває під захистом.

Зазначені дані вказуються лише у постанові (ухвалі) про заміну анкетних даних. Ця постанова (ухвала) до матеріалів справи не долучається, а зберігається окремо в органі, у провадженні якого перебуває кримінальна справа. У разі заміни прізвища особи, взятої під захист, на псевдонім з матеріалів справи вилучаються протоколи слідчих дій та інші документи, в яких зазначено достовірні відомості про цю особу, і зберігаються окремо, а до матеріалів справи додаються копії цих документів із заміною справжнього прізвища на псевдонім.

Частиною 2 ст. 52-3 КПК встановлюється, що відомості про заходи безпеки та осіб, взятих під захист, є інформацією з обмеженим доступом. На документи, що містять таку інформацію, не поширюються норми щодо процесуальних прав захисника (ч. 2 ст. 48 КПК), ознайомлення деяких учасників процесу з матеріалами справи (ст. 217 – 219) і забезпечення права на ознайомлення з матеріалами справи (ст. 255).

Разом з тим щодо подібної інформації в українському законодавстві існують деякі розбіжності. Так, ст. 52-3 КПК визначає цю інформацію як інформацію з обмеженим доступом. В той же час цю інформацію включено до Зводу відомостей, що становлять державну таємницю (ЗВДТ). Так, згідно з пунктом 4.31 ЗВДТ відомості про осіб, які беруть участь у кримінальному судочинстві і взяті під захист згідно з чинним законодавством України, носять гриф «цілком таємно» зі строком засекречення 10 років¹. Таким чином, варто конкретизувати положення названої статті КПК з віднесенням відомостей про заходи безпеки та осіб, взятих під захист, до державної таємниці.

Статтею 121 КПК України встановлюється недопустимість розголошення даних досудового слідства.

Зокрема, передбачено, що дані досудового слідства можуть бути оприлюднені тільки з дозволу слідчого або прокурора і в тому обсягу, в якому вони визнають можливим.

В окремих випадках слідчий попереджає свідків, потерпілого, цивільного позивача, захисника, експерта, фахівця, перекладача, понятих, а також інших осіб, присутніх при вчиненні слідчих дій, про обов'язок не розголошувати без його дозволу даних досудового слідства. Винні в розголошенні даних досудового слідства несуть кримінальну відповідальність за статтею 387 КК України.

¹ Наказ Голови Служби безпеки України «Про затвердження Зводу відомостей, що становлять державну таємницю» від 1 березня 2001 р. № 52.

Також слід зазначити, що у випадках, коли розголошення може завдати шкоди національній безпеці України, на дані досудового слідства відповідно до п. 4.46 ЗВДТ поширюються вимоги Закону «Про державну таємницю». Це питання ніяк не врегульоване КПК, хоча при цьому виникають розбіжності в питаннях оприлюднення даних слідства між КПК та Законом «Про державну таємницю».

§ 6 Службова таємниця

Наступний вид конфіденційної інформації охоплює широке коло відомостей, що збираються, обробляються, зберігаються в процесі діяльності органів державної влади та місцевого самоврядування, інших державних установ і організацій. Ще з радянських часів така інформація мала гриф «для службового користування» (ДСК), який використовувався практично безконтрольно.

Цю традицію, на жаль, наслідувала й Україна після проголошення незалежності. Парадоксальність сучасної ситуації в Україні полягає в тому, що існують величезні масиви інформації, режим якої визначається названим грифом, але на законодавчому рівні навіть не існує загального визначення подібної інформації, яку часто називають конфіденційною інформацією, що є власністю держави. Не кажучи вже про чіткі правила віднесення інформації до категорії «для службового користування» або перелік посадових осіб, які мають право встановлювати відповідний гриф.

У вже згаданій нами російській класифікації режим інформації, що становить службову таємницю, чомусь визначається на основі Цивільного кодексу і прив'язується безпосередньо до комерційного значення цієї інформації. Крім того, як це не дивно, цей нормативно-правовий акт не робить ніякої різниці між службовою таємницею і комерційною. Так, ст. 139 «Службова і комерційна таємниця» Цивільного кодексу Російської Федерації визначає: «Інформація становить службову або комерційну таємницю у випадку, коли інформація має дійсну або потенційну комерційну цінність через незнання її третіми особами, до неї немає вільного доступу на законних підставах і власник цієї інформації застосовує заходи до охорони її конфіденційності. Відомості, що не можуть становити службову або комерційну таємницю, визначаються законом або іншими правовими актами.

Інформація, що становить службову або комерційну таємницю, захищається способами, визначеними цим кодексом та іншими законами»¹.

Першим спірним питанням є взагалі доцільність регулювання питання про службову таємницю цивільним законодавством. Адже, повертаючись до наших міркувань про метод правового регулювання обігу інформації, ми можемо чітко сказати, що, на відміну від комерційної таємниці, в основі регулювання обігу якої диспозитивний метод правового регулювання, обіг інформації, що становить службову таємницю, регулюється імперативно на основі різного роду нормативно-правових актів, службових інструкцій тощо.

Так, згідно з відповідною інструкцією Кабінету Міністрів України, «переліки конфіденційної інформації, що є власністю держави і якій надається гриф обмеження доступу «для службового користування», розробляються і вводяться в дію міністерствами, іншими центральними органами виконавчої влади, Радою Міністрів Автономної Республіки Крим, обласними, Київською і Севастопольською міськими державними адміністраціями, в яких утворюються або у володінні, користуванні чи розпорядженні яких перебувають ці відомості»².

Крім того, в українському законодавстві застосовується поняття «державні інформаційні ресурси», які визначаються як «інформація, яка є власністю держави та (або) необхідність захисту якої визначено законодавством»³.

Таким чином, прямо вказуються дві ознаки інформації, що становить службову таємницю, — державна форма власності та необхідність захисту згідно з вимогами законодавства. В той же час інформація, що становить комерційну таємницю, знаходиться, як правило, у приватній власності і захищається відповідно до волі її власника.

І, нарешті, комерційна таємниця пов'язана зі здійсненням володарем цієї інформації комерційної діяльності, а службова таємниця, відповідно — із виконанням службових обов'язків. Не варто говорити, що це є два абсолютно різні види діяльності.

¹ Гражданский кодекс Российской Федерации. Часть первая. Принят 30 ноября 1994 г. № 51 — ФЗ // Собрание законодательства РФ. 1994. — № 32. — Ст. 3301.

² Постанова Кабінету Міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави» від 27 листопада 1998 р. № 1893.

³ Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України «Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах» від 24 грудня 2001 р. № 76.

Таким чином, для чіткого визначення службової таємниці (інформації для службового користування) нам насамперед потрібно визначити, які саме види діяльності слід вважати службою.

Так, згідно із ст. 1 Закону «Про державну службу»,¹ державна служба в Україні — це професійна діяльність осіб, які займають посади в державних органах та їх апараті щодо практичного виконання завдань і функцій держави та одержують заробітну плату за рахунок державних коштів. Ці особи є державними службовцями і мають відповідні службові повноваження.

