використання . Україною послуг відповідних приватних компаній існує ряд ризиків та перешкод, які насамперед пов'язані із сучасними фінансово-економічними труднощами дипломатичної служби. У зв'язку з цим приватні компанії безпеки розглядаються як важливий, проте перспективний ресурс вдосконалення системи забезпечення безпеки дипломатичних установ України, до якого за певних умов можна було б звернутися МЗС України в майбутньому.

Фролова Олена Григорівна
доктор юридичних наук, професор
Національного юридичного університету імені Ярослава Мудрого
(Україна, м.Харків)

ДО ВИЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СУЧАСНИХ ПРОБЛЕМ ЗАХИСТУ НАЙБІЛЬШ ВАЖЛИВОЇ ІНФОРМАЦІЇ ТА ЇЇ ОБІГУ

Молода за історичними масштабами Українська держава, яка ще проходить один з найскладніших етапів свого розвитку та демократичної і правової розбудови, у тому числі й один з найскладніших етапів розбудови та зміцнення свого державного і недержавного секторів безпеки, не може залишатися осторонь процесів загальної всесвітньої інформатизації суспільства і формування єдиного світового інформаційного простору. Значною мірою і сам процес такої розбудови, і сам процес міжнародно-правового визнання нашої держави, стали у певному розумінні інформаційним проривом у загальносвітових інформаційних потоках в умовах різноманітних за змістом, цільовим спрямуванням і призначенням, масштабами, силою, потужністю та тривалістю інформаційних війн. Саме доведення до відома в першу чергу державних діячів, а потім і населення інших країн відомостей про існування України як суверенної і демократичної держави та про наші насущні потреби, насамперед, необхідність забезпечення цілісності, єдності і незалежності нашої держави, недоторканності нашої території і кордонів, забезпечення безпеки існування та прогресивного розвитку державного і недержавного сектору сприяли створенню позитивного міжнародного іміджу України. Все це обумовило і міжнародне визнання України як геополітичної реальності, і підтримку України не тільки її власним населенням, але й іншими державами, їх населенням та міжнародним організаціями. Інформаційні фактори та інформаційна безпека виступили і продовжують виступати на практиці як частина національної безпеки, зокрема, й безпеки в державному і недержавному секторі та надзвичайно важливі чинники не тільки у внутрішньому загально-державному значенні, але й у всесвітньому визнанні України, як сучасної суверенної і демократичної держави, та відстоюванні її зовнішніх міждержавних інтересів.

Інформаційний суверенітет України - це, з одного боку, право держави на формування і здійснення національної інформаційної політики, та, з іншого боку, невід'ємне право людини і суспільства на самовизначення та участь у формуванні, розвитку і здійсненні національної інформаційної політики відповідно до Конституції, чинного законодавства України та міжнародного права в національному інформаційному просторі України. Об'єктами національного інформаційного простору є інформаційна продукція в усіх її різновидах, включаючи твори літератури і мистецтва, наукові праці, публічні виступи, використані в інформаційній діяльності, національні інформаційні ресурси, інформаційні послуги, організаційні та майнові функціональні елементи інформаційної інфраструктури тощо. Стаття 54 Закону «Про інформацію» підкреслює, що інформаційний суверенітет України

забезпечується: по-перше, виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету; по-друге, створенням національних систем інформації; по-третє, встановленням режиму доступу інших держав до інформаційних ресурсів України; по-четверте, використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами» [1]. Так, наприклад, в Меморандумі про взаєморозуміння щодо співробітництва в сфері телекомунікацій і розвитку Всесвітньої інформаційної інфраструктури між урядом України та урядом Сполучених Штатів Америки сторони наголосили на своєму намірі керуватись принципами створення Всесвітньої інформаційної інфраструктури, для чого впроваджувати приватні інвестиції, конкурентний ринок, гнучку регулюючу систему, доступ без дискримінації та універсальне обслуговування. Саме такі підходи були зафіксовані у рішеннях Першої Всесвітньої конференції з розвитку телекомунікацій Міжнародного союзу електрозв'язку (Буенос-Айрес, 1994 рік) [2].

На сучасному етапі розвитку суспільства потрібно усвідомлювати, що зростання і вдосконалення роботи всесвітніх тенет Інтернету і різноманітних комп'ютерних технологій, потужний розвиток технічних засобів, зростання і поглиблення досягнень науково-технічного прогресу та їх швидке впровадження у практичну діяльність, а також безліч інших об'єктивних і суб'єктивних факторів, обставин і реалій сьогодення призводять на практиці до розмивання державних інформаційних просторів, зникнення державних кордонів та взаємопроникнення більшості об'єктів та складових елементів інформаційного простору різних держав між собою, а також до так званих інформаційних «вибухів», «диверсій», «тероризму», «війн» та, врешті-решт, до кіберзлочинності. Внаслідок цього забезпечити належний стан захищеності інформаційних ресурсів та режимів їх збереження і використання на практиці як в державному, так і в недержавному секторі, і навіть в масштабах окремих держав у цілому в ряді випадків стає досить проблематичним або зовсім неможливим. Так, наприклад, на думку відомого американського дослідника Х. Клівленда, в «міжнародній політиці твердження проте, що інформація сьогодні є власністю суверенних держав, виявляється найбільшою помилкою» [3]. Одним з аргументів у цьому аспекті виступає й те, що кожен запущений комунікаційний супутник знижує життєвість доктрини, згідно з якою суверенні держави повинні володіти або хоча б контролювати свої інформаційні ресурси тощо. У цьому зв'язку слід зазначити, що міжнародно-правова практика будується сьогодні насамперед на принципі свободи інформації та забезпеченні гарантій інформаційних прав та свобод особи, одночасно розглядаючи права держави щодо регулювання інформаційних процесів лише в контексті її загальних суверенних прав.

