Організація

ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

ПІДРУЧНИК

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
Навчально-науковий інститут інформаційної безпеки

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

ПІДРУЧНИК

За редакцією Є.Д.Скулиша

Київ
Науково-видавничий відділ Національної академії СБ України
2011

Рекомендовано до друку рішенням Вченої ради Національної академії СБ України, протокол № 4 від 29 жовтня 2009 р.

РЕЦЕНЗЕНТИ: доктор юридичних наук, професор Р.А.КАЛЮЖНИЙ;
доктор економічних наук, професор В.І.ТЕРЕХОВ

Колектив авторів:
А.М.ГУЗ – передмова, розділи 1, 2, післямова;
О.Д.ДОВГАНЬ – розділ 1;
А.І.МАРУЩАК – 4; розділ 5;
Є.Д. СКУЛИШ – передмова (у співавторстві). розділи 3;
О.М.СОЛОДКА – розділ 5;
І.П.КАСПЕРСЬКИЙ – розділ 6;
А.С.ВОЛОЩЕНКО – розділ 7;
В.Ю.АРТЕМОВ – розділ 8;
О.О.ХМЕЛЬНИЦЬКИЙ – розділ 9.

Зтверджено МОН України як підручник для слухачів, курсантів та студентів вищих навчальних закладів (лист №1/11 – 751 від 28.01. 2011 р.).

Організація захисту інформації з обмеженим доступом : підручник / А.М.Гуз, О.Д.Довгань, А.І.Марущак та ін.. ; за ред. Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України , 2011. – 376 с.

Розкрито зміст правового регулювання процесів, спрямованих на захист інформації з обмеженим доступом, порядок організації заходів захисту різних видів названої інформації та окремі аспекти організаційного забезпечення захисту інформації.

Для студентів, що навчаються за напрямом підготовки “Організація захисту інформації з обмеженим доступом”. Буде корисним для всіх, хто вивчає питання організації захисту інформації з обмеженим доступом в Україні.

© Національна академія СБ України, 2011
© А.М.Гуз, О.Д.Довгань, А.І.Марущак,
О.М.Солодка, І.П.Касперський, А.В.Волощенко,
В.Ю.Артемов, О.О.Хмельницький, 2011

ПЕРЕДМОВА

Глобальна інформатизація українського суспільства вимагає забезпечення його інформаційного суверенітету. Висококваліфіковані фахівці мають здійснювати комплексний захист інформації в органах місцевого самоврядування та державного управління, установах, на підприємствах усіх форм власності, а також забезпечувати охорону державної, комерційної, банківської, лікарської таємниці, персональних даних та інших видів інформації з обмеженим доступом.

Крім того, реалізація державотворчих і соціально-економічних реформ сучасного етапу розвитку України чітко продемонструвала, що для їх швидкого та ефективного здійснення в конкретних організаціях та установах різного профілю бракує кваліфікованих працівників, здатних організовувати захист інформації з обмеженим доступом.

Потребу у фахівцях за напрямом підготовки "Організація захисту інформації з обмеженим доступом" зумовлюють такі фактори, як зростання попиту на таких спеціалістів, спричинене глобальною інформатизацією суспільства, та необхідність підвищення якості їхньої підготовки у зв'язку з ускладненням умов, у яких здійснюється захист інформації з обмеженим доступом.

У Києві з 2000 року фахівців із захисту інформації в галузі знань "Інформаційна безпека", напрям підготовки "Управління інформаційною безпекою", готують НТТУ "КПІ", НАУ, ДУІКТ, Європейський університет. Плани підготовки цих вищих навчальних закладів (ВНЗ) зорієнтовані переважно на технічний захист інформації.

Національна академія Служби безпеки України (далі – НА СБ України) є провідним українським ВНЗ, який 18 років готує фахівців для забезпечення державної безпеки, а останні 5 років і за напрямом 1602 – "Національна безпека" (галузь знань – 1601 "Військові науки, національна безпека, безпека державного кордону"). Починаючи з вересня 2004 року, Академія готує бакалаврів та магістрів за напрямом підготовки 160103 "Організація захисту інформації з обмеженим доступом"; вона стала одним із провідних вищих освітніх закладів, у якому сформувалася комплексна концепція та власна школа підготовки таких фахівців.

Надання освітніх послуг у Національній академії СБ України вирізняється більш досконалою програмою підготовки, яка адаптована до потреб замовника й формує в студентів уміння комплексного захисту інформації з обмеженим доступом (тобто передбачає не лише технічну, а й організаційно-правову та криптографічну, а також меншою мірою оперативно-розшукову складову).

Випускники повністю задовольняють кадрові потреби замовників: державних органів (у тому числі правоохоронних), органів місцевого самоврядування, підприємств, установ і організацій усіх форм власності та категорій режиму секретності. Дипломований фахівець може працювати (проходити службу) в режимно-секретних підрозділах; службах (підрозділах) безпеки; підрозділах захисту інформації та аналогічних їм відповідно до галузевої специфіки; у підрозділах, які забезпечують економічну безпеку підприємств, охорону інформації НАТО з обмеженим доступом.

У навчальному плані підготовки фахівця з організації захисту інформації з обмеженим доступом передбачено низку дисциплін, які формують відповідні знання, уміння та навички. Це "Вступ до спеціальності "Організація захисту інформації з обмеженим доступом", "Організаційно-правові основи захисту інформації з обмеженим доступом", "Законодавство у сфері регулювання суспільних інформаційних відносин", "Основи технічного захисту інформації", "Методологія захисту інформації", "Інформаційна безпека держави" тощо.

Деякі теми з цих дисциплін містить наш підручник. Зокрема він повною мірою забезпечить програму навчальної дисципліни "Організаційно-правові основи захисту інформації з обмеженим доступом", яка є нормативною при підготовці фахівців за напрямом "Організація захисту інформації з обмеженим доступом". Цей курс передбачає вивчення основ організації та функціонування підрозділу захисту інформації з обмеженим доступом, нормативно-правових актів, які регулюють професійну діяльність у цій сфері, та створює комплексне, системне уявлення про майбутню професію.

Вивчаючи навчальну дисципліну "Організаційно-правові основи захисту інформації з обмеженим доступом", студенти повинні знати:

- сутність державної інформаційної політики;
- основні принципи інформаційних відносин;
- місце інформації з обмеженим доступом у системі інформації;
- основи загальнодержавної та внутрішньоорганізаційної системи захисту інформації з обмеженим доступом;
- компетенцію органів державної влади, місцевого самоврядування та їхніх посадових осіб у сфері охорони інформації з обмеженим доступом;
- компетенцію СБ України у сфері охорони інформації з обмеженим доступом;
- поняття, види інформації з обмеженим доступом;
- відповідальність за порушення законодавства про інформацію з обмеженим доступом;
- систему охорони інформації з обмеженим доступом, основні організаційно-правові заходи охорони інформації з обмеженим доступом;

- основи технічного, криптографічного захисту інформації;
- роль і місце фахівця з організації захисту інформації з обмеженим доступом у системі підготовки кадрів України.

Підготовлений у НА СБ України фахівець може займати такі первинні посади (за ДК 003:2010. Національний класифікатор України. Класифікатор професій):

- фахівець з організації захисту інформації з обмеженим доступом;
- фахівець із режиму секретності;
- інспектор з організації захисту секретної інформації.

Такий спеціаліст організовує та проводить роботу із захисту інформації з обмеженим доступом, покладену на підрозділ, забезпечує виконання вимог керівних й інших документів із питань захисту інформації з обмеженим доступом; організовує діяльність структурних підрозділів підприємств, установ, організацій усіх форм власності з метою забезпечення цілісності, доступності, конфіденційності інформації з обмеженим доступом; координує організаційно-правовий, технічний, криптографічний захист інформації з обмеженим доступом на підприємстві; розробляє і здійснює заходи для забезпечення перепускного і внутрішньооб'єктового режиму, охорони організації, підприємства, контролює їх виконання; розробляє та здійснює конкретні заходи для запобігання розголошенню й витоку, незаконній модифікації, знищенню інформаційних ресурсів різних суб'єктів інформаційної діяльності; здійснює в підрозділах профілактичну роботу з усіма категоріями працівників із питань додержання вимог режиму охорони державної, комерційної, банківської таємниці, під час роботи з інформацією з обмеженим доступом; на підставі обґрунтованих пропозицій фахівців структурних підрозділів організації, підприємства і разом із цими фахівцями формує номенклатуру посад працівників, котрі підлягають оформленню на допуск до секретної інформації; вивчає та аналізує окремі напрями виробничо-технічної, науково-дослідної, дослідно-конструкторської й іншої діяльності організації, підприємства з метою виявлення та закриття можливих каналів витоку інформації з обмеженим доступом; бере безпосередню участь у проведенні службових розслідувань за фактами втрати та розголошення інформації з обмеженим доступом, порушення внутрішньооб'єктового й перепускного режиму; бере участь у розробленні та забезпеченні конкретних заходів охорони режимних підрозділів (приміщень, будівель тощо) і сховищ носіїв секретів, визначенні ефективності інженерно-технічних засобів охорони; забезпеченні підрозділу новітніми технічними засобами захисту інформації.

Пропонований підручник сприятиме засвоєнню організаційно-правових основ захисту інформації й розрахований на студентів, які здобувають професію за напрямом підготовки 160103 "Організація захисту інформації з обмеженим доступом".

РОЗДІЛ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ ЯК СТРАТЕГІЧНА ОСНОВА ОРГАНІЗАЦІЙНИХ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. ОСНОВНІ ВИЗНАЧЕННЯ, КАТЕГОРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇХНІЙ ЗМІСТ, ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ

Інформаційна індустрія нині перетворилася на один із секторів національної економіки, який бурхливо розвивається, а інформаційна сфера стає однією з найважливіших складових життєдіяльності нашого суспільства. Утім, необхідно враховувати, що інтенсивний розвиток інформаційних технологій, цілеспрямований рух України до створення національної інформаційної інфраструктури та її приєднання до європейської й загальносвітової глобальної інфраструктури сприяє посиленню небезпеки несанкціонованого втручання в роботу інформаційних і телекомунікаційних систем України.

Це зумовлює виняткове значення інформаційної безпеки, особливо в умовах широкої інформатизації всіх сфер діяльності громадянина, суспільства і держави; наслідки неправильної роботи інформаційних систем керування енергоресурсами країни, транспортом – повітряним, наземним – відомі.

Існує *два аспекти* вивчення *інформаційної безпеки в контексті національної безпеки.*

1. *Інформаційна безпека* – самостійний елемент національної безпеки будь-якої країни.

2. *Інформаційної безпека* – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т. д. У цьому складність розгляду проблематики інформаційної безпеки: часто предметом аналізу стає тільки одна галузь, наприклад сфера масової інформації, а інші лишаються поза увагою.

Зазначимо, що стрімкий і глобальний розвиток інформаційної сфери, сучасних інформаційних технологій значною мірою впливає на політичну, економічну, соціокультурну, оборонну та інші складові процесів розвитку суспільства й держави, а інформаційні ресурси в сучасних умовах стають системоутворювальним фактором їхньої життєдіяльності.

В умовах науково-технічного прогресу та переходу до постіндустріального суспільства ефективність системи державного управління національними інформаційними ресурсами і їхнім захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи державного управління цими процесами призводять до завдавання непоправних збитків суспільству й державі.

Тому сьогодні спостерігається особливо посилена увага до проблем інформаційної безпеки в будь-якій державі. Основні причини зростання значущості інформаційної безпеки в порівнянні з іншими складовими системи національної безпеки такі:

- розвиток інформаційних технологій привів до якісних та кількісних змін у змісті національних інтересів, національної й міжнародної безпеки, методах їхнього забезпечення. Сьогодні важливою складовою національних інтересів України є активне формування “інформаційного суспільства” і входження національної інформаційної інфраструктури в глобальну інформаційну інфраструктуру;
- інформаційна сфера, яка становить специфічну галузь діяльності суб’єктів громадського життя, пов’язану зі створенням, збереженням, поширенням, переданням, обробленням і використанням інформації, стала однією з найважливіших складових сучасного суспільства. Інтенсивний розвиток інформаційної інфраструктури, процеси глобалізації, що особливо яскраво виявляються в інформаційній сфері, інформатизація практично всіх сторін громадського життя, діяльності органів державної влади й управління істотно посилили залежність ефективності функціонування суспільства та держави від стану інформаційної сфери;
- інформаційна інфраструктура й інформаційні ресурси стають ареною міждержавної боротьби за світове лідерство. Тому цілеспрямований рух України до створення власної інформаційної інфраструктури й інтеграції до європейської та світової інфраструктури призводить до посилення небезпеки несанкціонованого втручання в роботу інформаційних і телекомунікаційних систем держави;
- демонополізація послуг зв’язку, створення ринку послуг і засобів зв’язку привели до появи на території України мереж та систем зв’язку, які належать акціонерним товариствам і приватним особам. Простежується певна економічна залежність операторів зв’язку від іноземних інвесторів. Різноманіття мереж і служб зв’язку зумовлює проблему координації зусиль щодо створення, розвитку й забезпечення інформаційної безпеки мереж зв’язку з урахуванням потреби зміцнення обороноздатності держави;

- індустрія інформатизації, телекомунікації та зв'язку, інформаційних послуг на сучасному етапі соціально-економічного розвитку є однією із сфер економіки, що найбільш динамічно розвивається, здатна конкурувати за прибутковістю з паливно-енергетичним комплексом, автомобіле- й авіабудуванням, іншими галузями виробництва. Більше того, інформаційна індустрія стала визначати наукоємність продукції, її конкурентоспроможність на світовому ринку.

З огляду на зазначене, забезпечення національних інтересів України в інформаційній сфері стає важливим фактором національної безпеки.

Дослідження будь-якої проблематики завжди починається з визначень. За деякими даними, налічується шістнадцять визначень інформаційної безпеки, за нашими підрахунками – понад тридцять. І це не межа, адже інформаційна безпека багатоаспектна і в процесі її вивчення виникають нові проблеми.

Очевидно, що інформаційна безпека в демократичному суспільстві повинна забезпечувати, з одного боку, вільний доступ до інформації, з іншого – її захист. Основні принципи поширення інформації в демократичній державі такі:

1. Вільний доступ громадян до публічної інформації.
2. Збереження суспільних даних.
3. Безпека держави і громадян.

Таким чином, під інформаційною безпекою слід розуміти такий стан захищеності життєво важливих інтересів особистості, суспільства й держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації. Уважаємо, таке визначення тією чи іншою мірою охоплює практично всі сфери інформаційної взаємодії суб'єктів у суспільстві, державі й усіх соціальних утвореннях. При цьому під інформаційною взаємодією слід розуміти процес створення, накопичення, опрацювання, збереження й поширення інформації. Важливого значення набувають визначення інформаційного простору та інформаційної інфраструктури. Вони несуть, як і перша дефініція, методологічне навантаження з погляду побудови політики інформаційної безпеки держави.

Під інформаційним простором пропонується розуміти певне середовище, у якому здійснюється формування, збирання, збереження, опрацювання й поширення інформації. При цьому свідомо не вжито термін "використання інформації", щоб вивести з інформаційного простору людину як суб'єкта, котрий споживає інформацію.

Інформаційна інфраструктура – це єдність таких компонентів: системи виробництва інформаційних продуктів, системи доставки їх до споживача, системи виробництва засобів виробництва інформаційних продуктів та їх доставки, системи виробництва інформаційних технологій, системи накопичення й збереження інформаційного продукту або інформаційного ресурсу, тобто системи сервісного обслуговування елементів інфраструктури і, нарешті, системи підготовки кадрів.

Основою цього визначення є принцип демократичної держави. Він полягає в тому, що держава повинна забезпечити кожному суб'єктові інформаційних відносин право на одержання повної, достовірної та своєчасної інформації.

Наступний принцип – ніхто не має права порушити інтереси суб'єкта інформаційних відносин шляхом інформаційного впливу. Власні інтереси мають поєднуватися з інтересами оточення.

Основними принципами забезпечення інформаційної безпеки України є:

- пріоритет прав людини;
- верховенство права;
- примат договірних (мирних) засобів у вирішенні інформаційних конфліктів;
- адекватність заходів захисту національних інтересів України в інформаційній сфері реальним та потенційним загрозам;
- громадський контроль за діяльністю органів державної влади, які входять до системи забезпечення інформаційної безпеки України;
- додержання балансу інтересів особи, суспільства, держави, їхня взаємна відповідальність;
- чітке розмежування повноважень та функцій органів державної влади в системі забезпечення інформаційної безпеки України.