Крім того, законом виділяються державні службовці зі спеціальним статусом (ст. 9), до яких належать: Президент України, Голова Верховної Ради України та його заступники, голови постійних комісій Верховної Ради України та їхні заступники, народні депутати України, Прем'єр-міністр України, члени Кабінету Міністрів України, Голова та члени Конституційного суду України, Голова та судді Верховного суду України, Вищого господарського суду, державні службовці, що працюють в апараті органів прокуратури, судів, дипломатичної служби, митного контролю, Служби безпеки, внутрішніх справ та інших. До цього переліку можна також додати військовослужбовців Збройних сил, Прикордонних військ тощо.

Іншим видом служби є муніципальна служба. Законом «Про службу в органах місцевого самоврядування»² (ст. 1) визначається, що «служба в органах місцевого самоврядування — це професійна, на постійній основі діяльність громадян України, які займають посади в органах місцевого самоврядування, що спрямована на реалізацію територіальною громадою свого права на місцеве самоврядування та окремих повноважень органів виконавчої влади, наданих законом».

На основі аналізу вищеперелічених нормативних актів ми можемо визначити ряд ознак інформації, яка становить службу таємницю.

По-перше, це конфіденційна інформація, що є власністю держави.

По-друге, одержання, використання, поширення і зберігання інформації, що становить службу таємницю, здійснюється посадовими особами, які є державними або муніципальними службовцями у зв'язку з виконанням ними своїх службових обов'язків відповідно до закону.

¹ Закон України «Про державну службу» від 16 грудня 1993 року № 3723-ХІІ // Відомості Верховної Ради України, 1993. — № 52. — Ст. 490.

² Закон України «Про службу в органах місцевого самоврядування» від 7 червня 2001 року № 2493-ІІІ.

По-третє, режим інформації, що становить службову таємницю, яким визначаються: порядок віднесення інформації до службової таємниці та її розсекречення, порядок захисту, зберігання, передачі та доступу до такої інформації, встановлюється спеціальними нормативно-правовими актами.

Враховуючи означені характеристики службової таємниці, цілком логічним і справедливим виглядає таке визначення службової таємниці:

Службова таємниця – це конфіденційна інформація, що захищається законом, яка стала відома у державних органах та органах місцевого самоврядування тільки на законних підставах і через виконання їхніми представниками службових обов'язків, а також службова інформація про діяльність державних органів, доступ до якої обмежений законом.¹

Загальні вимоги щодо захисту службової таємниці встановлено Законом «Про державну службу». Стаття 10 цього закону серед обов'язків державного службовця, зокрема, визначає «збереження державної таємниці, інформації про громадян, що стала їм відома під час виконання обов'язків державної служби, а також іншої інформації, яка згідно з законодавством не підлягає розголошенню»².

Положення Закону «Про державну службу» розкриваються також у Загальних правилах поведінки державного службовця, згідно з якими до загальних обов'язків державного службовця (п. 20) включено таке: «Державному службовцю забороняється розголошувати довірену йому державну таємницю, іншу інформацію з обмеженим доступом, установлену Законами України «Про інформацію» та «Про державну таємницю», у тому числі й після залишення ним державної служби, а також використовувати таку інформацію для власного інтересу або інтересу інших осіб шляхом порад чи рекомендацій. У той же час державний службовець не повинен приховувати від громадян факти та обставини, що становлять загрозу для життя, здоров'я і безпеки людей, крім випадків заборони розголошення відомостей, що становлять державну таємницю, вичерпний перелік яких визначений законом, а також завдавати шкоди державній інформаційній політиці, суб'єктам інформаційних відносин шляхом ухилення чи утримання від вжиття заходів

¹ Див.: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. / Под ред. акад. РАН Б.Н. Топорнина. – СПб.: «Юридический центр Пресс», 2001. – С. 554.

² Закон України «Про державну службу» від 16 грудня 1993 року № 3723-ХІІ // Відомості Верховної Ради України, 1993. – № 52. – Ст. 490.

щодо охорони державної таємниці та іншої інформації з обмеженим доступом».¹

У зазначених обов'язках державного службовця міститься важливе положення про недопущення використовувати інформацію з обмеженим доступом для власного інтересу або інтересу інших осіб шляхом порад чи рекомендацій. Тобто забороняється не лише розголошення подібної інформації, а й створення на її основі або з її використанням і розголошенням іншої інформації, яка сама по собі не несе грифа обмеження доступу, але тим чи іншим чином розкриває зміст інформації з обмеженим доступом.

Також специфічною вимогою є заборона використовувати інформацію з обмеженим доступом, що стала відомою державному службовцю у зв'язку з виконанням службових обов'язків, для власного інтересу. Причому необхідно зазначити, що ця вимога більшою мірою має етичний, ніж правовий характер, оскільки використання службової таємниці для власного інтересу може відбуватися без її розголошення. А для застосування правових обмежень необхідно встановити причинно-наслідковий зв'язок між відомою суб'єкту службовою таємницею і його діями.

Для забезпечення виконання державними службовцями такого обмеження використовується ряд обмежувально-профілактичних заходів. Це і вимога ст. 5 Закону «Про державну службу», згідно з якою державні службовці не повинні допускати дій і вчинків, які можуть зашкодити інтересам державної служби чи негативно вплинути на репутацію державного службовця. Це і обов'язкове декларування доходів державного службовця (а в деяких випадках і членів його сім'ї) при вступі на державну службу та щорічно. Це і обмеження, пов'язані з проходженням держслужби, як загальні, встановлені ст. 16 Закону «Про державну службу», так і спеціальні (на зразок заборони займатися підприємницькою діяльністю), що встановлюються іншими законодавчими актами щодо окремих категорій державних службовців.

Аналогічну вимогу щодо «збереження державної таємниці, інформації про громадян, що стала їм відома у зв'язку з виконанням службових обов'язків, а також іншої інформації, яка згідно із законом не підлягає розголошенню» містить і ст. 8 Закону «Про службу в органах місцевого самоврядування», якою встановлюються основні обов'язки посадових осіб місцевого самоврядування².

¹ Наказ Головного управління державної служби України «Про затвердження Загальних правил поведінки державного службовця» № 58 від 23 жовтня 2000 р.

² Закон України «Про службу в органах місцевого самоврядування» від 7 червня 2001 року № 2493-III // Відомості Верховної Ради України, 2001. — № 33. — Ст. 175.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

Підзаконне регулювання питань службової таємниці здійснюється переважно на галузевому рівні і є досить складним і заплутаним.

Основним нормативно-правовим актом, на основі якого здійснюється регулювання питань службової таємниці, є «Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави».¹

Цією інструкцією визначаються основні правила поведінки з носіями конфіденційної інформації, що становить службову таємницю, а саме:

- приймання і облік документів,
- розмноження і розсилання (відправлення) документів,
- формування виконаних документів у справи,
- використання документів,
- зняття грифа «для службового користування»,
- відбір документів для зберігання і знищення,
- забезпечення схоронності документів та перевірка їх наявності,
- облік, зберігання і використання печаток, штампів і бланків.