Так, наприклад, повертаючись до згаданих в якості «могильників інформаційного суверенітету» штучних супутників, у прийнятій 15.11.1972 року ЮНЕСКО Декларації керівних принципів щодо використання мовлення через супутники для вільного використання інформації, розвитку освіти і розширення культурних обмінів, передбачено, наприклад, що, по-перше, при мовленні через супутники повинні поважаться суверенітет та рівність усіх держав; по-друге, при підготовці програм прямого мовлення на інші країни повинні братися до уваги розбіжності в національних законах країн, об'єктів мовлення; по-третє, принципи цієї Декларації повинні застосовуватися з повною повагою до прав людини та її основних свобод тощо. Таким чином, сьогодні в часи найширшого запровадження сучасних інформаційних технологій та відкритої демократизації всіх суспільних процесів, вельми проблематично говорити про інформаційний суверенітет на територіальному рівні, і тим паче на

практиці забезпечувати його в аспекті недоторканності кордонів, недопущення зазіхань на територію тощо. Мабуть, саме тому, наприклад, згідно з розробками Українського центру економічних і політичних досліджень, інформаційний простір України розглядається як середовище, в якому здійснюється продукування, зберігання та поширення інформації і на яке розповсюджується юрисдикція України, а замість терміну «інформаційний суверенітет» більшість авторів сьогодні використовує більш актуальний термін «інформаційна безпека» громадян, суспільства, державного і недержавного сектору та держави у цілому [4]. Під поняттям інформаційної безпеки на практиці розуміється стан захищеності національних інтересів держави в інформаційній сфері, які визначаються сукупністю збалансованих інтересів особи, суспільства і держави. Таким чином, інформаційна безпека трактується як стан захищеності інформаційного середовища суспільства, який забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави.

Конкретний зміст поняття інформаційної безпеки, як зазначається в Законі України «Про основи національної безпеки», обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам, а всі види безпеки, в тому числі й інформаційна, пов'язуються зі станом захищеності життєво важливих інтересів її об'єктів, причому об'єктами називаються: по-перше, людина і громадянин — їхні конституційні права і свободи; по-друге, суспільство — його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; по-третє, держава — її конституційний лад, суверенітет, територіальна цілісність і недоторканність [5]. В свою чергу, об'єктами конкретно інформаційної безпеки більшістю науковців і практиків, як правило, визначаються інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни тощо [6].

У вузькому розумінні інформаційна (або мережна) безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів і інформаційних та телекомунікаційних систем може створити загрозу для міжнародної безпеки [7].

Проблеми захисту найбільш важливої інформації та застосування обмежень щодо її обігу є найдавнішими напрямками інформаційної безпеки. Від самого виникнення такого інституту, як держава, почала поширюватися, наприклад, практика оголошення різного роду відомостей таємними і встановлення відповідних правових норм для захисту цієї таємниці. Не втрачає актуальності ця проблема і нині, й окрім державної таємниці, яка, в свою чергу може розрізнятися за ступенем таємності, сьогодні, зокрема, для недержавного сектору з'явилися й інші різновиди таємниць, наприклад, фінансова, банківська, комерційна, конфіденційна тощо. Для чіткого визначення правової природи заборон і обмежень щодо обігу такої інформації з елементами різного роду та виду таємниць, потрібно визначитися з основними принципами обігу інформації в суспільстві. Цей обіг відбувається відповідно до цілого ряду факторів, серед яких можна вирізнити, по-перше, природні фактори, у тому числі дію різного роду фізичних, біологічних, медичних, фізіологічних та інших природних законів, які впливають на обіг інформації взагалі. До таких факторів, наприклад, фізичного характеру можна віднести швидкість

струменів світла, якою обмежуються передачі даних за допомогою електронних засобів комунікації, або фізичні якості фізичних носіїв інформації, які обумовлюють терміни зберігання інформації на цих носіях, можливість її відновлення чи зміни тощо. До факторів, наприклад, фізіологічного характеру можна віднести власні спадкові та здобуті за допомогою професійного досвіду чи спеціальних вправ на протязі життя фізіологічні характеристики й особливості стану здоров'я й певних видів талантів і здібностей особи індивіда як носія інформації, наприклад: рівень його інтелекту, який визначає можливості щодо збору і обробки інформації, обсяги та глибина його пам'яті, здатність до забування, чим обмежується й окреслюється строк, за який інформація може залишатися в пам'яті особи індивіда достатньо повною і точною, і без додаткового дублювання та збереження цієї інформації на інших спеціальних фізичних носіях, і таке інше.