1.2. НАЦІОНАЛЬНІ ІНТЕРЕСИ В ІНФОРМАЦІЙНІЙ СФЕРІ. ІНФОРМАЦІЙНІ ЗАГРОЗИ

Виділяють чотири складові національних інтересів України в інформаційній сфері.

Перша складова національних інтересів (СНІ1) – дотримання конституційних прав і свобод людини та громадянина у сфері одержання інформації та користування нею, забезпечення духовного відновлення України, збереження й

зміцнення моральних цінностей суспільства, традицій і гуманізму, культурного та наукового потенціалу держави.

Друга складова (СНІ2) – інформаційне забезпечення державної політики України.

Третя складова (СНІ3) – розвиток сучасних інформаційних технологій, вітчизняної інформаційної індустрії засобів інформатизації, телекомунікації й зв'язку, забезпечення потреб внутрішнього ринку продукцією і вихід цієї продукції на світовий ринок, забезпечення накопичення, збереження та ефективного використання вітчизняних ресурсів.

Четверта складова національних інтересів (СНІ4) – захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем на території України.

Найбільш небезпечні загрози інформаційній безпеці такі:

1. Слабке входження України у світове інформаційне поле, недостатня кваліфікованість й активність її інформаційних служб.

Уявлення про Україну формують у світовому інформаційному полі засоби масової інформації та агентства інших держав, виходячи із власних геополітичних, політичних, військових, економічних інтересів. Таким чином, виникає спотворений образ України, її зовнішньої та внутрішньої політики, що негативно впливає на її міжнародний авторитет. Крім того, Україна не може протистояти інформаційно-пропагандистським акціям інших держав, які через вторгнення в її інформаційний простір намагаються забезпечити свої політичні та економічні інтереси, що створює загрозу національній безпеці країни.

2. Використання політичними силами засобів масової інформації.

Для реалізації своїх планів певні політичні партії, рухи, громадські об'єднання України використовують вітчизняні засоби масової інформації, проводячи пропагандистські кампанії, поширюючи спеціально підібрану інформацію тощо. У боротьбі за посилення свого впливу, а також із метою реалізації вузькопартійних цілей вони забувають про необхідність збереження в Україні загальнонаціональної стабільності й злагоди, нехтують чинним законодавством. Відбувається нав'язування за допомогою засобів масової інформації певних політичних кліше, а також штучне загострення ситуації, роздмухування пристрастей, застосування погроз, закликів до помсти чи реваншу, використання однобічної, спеціально відібраної інформації.

3. Вплив міжконфесійних конфліктів.

Проблеми й конфлікти на релігійному ґрунті призводять до появи в інформаційному просторі України небезпечних явищ – погроз, нацьковування одних віруючих на інших, поширення необ'єктивної інформації, яка здатна загострити ситуацію.

4. Некомпетентність працівників державних органів і установ.

Цей чинник негативно впливає на якість і спрямованість інформаційного матеріалу й тим самим створює можливість соціально-політичних конфліктів; діє через неповну, запізнілу інформацію.

5. Недостатній професійний рівень працівників засобів масової інформації.

У засобах масової інформації, друкованій продукції з'являються матеріали, що пропагують вседозволеність, аморальність, нехтування патріотичними та громадянськими обов'язками. Це може призвести до загострення соціально-економічного й політичного становища.

6. Вплив на засоби масової інформації організованої злочинності, мафіозних структур.

Злочинні угруповання намагаються перешкодити розбудові потужної демократичної держави, створити в Україні умови всеосяжної корумпованості тощо. З'являється інформаційна продукція, що підриває авторитет і довіру до правоохоронних органів, державних структур, пропагує кримінальні "цінності".

7. Недосконалість технічного захисту інформаційного простору України.

У зв'язку з тим, що оброблення інформації, у тому числі й такої, що становить державну таємницю, здійснюється з використанням найсучасніших технічних засобів, виникає необхідність у її технічному захисті.

До напрямів протидії загрозам у сфері інформаційної безпеки відносять:

- організаційні заходи;
- заходи щодо захисту прав і свобод людини та громадянина;
- завдання розвитку матеріально-технічної бази системи інформаційної безпеки особи, держави й суспільства;
- науково-практичну роботу із забезпечення інформаційної безпеки;
- удосконалення нормативно-правової бази системи інформаційної безпеки.

Ключовою проблемою інформаційної безпеки є оцінювання відповідності інформаційного простору держави потребам її громадян, попиту та пропозиції інформаційних послуг у наближених до користувачів місцях та в зручний для них час.

Історичний досвід показує, що країни, які не спромоглися своєчасно поповнити національний інформаційний простір більш ефективними технологіями,

сповільнили свій економічний розвиток. І навпаки, держави з потужним інформаційним потенціалом швидко відновлювали свою роль у світовому розподілі сфер впливу навіть після воєнних поразок. Тому розроблення новітніх технологій, що здатні істотно підвищити як адекватність віддзеркалення реальності, так і продуктивність інформаційної діяльності в суспільстві, є нагальною потребою, що визначає можливості захисту національних інтересів.

Перспективи розвитку України як суверенної держави передусім пов'язані із створенням на її території більш досконалого інформаційного простору порівняно з успадкованим та наданням цьому простору властивостей, які притаманні постіндустріальним країнам.

Основні причини недосконалості інформаційного простору України такі:

1. Нагальні потреби управління національним виробництвом економічними методами перевищують можливості структурного й змістового наповнення інформаційного простору.

2. При подоланні інформаційної кризи наголошується не на розвиткові інформаційної периферії, яка повинна реєструвати та зберігати поточні записи у формі, придатній для оперативного використання, а на побудові аналітичних, ситуаційних та інших центрів, призначених споживати, а не створювати інформацію.

3. Національний інформаційний простір не налаштований на реєстрацію в безпаперовій формі фактографічних записів, які віддзеркалюють поточний кількісний вимір властивостей об'єктів.

З'явився великий обсяг нової інформації, наприклад житлові субсидії, персоніфіковані майнові сертифікати, декларації про доходи громадян, акції підприємств, митне обслуговування кордонів тощо, яка все більше завантажує інформаційний простір і відволікає значну кількість людей від виробничої сфери. Вона потребує відповідного перерозподілу фінансових та інших ресурсів. Поряд із цим, продовжують відтворюватися умови, за яких подальше споживання детальної інформації – продукту їхньої діяльності – може бути організоване лише як ієрархічна вертикаль відповідними посадовими посередниками шляхом виконання великих обсягів рутинних робіт за регламентованими механізмами узагальнення та звітування. На кожному щаблі узагальнення інформація, як правило, зазнає випадкових (або невипадкових) спотворень у приватних чи відомчих інтересах навіть при бездоганній відповідності записів базового рівня подіям реальності. Інформаційний простір України штучно розподіляється на сукупність

не узгоджених за семантичними ознаками й технологіями відомчих інформаційних анклавів, які безсистемно нашаровуються один на одного. Все це розпорошує ресурси, не забезпечує верифікацію записів базового рівня на засадах інтересів усіх суб'єктів суспільства. Такий стан інформаційного простору фактично робить органи управління вищих рівнів заручниками інформаційної діяльності підлеглих. Саме з цієї причини аналітичні матеріали, які використовуються при прийнятті рішень, тяжіють до макроекономічних показників або результатів соціологічних опитувань, що свідчить про ускладнене отримання або повну відсутність детальних записів у деяких сегментах економіки держави.

1.3. ДЕРЖАВНА ПОЛІТИКА В ІНФОРМАЦІЙНІЙ СФЕРІ. ХАРАКТЕРИСТИКА НАПРЯМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації. Головними напрямами та способами здійснення державної інформаційної політики є:

- забезпечення доступу громадян до інформації;
- створення національних систем і мереж інформації;
- зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;
- забезпечення ефективного використання інформації;
- сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
- створення загальної системи охорони інформації;
- сприяння міжнародному співробітництву в галузі інформації й гарантування інформаційного суверенітету України.

Державну інформаційну політику розробляють і проводять органи державної влади загальної компетенції, а також відповідні спеціальні інституції.

Державна інформаційна політики має створювати умови для реалізації конституційного права громадян своєї держави вільно отримувати й використовувати інформацію для вирішення таких важливих завдань, як створення націо-

нального інформаційного простору, включення його до світового інформаційного простору на засадах забезпечення інформаційного суверенітету та інформаційної безпеки й формування демократично орієнтованої свідомості.

Головною метою державної інформаційної політики стосовно національних інформаційних ресурсів є створення необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку й забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життєдіяльності громадянина, суспільства та держави.

Функції державного управління інформаційними ресурсами такі:

- розроблення й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та удосконалення механізмів реалізації норм чинного законодавства;
- визначення і здійснення повноважень державних органів, органів регіонального й місцевого самоврядування щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;
- розроблення та реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур та недержавного сектору у сфері формування й використання інформаційних ресурсів за умови координації діяльності згаданих інституцій;
- розроблення й реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів;
- здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) в процесі діяльності державних органів, органів регіонального та місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності;
- уведення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності державних органів, органів регіонального та місцевого самоврядування, державних підприємств і організацій для надання їх у вільний доступ громадянам й організаціям (крім інформаційних ресурсів, що мають відомості, віднесені до державної таємниці та іншої інформації з обмеженим доступом).

Державна політика в інформаційній сфері загалом та в галузі ІБ зокрема повинна бути спрямована на вирішення таких завдань:

- пом'якшення суперечностей між потребами суспільства в розширенні вільного обміну інформацією й необхідністю збереження деяких регламентованих обмежень на її поширення;
- підтримання необхідного балансу інтересів особи, суспільства та держави в інформаційній сфері, формування на території України конкурентоспроможних вітчизняних інформаційних агентств і ЗМІ;
- зменшення факторів дестабілізації соціально-економічної обстановки в суспільстві шляхом поліпшення забезпеченості прав громадян на доступ до інформації й недопущення маніпулювання інформацією;
- забезпечення реального захисту даних про фізичних осіб (персональних даних), прав громадян на недоторканність приватного життя, особистої та сімейної таємниці;
- унеможливлення витиснення українських інформагентств і ЗМІ з внутрішнього ринку шляхом проведення чіткої державної політики у сфері формування національного інформаційного простору;
- удосконалення системи забезпечення охорони державної таємниці;
- нарощування вітчизняного кадрового потенціалу наукових і виробничих колективів, котрі працюють у галузі створення засобів інформатизації, телекомунікацій, зв'язку й захисту інформації;
- зниження імовірності несанкціонованого доступу до національних інформаційних ресурсів та залежності України від іноземних виробників обчислювальної й телекомунікаційної техніки, програмного забезпечення тощо.

Основні функції держави – формування організаційної структури системи інформаційної безпеки, державних органів забезпечення національних інтересів в інформаційній сфері, обґрунтування функцій цих організацій і вимог до ефективності їхньої діяльності. Значну роль у забезпеченні інформаційної безпеки держави повинні відігравати аналітичні, прогностичні й контрольні функції.

Основні функції системи інформаційної безпеки такі:

- прогнозування, виявлення й оцінювання рівня потенційних загроз інформаційній безпеці, оцінювання наслідків їхньої реалізації;
- аналіз дестабілізаційних факторів в інформаційній сфері, причин їхньої появи й загострення;

- запобігання та ліквідація наслідків реалізації виявлених загроз і дестабілізаційних факторів, зменшення їхнього впливу на процеси забезпечення національних інтересів в інформаційній сфері;
- забезпечення реального балансу інтересів, потреб людини, суспільства й держави в обміні інформацією та необхідними обмеженнями на поширення інформації.

1.4. ХАРАКТЕРИСТИКА, ОСНОВНІ ЗАСОБИ ЗДІЙСНЕННЯ МОЖЛИВИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ (ОПЕРАЦІЙ)

Інформаційна війна може вестися як у воєнний, так і в мирний час. При цьому використовуються такі види інформаційної зброї:

- засоби пропагандистсько-психологічного впливу (через пресу, телебачення, радіо, інтернет, інші канали);
- засоби програмно-математичного впливу (комп'ютерні віруси, логічні "бомби", засоби придушення комп'ютерних мереж тощо);
- засоби психологічного впливу (голографічні зображення в атмосфері, синтезатори голосів відомих лідерів, "вірус-убивця" № 666 та ін.);
- психотронна зброя (методи парапсихології й біоенергоінформатики, програмування поведінки (зомбування) особистості тощо);
- засоби, засновані на впливі полів різної природи (радіоелектронне придушення, акустична зброя, електромагнітні ураження шляхом використання випромінювання хвиль різної довжини й т. ін.).

Комплекс проблем, зумовлених можливістю втягнення України в інформаційну війну, вимагає розроблення методологічних основ інформаційної безпеки як фундаменту для формування й реалізації політики забезпечення національних інтересів на інформаційному рівні та створення національної системи інформаційної безпеки України. У цьому випадку під методологічними основами інформаційної безпеки слід розуміти єдність концептуальних, теоретичних і технологічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної й суспільної діяльності (політичної, економічної, соціальної, військової, екологічної, духовної та ін.), а також формування, циркуляція, накопичення й використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління у всіх різновидах діяльності тощо).

Тут варто наголосити на актуальності проблеми безпеки, її технологічних аспектів при інформаційно-аналітичному забезпеченні органів державного управління. Останнім часом сформувалося поняття “інформаційний фантом в управлінні”, сутність якого полягає в істотному підвищенні ролі аналітиків і радників у державному управлінні. Від якості, відповідності реальній ситуації підготовлених ними аналітичних документів (інформаційно-аналітичних оглядів, довідок) залежить ефективність прийнятих на їхній основі державних рішень.

Об’єктом методології інформаційної безпеки виступають інформаційні процеси в соціо- й соціо-технічних системах, предметом – дослідження механізмів інформаційного впливу на особистість, суспільство і державу, а також способів, методів, засобів і каналів реалізації загроз національним інтересам на інформаційному рівні. Головне завдання методології інформаційної безпеки – створення науково-методичних основ своєчасного виявлення потенційних інформаційних загроз у різних сферах діяльності та механізмів їх реалізації, а також попередження й нейтралізації.

Убачаться, що ядром методології інформаційної безпеки є поняття інформаційної боротьби, триєдина сутність якого відображена в таких взаємопов’язаних визначеннях:

- інформаційна боротьба – це об’єктивно існуюча форма прояву відносин між суб’єктами при вирішенні ними завдань, що містять елементи конфліктності різної природи на інформаційному рівні;
- інформаційна боротьба – це наука про механізми, прийоми, методи й засоби інформаційного протиборства;
- інформаційна боротьба – це комплекс заходів, спрямованих на вирішення завдань, що стоять перед суб’єктом, шляхом застосування методів і засобів боротьби.

Існування інформаційної боротьби зумовлене як наявністю інформації, так і природністю процесу використання її властивостей для вирішення різних завдань. Із визначення інформаційної боротьби випливає, що вона, на відміну від інформаційної війни, по суті неагресивна. До її методів і засобів удаються, наприклад, із метою обґрунтування доцільності впровадження у виробництво технологічних рішень. Інформаційна боротьба має свої цілі, завдання, закономірності, способи, методи й засоби ведення.

Метою інформаційної боротьби є забезпечення переваги однієї сторони над іншою у вирішенні певних завдань за рахунок досягнення вищості на інформаційному рівні. Цю мету можна досягти різними шляхами, а саме:

1. Цілеспрямованим добуванням інформації про поточну ситуацію з жорсткими вимогами щодо її своєчасності, якості, обсягу, повноти й темпів оновлення, оцінюванням на основі цієї інформації політичної (військово-політичної, військової, економічної, екологічної та ін.) ситуації. Вирішення цього комплексу завдань ускладнюється умовами інформаційної протидії. При цьому аналізована інформація відзначається непевністю об'єктивного й суб'єктивного характеру, неповнотою щодо одних аспектів і надмірністю щодо інших, суперечливістю, наявністю частково знищеної та спотвореної інформації, зокрема дезінформації.