На основі цієї інструкції органами державної влади розробляються і затверджуються відомчі інструкції з питань обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, та розробляються і вводяться в дію переліки конфіденційної інформації, що є власністю держави.

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

Разом з тим ця інструкція не містить жодних критеріїв або характеристик, на основі яких інформація могла б бути визначена як конфіденційна інформація, що є власністю держави. Таким чином, переліки цієї інформації різних органів державної влади істотно відрізня-

¹ Постанова Кабінету Міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави» від 27 листопада 1998 р. № 1893.

ються.

Існують також інші підходи до забезпечення конфіденційності службової інформації. Серед органів державної влади однією з найбільш розвинутих електронних інформаційних систем володіють митні органи, зокрема, інтерес являє запроваджена в митній службі класифікація митної електронної інформації за ступенем її конфіденційності. Згідно з наказом ДМС «Про електронну інформацію в митній системі України»¹ (п. 2), було встановлено, що будь-яка митна електронна інформація, яка обробляється засобами електронної обчислювальної техніки митної установи, є інформацією з обмеженим доступом.

Ця інформація з обмеженим доступом за ступенем конфіденційності поділяється на три категорії:

А. Інформація та інформаційно-програмне забезпечення, яке не несе в собі даних, що безпосередньо визначають або обумовлюють характер митної діяльності (технічні дані обладнання, документи по роботі з персоналом, загальносистемне програмне забезпечення для передачі, обробки та збереження митної інформації, прикладне програмне забезпечення тощо).

Б. Технологічна інформація діяльності митних органів (зміст митних декларацій, провізних відомостей, протоколів порушень митних правил та контрабанди, гарантійних листів тощо) та нормативно-довідкова інформація (кадри, бухгалтерія тощо).

В. Нормативно-правова інформація суто службового призначення, інформація про зовнішньоекономічну діяльність, інформація щодо групових статистичних баз даних.

Відповідно встановлено і порядок доступу до цієї інформації, згідно з яким (п. 4.2.):

- Інформація категорії «А» готується і використовується будь-яким працівником митної установи. Згідно з вимогами авторського права та умовами дотримання права власності на програмне забезпечення, яке виробляється власними силами або купується в інших установах, вона не може поширюватись без відповідного дозволу власника інформації.

- Інформація категорії «Б» готується працівником митної установи за розпорядженням керівництва. За розпорядженням або дозволом керівника митної установи інформація цієї категорії може передаватись для використання іншим митним установам України. Передача

¹ Наказ Державного митного комітету «Про електронну інформацію в митній системі України» № 48 від 08 лютого 1996 р.

інформації категорії «Б» відомствам та установам, що не входять в митну систему України, в кожному окремому випадку погоджується з керівництвом Державної митної служби України.

• Інформація категорії «В» готується та використовується виключно персоналом, який має спеціальний дозвіл. Ця інформація повинна зберігатись у закодованому вигляді, до неї мають вживатися заходи організаційного та програмно-апаратного захисту. Вона не може бути розповсюджена без письмового дозволу керівництва Державної митної служби України.

Цей приклад ще раз підтверджує необхідність створення єдиної системи класифікації та доступу до конфіденційної службової інформації. Взагалі, на думку багатьох фахівців, інформація, що становить службу таємниці, може бути класифікована на два основні типи.

По-перше, це службова інформація про діяльність державних органів, доступ до якої обмежено законом в цілях захисту державних інтересів.

По-друге, це інформація, що підлягає охороні, яка стала відома через виконання службових обов'язків посадовим особам державних органів і органів місцевого самоврядування: комерційна, банківська таємниця, професійна таємниця, а також конфіденційна інформація про приватне життя особи.¹

Різниця в цій класифікації полягає у механізмі виникнення у державних органів права власності на таку інформацію. В першому випадку ця інформація безпосередньо створюється в процесі діяльності державних органів, і таким чином держава в їх особі стає власником цієї інформації на основі авторського права (права виробника інформації). За таких умов держава і її органи абсолютно вільні у вирішенні питань (ясна річ, відповідно до встановлених законом процедур) щодо розповсюдження цієї інформації.

У другому випадку конфіденційна інформація третіх фізичних або юридичних осіб передається у встановленому законом порядку державним органам на вимогу останніх. Державні органи, які володіють цією інформацією, вправі використовувати її у своїй діяльності, але вони обмежені щодо передачі такої інформації третім особам волею права володаря конфіденційної інформації, який передав її державним орга-

¹ Див.: Лопатин В.Н. О путях развития таможенной системы России в условиях переходного периода // Учен. зап. СПб им. В.Б. Бобкова филиала Российской таможенной академии. – 1999. – № 1 (8). – С. 5–10.

нам. Ця ситуація дуже схожа на продаж програмного забезпечення, коли покупець має право користуватися програмою, але не має права передавати або продавати її третім особам.

Хоча слід зазначити, що українське законодавство не має дієвих механізмів охорони конфіденційної інформації фізичних та юридичних осіб, переданої державним органам.

Значною вадою нормативно-правового регулювання режиму конфіденційної інформації, що є власністю держави, можна назвати і те, що на законодавчому рівні встановлено лише загальні положення щодо зберігання службової таємниці державними та муніципальними службовцями. На сьогоднішній день встановлення конкретних норм щодо службової інформації з обмеженим доступом здійснюється на підзаконному рівні міністерствами, відомствами, органами державної влади та місцевого самоврядування. Тож можна говорити практично про відсутність будь-якої систематизації в цій сфері, на відміну від сфери державної таємниці. Згадки про додержання конфіденційності інформації містяться у різних нормативно-правових актах, що регулюють діяльність тих чи інших державних органів, дуже часто без будь-яких конкретних вказівок на те, що саме мається на увазі під конфіденційною інформацією.

В той же час, на нашу думку, критично-необхідним для забезпечення інформаційної безпеки України є прийняття Закону «Про службу таємниці», одними з основних завдань якого є:

- встановлення єдиного переліку відомостей, що становлять службу таємниці, доступ до яких може бути обмежено;
- встановлення механізмів захисту конфіденційної інформації фізичних і юридичних осіб, що стала відомою державним органам при виконанні своїх функцій;
- встановлення переліку інформації державних органів, доступ до якої не може бути обмежено;
- встановлення єдиних правил обмеження доступу до службової інформації державних органів та зняття цих обмежень;
- встановлення єдиних правил допуску до такої інформації, її зберігання та передача іншим фізичним і юридичним особам.