Залежно від виду інформації законодавство передбачає наявність або відсутність тих чи інших обмежень або заборон в її обігу, згідно з якими всю інформацію умовно можна поділити на дві групи або два основних вида: перший вид - відкрита інформація, яка вільно розповсюджується в інформаційній сфері, та другий вид - інформація обмеженого доступу, розповсюдження якої можливе лише на умовах конфіденційності або таємності. До відкритої інформації, наприклад, належать: інформація, що створюється в процесі творчості (витвори науки та мистецтва, відкриті патенти та авторські свідоцтва); документована інформація, що надається обов'язково;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).

Разом з тим, наведена вище класифікація інформації на види не є повною і вичерпною, і не охоплює ряд винятків та обмежень. Так, наприклад, подібна класифікація не відчуває 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 можемо стверджувати, що і вона може бути закритою для певного кола осіб.

Цікавою, на нашу думку, є класифікація інформації за основними і загальновідомими методами адміністративно-правового регулювання, що застосовуються для регулювання суспільного обігу того чи іншого виду інформації, а саме: диспозитивним та імперативним методами. Так, при застосуванні диспозитивного методу умови обігу інформації, її використання, розповсюдження та передачі прав на неї третім особам визначаються або власником цієї інформації особисто, або на основі договору з іншими зацікавленими особами. Це зовсім не означає відсутності нормативно-правового регулювання обігу такої інформації, але в рамках такого регулювання існує і певна свобода дій (див., наприклад, законодавство про авторські права, право інтелектуальної власності, охорону інформації про особисте життя і персональні дані, разом з цим, ці дані також можуть бути оприлюднені за згодою цієї особи тощо). Існує і 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 обігу інформації, яка містить у собі державну,

службову, лікарську, адвокатську таємниці, певні види статистичної інформації, персональні дані тощо. Таким чином, метод правового регулювання обігу інформації виступає однією з важливих вихідних юридичних характеристик інформації. Разом з тим, 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 цивільного 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. 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. 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.

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. Таким чином, віднесення інформації до комерційної таємниці не є так званим «грифом таємності», а лише вказує на те, що право власності на дану інформацію охороняється законодавством. Звідси виникає запитання, чи взагалі слід розглядати будь-які заходи щодо захисту інформації частиною національної інформаційної безпеки. Вважаємо, що ні. І ось чому: згідно із ст. 17 Конституції України, 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 [8]. 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 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 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 та її компетентними органами, але вже не в рамках функції захисту інформаційної безпеки, а в рамках правоохоронної функції, як захист права власності.

Основою правового регулювання захисту та обмеження доступу до інформації є норми ч. 2. ст. 32 Конституції України, 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.

Інформація з обмеженим доступом, в свою чергу, поділяється на конфіденційну і таємну (ст. ЗО Закону «Про інформацію») тощо. 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. ЗО 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.

Ми зупинилися стисло і лише на деяких із сучасних проблем інформаційної безпеки і захисту найбільш важливої інформації, як в державному, так і в недержавному секторах. Зрозуміло, що вищерозглянуті та інші проблеми в цій сфері потребують свого подальшого і поглибленого дослідження. Враховуючи значне розширення міжнародного співробітництва України, в тому числі в сферах оборони, боротьби зі злочинністю, військово-технічного співробітництва, питання міжнародно-правового регулювання інформаційної безпеки і, зокрема, захисту таємної інформації в цих та інших сферах набуватимуть дедалі все більшого значення.

Список використаних джерел: 1. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст.650; 2. Меморандум про взаєморозуміння шодо співробітництва в сфері телекомунікацій і розвитку Всесвітньої інформаційної інфраструктури між Урядом України та Урядом Сполучених Штатів Америки від 22 листопада 1994 р. м. Вашингтон (http://www.rada.kiev.ua). 3. Cleveland H. The knowledge executive. Leadership in an information society. – New York: Truman Talley books, 1989. – P. 82; 4. Баранов. А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона, 2001. - №1. - С.71; 5. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. //Голос України. – 22 липня 2003 р. – № 134; 6. Кормич Б.А. Правові методи попередження та ліквідації загроз інформаційній безпеці людини. // Митна справа. Науково - аналітичний журнал з питань митної справи та зовнішньоекономічної діяльності. – № 5 (вересень-жовтень). – 2002. – С. 75. – 89; 7. Developments in the field of information and telecommunications in the context of international security / Report of the Secretary-General. Fifty-six session. 3 July 2001. United Nations. A/56/164; 8. Северин В.А. Правовые проблемы информационной безопасности предприятия // Юристъ, 2001. – № 6. – С. 29.