2. Цілеспрямованим і комплексним впливом на свідомість, інформаційні ресурси країни на всіх етапах їхнього виробництва, поширення і використання, а також на інфосферу машинно-технічних систем протиборчої (конкуруючої) сторони з метою нав'язування "бажаних" рішень і "керування поведінкою". При цьому особливої значущості набуває не стільки руйнівна, скільки цілеспрямована впливова дія із спотворення змісту інформації для забезпечення своїх інтересів у різних сферах діяльності особи, суспільства, держави. У такому контексті надзвичайно важлива можливість використання інформації (інформаційних потоків) як ефективного засобу формування позитивного іміджу України на міжнародній арені та зняття політичної, економічної, соціальної, військово-політичної, військової напруженості у відносинах з іншими країнами, а також у регіонах держави.

3. Захист власних інформаційних ресурсів та інформаційної сфери машинно-технічних систем від впливу на них протиборчої сторони. Не применшуючи важливість вирішення завдань технічного захисту інформації для забезпечення її конфіденційності, наголосимо на особливій значущості захищеності змісту інформації від навмисного його спотворення або зміни, в тому числі механізмів виявлення дезінформації. До цього ж комплексу входять також завдання відновлення цілісності змісту частково зруйнованої або перекрученої текстової природно-мовної інформації.

Отже, соціальними об'єктами інформаційної боротьби є індивід (особистість), соціальні групи, суспільство, держава. А якщо точніше – свідомість і підсвідомість індивіда, колективна свідомість, а також інформаційні ресурси й інфосфера машинно-технічних систем.

Основні проблеми ефективного вирішення завдань інформаційної боротьби пов'язані з науково-методичним забезпеченням цих завдань та їх інструментально-технологічною підтримкою. Як уже зазначалося, ядром методологічного підґрунтя інформаційної безпеки є інформаційна боротьба, а теоретичною основою – інформатика як наука про інформаційні процеси в соціо- й соціо-технічних системах, особливо один із найважливіших її розділів – теорія інформодинаміки.

ЗАПИТАННЯ І ЗАВДАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Розкрийте основні категорії інформаційної безпеки та принципи їх забезпечення.
2. Охарактеризуйте національні інтереси в інформаційній сфері й інформаційні загрози.
3. Визначте сутність державної політики в інформаційній сфері.
4. Розкрийте напрями забезпечення інформаційної безпеки.
5. Проаналізуйте можливі інформаційні впливи (операції), основні засоби їхнього здійснення.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гончаренко О.М. Пріоритети та засади формування інтегральної стратегії національної безпеки на перспективу / О.М.Гончаренко // Стратегічна панорама. – 1998. – № 1–2.
2. Гриняев С. Концепция ведения информационной войны в некоторых странах мира / С.Гриняев // ЗВО. – 2002. – № 2.
3. Данільян О.Г. Національна безпека України: сутність, структура та напрямки реалізації / О.Г.Данільян, О.П.Дзьобань, М.І.Панов. – Х. : Фоліо, 2002. – С. 5–22.
4. Дергачов О. Небезпека як атрибут державності / О.Дергачов // Політична думка. – 1997. – № 1.

5. Закон України “Про основи національної безпеки України” від 19.06.2003 р.

6. Конституція України. – К. : Просвіта, 1996.

7. Концепція (основи державної політики) національної безпеки України, схвалена ВР України 16 січня 1997 року // Національна безпека України, 1994–1996 рр. : наук. доповідь НІСД / Редкол.: О.Ф.Бєлов (голова) та ін. – К. : НІСД, 1997. – С. 184–195.

8. Косевцов В.О. Національна безпека України: проблема та шляхи реалізації пріоритетних національних інтересів / В.О.Косевцов, І.Ф.Бінько. – К. : НІСД, 1996. – 77 с. – (сер. “Національна безпека”).

9. Косевцов В.О. Національна безпека України: теорія, реальність, прогноз. / В.О.Косевцов. – К. : ЦМБСС, 2000. – 92 с.

10. Крысько В. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В.Крысько ; под ред. А.Е.Тараса. – Мн. : Харвест, 1999. – 447 с.

11. Лисичкин В.А. Третья мировая информационно-психологическая война / В.А.Лисичкин, Л.А.Шелепин. – М. : ИСПИ АСН, 2000.

12. Національна безпека України 1994–1996 рр. – К. : НІСД, 1997.

13. Почепцов Г.Г. Информационные войны / Г.Г.Почепцов. – М. : “Рефл-бук”, 2000.

14. Про державну таємницю : Закон України від 21.09.1999 р. // Голос України. – 1999. – 26 жовтня.

15. Про інформацію : Закон України від 11.05.2004 р. // Голос України. – 2004. – 26 травня.

16. Ситник Г.П. Розвиток концептуальних підходів щодо забезпечення національної безпеки – ключова проблема державного управління / Г.П.Ситник // Збірник наукових праць УАДУ. – 2003. – Вип. 1. – С. 265–278.

17. Стратегія національної безпеки України в контексті досвіду світової спільноти : матер. міжнар. конф. – К. : НІСД, 2001. – 222 с.

РОЗДІЛ 2

ІСТОРИЧНИЙ ДОСВІД ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

2.1. ЗАХИСТ ІНФОРМАЦІЇ НА ТЕРИТОРІЇ УКРАЇНИ В СКЛАДІ РОСІЙСЬКОЇ ІМПЕРІЇ (XVII – поч. XX ст.)

2.1.1. ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ТЕРИТОРІЇ УКРАЇНИ В XVII-XIX СТ.

Звернімося до історичного досвіду захисту інформації з обмеженим доступом в Україні. Уряд Б.Хмельницького, поряд із активним будівництвом держави, вчасно вживав необхідних заходів у сфері захисту військово-політичної інформації від ворожої Польщі. Завдяки цьому вдавалося зберігати в таємниці плани найголовніших військових кампаній, розкривати змови, організовані ворожими шпигунами, протидіяти спробам панівних кіл Речі Посполитої спровокувати міжусобну боротьбу в українському суспільстві, внести розкол у лави національно-патріотичних сил.

У Запорізькій Січі також велику увагу приділяли захисту військової інформації, оскільки вона була військовим об’єднанням й, очевидно, осавул і писар, які відали прикордонними роз’їздами та управляли розкиданими по степових слободах і хуторах козаками (т. зв. “сиднями”), займалися її захистом. На роз’їзди покладалася розвідка становища за межами кордону, про результати якої повідомлялося в Січ.

Фактично можна зазначити, що в умовах розбудови держави формувалася й організація захисту інформації. Наступні гетьмани України І.Виговський, Ю.Хмельницький, П.Тетеря, І.Брюховецький, П.Дорошенко, Д.Многогрішний, І.Мазепа, І.Скоропадський, П.Полуботок, К.Розумовський теж приділяли увагу захисту військово-політичних планів країни.

Активні дипломатичні відносини з Кримом вів І.Виговський, перебуваючи на посту писаря за часів Б.Хмельницького і пізніше – на посту гетьмана. Свого часу Б.Хмельницький викупив І.Виговського з полону в хана Іслам-Гірея III.

Відтоді він присягнув гетьману і став у нього на службі. З ім'ям І.Виговського зокрема пов'язують одну з провідних ролей у створенні системи захисту інформації на тогочасних українських землях, а саме – спеціальних органів, які займалися захистом військово-політичної інформації – розвідки та контррозвідки України. Перебуваючи на посаді писаря, він керував підрозділом розвідників у кількості 2000 осіб. Його агентом у Криму був татарський перекладач великого візира Сефер Кази-аги, який під час сепаратних польсько-кримських переговорів під Кам'янець-Подільським у грудні 1653 року передав генеральному писарю відомості про їхній зміст.

Позаяк, саме писарю було доручено захист військово-політичної інформації в державі та здобуття найбільш важливих відомостей через драгоманів (товмачів).

І.Мазепа доклав особливих зусиль у захисті військово-політичної інформації. Гетьман кілька років вів таємні переговори з королем Швеції і практично спромігся захистити, уберегти від розголошення інформацію про зміст цих відносин. Навіть цар не знав про суть переговорів, хоча його неодноразово попереджали наближені до гетьмана особи. Очевидно, Мазепа володів ремеслом захисту інформації. Передусім до важливої інформації він надавав доступ вузькому колу наближених осіб. Полковникам не довіряв, оскільки знав, що більшість із них і їхнє оточення передасть ці відомості до Москви. Переговори, які вів Мазепа з Карлом XII, закінчились таємною, підписаною між "королем шведів, готів і вандалів і гетьманом України угодою" про боротьбу з Росією.

Свідченням того, що і гетьманська, й царська влада докладали максимум зусиль, щоб захистити інформацію, є правові джерела цього періоду, які закріплюють кримінальну відповідальність за розголошення такого виду інформації, як державна таємниця. Так, у р. 2, 7 ст. 2 Соборного уложення 1649 р. зазначається: "Кто при державе царского Величества с недруги учнет дружится, и советными грамотами ссылатися, и помочь им всячески чинити… такова казнити смертию"; стаття 20 цього ж документа зазначає: "Кто, будучи на государевой службе в полках, учнет изменою из полков переезжати в неприятельские полки там и сказывати про вести и про государевых ратных людей, … такова переезщика казнити смертию, провести против неприятельских полков, а поместья его и вотчины и животы взяти на государя".

На нашу думку, звернення до законодавчого закріплення покарання за розголошення такого виду інформації, як державна таємниця, є одним з елементів захисту інформації, використовуваним у ті часи.

Ще в одному правовому джерелі, Генеральному регламенті (Статут державних колегій) 1720 р., у р. 50 ст. 4 зазначається: "Когда кто постороннему, кому не надлежит, тайности колегины сообщит, резолюции, прежде времени объявит протоколы … таковым за преступление надлежит чинить смертная казнь или вечная на галеру ссылка с вырезанием ноздрей и отнятием всего имения". Це джерело теж підтверджує раніше висунуту тезу.

У правовому джерелі XVIII ст., яке діяло на території гетьманської України, теж знаходимо підтвердження захисту найважливішого виду інформації – державної таємниці, що законодавчо було закріплене в "Правах, за якими судиться малоросійський народ" 1722 р. Зокрема в р. 3 арт. 2 п. 6 ішлося: "Кто бы с неприятелем согласие какое имел, письмами с ним пересылаясь или посланников посылая, … либо, оберегая в чем неприятеля, пособлял оному, открывая государя своего тайную волю, намерения, уставы и дела, … такового смертию казнить, четвертовать".

Це ж саме зазначено в р. 3 гл. 2; р. 5 гл. 10 ст. 290 "Уложення про покарання кримінальні та виправні" 1743 р.: "Кто из Российских поданных откроет какую-либо государственную тайну иностранным, хотя и не враждебным с нею державам, или сообщит им планы Российских крепостей или иных укрепленных мест, или гаваней, портов, арсеналов, или публикует сии планы дозволения правительства, тот за сие приговаривается к лишению всех прав состояния и к ссылке на поселение в отдаленных местах Сибири"; ст. 292 – "кто из Российских поданных будет иметь тайную переписку с поданными неприязненных государств, хотя и без намерения вредить своему отечеству, но однако же столь неосторожно и нескромно, что неприятель может сообщаемыми им в сей переписке сведениями воспользоваться для успеха своих предприятий против России, тот за сие приговаривается к заключению в крепости на время от 6 месяцев до 1 года"; ст. 468 – "за разглашение дел, подлежащих тайне и недозволенное сообщение кому-либо бумаг, отмеченных надписью секретно, виновный подвергается, смотря по важности дела и происшедшим или долженствовавшим произойти от того последствиям, более или менее вредным, или отрешению от должности, или исключению из службы, или же сверх того, и заключению в

смирительном доме на время от 6 месяцев до 1 года", ст. 469 – "за открытие должностным лицом какому-либо постороннему принадлежащего правительству или частному человеку секрета, для производства изделий, работ, машин, медицинских или иных составов и т.п., виновный, сверх вознаграждения за причиненные им убытки, подвергается отрешению от должности и заключению в тюрьме на время от 6 месяцев до 1 года", ст. 470 – "за открытие с намерением государственных тайн иностранным правительствам, виновный подвергается наказаниям, определенным за государственную измену в статьях 288 и 290 сего Уложения. За обнаружение государственных тайн без намерения, а по неосторожности, виновный в том исключается из службы, и, смотря по важности дела и тайны и другим обстоятельствам, более или менее увеличивающим или уменьшающим вину его, приговаривается к заключению в крепости на время от 6 месяцев до 1 года".

У Кримінальному уложенні 1845 р., розділ 4, 37, ст. 111 – "виновный в опубликовании или сообщении правительству или агенту иностранного государства, не находящегося в войне с Россией, плана рисунка, документа копии с оных или сведения, которые заведомо долженствовали в видах внешней безопасности России хранится в тайне от иностранного государства, наказывается каторгой не свыше 8 лет. Если сии план, рисунок, документ, копия с оных или сведения вверены были виновному по службе, или если он получил их или ознакомился с ними по своему служебному положению, или если ему объявлено было воспрещение публиковать или сообщать оные, то он наказывается срочной каторгой", ст. 653 – "служащий, виновный в оглавлении сделавшихся ему известными по службе или вследствие злоупотребления им служебными полномочиями и долженствующих заведомо хранится в тайне правительственных распоряжений, сведений или документов, наказывается арестом. Если оглашенное могло причинить важный вред для порядка управления или для казенного, общественного или частного интереса, то виновный наказывается заключением в тюрьме. Если же оглашенное виновным составляло тайну, касающуюся внешней безопасности России, то он, если не подлежит наказанию за измену, наказывается заключением в исправительном доме или заключением в крепости".

У законі Російської імперії "Про державну зраду шляхом шпигунства" 1912 р., ст. 111 – "виновный в опубликовании, сообщении или передаче другому лицу, в интересах иностранного государства, без надлежащего уполномо-

чия: долженствующихся сохранится в тайне сведений или предметов, касающихся внешней безопасности России или вооруженных ея сил или сооружений, предназначенных для военной обороны страны; плана, чертежа, рисунка либо иного изображения или описания российского укрепленного места, установленных района либо эспланады онаго, военного судна либо иного сооружения, предназначенного для военной обороны страны, или документа, касающегося мобилизации и вообще распоряжений на случай войны, наказывается: в случае, пунктом 1 сей статьи предусмотренном, – каторгою на срок не свыше 8 лет, а в случае, пунктом 2 сей статьи предусмотренном, – срочною каторгою".

Усі ці приклади свідчать, що із середини XVII ст. в Росії та на українських землях у її складі велика увага приділялася захисту інформації. Причому держава була зацікавлена в надійному захисті державних секретів, про що свідчать жорстокі покарання тих, хто шкодив інтересам держави, розголошуючи найважливіші військово-політичні відомості. Тому напевно в цей період починає розвиватися система захисту інформації держави, а саме законодавчі акти, які регламентували захист інформації; з'являються органи таємної поліції, на які було покладено збирання і захист інформації про військово-політичне становище в державі. Разом із цим, оскільки українські землі входили до складу Російської імперії, існували автономні органи влади, очолювані гетьманами, які розробляли власні форми захисту інформації, про які ні цар, ні сусідні держави не повинні були знати.

Із кінця XVIII ст. Україна знов увійшла в бездержавний період існування. На цей час майже на всіх її землях (крім Галичини, Буковини, Закарпаття, які перебували у складі Австро-Угорської імперії) суспільний устрій, управлінські структури, правовий статус станів, верств і соціальних груп було приведено у відповідність до суспільного устрою й державного ладу Росії.

У результаті неодноразових адміністративно-територіальних змін до XIX ст. російський уряд поділив Україну на дев'ять губерній: на Лівобережжі – Слобідсько-Українську (у 1835 р. перейменовану на Харківську), Полтавську й Чернігівську; на Правобережжі – Київську, Волинську і Подільську; на півдні – Катеринославську, Таврійську та Херсонську. Їх організація супроводжувалася посиленням і розгалуженням місцевого адміністративно-управлінського апарату.

Перша чверть XIX ст. характеризувалася створенням системи вищих і центральних державних органів управління. Зумовлені внутрішніми й зовнішніми

обставинами, ці перетворення були також пов'язані з грандіозними планами Олександра I, який, ступивши 1801 р. на престол, видавав себе за ліберала, хоча насправді залишався самодержцем-абсолютистом. Важливою частиною створюваної системи з 1802 р. стали нові органи управління – міністерства (спочатку їх було вісім). На чолі міністерства стояв міністр-єдиноначальник. Діяльність міністрів координував Комітет міністрів – дорадчий орган при імператорі (він же головував на засіданнях Комітету).