Слід зазначити, що останнім часом в Україні зроблено певні кроки до забезпечення прозорості діяльності органів державної влади та виключення можливостей необґрунтованого обмеження права громадян на інформацію. Так, згідно з указом Президента України «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної

влади» (п. 3 ст. 2), Кабінету Міністрів України доручається «підготувати... та внести в установленому порядку пропозиції щодо вдосконалення діяльності в інформаційній сфері та проекти відповідних нормативно-правових актів, у яких, зокрема, передбачити... вичерпний перелік видів інформації, вільне збирання, зберігання, використання і поширення якої в будь-який спосіб може бути обмежено 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 та вдосконалення порядку здійснення контролю за наданням такої інформації».¹

Якщо це положення вдасться реалізувати, це сприятиме забезпеченню прав і свобод людини в Україні, підвищенню ефективності діяльності органів державної влади та досягненню відповідних завдань адміністративної реформи. Треба відзначити два основоположні принципи, на яких наголошено в даній нормі указу. По-перше, це *вичерпність переліку*, причому це потрібно зробити на законодавчому рівні, а не підзаконним актом Служби безпеки. По-друге, це поширення цього вичерпного переліку на *будь-який спосіб обмеження* свободи інформації. Тобто йдеться про закриття прогалін у законодавстві, які дають змогу, крім державної таємниці, абсолютно безконтрольно встановлювати різного роду грифи «для службового користування» і тому подібне. Це сприятиме подоланню тієї негативної інформації в сфері службової таємниці, на існуванні якої ми наголошували вище. Залишається лише сподіватися, що цей указ не спіткає доля сотень інших указів, програм, концепцій, які так і залишилися на папері.

§ 7 Комерційна таємниця

Іншим видом конфіденційної інформації є так звана «комерційна таємниця». Ми вже говорили (підрозділ 2.4.) про те, що питання захисту комерційної таємниці, по суті, не є питанням захисту інформаційної безпеки, оскільки сам по собі інститут комерційної таємниці ґрунтується не на прямих вказівках закону, а на праві власності на ті чи інші

¹ Указ Президента України «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади» від 1 серпня 2002 р. № 683/2002.

відомості. Доступ до цієї інформації означає набуття певних матеріальних благ. Таким чином, мова йде саме про захист права власності і пов'язаних з ним прав. Але, на жаль, національне законодавство не є таким однозначним в цьому питанні.

Так, згідно з ч. 1 ст. 30 Закону «Про підприємства в Україні», «під комерційною таємницею підприємства маються на увазі відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам»¹. Але це формулювання не розкриває важливого аспекту права власності на цю інформацію.. Адже певні відомості щодо виробництва можуть належати не лише підприємству, а й третім особам. Визначення цього питання є дуже важливим з ряду причин. Так, по-перше, за існуючого визначення фактично можливо оголосити будь-яку комп'ютерну програму, технологію, придбану підприємством, його комерційною таємницею, хоча насправді правом розпоряджатися цією інформацією володіють інші особи. По-друге, можна завдати шкоди інтересам підприємства і розголошенням інформації, яка тою чи іншою мірою стосується підприємства, але є власністю третіх осіб (наприклад, дослідження якості продукції цього підприємства або ставлення споживачів до неї). Чи справедливими в такому разі будуть намагання якимось чином це заборонити? Мабуть, ні.

Однією з головних характеристик, що визначає режим доступу до комерційної таємниці, є право власності на цю інформацію. По-перше, ця інформація не є власністю держави в особі органів державної влади, а належить фізичним та юридичним особам – суб'єктам підприємницької діяльності. Норми Закону «Про інформацію» прямо вказують на право власності на конфіденційну інформацію як правову основу її захисту. Так, згідно з нормами ч. 1 ст. 30 Закону «Про інформацію»², конфіденційна інформація «знаходиться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб». Таким чином, виходячи з положень ч. 4 ст. 1 Закону «Про власність»³ та ст. 86 Цивільного кодексу України⁴, конфіденційна

¹ Закон України «Про підприємства в Україні» від 27 березня 1991 року № 887-ХІІ // Відомості Верховної Ради України, 1991. – № 24. – Ст. 272.

² Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України, 1992. – № 48. – Ст. 650.

³ Закон України «Про власність» 7 лютого 1991 року № 697-12 // Відомості Верховної Ради України, 1991. – № 20. – Ст. 249.

⁴ Цивільний кодекс України (зі змінами і доповненнями станом на 1 січня 2002 р.) – Харків. – 2002.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

інформація, що становить комерційну таємницю, може перебувати або у приватній, або у колективній власності, або в оперативному розпорядженні державних підприємств, установ та організацій.

Але нормами ч. 2 ст. 13 Закону «Про власність» встановлено, що об'єктами права власності громадян є твори науки, літератури та мистецтва, відкриття, винаходи, корисні моделі, промислові зразки, раціоналізаторські пропозиції, знаки для товарів і послуг та інші результати інтелектуальної праці.

Право власності безпосередньо на інформацію не визначається, а інформація, наприклад, щодо нарощування обсягів виробництва, планів співробітництва, повсякденної діяльності навряд чи може вважатися об'єктом інтелектуальної праці, але буде надзвичайно важливою з комерційної точки зору. Таким чином, головна основа захисту комерційної таємниці як такої фактично відсутня.

Згідно з ч. 2 ст. 30 Закону «Про інформацію», громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної та встановлюють для неї систему (способи) захисту.

Встановлення системи захисту на власний розсуд також є характерною відмінністю комерційної таємниці від інших видів конфіденційної інформації. Згідно з нормами ч. 2 ст. 30 Закону «Про підприємства в Україні», склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства. Відомості, які не можуть становити комерційної таємниці, визначаються Кабінетом Міністрів України.

Згідно з даним переліком, комерційну таємницю не становлять:

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

- документи про сплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, що відповідно до чинного законодавства підлягають оголошенню.¹

Встановлення переліку відомостей, доступ до яких не може бути обмежено суб'єктами підприємницької діяльності, є однією з заборук забезпечення поінформованості державних органів та громадськості про важливі аспекти їхньої діяльності. Це гарантує як виконання державою своїх контрольних та фіскальних функцій, так і забезпечення прав окремих осіб та інтересів суспільства і таким чином має велике значення для інформаційної безпеки в цілому. Для цього передбачено, що підприємства зобов'язані подавати перелічені у відповідній постанові Кабінету Міністрів відомості органам державної виконавчої влади, контролюючим і правоохоронним органам, іншим юридичним особам відповідно до чинного законодавства на їх вимогу.

Але, на нашу думку, такого переліку недостатньо. Потрібно на законодавчому рівні встановити загальні критерії інформації, яка може оголошуватися комерційною таємницею. І на це є певні причини.

По-перше, це дало б змогу більшою мірою реалізувати можливість кожного громадянина подавати запити до комерційних структур, наприклад, щодо забруднення навколишнього середовища або офіційних характеристик продукції в цілях захисту прав споживачів.

По-друге, зі встановленням переліків інформації, що становить комерційну таємницю, керівниками підприємств на власний розсуд пов'язана інша проблема.