У Міністерстві закордонних справ (МЗС) Росії питаннями забезпечення захисту такого виду інформації, як державна таємниця, у сфері зовнішньої політики займалися:

- шифрувальний департамент (організація криптографічного захисту каналів зв'язку);
- посли й консули, на яких був покладений увесь спектр обов'язків, починаючи від підбору технічного персоналу і закінчуючи організацією відправлення дипломатичної пошти.

Наприкінці XIX століття шифрувальна служба МЗС була організована таким чином. При канцелярії міністра діяв шифрувальний департамент із двома відділеннями. Їхні функції полягали у:

- перше відділення – веденні усього шифролистування із закордонними установами (його очолював барон К.І.Таубе);
- друге відділення – дешифруванні чужої дипломатичної переписки.

Спеціального навчального закладу, де б викладали мистецтво криптографії, в Росії не було, і тому чиновниками в шифрувальний департамент, як і в усі інші департаменти міністерства, призначалися не особи з неабиякими знаннями й певними здібностями, а ті, хто закінчив ліцей або юридичний факультет. Отже, з XIX століття в Російській імперії починають створюватися спеціальні органи, до компетенції яких було віднесено розвинутий на той час в усій Європі спосіб захисту інформації – криптографічний. Також починають формуватись організаційно-правові основи захисту інформації, про що свідчать вказані вище документи. Якщо раніше, за часів Київської Русі, держави Б.Хмельницького, ми говорили про захист інформації військово-політичного змісту, щодо особи князя чи гетьмана тощо, то в Російській імперії на рівні держави дбали про захист інформації, яка в разі розголошення могла завдати шкоди державі або її інтересам. Цю інформацію стали називати державною таємницею.

2.1.2. Організація захисту інформації в російській армії (XIX – поч. XX ст.)

У Російській імперії не було централізованої системи захисту державної таємниці. Міністерство закордонних справ, Військове відомство і Департамент поліції самостійно докладали зусиль у забезпеченні охорони державної таємниці. При цьому Департамент поліції славився своєю системою конфіденційного діловодства, а МЗС і Військове відомство мали досягнення в галузі криптографії. У той же час, заходи, направлені на забезпечення захисту інформації в державі, здійснювані цими відомствами, мали хаотичний характер і не могли гарантувати ефективний захист державних секретів.

Уже в перші роки XX століття всі великі світові держави почали підготовку до війни, напружено стежачи за тим, що роблять потенційні союзники й противники. У мирний час спецслужби "полювали" на мобілізаційні плани, новинки військової техніки й інформацію про підготовку до майбутньої війни. Унаслідок цього, у військовому відомстві почалися активні дії зі створення й удосконалення системи захисту військової таємниці. Робота велася в чотирьох напрямах:

1. Створення й удосконалення системи контррозвідувальних органів. Їхнім основним завданням була протидія шпигунству противника в мирний і воєнний час.

2. Організація комплексної системи захисту інформації, що містить військову таємницю.

3. Удосконалення системи фельд'єгерського зв'язку.

4. Організація військової цензури.

У російському суспільстві проблема протидії шпигунству противника регулярно обговорювалася на сторінках газет "Русский инвалид", "Новое время", "Военный сборник". Але всі матеріали мали дискусійний характер і були цікаві лише вузькому колу фахівців. Зрідка виходили монографії, присвячені проблемі військового шпигунства.

Коли почалася Перша світова війна, з'ясувалося, що армія разом із державою не здатна забезпечити необхідний рівень захисту військової таємниці. І, як наслідок цього, населення не було готове активно допомагати органам контррозвідки.

Першою спробою виразити думку влади про ставлення до захисту військової таємниці в Російській імперії було звернення до громадян, опубліковане

22 червня 1914 року в газеті “Русский инвалид”. У ньому влада закликала населення тримати в таємниці інформацію про дислокації, переміщення і чисельність військ; не вірити чуткам і зберігати спокій. Уряд обіцяв інформувати про реальну обстановку на фронті. На жаль, час уже було втрачено. Хвиля шпигуноманії, яка охопила Росію, як і інші європейські країни, не сприяла активізації заходів із захисту військової таємниці.

Як писав один із офіцерів військової контррозвідки: “Не тільки в тому цивільному товаристві, в якому я постійно бував, не мали жодного уявлення про контррозвідку, її призначення й мету, але й серед військових було досить невиразне уявлення про сутність цієї украй складної інституції”.

Інший офіцер російської армії М.Д.Бонч-Бруєвич, котрий займався питаннями контррозвідки в Петербурзі в період Першої світової війни й розробив “Проект з організації контррозвідки в діючій армії”, цілком поділяв думку свого колеги. Він згадував, що таємна війна, яка велася паралельно явній, була мало кому відома. Про явну війну писали всі газети, друкували незліченні фотографії та знімали кінострічки, про неї розповідали мільйони учасників – солдатів і офіцерів; про таємну війну усе було найсуворішим чином засекречено.

Орган військової контррозвідки спочатку був названий “розвідувальним відділенням”, створювався негласно, “без офіційної установки”, інакше, на думку організаторів, губився головний шанс на його ефективну діяльність. Цей принцип зберігся до 1917 року. Навіть посада начальника розвідувального відділення з метою конспірації називалася “...состоящей в распоряжении начальника Генерального штаба”.

У російській армії проведення контррозвідувальних заходів покладалося на службу генерал-квартирмейстера. Аналіз навчального посібника для офіцерів Генерального штабу “Служба генерального штаба. Разведывательные органы армии”, виданого в 1901 році в Петербурзі, дав змогу виявити певні функції контррозвідки.

Відповідно до змісту цього посібника питаннями контррозвідки повинен займатися комендант. У його обов’язки входила організація утримання під вартою шпигунів противника, дезертирів і полонених. Як бачимо, на коменданта були покладені суто поліцейські функції.

Найнебезпечнішим під час бойових дій уважалося перехоплення противником повідомлень і розпоряджень. Тому рекомендувалося надсилати кілька примірників повідомлення для більшої ймовірності доставляння його адресатові.

Якщо повідомлення надсилалося польовим телеграфом, вказувалося, що противник може тільки зруйнувати лінії зв'язку. Про можливості знімання інформації або використання ліній телеграфу противником не йшлося.

У 1903 році канцелярія військово-облікового комітету Генерального штабу Військового міністерства підготувала секретний шестисторінковий проект організації контррозвідувальної служби у військовому відомстві. Передбачалося, що штат контррозвідувального органу буде невеликим: шість – сім агентів, писар, діловод, а очолить відділ штаб-офіцер у чині майора або підполковника. Із червня 1903 року цей контррозвідувальний орган почав активно працювати.

Після закінчення російсько-японської війни були розпочаті заходи із докорінного поліпшення організації контррозвідувальної служби. Це було пов'язано з бездіяльністю російських спецслужб на сопках Маньчжурії зокрема через відсутність професійних контррозвідників. Тому й була посилена взаємодія офіцерів Генерального штабу з охоронним відділенням, яке виділяло в розпорядження штабу своїх досвідчених агентів.

У 1908 році під час київського з'їзду старших ад'ютантів розвідувальних відділень була розроблена загальна система організації військової контррозвідки в мирний час. Відповідно до цієї системи контррозвідкою повинні були займатися чини окремого корпусу жандармерії, прикордонної сторожі під керівництвом старших ад'ютантів розвідувальних відділень штабів військових округів. Їхню діяльність контролювало п'яте діловодство Головного управління Генерального штабу. Був установлений таємний контроль за всіма іноземними громадянами, що проживали на території військових округів.

Починаючи з 1908 року, уряд створює кілька міжвідомчих комісій. Ключове питання – формування системи контррозвідки при МВС або Військовому відомстві.

У 1909 р. була зібрана чергова спеціальна міжвідомча комісія на чолі з директором Департаменту поліції. На засіданні комісії було прийняте рішення залучити до контррозвідки особливих жандармських офіцерів. Утім, комісія так і не вирішила питання про взаємодію жандармерії й штабів військових округів, застосування до іноземців особливих правил спеціального нагляду, підсудність справ із шпигунства спеціальному суду. Натомість МВС і міністерство фінансів

(якому підпорядковувалася прикордонна й митна варта) вели неухильну боротьбу зі шпигунством.

8 червня 1911 року військовий міністр затвердив "Положення про контррозвідувальні відділення". Системою цих відділень керував генерал-квартирмейстер Головного управління Генерального штабу (ГУ ГШ). Центральний орган був представлений Петербурзьким відділенням, яке стало спадкоємцем розвідувального відділення. Місцеві відділення створювалися при штабах військових округів: петербурзьке, московське, віленське, варшавське, київське, одеське, тифліське, іркутське і хабаровське контррозвідувальні відділення (КРВ).

У період Першої світової війни при Штабі Верховного головнокомандуючого, штабах фронтів і армій були сформовані спеціальні контррозвідувальні відділення, які розгорнули активну діяльність щодо виявлення і знищення ворожої агентури та шпигунів. Наприкінці 1916 року у всіх союзницьких країнах (Англія, Франція і Росія) були засновані контрольні бюро, метою яких був обмін відомостями про осіб, яких підозрюють у військовому шпигунстві. Таке контрольне бюро у складі особливого діловодства відділу генерал-квартирмейстера ГУ ГШ у 1917 році називалося військово-реєстраційним бюро.

Веденням секретного листування з усіх питань займався восьмий стіл VII відділення ведення військової статистики іноземних держав другого управління генерал-квартирмейстера, до компетенції якого було віднесено:

- ведення листування із секретних питань;
- ведення листування з агентурної розвідки;
- забезпечення роботи іноземних офіцерів, відряджених до російської армії.

Саме це відділення займалося організацією розвідки. А VIII відділення відало архівно-історичними питаннями. Розподіл функцій усередині відділення був таким:

- 1 стіл – видача документів;
- 2 стіл – видача книг;
- 3 стіл – діловодство з допуску до занять в архівах і бібліотеках.

Із викладеного випливає, що це відділення виконувало функції звичайної бібліотеки і спецвідділу, що регламентував питання допуску до роботи із секретними документами.

Крім того, був ще один підрозділ у структурі Генерального штабу, пов'язаний із організацією таємного листування: "Канцелярія. Журнальна частина. Ведення переписки і журналів за вхідними і вихідними секретними документами".

Також діяла в Генеральному штабі і своя криптографічна служба. У другій половині XIX століття більшість шифрів Військового міністерства становили коди малого (до 1000 словникових величин) обсягу. Кодовими позначеннями були три- й чотиризначні числа. Військові шифри цього типу використовувалися протягом тривалого часу. Перероблявся лише словник, який відносно швидко застарівав, що пояснювалося, наприклад, зміною географії воєнних дій тощо. Словникові ключі були найбільш поширеним типом шифрів, які використовувалися наприкінці XIX століття у військовому відомстві. Їх називали "військовими ключами".

Попри універсальні принципи побудови, шифри Військового міністерства кінця XIX – початку XX століття відрізнялися один від одного деякими особливостями.

Зокрема ключ Військового міністерства № 6 1906 року становив тризначний різноманітний цифровий код із замаскованим і схованим початком повідомлення. Ключ Військового міністерства № 7 1905 року був алфавітним тризначним цифровим кодом на 900 словникових величинах, розміщених на 18 таблицях 5 х 10.

Особлива увага приділялася правильному використанню шифрів. У військовому відомстві у випадку втрати хоча б одного примірника шифру або при підозрі, що він "зламаний" дешифрувальниками противника, пропонувалося негайно виводити цей шифр з обігу й заміняти новим.

Зняття копій із шифрів категорично заборонялося. Тому у воєнний час польові штаби армій, окремих корпусів і загонів забезпечувалися запасними примірниками шифрів. Їх видавали в необхідних випадках тим особам, яких не було в списку, але яким, на думку командуючих арміями або інших головних військових начальників, потрібно було мати той чи інший шифр.

Примірники ключів воєнного часу, видані командуючими військами в округи, командирам корпусів, комендантам фортець і наказним отаманам, хоча й були в безпосередньому розпорядженні цих осіб, мали зберігатися в приміщеннях відповідних штабів у "замкнених секретних сховищах" (скринях, ша-

фах, шухлядах), обов'язково в особливо секретних пакетах, опечатаних особистою печаткою тих осіб, на чиє ім'я вони були видані.

У такому самому порядку зберігали примірники шифрів (ключів) і начальники головних управлінь Військового міністерства й штабів округів. Заміну старих примірників шифрів, передання шифрів від військовослужбовців, котрі звільняються, було віднесено до компетенції Генерального штабу. Він визначав і термін дії шифрів.

Із метою збереження шифрів у таємниці інструкції вимагали в жодному разі не залишати у справах зашифровані документи. Особи, які використовували шифр, зобов'язані були поміщати до справ копії відправлених шифроповідомлень, викладені "звичайним текстом". Чернетки знищувалися, особа, котра одержала шифроповідомлення, також повинна була знищити оригінал, помістивши в досьє вхідних документів відповідну копію, виконану "звичайним текстом". Перевірка шифрів воєнного часу, що знаходяться в окрузі, проводилася не рідше одного разу на рік.

Зрозуміло, що рекомендації з використання шифрів часто мали половинчастий характер. Так, під час російсько-японської війни "не тільки на приймальній, але й на передавальній станції повинні були залишатися копії усіх розпоряджень, і це, за тієї умови, що шифрувати депешу не завжди був час, є зовсім небажаним".

Військове відомство мало спеціальні шифри для воєнного часу. Але в них були численні недоліки. Задовго до війни створили спеціальний шифр для військових з'єднань. Це був досить складний шифр подвійної вертикальної перестановки за двома номерними рядами-розподільниками, з частою зміною ключів.

До Першої світової війни в жодній країні світу, крім Франції й Австро-Угорщини, не було військових дешифрувальних органів. Створене в листопаді 1911 року при Генштабі Австро-Угорської армії криптографічне бюро безуспішно намагалося зламати російські дипломатичні й військові криптосистеми.

Правда, ситуація різко змінилася в період Першої світової війни. Тоді дешифрувальна служба Австро-Угорщини майстерно розкривала російські криптографічні системи завдяки численним непорозумінням, пов'язаним із військовою мобілізацією в Росії.

Боячись появи в Росії свого талановитого, ще одного Редля, начальник армійського шифрувального бюро полковник Андрєєв до останньої хвилини перед

початком бойових дій утримувався від розсилання копій нових шифрів, призначених для використання в період війни. Цей захід призвів до сумних наслідків.

Так, російськими планами ведення воєнної кампанії проти Німеччини передбачалося вторгнення двох армій на територію Східної Пруссії. Армія під командуванням генерала Раненкампфа повинна була вести наступ у західному напрямі й бойовими діями скувати німців. Перед армією генерала Самсонова, розташованою південніше, було поставлене завдання обійти Мазурські болота, увійти в тил до німців і, блокувавши шляхи відходу, знищити ворога. Природно, що успішне вирішення цього завдання передбачало погоджену й ретельно сплановану взаємодію двох російських армій.

Однак російська служба зв'язку зовсім не відповідала висунутим до неї вимогам. Коли армії Раненкампфа і Самсонова виявилися розділеними Мазурськими болотами й стали здійснювати зв'язок один із одним переважно за допомогою радіо, з'ясувалося, що армія Раненкампфа одержала новий шифр, а старий знищила, а в Самсонова усе ще діяв старий шифр. Тому переговори між ними велися якийсь час за допомогою радіо відкритим текстом.

До цього треба додати, що матеріальне постачання армій було налагоджено дуже погано. У розпорядженні армії Самсонова було понад 600 км дроту для забезпечення зв'язку, який був швидко витрачений.

У той час радіозв'язок використовували в штабах обох російських армій і в штабах підпорядкованих їм корпусів. Штаби дивізій і штаби нижчої ланки радіозв'язку не мали. Тому штаби корпусів для зв'язку з дивізіями використовували дротові засоби. А штаби армій натомість утратили мізерні запаси дроту для зв'язку з тиловим командуванням. Тому радіо залишалося єдиним засобом зв'язку між штабом корпусу й армії.

Зміст таких радіопереговорів не був таємницею для противника. Загальна неефективність проведення Росією мобілізації згубно позначилася й на доведенні до військ нових військових шифрів і ключів. Наприклад, 13-й корпус армії Самсонова не мав ключів для читання криптограм, що надходили від його сусіда, 6-го корпусу. Після двох тижнів від початку війни російські зв'язківці навіть не намагалися шифрувати повідомлення, а передавали їх радіозв'язком відкрито.

Плутанина зі зв'язком спостерігалась і в інших російських арміях. Шведський криптограф Гульден писав, що в документах німецького імперського ар-

хіву можна прочитати, що російські радіостанції дуже часто передавали свої повідомлення відкритим текстом, військові радіостанції не одержували під час мобілізації комплекти, необхідні для зв'язку шифрів.

При такому безладі на початку війни радіостанції, які належали різним радіопідрозділам, часто не могли обмінятися шифрованими повідомленнями з тієї простої причині, що деякі радіороти постачали свої радіостанції власними шифрами.

Оскільки на ту саму ділянку фронту могли потрапити радіостанції різних рот, то в перші ж дні війни з'ясувалося, що радіостанції, надані одному й тому самому армійському корпусові або кавалерійській дивізії, "розмовляють" різними шифромовами. Тому за відсутності надійного дротово-телеграфного зв'язку доводилося повторювати шифроповідомлення відкритим текстом.

Але найтрагічніший момент для російської армії настав у серпні 1914 року, коли в результаті катастрофи біля Мазурських озер з оточення зуміло вирватися менше 2 тис. бійців армії Раненкампфа. Гофман, один із розробників цієї операції, у книзі "Війна втрачених можливостей" писав: "Російська радіостанція передала наказ у незашифрованому вигляді, й ми перехопили його. Це був перший із низки інших незліченних наказів, що передавалися в росіян спочатку з неймовірним легкодумством ... Таке легкодумство дуже полегшувало нам ведення війни на сході, іноді лише завдяки цьому взагалі можливо було здійснювати операції".

Хоча на початку війни Росія зазнала великих труднощів у забезпеченні своїх військ усім необхідним, у тому числі засобами зв'язку, вже в першій половині вересня 1914 року їй удалося цілком забезпечити їх шифрувальними засобами. 14 вересня 1914 року Ставка Верховного головнокомандуючого віддала розпорядження про те, що всі військові накази підлягають зашифруванню.

Прийнята шифросистема ґрунтувалася на "багатоалфавітному" шифрі цифрової заміни, у якому допускалося зашифрування кількох букв підряд за одним алфавітом. Але вже 19 вересня молодий обдарований начальник російського відділення дешифрувальної служби Австро-Угорщини капітан Герман Покорний розкрив цю систему. Такі шифросистеми не були непосильними для криптоаналітиків. До того ж спочатку росіяни-зв'язківці нерідко вставляли відкритий текст у шифрований. Незабаром одночасне використання відкритих і шифрованих

текстів у повідомленнях було заборонено, але було вже надто пізно, і вже 25 вересня 1914 р. криптосистема була зламана остаточно.

Про те, що криптосистема остаточно скомпрометована, росіяни здогадалися тільки 19 жовтня. До цього дня більшість наказів, прийнятих німецьким командуванням, ґрунтувалося на даних радіоперехоплення. І це не випадково. Часом росіяни самі розкривали найбільше уразливі місця у своїй обороні.

Спроба замінити всі елементи криптосистеми дала змогу росіянам до 25 жовтня брати верх над військами генерала Маккензина і загнати їх у "мішок", але після розшифрування однієї з телеграм німцям стало відомо слабке місце в кільці російських військ. Оточення було успішно розірване.

До весни 1915 року в російських військах повністю відмовилися від старої системи шифрів і стали застосовувати простий шифр Цезаря. Велика кількість таблиць, використовуваних у період ведення активних дій, та щоденна зміна ключів ставили непосильне завдання перед зв'язківцями. У цих умовах розкриття чергового російського шифру для дешифрувальних служб Австро-Угорщини й Німеччини не становило труднощів.

Читання російських криптограм дозволило країнам німецького блоку приймати час від часу правильні тактичні рішення. Російський Генеральний штаб був здивований прозорливістю противника. Один раз німці залишили займані ними позиції за два дні до початку великого наступу російських військ. Одним із пояснень цього рішення німецького командування росіяни уважали аерофотознімання.

Утім, поступово міцніло переконання, що противник читає російську шифролистування. Коли німецький весняний наступ другого року війни досяг апогею, росіяни знову змінили шифр. Але ця зміна додала більше турбот їм самим. Майже всі шифровки, передані за допомогою радіо в перші два дні після зміни шифрів, через допущені помилки так і не були прочитані адресатами.

У червні 1916 року знову відбулася зміна способу шифрування – росіяни увели свій перший код. Можливо, це було зроблено під впливом Франції, якій із дешифрованих німецьких криптограм стало відомо, що німці читають російські шифроповідомлення, або завдяки власній службі радіоперехоплення, що почала функціонувати в 1916 році.

Наростання дезорганізації російської армії впливало і на службу зв'язку: пропорційно зниженню дисципліни у військах зростала балакучість радистів.

На початку 1917 року тільки протягом одного дня австрійська дешифрувальна служба прочитала понад 300 російських шифротелеграм, із чого випливало, що служба забезпечення зв'язку Росії швидко розвалювалася. Наявність примітивних військових шифрів, недостатньо продуманих інструкцій до них, велика кількість порушень шифродисципліни – усе це в сукупності призводило до того, що російські шифри успішно розкривали австрійські й німецькі фахівці.

Проблеми з перехопленням повідомлень, які передавали телеграфом, виникли ще в російсько-японську війну. Якщо повідомлення в обложений Порт-Артур шифрували, то телеграфом інформація передавалася у відкритому вигляді.

Уже в 1904 році японські спецслужби вперше в історії радіотехнічної розвідки реалізували на практиці схему дистанційного знімання акустичної інформації (мікрофон – кабель – приймач (спостерігач). Натомість тільки в 1915 році в російській пресі було опубліковано повідомлення про те, що під час бойових дій у період російсько-японської війни були випадки перехоплення телеграфних повідомлень, якими обмінювалася Ставка головнокомандуючого і війська.

Дротовий телеграф, особливо апарати "ЮЗА", російське командування уважало абсолютно надійним для передавання секретних телеграм у незашифрованому вигляді, хоча насправді це не так.

Усі питання, пов'язані з організацією, збереженням, пересиланням й обробленням мобілізаційних планів, регламентувалися спеціальною інструкцією. У кожному військовому окрузі інструкція була розроблена з урахуванням місць дислокації військових частин і штабу округу. Кожен примірник інструкції мав гриф "таємно" й номер. Тираж інструкції друкувався тільки у військовій друкарні.

У розділі 1 типової інструкції "Пункти збереження" детально розписувалося, де й за яких умов потрібно зберігати мобілізаційні плани; вказувалися місто або залізнична станція, місце і спосіб збереження. Місцем збереження мобілізаційних планів звичайно були:

- мобілізаційний відділ штабу округу;
- приміщення вартового начальника гарнізонної гауптвахти;
- грошова комора гарнізонної гауптвахти;
- карцер при гауптвахті.

Також слід виділити два способи збереження секретних документів: у залізній шухляді або залізній шухляді, вкладеній у дерев'яну скриню.

У розділі 2 інструкції докладно розкривалася процедура передання документів у військові частини на збереження.

Так, у першому параграфі другого розділу говорилося, що документи мають зберігатися в опечатаних залізних шухлядах, а шухляди повинні додатково вкладатися в дерев'яні скрині (по дві в кожну скриню). Самі скрині слід прикріпляти до підлоги.

У другому параграфі цього розділу йдеться про те, що передання залізних шухляд із документами на збереження та вкладання їх у дерев'яні скрині здійснюються уповноважені від начальника пересування військ і начальника залізниці. Ці особи мали посвідчення затвердженого зразка. При цьому вони не могли передавати шухляди незалежно один від одного, а лише за умови одночасної явки обох представників.

Коменданти міст і Штабу військового округу завчасно сповіщалися начальниками пересування військ про час доставляння шухляд і про те, хто з офіцерів округу відряджений із цією метою.

У третьому параграфі йдеться про місце укладання документів у шухляду. Далі докладно описувався сам процес опечатування шухляди. Так, відповідно до вимог інструкції залізні шухляди, призначені для збереження в дерев'яних скринях, опечатувалися в такий спосіб: у кришці кожної шухляди, біля переднього її краю і в передній стінці просвердлювалися отвори, призначені для протягування двох мотузок, у які вплітали тоненький дріт. Після закриття шухляди одну з мотузок пропускали через вушко ключа, зав'язували вузлом і кінці припечатували до особливої маленької дощечки печатками начальника залізниці й начальника пересування військ.

Після того, як шухляди доставлялися в пункти збереження та розміщувалися в загальній дерев'яній скрині, кінці другої мотузки (зв'язаної вузлом із першою) припечатувалися номерними печатками начальника залізниці та начальника пересування військ до стінки дерев'яної скрині.

Зліпки з печаток, вкладені у футляри, передавалися під особисту відповідальність комендантові міста, який зберігав їх у особливій залізній шухляді або дерев'яній скрині.

Одержавши зліпки й упевнившись у цілісності та дійсності печаток, комендант міста або секретар штабу округу опечатували дерев'яні скрині своїми печатками і приймали на збереження всі матеріали. Після цього складався акт установленої форми у двох примірниках за підписами осіб, які прийняли на

збереження скриню, та уповноваженого на її передання. Один примірник акта передавався начальникові залізниці, інший, разом із представленим посвідченням про особу, зберігався в коменданта міста або канцелярії штабу округу. Коменданти міст і секретар штабу округу несли повну відповідальність за цілісність печаток на залізних шухлядах.

У п'ятому параграфі йдеться про те, що залізні шухляди, передані на збереження без дерев'яних скринь, опечатувалися двома сургучевими печатками: начальника залізниці й начальника пересування військ. Ключ від цих залізних шухляд передавався або помічникові начальника мобілізаційного відділу, або уповноваженому від залізниці агентові, або іншій посадовій особі для збереження в особливій залізній шухляді чи добре закритій дерев'яній скрині.

У сьомому параграфі були описані особливі умови збереження в деяких населених пунктах. Зокрема в Штабі військового округу скриня з секретними справами мобілізаційного відділу охоронялася в позаслужбовий час вартовим, у робочий час була під наглядом старшого ад'ютанта мобілізаційного відділу.

Третій розділ інструкції присвячений описовій процедурі обміну документів. Так, у першому параграфі цього розділу йдеться про те, що обмін залізних шухляд або мобілізаційних документів проводився уповноваженими начальника залізниці й начальника пересування військ за їхніми підписами. У другому параграфі наголошувалося, що призначені для вкладення в шухляди нові документи доставлялися в пункти збереження в залізних шухлядах, отриманих в управлінні залізниці.

У третьому й четвертому параграфах докладно описувалася сама процедура заміни документів. Зокрема у присутності коменданта міста або секретаря штабу, чи начальника мобілізаційного відділу або його помічника відкривалася дерев'яна скриня, а уповноважений перевіряв цілісність печаток. Знявши печатки і зробивши обмін залізними шухлядами або документами в залізних шухлядах, уповноважені знову накладали установлені печатки і складали акт. Далі відбувалися дії, аналогічні тим, що виконувалися при первинному вкладенні залізної шухляди в дерев'яну скриню.

У п'ятому параграфі зауважувалося, що уповноважений допускався до залізної шухляди для обміну документів відразу ж після прибуття, за винятком вимог параграфу 219 Гарнізонного статуту.

У четвертому розділі інструкції докладно описана процедура вилучення мобілізаційних планів при оголошенні часткової або повної мобілізації.

Утім, спроби неухильно дотримуватися вимог інструкції з організації збереження секретного листування часто закінчувалися невдачею. Зокрема ще до початку російсько-японської війни в "Записке о работах, необходимых для улучшения Сибирской железной дороги со стратегической целью", датованій 10 жовтня 1901 року, серед іншого зазначалося про необхідність придбання вогнетривких шаф і шухляд, оскільки дотримання вимог цієї інструкції в Сибіру не гарантувало необхідного рівня збереження мобілізаційних документів, що було пов'язано зі складною криміногенною обстановкою в регіоні. Більшість населення становили каторжани, згодні піти на будь-які злочини заради наживи; функціонували численні іноземні фірми, готові допомогти своїм державам у здобутті цих документів. Натомість уся секретна переписка, у тому числі з мобілізаційних питань, зберігалася у звичайних дерев'яних шухлядах.

Ще одним напрямом, залишеним без уваги військової контррозвідки, була цензура друкованих видань. Наприклад, до початку російсько-японської війни навіть такий спеціальний військовий друкований орган, як "Русский инвалид", поміщав на своїх сторінках усі розпорядження військового міністерства, зокрема секретні. Щорічне видання "Краткое описание сухопутных сил", яке містило докладний перелік усіх частин царської армії з указівкою місць їхньої постійної дислокації й прізвищ командирів дивізій, полків й окремих батальйонів (стрілецьких і резервних), міг купити кожен бажаючий.

Особливо яскраво це проявилося під час російсько-японської війни. Уся дислокація російських резервних частин, переміщення другорядних замість польових, які відправили на Далекий Схід, друкувалися в "Русском инвалиде". Після кожного бою видання подавало списки вбитих і поранених офіцерів із зазначенням їхніх частин.

У Маньчжурії були свої газети, в яких публікувалися матеріали, що становили державну таємницю. Особливо вирізнявся цим "Вестник Манчжурии". Незважаючи на існування "особливого цензурного відділення", на чолі якого стояв офіцер генерального штабу, видання поміщало відомості, які давали противникові можливість судити не тільки про склад російської армії, але й про підхід підкріплень. Схоже, що військово-цензурні відділення штабу головнокомандуючого не приділяли належної уваги цим публікаціям.

Роботу фельд'єгерського корпусу регламентували інструкції, зокрема від 25 липня 1892 року – "Инструкция чинам фельдъегерского корпуса".

Під час російсько-японської війни 15 офіцерів і 13 фельд'єгерів були відряджені в діючу армію. Вони повинні були не тільки забезпечувати доставляння наказів і розпоряджень командуючих у межах діючої армії, але й доставляти в столицю найбільш термінові, важливі повідомлення головнокомандуючого російськими військами на Далекому Сході.

У 1913 році "Инструкция чинам фельдъегерского корпуса" була переглянута і 12 вересня 1913 року затверджена знову. У ній були більш чітко визначені обов'язки та правила поведінки чинів фельд'єгерського корпусу як на службі, так і в позаслужбовий час. Крім того, перший розділ "Об общих обязанностях чинов фельдъегерского корпуса" був доповнений розділом "Об автомобилях и подрядческих лошадях". А в параграфі 62 регламентовано поводження із секретними пакетами. Пакети від імператора на ім'я міністрів і головнокомандуючих доставлялися чинами корпусу, коли ті прибували до Санкт-Петербурга, прямо військовому міністрові, міністру закордонних справ або голові Ради міністрів, навіть у нічний час. При цьому в розсильних книгах, крім розписки, позначалися: одержувач, місяць, число й година здачі пакетів.

На початку Першої світової війни начальник фельд'єгерського корпусу видав наказ про посилення режиму секретності: "Оголошую чинам корпусу про безумовну необхідність остерігатися випадкових знайомств і розпитувань сторонніх осіб, особливо щодо службової діяльності чинів корпусу. Цієї війни необмежено поширений ворожий шпіонаж, тому треба бути обережним у відповідях навіть на, здавалось би, найбільш невинні запитання, які ставляться з єдиною метою – зібрати докладні відомості для противника про всі, не тільки військові, але й загальнодержавні, заходи, викликані війною і здійснення яких приховано від ворога становить один із засобів досягнення Росією успіху у війні і подальшій перемозі над ворогом".

Отже, як підсумок можна процитувати слова А.Рєзанова, сказані їм на другий рік Першої світової війни: "Хоч в останні роки військове керівництво докладало значних зусиль в охороні військової таємниці, але промахи були дуже часті, і це зрозуміло: після низки років розпущеності в цій сфері потрібний час, щоб прищепити військовим чинам звичку вдумливого ставлення до понять військового секрету й військової потайливості".

На жаль, ці слова так і залишилися побажанням. Звичку "вдумливого ставлення до поняття військового секрету й військової потайливості" змогли прищепити суспільству тільки в радянській Росії.

2.2. ФОРМУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ПЕРІОД ВІДРОДЖЕННЯ УКРАЇНСЬКОЇ НАЦІОНАЛЬНОЇ ДЕРЖАВНОСТІ (1917–1921 рр.)

2.2.1. Організація захисту інформації в період Центральної Ради

Перша світова війна та її результати привели до кардинальної зміни всієї системи міжнародних відносин. На політичній карті Європи, особливо на сході континенту, з'явилися нові держави, які закладали підвалини повоєнних відносин. Серед них була й незалежна Україна, яка у своїй розбудові пройшла різні етапи.