Згідно з ч. 3 ст. 30 Закону «Про підприємства в Україні», відповідальність за розголошення відомостей, які становлять комерційну таємницю підприємства, і порядок охорони таких відомостей встановлюються законодавчими актами України.

¹ Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. № 611.

Кримінальний кодекс України¹ встановлює відповідальність за злочинні дії щодо інформації, яка становить комерційну таємницю. Так, стаття 231 КК передбачає відповідальність за незаконне збирання з метою використання відомостей, що становлять комерційну таємницю, під якими розуміють «умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей (комерційне шпигунство), а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності». А стаття 232 КК встановлює відповідальність за розголошення комерційної таємниці, яку розуміють як «умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності».

Але кодекс не дає відповіді на питання, що саме є комерційною таємницею. І якщо у випадку відповідальності за розголошення державної таємниці ми можемо говорити про відсильну диспозицію відповідної норми КК і звертатися до законодавства про державну таємницю, то щодо комерційної таємниці такого законодавства просто не існує.

Якщо звернутися до основних принципів кримінальної відповідальності, то можна говорити про те, що підставою кримінальної відповідальності є вчинення особою суспільно небезпечного діяння, яке містить склад злочину, передбаченого КК (ч 1 ст. 2 КК), а злочинність діяння, а також його караність та інші кримінально-правові наслідки визначаються тільки Кримінальним кодексом (ч. 3 ст. 3 КК). Навіть у випадках відсильної диспозиції (правила дорожнього руху, державна таємниця тощо) ми можемо назвати загальний принцип визначення злочинності діяння лише на основі закону.

Але у випадку зі злочинами проти комерційної таємниці фактично злочинність діяння (належність інформації, щодо якої вчинено певні дії, до комерційної таємниці, а відповідно і протиправність дій щодо неї) визначається не законом, а розпорядженням керівника підприємства, яке не є нормативно-правовим актом. Чи не є така ситуація абсурдною, надто враховуючи недосконалість законодавства, що регулює

² Кримінальний кодекс України. Прийнятий сьомою сесією Верховної Ради України 5 квітня 2001 р. – Київ: Юрінком-Інтер, 2001.

право власності на інформацію? На нашу думку, це справді абсурд. І це є головною причиною необхідності законодавчого встановлення переліку відомостей, які можуть бути оголошені комерційною таємницею.

§ 8 Професійна таємниця

Окремим різновидом інформації з обмеженим доступом є професійна таємниця. Право фізичних та юридичних осіб захищати інформацію професійного характеру передбачене ст. 30 Закону «Про інформацію». Існують певні загальні критерії, за якими інформація може бути віднесена до професійної таємниці:

- інформація довірена або стала відомою особі виключно через виконання нею своїх професійних обов'язків;
- особа, якій довірено інформацію, не перебуває на державній або муніципальній службі (в іншому випадку інформація вважається службовою таємницею);
- заборону на поширення довіреної або такої, що стала відомою, інформації, яка може зашкодити правам або законним інтересам довірителя, встановлено законом;
- інформація не належить до відомостей, що становлять державну або комерційну таємницю.¹

За такими критеріями, як правило, виділяють лікарську, адвокатську, нотаріальну, страхову, банківську та деякі інші види таємниці.

Також потрібно наголосити на особливих характеристиках професійної діяльності, для якої передбачена наявність професійної таємниці. Як правило, сукупність правових норм, що регулює таку професійну діяльність, утворює окремий правовий інститут або галузь законодавства. Належність до подібного виду професійної діяльності обумовлює наявність у її суб'єкта специфічних прав та обов'язків. В ряді випадків можна також говорити і про так звану «вільну професію, що має громадський характер».²

На останній тезі слід акцентувати увагу. Адже особливі права і обов'язки у суб'єктів певних видів професійної діяльності виникають не

¹ Бачило І.Л., Лопатин В.Н., Федотов М.А. Информационное право / Под. ред. акад. РАН Б.Н. Топорнина. – СПб.: Юридический центр Пресс», 2001. – С. 538.

² Див.: Святоцький О.Д., Михеєнко М.М. Адвокатура України. – К.: Ін Юре, 1997. – с. 78.

просто так. Всі з названих нами видів професійної діяльності: лікарської, адвокатської, нотаріальної, страхової, банківської – виконують важливу суспільну функцію в рамках громадянського суспільства, чи то охорона здоров'я, правовий захист або робота фінансово-кредитної системи тощо. З цих причин більшість з перерахованих видів професійної діяльності безпосередньо згадується в нормах Конституції України.

Саме великим суспільним значенням функцій названих видів професійної діяльності і обумовлюється застосування додаткових заходів як щодо забезпечення цієї діяльності, так і для забезпечення прав і інтересів тих, хто звертається до їх послуг.

Ще однією особливістю правового регулювання професійних таємниць слід вважати те, що відповідні правила поведінки своїм виникненням зобов'язані не загальнолюдським моральним нормам, а нормам корпоративної моралі, або, як її ще називають, професійної етики. Ці норми виникли в процесі здійснення того чи іншого виду діяльності і для людей, які не належать до відповідної професії, можуть бути неприйнятними. Найбільш яскравим і давнім прикладом професійної таємниці можна вважати лікарську таємницю, корені якої сягають ще Стародавньої Греції і яка була викладена у клятві Гіппократа на межі V – IV століття до нашої ери.

В Україні на законодавчому рівні лікарську таємницю закріплено в «Основах законодавства України про охорону здоров'я»¹. Стаття 40 цього закону визначає, що медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків. При використанні інформації, що становить лікарську таємницю, в навчальному процесі, науково-дослідній роботі, в тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта.

Таким чином, властивою характеристикою лікарської таємниці є те, що сама інформація про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя людини конфіденційною не вважається, адже її дозволяється використовувати у навчальному

¹ Закон України «Основи законодавства України про охорону здоров'я» від 19 листопада 1992 р. № 2801-ХІІ // Відомості Верховної Ради України, 1993. – № 4. – Ст. 19.

процесі або розповсюджувати через спеціальну літературу. Конфіденційною є інформація щодо ідентифікації відомостей медичного характеру з конкретною людиною, за допомогою яких можна дізнатися про стан здоров'я конкретної людини.

З нормами, що регулюють лікарську таємницю, пов'язується обов'язок лікаря щодо надання медичної інформації (ст. 39 Основ законодавства України про охорону здоров'я). Згідно з нормами цієї статті лікар зобов'язаний пояснити пацієнтові в доступній формі стан його здоров'я, мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі наявності ризику для життя і здоров'я. Пацієнт має право знайомитися з історією своєї хвороби та іншими документами, що можуть слугувати для подальшого лікування.