Війна показала, що захист усіх видів інформації в Росії, російській армії вимагав значних змін і серйозної централізованої організації. Звісно, про досвід, напрацьований у Російській імперії, знали і в урядах Української держави 1917-1921 років, які приділяли багато уваги побудові дієвої системи захисту не лише військових та державних секретів, а й усієї важливої військово-політичної інформації; створенню спеціальних органів, які б займалися цими проблемами.

У період Центральної Ради можна виділити кілька видів інформації, які підлягали захисту, зокрема: військова, державна, інформація з обмеженим доступом, службова, слідча, персональна тощо. Починаючи з 1917 і до 1921 року пріоритет надавався захисту різних видів інформації.

Характер нормативної бази, що регламентувала захист інформації з обмеженим доступом у 1917-1921 роках, багато в чому визначався особливостями цього історичного періоду й тими чинниками, що впливали на дії вищих органів влади в тогочасній Україні.

Усе це зумовило головні риси нормативної бази органів безпеки України, а також особливості пов'язаної з її застосуванням практики: помітний поспіх у прийнятті власних нормативних актів і в багатьох випадках низька їхня якість як із юридичного, так і з судового погляду; широке застосування нормативно-правових актів Російської та Австро-Угорської імперій (як безпосереднє, так і при розробленні власної нормативної бази); значне переважання підзаконних нормативних актів ("Закон про встановлення в складі Міністерства внутрішніх

справ Департаменту політичної інформації" від 23 травня 1919 р.; Постанова уряду "Про зміну існуючих законів про міліцію і утворення Державної варти" від 18 травня 1918 р.; "Статут Української Державної варти"; "Інструкція зі збирання інформації"; Інструкції МВС "Інструкція щодо заходів боротьби з бандитизмом"; "Тимчасове положення про прикордонні пункти"; "Інструкція начальникам прикордонних пунктів на кордоні з Великоросією" тощо).

За часів Центральної Ради функціонував Генеральний Секретаріат України, до складу якого входив Крайовий комітет оборони нового ладу з комісіями: інформаційною, військовою, слідчою й т. ін.

Крайовий комітет складався з представників організацій, перерахованих у проекті С.Петлюри, а також Центрального крайового бюро професійних спілок. Причому перелік організацій не був остаточним, оскільки при утворенні нових революційно-демократичних організацій за постановою Крайового органу до нього могли входити і представники цих формувань.

Згідно з постановою про крайовий орган його очолював один із членів Генерального Секретаріату (за погодженням між урядом і Секретаріатом). Товариша Голови Комітету обирав Комітет із свого складу; кожна організація сама обирала представника до названої установи. Отримав орган і свою остаточну назву – Крайовий комітет оборони нового ладу при Генеральному Секретаріаті.

Розгортання українського військового руху вимагало створення координаційних органів. У складі Генерального Секретаріату діяв секретаріат військових справ на чолі із С.Петлюрою. Крім того, на І Всеукраїнському військовому з'їзді було створено Генеральний військовий комітет, який відрядив своїх представників до військового міністерства Тимчасового уряду й до Генерального штабу Росії. У складі Генерального комітету було сформовано "Комісію спеціальних служб", яку очолював генерал Л.Кіндратович.

Крім того, зростав інтерес до української "автономії" з боку провідних іноземних країн. Переважно здобували інформацію про становище в Україні держави Антанти, США, Японії через можливості військової дипломатії, консульські установи, силами емісарів та журналістів.

Іноземні інформатори намагалися вивчати широкий спектр питань щодо тенденцій розвитку політичних і військово-політичних подій в Україні, намірів її керівництва, позицій провідних суспільно-політичних кіл, українізації збройних сил. Крім того, через легальні й нелегальні можливості спеціальних служб і

військової дипломатії робилися спроби активно вплинути на провід України для забезпечення спрямування політичних подій.

Професійний інтерес до України виявляла й американська розвідка. У травні 1917 року відповідно до рішення Ради національної оборони США до Росії через Владивосток прибула "економічна розвідка". Американські фахівці в цій галузі установили контакт із діячами українського парламенту, неодноразово зустрічалися з О.Шульгіним.

12 грудня 1917 р. рішенням Генерального Секретаріату Комісії з охорони ладу надано право видавати обов'язкові постанови з умовою, що всі вони доводитимуться до відома уряду. Проте робота комісії не відзначалася результативністю. На засіданні Генерального Секретаріату 15 грудня 1917 р. Л.Абрамович заявив, що комісія не може працювати планомірно й виконувати свої обов'язки через нестачу потрібних сил. М.Порш уніс пропозицію створити Колегію з охорони України, "організувати штаб, надіслати РНК ультиматум із вимогою припинити війну, оповістити людність про справжній стан справ". Колегія повинна була здійснити облік сил і зброї, використати Вільне козацтво, підпорядкувати міліцію. Крім того, указувалося на необхідність надання права діяти від імені Генерального Секретаріату, а також у разі потреби давати розпорядження щодо розбирання залізничних колій. Була ухвалена постанова: негайно надіслати РНК ультиматум із вимогою припинити війну й відкликати радянські війська з України. Вирішили також обрати особливий Комітет з оборони України в складі генеральних секретарів Порша, Петлюри і Єшенка. Таким чином, паралельно з Комісією з охорони ладу в Україні почав діяти особливий Комітет з оборони України. Їхні функції не були розмежовані, що негативно відбилося на подальшій роботі. 17 грудня 1917 р. ЦВК рад України опублікував маніфест про повалення української Центральної Ради й Генерального Секретаріату, а з Росії прибули більшовицькі частини під командуванням Єгорова, Сіверса, Сабліна й повели наступ на Донбас і південь країни. 25 грудня 1917 р. Антонов-Овсієнко віддав наказ про загальний наступ радянських військ проти УНР. Першим зазнав більшовицького удару Катеринослав, потім Олександрівськ та Полтава.

У цих складних умовах як Комісія з охорони ладу в Україні, так і особливий Комітет з оборони України, судячи з документів, не виявляли практичної активності. Щоправда, на засіданні Генерального Секретаріату 23 грудня 1917 р. Л.Абрамович доповів проект постанови про умови, за яких названа Комісія може

існувати. Постановили ці вимоги задовольнити. На засіданні уряду 7 січня 1918 р. за поданням Генерального секретарства внутрішніх справ був затверджений статут Комісії. Зміст цих документів не відомий, оскільки самі вони не виявлені. 6 квітня 1918 р. за поданням міністра внутрішніх справ постановою Ради народних міністрів Комісія з охорони порядку була скасована, а таємні матеріали й документи передані в Адміністративно-політичний департамент МВС.

Отже, аналіз передумов та особливостей створення перших органів із захисту інформації й державної безпеки України показує, що останні на початковому етапі свого функціонування намагалися зробити посильний внесок у державотворення та забезпечення існування України. Однак їх діяльність була малоефективною.

Якщо говорити про причини цього, то можна виділити три найбільш суттєві. По-перше, створення координаційного органу з питань безпеки й оборони стало нагальною потребою тогочасного суспільно-політичного життя в Україні. Проте в керманичів країни не було чіткого уявлення про статус, функції, компетенцію і стратегічну діяльність цієї інституції. Це викликало взаємні непорозуміння й гальмувало ініціативу як одних, так і інших. По-друге, до створення цих інституцій практично не залучались висококваліфіковані військовики та досвідчені керівники й співробітники спеціальних служб, які були в розпорядженні Генерального Секретаріату. По-третє, не здійснювався необхідний результативний контроль за діяльністю створених комітетів і комісій, а також не захищалися їхні рішення й постанови.

2.2.2. Організація захисту інформації в українській державі гетьмана П.Скоропадського

Уряд П.Скоропадського діяв у непростих політичних умовах. Внутрішня та зовнішня обстановка в державі ускладнювалася партійними й класовими суперечностями. Разом із тим, система захисту інформації вже почала функціонувати. Професіоналізм гетьманської розвідки дав можливість певною мірою протидіяти іноземному шпигунству та диверсійно-терористичним акціям антидержавних елементів.

Комуністичне підпілля дислокувалося переважно в робітничих центрах України. Його головним завданням було ведення політичної агітації, організація страй-

ків та диверсій, створення збройних формувань. Розгалужена підпільна мережа діяла на Донбасі. У Києві до літа 1918 року підпільні організації налічували близько 650 членів, функціонувало шість нелегальних райкомів компартії. Історик І.Нагаєвський зазначав, що діяльність радянської агентури здебільшого мала диверсійний характер. Так, 6 червня внаслідок диверсії вибухнули порохові склади в передмісті Києва – Звіринці. При цьому більше 200 осіб загинуло, понад 1000 дістали поранення, близько 10 тис. утратило притулок.

Велику небезпеку суверенітету й громадському спокою Української держави несла діяльність російських шовіністичних організацій під прапором "білого" руху. Роботу "білого" підпілля полегшувала наявність у країні добре скоординованих та озброєних організацій російських націоналістів. Наприкінці 1918 року 40 тис. офіцерів перебувало в Києві, 15 тис. – у Херсоні, 10 тис. – у Сімферополі, 8 тис. – у Катеринославі тощо.

У 1917 році в Києві виникла конспіративна організація "Азбука" на чолі з В.Шульгіним, котра спеціалізувалася на збиранні інформації політичного характеру. Так, її члени зуміли здобути текст таємної телеграми кайзера Вільгельма II командуванню німецькими військами в Україні, де він дав згоду на обрання П.Скоропадського гетьманом України.

Великі можливості для таємної роботи в Україні мали спеціальні служби країн австро-німецького блоку. Їхні дипломатичні установи регулярно надсилали змістовні доповіді про економічне й суспільно-політичне становище в Україні. В Україні було запроваджено мережу їхніх консульських установ: німецькі представники діяли в Києві, Одесі, Миколаєві та Харкові, австрійські – у Києві й Одесі. Посол України у Відні В.Ліпинський повідомляв своїми каналами про наявність у Києві великої австро-угорської шпигунської групи.

З огляду на ці події, слід було вжити адекватних заходів на захист військово-політичної інформації в державі. Натомість урядовці, усвідомлюючи шкоду, яку завдавали іноземці, дієвих заходів та установ, які б могли здійснювати захист зазначеної інформації, не створили.

З осені 1918 року серйозним противником силових структур стає селянський ватажок – анархіст Н.Махно. Так, у с. Михайлове-Лукашове махновці розстріляли голову волосної Державної варти Іванова, трьох офіцерів та двох козаків повітової "охоронної сотні", а потім у мундирах чинів варти проникли до садиби поміщика Миргородського. Махновці-розвідники часто маскувалися під варту, весільні процесії, селян, котрі йдуть базарувати. Навіть сам "батько" хо-

див у розвідку переодягнений у жіночий одяг. На той час це був один із засобів здобуття й збереження важливої інформації.

15 листопада 1918 року силами опозиції створений координаційний орган із підготовки й проведення антигетьманського повстання під назвою "Головний оперативний штаб Військово-революційного комітету" (або Конспіративний повстанський штаб), до якого увійшли В.Винниченко, директор одного з департаментів Міншляхсполучення А.Макаренко, О.Отецький, командир січових стрільців полковник Є.Коновалець. У ніч на 13 листопада 1918 року в приміщенні Міншляхсполучення відбулася таємна нарада, на якій було сформовано Директорію – орган політичного керівництва на період повстання та захоплення влади.

18 травня 1918 року П.Скоропадський затвердив Постанову Ради Міністрів "Про зміну існуючих законів про міліцію й утворення Державної варти". Положення про Департамент Державної варти базувалося на ст. 361, 362 "Зводу законів Російської імперії". До складу Департаменту Державної варти входили: директор, віце-директор, чиновники для особливих доручень, начальники відділів, секретар тощо. Відділи проводили оперативно-розшукову роботу та необхідні процесуальні дії у кримінальних справах. При проведенні дізнання співробітники Державної варти в карно-розвідувальній сфері перебували в безпосередній підлеглості осіб прокурорського нагляду згідно із постановами Статуту кримінального судочинства.

Освідомчі (контррозвідувальні) підрозділи Державної варти (інша назва – "інформаційні") здійснювали попередження, виявлення і припинення злочинів проти державного ладу й безпеки країни, збір інформації про політичні партії тощо. У складі освідомчих відділів виділялися діловодства за напрямами: загальне, таємне, агентурне, залізничне; реєстраційна частина та фотолабораторія.

Місцеві освідомчі відділи були зобов'язані висвітлювати політичну обстановку у своєму районі, вивчати характер діяльності місцевих політичних організацій і рухів, вербувати таємну агентуру й керувати її роботою, організовувати зовнішній нагляд, перлюстрацію кореспонденції тощо. Завдання освідомчих відділів на місцях конкретизувалося в Інструкції начальникам освідомчих відділів при губернських старостах і градоначальниках, яка містила окремі, фрагментарні рекомендації щодо захисту інформації. Утім, викладених у ній положень було явно недостатньо.

Цікавим є і те, що відповідно до Правил спільної роботи цивільні установи зобов'язувалися доводити до освідомчих відділів інформацію, потрібну їм для виконання оперативних заходів.

Керівництво Департаменту Державної варти вперше в Україні створило мережу конспіративних та явочних квартир для роботи з агентурою.

Добування інформації про суспільно-політичне становище в Україні здійснювалося також шляхом опрацювання й узагальнення відкритих періодичних (особливо партійних) видань. Створення дієвої цензури засобів масової інформації могло б зупинити витік інформації про військово-політичне становище в державі через друковані органи.

2.2.3. Організація захисту інформації в період Директорії

Організація захисту військової інформації в період Директорії (1919-1920 рр.) здійснювалася в Генеральному штабі УНР. Відповідальним за захист інформації був контррозвідувальний відділ та його окремий загін – загін польової артилерії. Сюди ж входив загін особистої охорони Головного отамана. Агентурою контррозвідки опікувалися контррозвідувальні відділи штабів військових з'єднань.

Під час Директорії за рішенням уряду був створений при Міністерстві внутрішніх справ Політичний департамент, а при губернських і повітових комісарах – губернські та повітові політичні відділи. Головні завдання Політичного департаменту були такі: виявлення й припинення антидержавної діяльності політичних противників УНР, передусім партії комуністів, боротьба зі шпигунством, вивчення тилу противника та його військ. Виконував він і розвідувальну роботу щодо країн – потенційних противників УНР та можливих союзників.

Для співробітників Політичного департаменту була розроблена Інструкція із збирання інформації. Документ цікавий передусім тим, що дає уявлення про пріоритетні інтереси та напрями діяльності цієї спецслужби. Зокрема збиралася інформація про діяльність некомуністичних партій (українських, російських, польських, чеських); відомості про їхні програми, організаційну структуру; ставлення до радянської влади та директорів УНР; популярність серед населення; настрої населення республіки, його ставлення до уряду УНР, радянської влади, Польщі; рівень національної свідомості; відомості про збройні повстання, гасла, під якими вони розгортаються, характер дій повстанців (чи не є вони бандитизмом).

Збиралися відомості про становище влади в неконтрольованих Директорією регіонах. З'ясовувалося, наскільки радянська влада міцно тримається в селах і містах, ставлення до неї населення, яку збройну силу вона має й проти кого проводить прогресивну політику; особовий склад надзвичайних комісій та міліції, напрями діяльності й об'єкти зацікавленості; інформація про міжнаціональні відносини в Україні, політика радянської влади стосовно українців і української мови; відомості щодо виходу періодичних видань, роботи шкіл, життєвого рівня населення, цін на основні продукти харчування, обігу грошей, кооперативного руху.

Крім того, збиралася військова інформація про місця дислокації й плани з передислокації військ противника, їх назви, озброєння, постачання, одяг, харчування, політичні настрої особового складу, рівень дисципліни і ставлення до населення; а також відомості про громадян, які активно співпрацювали з окупаційною владою або, навпаки, найбільш рішуче чинили їй опір тощо.

Отже, із цього документа випливають основні питання, які цікавили Директорію і становили найбільший інтерес для забезпечення безпеки держави. Очевидно, що і цю саму інформацію, яка викладена в Інструкції й циркулювала в УНР доби Директорії, першочергово необхідно було захищати Політичному департаменту. Отже, саме Директорії вдалося створити орган, який би забезпечував захист інформації в державі. Звичайно, про ефективність його діяльності у такий буремний час говорити не доводиться.

2.2.4. Специфіка та особливості організації захисту інформації в Західноукраїнській Народній Республіці

Із перших днів свого існування ЗУНР, особливо збройні сили, стали об'єктом розвідувально-підривної роботи. Зокрема було завербовано кілька високопосадовців командного складу Української галицької армії.

Служба безпеки загальнодержавного рівня в цьому державному утворенні була представлена Корпусом української державної жандармерії. Він мав чітку організаційну структуру – провідну команду та регіональні органи. Розгортається диференційована система підготовки кадрів для жандармерії.

Коли Австро-Угорська імперія розвалилася, 18 жовтня 1918 р. у Львові зібралися представники української громадськості, щоб утворити Національну Раду – вищий орган майбутньої держави на чолі з Є.Петрушевичем.

І в цей час уперше спостерігається боротьба української та польської спеціальних служб. Адже Польща також готується взяти владу в Галичині. Щоб запобігти цьому, Національна рада займає збройними силами Львів, а потім і всю територію Східної Галичини. Це організовує голова Військового комітету (Українського генерального військового комісаріату) Д.Витовський. Організатори виступу, маючи у своєму розпорядженні незначну кількість (не більше двох тисяч) вояків-українців, оволоділи 200-тисячним Львовом, що вказує на хорошу систему захисту інформації з обмеженим доступом.

Проте втримати надовго Львів було дуже тяжко – західноукраїнська державність одразу стала об'єктом агресії з боку Заходу. Серйозним фактором, що робив проблематичним успіх українського повстання, була наявність численного, добре організованого польського підпілля. У розвідувальному забезпеченні дій польської сторони брало активну участь місцеве населення, яке добре знало місто (на відміну від вояків – українців, які були мобілізовані з інших місць).

На думку В.Сідака, прорахунком керівників ЗУНР була відсутність налагодженої системи розвідки сил і можливостей противника. При підготовці до повстання й на початковому етапі збройного виступу з ініціативи Генеральної команди та інших військових керівників у місця розташування польських груп опору надсилалися вояки для збору відомостей про їхню кількість, пересування, дислокацію штабів, складів, важких вогневих запасів та настрої особового складу.

Досить конкретно завдання військової розвідки розкрив у своїх спогадах її співробітник Іван Вислоцький: "Новітня армія послуговується двоякого роду розвідкою, явною і тайною. Явну розвідку ведуть бойові відділи, на близьку відстань, дальшу, що сягає на зади ворога. Завдання тайної розвідки є прослідкувати вороже запілля та все те, що торкається ворожої армії, її організації, озброєння, рухів, військових споруджень, постачання, включно з усіма господарськими ділянками, і настроїв населення".

Необхідно зауважити, що керівництво ЗУНР створило у збройних силах розвідувальну й контррозвідувальну служби значно оперативніше, ніж влада УНР.

2.2.5. Особливості захисту інформації органами МВС Державного центру УНР в екзилі

Підґрунтям функціонування Державного центру УНР (далі – ДЦ УНР) був наявний на території України широкий антирадянський повстансько-підпільний рух і дислокована за кордоном частина військ УНР, котрі могли здійснити наступ на територію УСРР для підтримання повстанських формувань.

Передусім був унормований правовий статус українських військ, урегульований інструкцією Міністерства військових справ Польщі від 2 грудня 1920 р., за якою Армія УНР трактувалася як дружня та союзна.

Одним із першочергових завдань уряду УНР в еміграції було реформування спеціальних служб з урахуванням нових умов. Спецслужба загальнодержавного рівня – Департамент політичної інформації (ДПІ) – входив у структуру Міністерства внутрішніх справ УНР.

До компетенції Департаменту були віднесені “справи щодо боротьби з елементами та вчинками, які направлені проти державності УНР, із їх попередження, виявлення й розслідування”. Визначалися і способи, за допомогою яких ці функції можна було виконувати, а саме: збирання різного роду інформації та направлення відомостей за належністю; здійснення через суд висилок, арештів й інших заходів боротьби з державними злочинцями в тих випадках, коли це згідно з певними законами належить до юрисдикції міністра внутрішніх справ або перевищує компетенцію місцевих адміністративних органів.

Протягом червня 1921 р. Комісія розробила структуру ДПІ й визначилася щодо компетенції його підрозділів:

1. Загальний відділ – приймання та розподіл кореспонденції Департаменту; листування ДПІ загального характеру; складання проектів наказів по Департаменту; справи особового складу; фінансове забезпечення та звітність; справи господарського й матеріального характеру.

2. Внутрішній відділ – таємні агентурні справи; створення апарату таємної агентури; викриття політичних злочинів та боротьба з ними; складання періодичних звітів і доповідей про внутрішнє становище на місцях на всій території перебування уряду та його органу; складання періодичних звітів і доповідей про діяльність політичної агентури. Є всі підстави уважати цей відділ контррозвідувальним підрозділом.

3. Закордонний відділ – справи закордонної агентури; складання періодичних звітів та доповідей за донесеннями закордонних агентів; складання звітів про діяльність українських політичних партій за кордоном та їх ставлення до влади УНР; передання внутрішньому відділу відомостей про іноземних політичних агентів, котрі виїжджають в Україну або до місця розташування уряду УНР; перевірка закордонних паспортів; справи політичних емігрантів. Цей відділ можна назвати розвідувальним.

4. Реєстраційний відділ – інструктування агентів (штатних) щодо реєстрації державних злочинців і політично підозрілих осіб (реєстраційні, алфавітні, фотографічні картки тощо); видання окремих циркулярів про розшук політичних злочинців; збирання про певних осіб та організації інформації політичного, персонального, громадського, національного, економічного та іншого характеру; загальна реєстрація всіх осіб, активних у справі відбудови УНР, а також її противників.

5. Пресовий відділ – координація роботи з пресовими відділами інших міністерств; створення бібліотеки з різними матеріалами та літературою; організація роботи з формування громадської думки; налагодження зв'язків із редакціями газет.

6. Відділ зв'язку – забезпечення безперебійного надійного зв'язку з повстансько-підпільними формуваннями на території УСРР.

Основні завдання та організаційні засади Департаменту політичної інформації досить чітко викладені в доповіді виконуючого обов'язки директора ДПІ С.Івановича міністрові внутрішніх справ від 15 січня 1921 р. Умовно цю доповідь можна поділити на дві частини. Спочатку в ній ішлося про засоби, використовувані в політичній боротьбі на території України: агітація на мітингах, сходах, у пресі з метою здобуття прихильників серед населення; провокації, поширення дезінформації про становище й наміри уряду та військ УНР; шпигунство, за допомогою якого виявляються і знищуються організації та діячі – борці за волю України; підкуп преси для формування потрібної громадської думки; підкуп впливових осіб із метою перетягування партій і груп у свій табір, сіяння чвар поміж українськими політичними партіями для їх послаблення, руйнації єдиного фронту національних сил; засилання провокаторів на службу до урядових інституцій УНР для шпигунства та виклику невдоволення урядом службовців та інших громадян; сприяння в скоєнні державних злочинів.

Провід у політичній боротьбі всередині держави належав Міністерству внутрішніх справ, котре через свій Департамент політичної інформації повинно було керувати цією боротьбою, з чого і випливають завдання Департаменту. ДПІ мав створити таку організацію, яка могла б не тільки успішно протидіяти підривним акціям ворогів української державності, але й готувати ґрунт для подальшої боротьби за самостійність України, тим більше, що вся територія захоплена ворогом, а уряд і армія перебувають на чужій землі.

Ця організація повинна "охопити" агентурною мережею всю Україну, хоч би яка там існувала влада. Відповідно до реальних обставин було необхідно для тимчасового практичного виконання завдань Департаменту організувати дві – чотири агентури (резидентури) на кордоні України, а саме: під Збручем і на Волині, з обох боків кордону. Завдання цих агентур – підтримувати щільний зв'язок між ДПІ й усіма його агентами на території України. У кожному повіті повинно бути не менше двох агентів, котрі мають працювати незалежно один від одного. Ці агенти надсилають свою інформацію та звіти в прикордонні резидентури для передання в ДПІ. З метою інформування й контролю агентів на місцях, а також для зв'язку задіювалося 12 кур'єрів. Пропонувалося також тримати агентів у районах розташування уряду УНР, у тих місцях закордону, де проживає багато біженців з України або гуртуються українські політичні партії та організації.

Велика увага приділялася агентам ДПІ, які повинні були виконувати такі завдання:

- стежити за діяльністю більшовицьких і всіх інших ворожих українській державності угруповань та створювати нові й підтримувати наявні антибільшовицькі партійні організації, повстанські загони тощо;
- інформувати населення про діяльність і наміри уряду УНР, підтримувати дух та настрій українців;
- виявляти більшовицьких шпигунів і провокаторів та інших ворожих українській державності осіб, стежити за тим, щоб такі особи не були на державній службі;
- попереджати політичні злочини, боротися з політичними злочинцями;
- стежити за діяльністю політичних організацій і партій, впливових громадських діячів, щоб знати їхні наміри та настрої, ставлення до влади УНР.

Для організації діяльності таємної політичної агентури планувалося мати чотири категорії співробітників: урядовці, агенти, кур'єри та залучені до співпраці повстанці.

Контррозвідка ДПІ також мала певні здобутки. Зокрема уряд отримував від неї різну інформацію стосовно ситуації в таборах перебування українських старшин і козаків: які частини розташовані в таборах, їхній склад; ставлення польської влади до старшин і козаків, українців узагалі. Багато уваги приділялося вивченню життя українців у таборах й оточенні, насамперед таким питанням: моральний і матеріальний стан війська та окремих осіб; культурно-освітня робота, її зміст; проведення муштри і її характер; стосунки між старшинами й козаками.

Отже, в несприятливих зовнішніх умовах, за наявності внутрішніх суперечностей у проводі УНР в еміграції, не маючи надійних союзників, Партизансько-повстанський штаб розгорнув роботу організаційного й розвідувально-підривного характеру з підготовки широкого антирадянського повстання в УСРР.

Так була налагоджена досить дієва робота ДПІ із захисту інформації в українському уряді в екзилі. Лише політичні обставини стали на заваді реалізації зазначених вище планів та принципів. Радянська влада, яка перемогла на теренах України, у цей самий період теж приділяла чимало уваги створенню системи захисту інформації.

2.3. ФОРМУВАННЯ УКРАЇНСЬКОЇ РАДЯНСЬКОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ (1920–1930 рр.)

2.3.1. Організація захисту державної таємниці

Як зазначалося вище, створення власних органів, які б захищали українські державні утворення від витоку інформації з обмеженим доступом та розвідувально-підривної діяльності ворожих спецслужб, почалося ще за часів національних змагань 1917–1921 рр. Проте нетривале існування цих утворень, стан війни не дали змоги налагодити ефективну систему захисту інформації з обмеженим доступом та нормальне функціонування окремих її інститутів.

До 1921 року більшовики не робили спроб упорядкувати процес оброблення і збереження документів, що містять державну таємницю. Наприклад, у виданому Управлінням військово-навчальних закладів Західного фронту в 1921 році навчальному посібнику "Військова таємниця" розглядалися не тільки найпростіші методи організації секретного діловодства, але й перелік зведень, які могли бути військовою таємницею. Автор навчального посібника – офіцер військової розвідки царської армії Н.Какурін – намагався в такий спосіб вирішити проблему захисту військової таємниці в діючій Червоній Армії.

Одночасно 13 жовтня 1921 року Декретом РНК був затверджений "Перелік відомостей, які становлять таємницю і не підлягають поширенню", у якому відомості поділялися на дві групи: військового й економічного характеру.

Необхідність захисту інформації з обмеженим доступом більшовики усвідомили не відразу. Першочерговим завданням стало утримання захопленої влади, придушення всілякого збройного спротиву та саботажу. У цих умовах організація ефективних органів, які б займалися захистом секретної інформації, стала для нової влади питанням виживання. Першим кроком у цьому напрямі було створення органів контррозвідки – Всеукраїнської надзвичайної комісії по боротьбі з контрреволюцією, спекуляцією, саботажем та злочинами за посадою (ВУНК) – згідно з Декретом Тимчасового робітничо-селянського уряду України від 3 грудня 1918 року.

Оскільки від успіхів на фронтах громадянської війни залежало існування влади більшовиків, цілком природно, що на цьому етапі пріоритетним став захист інформації саме військового характеру. Отже, перед новою владою постало завдання створення органів або окремих структурних одиниць у їхньому складі, які б могли ефективно протидіяти шпигунській діяльності у військах і тилу, а також розголошенню секретної інформації особами (військовослужбовці, співробітники державних установ), котрі мали до неї доступ, зокрема під час особистого спілкування, а також через органи друку.

Боротьба із шпигунством стала одним з основних завдань ВУНК. Як уже зазначалось, особлива увага приділялась саме їй та забезпеченню охорони військової таємниці в армії.

Ще одним важливим заходом було створення 5 травня 1921 року 8-го спецвідділу при ВНК. Із 6 лютого 1922 р. до 25 грудня 1936 р. цей орган називався "спецвідділ при ДПУ-ОДПУ-ГУ ДБ НКВС СРСР". А з 25 грудня 1936 р. до 9 червня 1938 р. – 9-й спецвідділ при ГУ ДБ НКВС СРСР. Перше відділення

цього спецвідділу займалося “спостереженням за всіма державними установами, партійними й громадськими організаціями з питань збереження державної таємниці”. Саме спецвідділ був головною організацією, яка координувала всі заходи щодо захисту державної таємниці, хоча основним його завданням було розроблення керівних документів, які регламентували різні аспекти організації цього захисту.

9 березня 1919 року Всеросійська надзвичайна комісія (ВНК) прийняла рішення про організацію в Україні особливих відділів на зразок діючих у Російській Соціалістичній Федеративній Радянській Республіці (РСФРР). Після цього ВНК почала формувати підпорядковані їй особливі відділи у військових частинах Українського фронту, а 6 травня 1919 р. Рада народних комісарів (РНК) Української Соціалістичної Радянської Республіки (УСРР) ухвалює “Положення про особливий відділ при ВУНК”, якому доручено проводити боротьбу з контрреволюцією та шпигунством у Червоній Армії й на флоті УСРР як на фронтах, так і в тилу. Повноваження ВУНК здійснювати боротьбу з усіма контрреволюційними проявами, шпигунством, злочинами за посадою як на внутрішньому фронті, так і в армії й на флоті, були закріплені в новому “Положенні про Всеукраїнську і місцеві надзвичайні комісії”, прийнятому Всеукраїнським центральним виконавчим комітетом (ВУЦВК) 30 травня 1919 року.

Отже, захист таємних відомостей став однією з основних функцій новоствореної установи майже з перших днів її функціонування. На цьому етапі окремого підрозділу, виключною прерогативою якого був би захист таємної інформації чи інформації з обмеженим доступом, не було. Цю функцію виконували кілька органів під час проведення контррозвідувальних заходів у найважливіших сферах життєдіяльності держави (військовій, економічній тощо).

У міру того, як придушувався збройний спротив новій владі, змінювались і пріоритети у сфері захисту інформації. Все більшої важливості набуває питання захисту економічних відомостей, тоді як актуальність захисту відомостей військового характеру поступово знижується.

Вище вже йшлося про те, що 5 травня 1921 р. була прийнята постанова Малого Раднаркому при ВНК про створення спеціального відділу під керівництвом Г.І.Бокія. Це відбилось на структурних змінах ВУНК: у травні 1921 р. особливий відділ увійшов до створеного секретно-оперативного управління, яке вело боротьбу зі шпигунством і контрреволюцією в Червоній Армії й Військово-Морському флоті, а також вирішувало контррозвідувальні завдання й боролось із політичним

бандитизмом на території країни. Водночас на базі економічного відділу ВУНК було створено економічне управління (ЕКУ), уповноважене на боротьбу з економічним шпигунством, контрреволюційним саботажем, спекуляцією й посадовими злочинами в установах і на підприємствах промисловості.

Як зазначалось вище, не менш важливим завданням, яке необхідно було вирішувати, стало недопущення розголошення таємних відомостей. Крім оперативних заходів, які проводились чекістськими органами з метою запобігання розголошенню військовослужбовцями секретної інформації, було уведено військову цензуру, яка стала елементом радянської системи захисту інформації.