Разом з тим передбачається ще один випадок застосування лікарської таємниці. Згідно з ч. 3 ст. 39 Основ, в особливих випадках, коли повна інформація може завдати шкоди здоров'ю пацієнта, лікар може її обмежити. В цьому разі він інформує членів сім'ї або законного представника пацієнта, враховуючи особисті інтереси хворого. Таким же чином лікар діє, коли пацієнт перебуває в непритомному стані.

Вищезазначена норма практично є єдиним випадком, коли людина може бути обмежена щодо отримання персональної інформації про себе, яка не становить державної таємниці.

Аналогічні вимоги містяться і в Законі «Про психіатричну допомогу»¹. Зокрема, ст. 6 цього закону передбачає, що медичні працівники, інші фахівці, які беруть участь у наданні психіатричної допомоги, та особи, яким у зв'язку з навчанням або виконанням професійних, службових, громадських чи інших обов'язків стало відомо про наявність в особи психічного розладу, про факти звернення по психіатричну допомогу та лікування у психіатричному закладі чи перебування в психоневрологічних закладах для соціального захисту або спеціального навчання, а також інші відомості про стан психічного здоров'я особи, її приватне життя, не можуть розголошувати ці відомості.

Ця інформація може передаватися за згодою особи або її законного представника для проведення обстеження та лікування чи захисту її прав і законних інтересів, для здійснення наукових досліджень, публі-

¹ Закон України «Про психіатричну допомогу» від 22 лютого 2000 р. № 1489-III // Відомості Верховної Ради України, 2000. – № 19. – Ст. 143.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

кацій у науковій літературі, використання у навчальному процесі, а також без зазначеної згоди для організації надання особі, яка страждає на тяжкий психічний розлад, психіатричної допомоги; для провадження дізнання, попереднього слідства або судового розгляду за письмовим запитом особи, яка проводить дізнання, слідчого, прокурора та суду.

Важливу функцію щодо забезпечення права на захист від обвинувачення та надання правової допомоги при вирішенні справ у судах та інших державних органах, згідно зі ст. 59 Конституції України, виконує адвокатура.

Встановлена законодавством адвокатська таємниця, яку адвокат зобов'язаний зберігати, є однією з гарантій сумлінного виконання адвокатом своїх професійних обов'язків та забезпечення прав і законних інтересів його клієнта. Згідно із ст. 9 Закону «Про адвокатуру»,¹ предметом адвокатської таємниці є питання, з яких громадянин або юридична особа зверталися до адвоката, суть консультацій, порад, роз'яснень та інших відомостей, одержаних адвокатом при здійсненні своїх професійних обов'язків. Крім того, дані попереднього слідства, які стали відомі адвокату у зв'язку з виконанням ним своїх професійних обов'язків, можуть бути розголошені тільки з дозволу слідчого або прокурора. Адвокату, помічнику адвоката, посадовим особам адвокатських об'єднань забороняється розголошувати відомості, що становлять предмет адвокатської таємниці, і використовувати їх у своїх інтересах або в інтересах третіх осіб.

Слід зазначити, що вимоги щодо збереження адвокатської таємниці не мають строку давності. Крім того, конфіденційність інформації, що становить адвокатську таємницю, має найбільші серед інформації з обмеженим доступом правові гарантії. В той час, коли інші види конфіденційної інформації можуть бути отримані державними органами відповідно до певних процедур, нормами ст. 10 Закону «Про адвокатуру» взагалі «забороняється... вимагання від адвоката, його помічника, посадових осіб і технічних працівників адвокатських об'єднань відомостей, що становлять адвокатську таємницю». Більше того, з цих питань вони не можуть бути допитані як свідки. Документи, пов'язані з виконанням адвокатом доручення, не підлягають оглядові, розголо-

¹ Закон України «Про адвокатуру» від 19 грудня 1992 р. № 2887-ХІІ // Голос України. – 1993. – 29 січня // Бюлетень законодавства і юридичної практики України «Адвокатура в Україні» – Київ: «Юрінком», 2000. – № 1.

шенню чи вилученню без його згоди. Законом встановлюється особливий порядок надання дозволу на прослуховування телефонних розмов адвокатів у зв'язку з оперативно-розшуковою діяльністю.

Адвокати, винні в розголошенні конфіденційних відомостей, що становлять адвокатську таємницю, несуть дисциплінарну відповідальність, а в разі розголошення ними без дозволу слідчого або прокурора даних попереднього слідства – і кримінальну відповідальність.

Найбільш детально правова й етична природа професійної адвокатської таємниці викладена у Загальному кодексі правил для адвокатів країн Європейського Співтовариства¹. Згідно з п. 2.3 цього кодексу, особливість професії адвоката полягає в тому, що він одержує від клієнта відомості, які той не буде повідомляти іншій особі, а також іншу інформацію, яку йому належить зберігати в таємниці. Довіра до адвоката може виникнути лише за умови обов'язкового додержання ним принципу конфіденційності. Таким чином, конфіденційність є першорядним і фундаментальним правом та обов'язком адвоката.

Відповідно до цього, режим конфіденційності інформації, пов'язаної з професійною діяльністю адвоката, визначається рядом правил:

- адвокат зобов'язаний однаковою мірою зберігати в таємниці як відомості, одержані ним від клієнта, так і інформацію про клієнта, одержану ним у процесі надання послуг клієнту;
- на обов'язок додержання конфіденційності не поширюється дія строку давності;
- адвокат зобов'язаний вимагати додержання конфіденційності від помічників і від будь-яких інших осіб, які беруть участь у наданні послуг клієнту.

На жаль, сьогоднішні українські реалії свідчать, що органи державної влади, зокрема слідчі та судові, дуже часто намагаються ставити перешкоди щодо виконання адвокатом своїх професійних обов'язків, у тому числі й щодо збереження адвокатської таємниці. Але слід зазначити, що адвокат є особою, що має вищу юридичну освіту і наділена широкими процесуальними правами, і таким чином має істотні можливості домагатися виконання вищезазначених норм законодавства. Це, зокрема, залежить і від особистої позиції адвоката та його сумлінного ставлення до своїх обов'язків.

¹ Загальний кодекс правил для адвокатів країн Європейського Співтовариства. Прийнято делегаціями дванадцяти країн-учасниць на пленарному засіданні у Страсбурзі в жовтні 1988 р.

Ще одним із передбачених законодавством видів конфіденційної інформації, пов'язаної з професійною діяльністю, є «таємниця вчинюваних нотаріальних дій», як вона визначається нормами ст. 8 Закону «Про нотаріат».¹ Нотаріуси та інші посадові особи, які вчиняють нотаріальні дії, зобов'язані додержуватися таємниці цих дій. Обов'язок додержання таємниці вчинюваних нотаріальних дій поширюється також на осіб, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків.

Законом також передбачено ряд гарантій додержання нотаріальної таємниці. Нормами тієї ж ст. 8 Закону «Про нотаріат» визначено вичерпний перелік випадків розголошення цих відомостей. Так, довідки про вчинені нотаріальні дії та документи і копії з них видаються:

- тільки громадянам та юридичним особам, за дорученням яких або щодо яких вчинялися нотаріальні дії;
- на письмову вимогу суду, арбітражного суду, прокуратури, органів дізнання і слідства у зв'язку з кримінальними, цивільними або господарськими справами, що перебувають у їх провадженні;
- на письмову вимогу державної податкової адміністрації, необхідні для визначення правильності стягнення державного мита та цілей оподаткування;

- довідки про заповіти видаються тільки після смерті заповідача.

Законом передбачено відповідальність за порушення нотаріальної таємниці.

Дуже схожою за своїми ознаками з нотаріальною є таємниця страхування, передбачена Законом «Про страхування», в ст. 19 якого одним з обов'язків страхувальника (п. б) називається «тримати в таємниці відомості про страхувальника і його майновий стан, за винятком випадків, передбачених законодавством України».²

Ще одним специфічним видом конфіденційної інформації є банківська таємниця. В Законі «Про інформацію» (ст. 30) цей вид конфіденційної інформації називається поряд з професійною та комерційною таємницями, що в принципі дає можливість розглядати банківську таємницю як самостійний вид конфіденційної інформації. Хоча не можна не зазначити, що банківська таємниця має ті самі ознаки і природу, що й професійна таємниця.

¹ Закон України «Про нотаріат» від 2 вересня 1993 року № 3425-XII // Відомості Верховної Ради України, 1993. – № 39. – Ст. 383.

² Закон України «Про страхування» від 7 березня 1996 року № 85/96-ВР // Відомості Верховної Ради України, 1996. – № 18. – Ст. 78.

Так, ст. 60 Закону «Про банки і банківську діяльність» визначає, що «інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту, є банківською таємницею».¹

Банківською таємницею, зокрема, є відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку України; операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; фінансово-економічний стан клієнтів; системи охорони банку та клієнтів; інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності; відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню; коди, що використовуються банками для захисту інформації. Але згідно з роз'ясненнями Національного банку України, цей перелік не є вичерпним і банки самостійно визначають перелік такої інформації².

На основі цього визначення ми можемо встановити основні ознаки банківської таємниці: 1) це конфіденційна інформація, яка отримана банком від його клієнтів у зв'язку з наданням банківських послуг; 2) оскільки банківські послуги фізичним та юридичним особам в Україні надаються комерційними банками, то банківські службовці, яким довірено цю інформацію, не перебувають на державній або муніципальній службі; 3) розголошення інформації, що становить банківську таємницю, прямо заборонене законом; 4) і, нарешті, ця інформація не належить до державної таємниці.

Такі міркування дають змогу говорити про банківську таємницю як про специфічний вид конфіденційної інформації, що пов'язана з виконанням юридичними особами банківської діяльності та належністю фізичних осіб до відповідної професії – банківських службовців. Це цілком вкладається в рамки професійної таємниці, адже її суб'єкта-

¹ Закон України «Про банки і банківську діяльність» від 7 грудня 2000 року № 2121-III // Відомості Верховної Ради України, 2001. – № 5- 6. – Ст. 30.

² Роз'яснення Національного банку України з питань виконання окремих вимог Закону України «Про банки і банківську діяльність» № 18-112/1467 від 19 квітня 2001 р.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації

ми є не тільки люди відповідної професії – лікарі, адвокати, працівники страхових компаній, а й юридичні особи – медичні заклади і установи, адвокатські фірми, об'єднання, страхові компанії тощо.

Законом «Про банки і банківську діяльність» (ст. 61) передбачено ряд заходів щодо збереження банківської таємниці. Зокрема, банки несуть обов'язок щодо:

- обмеження кола осіб, які мають доступ до інформації, що становить банківську таємницю;
- організації спеціального діловодства з документами, що містять банківську таємницю;
- застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;
- застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Службовці банку при вступі на посаду підписують зобов'язання щодо збереження банківської таємниці. Керівники та службовці банків зобов'язані не розголошувати і не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні своїх службових обов'язків. Це саме стосується і приватних осіб та організацій, які при виконанні своїх функцій або наданні послуг банку отримали інформацію, що є банківською таємницею. У разі заподіяння розголошенням банківської таємниці шкоди інтересам банку чи клієнта вона підлягає відшкодуванню за рахунок особи, винної у розголошенні.

Інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками лише в передбачених законом випадках (п. 1 – 4 ст. 62 цього закону), зокрема:

- на письмовий запит або з письмового дозволу власника такої інформації;
- на письмову вимогу суду або за рішенням суду;
- органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;
- органам Державної податкової служби України на їх письмову вимогу з питань оподаткування або валютного контролю стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу.

Довідки по рахунках (вкладах) у разі смерті їхніх власників надаються банком особам, зазначеним власником рахунку (вкладу) в заповідальному розпорядженні банку, державним нотаріальним конторам або приватним нотаріусам, іноземним консульським установам у справах спадщини за рахунками (вкладами) померлих власників рахунків (вкладів).

Крім того, доступ до банківської таємниці мають працівники Національного банку при виконанні ними своїх службових обов'язків. Банк також може передавати інформацію, що є банківською таємницею, іншим банкам при отриманні кредитів за умови надання гарантії конфіденційності.

Органи Державної податкової служби, прокуратури, СБУ, МВС мають право отримати будь-яку інформацію, віднесена законом до банківської таємниці, з дозволу власника цієї інформації та за рішенням суду. Крім того, ці органи мають право отримати на письмову вимогу лише інформацію стосовно операцій за рахунками юридичних осіб та фізичних осіб – суб'єктів підприємницької діяльності за конкретний проміжок часу. Інші державні органи мають право отримати таку інформацію лише з дозволу власника цієї інформації та за рішенням суду.

У запитах повинен бути чітко вказаний календарний проміжок часу, за який необхідно надати інформацію стосовно операцій за рахунками, вони повинні містити посилання на норми відповідних законів, які визначають права державних органів, в тому числі і на отримання такої інформації.

Оскільки банку забороняється надавати інформацію про клієнтів іншого банку, навіть якщо їхні імена зазначені у документах, угодах та операціях клієнта, при наданні інформації, що є банківською таємницею (ч. 4 ст. 62), банки повинні надавати інформацію про рух коштів на рахунку клієнта без зазначення відправника цих коштів та їх одержувача (які є як клієнтами іншого банку, так і клієнтами запитуваного банку).¹

Інститут банківської таємниці є дуже важливим чинником забезпечення прав і свобод людини, включаючи право на заняття підприємницькою діяльністю, не забороненою законом, право на невтручання у приватне життя тощо. Крім того, ступінь забезпеченості банківської таємниці є фактором, що обумовлює привабливість країни для

¹ Див.: Роз'яснення Національного банку України з питань виконання окремих вимог Закону України «Про банки і банківську діяльність» № 18-112/1467 від 19 квітня 2001 р.

іноземного капіталу, а також для вирішення актуальної для України проблеми зменшення тіньового сектора економіки та повернення вивезених капіталів в Україну.

§ 9 Обмеження щодо виробництва та ввезення в Україну інформаційної продукції

Як ми вже зазначали, обмеження свободи інформації здійснюється шляхом застосування заходів щодо захисту інформації та шляхом нормативно-правового обмеження її вільного обігу в суспільстві. Якщо до таємної і конфіденційної інформації застосовувалися обидва методи (і захист, і обмеження обігу), то в іншому випадку застосовується виключно обмеження вільного обігу інформації. Це стосується передбаченого багатьма міжнародно-правовими актами, зокрема Конвенцією про захист прав і основних свобод людини (ч. 2 ст. 10),¹ обмежень для забезпечення територіальної цілісності або громадського порядку, для захисту здоров'я і моралі.

У попередніх розділах ми вже зупинилися на питанні обмеження свободи слова в тих випадках, коли це порушує права третіх осіб або суспільства в цілому. Тому зараз ми підкреслимо той факт, що в Україні існує ціла система норм, різних законодавчих актів, які покликані обмежити або заборонити поширення інформації, яка може зашкодити територіальній цілісності, громадському порядку, суспільному здоров'ю та моралі.

Так, стаття 13 Основ законодавства України про культуру,² яка регулює питання розповсюдження та популяризації творів літератури і мистецтва, визначає також вичерпний перелік підстав обмежень. Частиною 2 ст. 13 Основ забороняється розповсюдження творів, що містять заклики до зміни насильницьким шляхом конституційного ладу; пропаганду війни, насилля, жорстокості, расової, національної, релігійної ворожнечі або ненависті; порнографію; підбурювання до вчинення злочинів. Ця загальна норма стосується безпосередньо розповсюдження означених творів. Але, крім цього, рядом законодавчих

¹ Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4.XI.1950) / «European Treaty Series» – № 5.

² Закон України «Основи законодавства України про культуру» від 14 лютого 1992 р. № 2117-XII // Відомості Верховної Ради України, 1992. – № 21. – Ст. 294.

актів, що регулюють діяльність щодо масового виробництва та розповсюдження інформації, встановлено аналогічні заборони.

Так, Законом «Про видавничу справу»¹ (ст. 28) встановлено, що діяльність у видавничій справі не може бути використана для закликів, спрямованих на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, пропаганду війни, насильства, розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на права і свободи людини, здоров'я населення. З цією метою, зокрема, забороняється:

- виготовляти чи розповсюджувати продукцію, яка містить інформацію, віднесена до недобросовісної реклами, або рекламувати товари, послуги, які можуть завдати шкоди громадянам, підприємствам, установам, організаціям або державі;
- виготовляти чи розповсюджувати видавничу продукцію порнографічного характеру і таку, що пропагує культ насильства і жорстокості;
- виготовляти чи розповсюджувати видавничу продукцію, що проповідує релігійні віровчення, які загрожують життю, здоров'ю, моралі громадян, порушують їхні права і свободи або закликають до порушення громадського порядку.

Нормами ч. 2 ст. 2. Закону «Про телебачення і радіомовлення»¹ встановлено, що телерадіоорганізації не мають права у своїх програмах розголошувати дані, що становлять державну таємницю або іншу таємницю, яка охороняється законодавством, закликати до насильницької зміни або повалення існуючого державного і суспільного ладу, порушення територіальної цілісності України, вести пропаганду війни, насильства і жорстокості, розпалювання расової, національної, релігійної ворожнечі, поширювати порнографію або іншу інформацію, яка підриває суспільну мораль або підбурює до правопорушень, принижує честь і гідність людини.

Вищеперелічені норми законодавчих актів покликані унеможливити створення і розповсюдження подібної інформації та її носіїв всередині України. Ще одна група правових норм спрямована на недопущення ввезення подібної інформаційної продукції на територію України або вивезення її з цієї території.

¹ Закон України «Про видавничу справу» від 5 червня 1997 р. № 318/97-ВР.

² Закон України «Про телебачення і радіомовлення» від 21 грудня 1993 р. № 3759-ХІІ // Відомості Верховної Ради України, 1994. — № 10. — Ст. 43. (В редакції закону від 11.05.2000 № 1709-ІІІ)

Згідно з Законом «Про порядок ввезення (пересилання) в Україну, митного оформлення й оподаткування особистих речей, товарів та транспортних засобів, що ввозяться (пересилаються) громадянами на митну територію України»¹ (ст. 9), не підлягають пропуску через митний кордон України: ...літературні та художні твори, поліграфічна та інша друкована продукція, кіно-, фото-, аудіо- та відеоматеріали, що пропагують війну, жорстокість, порнографію, расову, етнічну або релігійну ворожнечу, закликають до насильницького повалення конституційного ладу в Україні.

Аналогічні вимоги містяться і в Тимчасовому положенні про порядок пропуску товарів, майна та транспортних засобів, згідно з яким до ввезення на митну територію України заборонено «...друковані матеріали, кліше, негативи, відзняті плівки, фотографічні знімки, кінострічки, відеозаписи, копії магнітної інформації для ЕОМ, рукописи, платівки та інші звукозаписи, малюнки й інші друковані та образотворчі матеріали, що містять пропаганду ідей війни, расизму, расової дискримінації та геноциду, а також спрямовані на підриг територіальної цілісності України, її політичної незалежності, державного суверенітету, а також продукція порнографічного характеру».²

Взагалі, характеризуючи вектор державної політики інформаційної безпеки, спрямований на захист і обмеження доступу до інформації, слід відзначити два взаємопов'язані фактори, якими ця політика обумовлюється.

З одного боку, це існування значного правового та організаційного досвіду «радянських часів» щодо застосування різного роду обмежених режимів доступу до інформації та захисту цієї інформації. Цей досвід дозволив створити велику кількість нормативно-правових актів у цій сфері і досить ефективно їх застосовувати.

Але, з другого боку, той же «радянський досвід» є наслідком системи державної влади, яка нехтувала демократичними принципами, при якій фактично не існувало свободи слова. І правові акти щодо обмеження доступу і захисту інформації, побудовані на старому багажі, дуже часто несумісні з демократичними реформами в державі. Зокрема, це

¹ Закон України «Про порядок ввезення (пересилання) в Україну, митного оформлення й оподаткування особистих речей, товарів та транспортних засобів, що ввозяться (пересилаються) громадянами на митну територію України» від 13 вересня 2001 р. № 2681-III.

² Наказ Держмитслужби України «Про Тимчасове положення про порядок пропуску товарів, майна та транспортних засобів» № 7 від 30 грудня 1991 р.

стосується підзаконних актів, які дозволяють органам державної влади та різного роду установам, підприємствам і організаціям практично довільно обмежувати доступ до інформації.

Тому основним напрямком реформування законодавства в цій галузі слід назвати шлях поєднання існуючого досвіду з принципами відкритості та розумної достатності щодо обмеження доступу до інформації.