У РСФРР Військово-цензурне відділення при оперативному відділі Народного комісаріату з військових справ почало діяти з січня 1918 року. Це відділення та місцеві цензори при окружних, губернських і повітових військових комісаріатах здійснювали поштово-телеграфний контроль. Унаслідок об'єднання військових органів та військового командування радянських республік України, Росії, Латвії, Литви й Білорусії, передбаченого Постановою ВЦВК від 1 червня 1919 року, і їх підпорядкування РКП(б) та уряду Росії органи військової цензури почали діяти й на території України, окупованій більшовиками. Зі створенням особливих відділів у системі чекістських органів служба військової цензури перейшла в їхнє розпорядження – стіл військової цензури структурно входив до інформаційної частини оперативного відділу особливого відділу ВНК.

Відповідно до "Положення про військову цензуру", прийнятого в грудні 1918 року, військова цензура з метою збереження військової таємниці здійснювала попередній огляд усіх публікацій преси, малюнків, фото- й кінознімків, призначених до оприлюднення, у яких повідомлялись відомості військового характеру; усіх призначених для оприлюднення наказів, офіційних повідомлень тощо, що містили військові відомості; перегляд міжнародних і, в разі потреби, внутрішніх поштових відправлень та телеграм; контроль за міжміськими переговорами. Постановою РНК РСФРР від 13 жовтня 1921 року було затверджено "Положення про військову цензуру ВНК".

Ще одним каналом витоку інформації з обмеженим доступом, відомостей таємного характеру могли стати друковані видання. Тому влада більшовиків взяла курс на поступове установлення контролю над видавничою справою.

На території України, зайнятій більшовиками, видавничим монополістом став відділ пропаганди й агітації при ВУЦВК, який централізував усю видавни-

чу справу, завідуючи розподілом паперу і поліграфічними засобами для видання різного змісту друкованих творів у загальноукраїнському масштабі, регулюючи та контролюючи видання, які друкувались як у підпорядкованих комісаріатам, так і в приватних видавництвах.

У травні 1919 року всі окремі видавництва при комісаріатах були об'єднані у Всеукраїнське видавництво, створене при ВУЦВК. Приватні видавництва, а також видавництва при різноманітних спілках, кооперативах підлягали реєстрації у Всеукраїнському видавництві для отримання від нього права на одержання паперу й друкування. Останньому надавались повноваження скорочувати і повністю припиняти вихід у світ тих чи інших періодичних видань.

Такі заходи були направлені на установлення контролю над випуском друкованої продукції для запобігання "ідеологічній контрреволюції", але об'єктивно вони також сприяли запобіганню витоку інформації з обмеженим доступом через друковані засоби.

Після завершення громадянської війни для того, щоб вистояти в обстановці міжнародної ізоляції, а також активно діяти на міжнародній арені в майбутньому, радянським республікам потрібно було нарощувати економічний потенціал, створювати оборонну промисловість.

За цих умов пріоритети в питанні захисту інформації змінюються остаточно. Все більшого значення для держави набуває захист секретної інформації економічного, зокрема оборонного, характеру. Відповідно статус, завдання органів, котрі забезпечували збереження державної таємниці, та їхня структура також підлягали коригуванню. Крім того, економічні перетворення, які почались у країні, потребували уніфікації режимно-секретної діяльності в державному масштабі та виділення окремого органу, який би контролював і координував режимно-секретну діяльність усіх радянських установ та підприємств.

22 березня 1922 року ВУЦВК прийняв постанову про ліквідацію Всеукраїнської надзвичайної комісії і про організацію Державного політичного управління при НКВС УСРР, одним із основних завдань якого було "вжиття заходів охорони й боротьби зі шпигунством" на всій території України. На підставі відповідних угод урядів РСФРР і УСРР було уведено інститут повноважних представників ДПУ в Україні для координації спільних дій у боротьбі з контрреволюцією. Голова Держполітуправління УСРР був одночасно повноважним представником ДПУ РСФРР на території України.

Керівництво ДПУ намагалося розмежувати контррозвідувальні функції між оперативними підрозділами. У травні 1922 року було реорганізовано Особливий відділ, із якого виділено контррозвідувальний відділ (КРВ) у складі секретно-оперативного управління ДПУ в центрі (аналогічно й на місцях у складі СОУ губвідділів ДПУ). На КРВ покладалось ведення контррозвідувальної роботи за кордоном і на території нашої країни (на об'єктах промисловості, транспорту та ін., а також у Червоній Армії й Військово-Морському флоті).

Після створення в грудні 1922 року Союзу Радянських Соціалістичних Республік постановою Президії ЦВК СРСР від 2 листопада 1923 р. створено Об'єднане державне політичне управління (ОДПУ) при РНК СРСР. При РНК республік ОДПУ мало своїх уповноважених, через яких координувало роботу місцевих органів держбезпеки. Голова ДПУ УСРР одночасно був і уповноваженим ОДПУ СРСР при РНК УСРР.

Із початком розбудови в СРСР військової промисловості посилювались і контррозвідувальні заходи, спрямовані на недопущення витоку секретної інформації з оборонних об'єктів. У 1927 році у складі економічного управління ОДПУ створено спецвідділ, якому було доручено організувати контррозвідувальну роботу на об'єктах військової промисловості. На всіх підприємствах, а особливо на важливих об'єктах, були присутні органи держбезпеки.

Крім того, вживалися заходи із засекречування й маскування об'єктів військової промисловості. 9 липня 1927 року спільним наказом Вищої ради народного господарства (ВРНГ), Народного комісаріату військових і морських справ і ОДПУ було уведено в дію систему заходів із засекречування роботи підприємств військової промисловості.

Забезпечення секретності здійснюваних заходів потребувало належної уваги не лише спеціальних органів, але й усіх міністерств, відомств, установ і підприємств, діяльність яких була пов'язана з державною таємницею. Тому виникла необхідність створення органу, який би координував окремі види діяльності щодо її захисту. 3 січня 1924 року у складі ДПУ України було сформовано спецвідділ, який об'єднував шифрувальну справу у всіх народних комісаріатах і центральних установах республіки (при ВНК РСФРР спецвідділ діяв із 6 лютого 1922 року). Співробітники спецвідділу ДПУ УСРР проводили інструктажі з шифрувальної роботи в усіх народних комісаріатах і центральних установах, розробляли шифри для всіх центральних відомств і установ, підбирали

кадровий склад для шифрувальних органів, вели загальний облік і спостереження за дотриманням правил конспірації шифрувальної роботи.

Потрібно було також на державному рівні сформулювати єдині вимоги до виготовлення, користування, збереження, передання, транспортування та обліку секретних документів, режиму секретності на підприємствах, в установах і організаціях. Ще у 1922 році Секретаріат ЦК РКП(б) ухвалив Постанову "Про порядок збереження і руху секретних документів", у якій було вперше зафіксовано, що для організації й ведення секретного діловодства необхідно створити секретні частини.

Секретне діловодство регламентували також відомчі інструкції та накази. У 1926 році було видано низку загальносоюзних інструкцій, зокрема: Інструкція з ведення секретного і шифрувального діловодства; Інструкція місцевим органам ОДПУ за спостереженням за постановкою секретного і мобілізаційного діловодства; Інструкція з ведення архівного діловодства і передачі справ в органи Центрархіву; Інструкція про порядок підготовки і конвертування кореспонденції, яка надсилається дипломатичною поштою; Постанова РНК СРСР "Про створення воєнізованої охорони для охорони підприємств і споруд, що мають особливе значення для держави, і про організацію силами військ ОДПУ військової охорони підприємств і споруд, що мають виняткове значення для оборони країни" (травень 1927 року); Інструкція із секретного діловодства та Інструкція із шифрувального діловодства (1928 рік). Ці інструкції діяли недовго. У 1928 році було прийняте рішення про необхідність відокремлення секретного діловодства від шифрувального.

У 1928 році спецвідділом ОДПУ видано першу загальносоюзну Інструкцію з таємного діловодства, відповідно до якої саме спеціальний відділ при ОДПУ СРСР здійснював керівництво державними, партійними, професійними, кооперативними і громадськими установами й організаціями всіх республік СРСР із питань секретного діловодства шляхом загального спрямування цієї роботи, інспектування в цьому відношенні центральних і місцевих установ, організації секретних і шифрувальних органів. Усі розпорядження зазначеного підрозділу, що стосувались секретного й мобілізаційного листування, а також шифрувальної роботи, були обов'язковими до виконання.

У відомствах, організаціях і установах, на території союзних республік за роботою секретних та шифрувальних органів спостерігали спеціальні відділення повноважних представництв ОДПУ в республіках, які безпосередньо підпорядковувались спеціальному відділу ОДПУ.

Спеціальне відділення організовувало таємне й шифрувальне діловодство у всіх установах як місцевого, так і союзного значення, розміщених на території України, здійснювало контроль за порядком ведення та зберігання мобілізаційних і шифрувальних матеріалів, узгоджувало питання про допуск громадян до секретного й шифрувального діловодства, вело облік осіб, які завідували секретним діловодством в установах, розробляло шифри й забезпечувало ними всі установи на території повноважного представництва, крім тих, що користувались шифром, установленим спеціальним відділом ОДПУ.

На місцях повсякденне спостереження та роботу з обслуговування секретних органів губернських, окружних, залізничних установ і військових частин Робітничо-селянської Червоної Армії (РСЧА) проводили відповідно місцеві органи ОДПУ (губвідділи, окрвідділи, прикордонні, транспортні й особливі відділи ОДПУ) за інструкціями під керівництвом спецвідділу при ОДПУ чи спецвідділень при повноважених представництвах ОДПУ.

24 квітня 1926 року Постановою РНК було затверджено новий “Перелік відомостей, що є за своїм змістом спеціально охоронюваною державною таємницею”. Це був фактично перший відкритий перелік відомостей для органів державної влади, які працювали з державною таємницею. Усі відомості були розподілені на три групи: військового, економічного й іншого характеру. Крім цього, увели три категорії таємності. Зазначеним у Переліку відомостям був присвоєний один із трьох грифів таємності: “цілком таємно”, “таємно” й “не підлягає оголошенню”.

Перелік мав низку недоліків. Тому через два місяці спецвідділ при ОДПУ видав секретний “Перелік питань цілком таємної, таємної і такої, що не підлягає розголошенню, інформації”, у якому були враховані всі недоліки попереднього документа. Змінилася і сама структура. Тепер усі відомості були розподілені на чотири категорії: питання військового, фінансово-економічного, політичного (зокрема партійного) й загального характеру. Для розмежування документів за ступенем секретності установи розробляли перелік питань, який узгоджувався із спеціальним відділом при ОДПУ чи відповідним спецвідділенням.

У 1929 році була прийнята нова “Інструкція місцевим органам ОДПУ по спостереженню за станом секретного і мобілізаційного діловодства установ і організацій”. Тим самим, були підтверджені функції ОДПУ з контролю за дотриманням вимог секретного діловодства.

Тоді ж, наприкінці 20-х років, було проведено уніфікацію складу секретних органів і встановлено стандартну номенклатуру посад секретних апаратів установ й організацій. У центральних апаратах наркоматів створені секретні відділи або секретні частини, а в головкомах, управліннях і відділах – секретні частини й секретні відділення.

Номенклатура посад секретних органів передбачала такі посади: завідувач, інструктори, секретарі (помічники секретарів), кореспонденти, старші друкарки (друкарки), помічники секретарів, архіваріуси. Структура секретних органів була така: секретне діловодство, машбюро, креслярське бюро, стенографічне бюро, група контролю, група із обліково-розподільної роботи, бюро перепусток і довідок.

Конкретний склад таких органів визначався наркоматами за узгодженням зі спецвідділом при ОДПУ. Служби захисту секретної інформації називалися по-різному: секретні частини, підвідділи секретного діловодства, шифрувальні відділи тощо.

Прийняті наприкінці 20-х років інструкції діяли до 1940 року; значно довше проіснувала без змін номенклатура посад та структура режимно-секретних органів.

2 січня 1940 р. Постановою РНК затверджено нову “Інструкцію з ведення секретних і мобілізаційних робіт і діловодства в установах і на підприємствах”. Ця інструкція регламентувала такі питання: категорування відомостей за ступенями їх секретності, порядок розроблення переліку відомостей, що підлягають засекречуванню, і порядок установлення і зміни грифа таємності; функції 7 відділу УДБ, функції й відповідальність керівників установ за стан режиму секретності; назви секретних органів, порядок їх створення і ліквідації, основні завдання; вимоги до працівників, які допущені до роботи із секретною інформацією; порядок оформлення допусків до секретних робіт і документів; вимоги з обмеження доступу до секретної інформації; порядок ведення секретного діловодства й роботи з документами в секретних бібліотеках і архівах; порядок поводження із шифротелеграмами в установах, що не мають шифрувальних органів; порядок збереження секретних і мобілізаційних документів; порядок обліку, збереження спецпродукції та поводження з нею; вимоги до виробництва кіно- і фотозйомки; порядок проведення секретних засідань. Зазначена інструкція була направлена на посилення режиму секретності, вироблення єдиної системи секретного діловодства та забезпечення охорони секретної інформації в установах і на підприємствах СРСР та УРСР.

2.3.2. ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ПРЕСІ ТА ВИДАВНИЧІЙ ГАЛУЗІ

Ще однією формою діяльності, яка застосовувалася державними органами для захисту інформації з обмеженим доступом, секретної інформації, у той період була цензура – феномен радянської системи захисту інформації. Вона була як відкрита – стосовно друкованих видань, так і закрита, здійснювана органами ДПУ. Слід відмітити, що зміна пріоритету характеру захищуваної інформації відбилась як на функціях органів цензури, так і на їхній організаційно-штатній структурі.

Для посилення контролю за видавничою справою держава намагалася встановити в цій галузі власну монополію, особливо щодо випуску книжкової продукції. Тому 6 вересня 1920 р. кооперативний комітет УСРР ухвалив Постанову "Про об'єднання кооперативно-видавничої справи у республіці", а 21 грудня 1922 р. було створено Всеукраїнську книготоргову спілку. На засіданні малої колегії Головполітосвіти 26 грудня 1922 р. розглядалося питання про практичні заходи боротьби з розповсюдженням антирадянської літератури. Члени колегії ухвалили посилити адміністративний тиск на видавництва, зобов'язавши взяти їх пайовиками Головполітосвіту, Держвидав, КСМУ та Книгоспілку; предметом особливої уваги мала стати радянська література. Стосовно приватних видавництв РНК УСРР розробив у жовтні 1921 р. спеціальні правила, відповідно до яких кожне видавництво подавало Всеукрвидаву загальний видавничий план та мусило отримати спеціальний дозвіл на друкування книг. Приватні видавництва обов'язково реєстрували статути в органах НКВС. У положенні "Про порядок розподілу друкованих видань" від 14 жовтня 1921 р. розкривалися основні правила розподілу друкованих видань. Тут зазначалося, що їхнє розповсюдження здійснювали Всеукрвидав та Держвидав, а також приватні видавництва в порядку виконання держплану. Націоналізовані книжкові фонди колишніх приватних власників стали належати Всеукрвидаву, котрий мав монопольне право на оптову закупівлю продукції в будь-яких видавництвах. Приватні особи і кооперативи могли відкривати підприємства для продажу друкованих видань за попереднім дозволом Всеукрвидаву або його місцевих органів, які реєстрували підприємства, здійснювали нагляд за ними та торгів-

лею книгами, ухвалювали рішення про їх ліквідацію в разі порушення статуту й норм діяльності, але за погодженням із судовими органами.

Діяльність кооперативних і приватних видавництв відбувалася під жорстким контролем розгалуженої системи органів радянської цензури. Так, у грудні 1920 р. при Наркоматі освіти УСРР виникло Головне управління з питань політосвіти (Головполітосвіта), до функцій якого входила не лише політико-освітня робота в масах, а й цензура друку. 19 вересня 1922 р. було створене Центральне управління у справах друку при Головполітосвіті Наркомосу УСРР (ЦУД), яке займалося контрольно-ревізійними справами. Воно активно співпрацювало з органами Державного політичного управління (ДПУ). У другій половині 20-х рр. відбулася модернізація функцій ЦУДу. 6 жовтня 1925 р. на підставі постанови РНК УСРР замість ЦУДу виник Комітет із нагляду за діяльністю видавництв і розповсюдженням друкованих видань при Наркоматі внутрішньої торгівлі УСРР. Він займався регулюванням господарсько-економічної та торговельної діяльності громадських і власних видавничих підприємств та організацій із видання, торгівлі й розповсюдження друкованих видань. У березні 1928 р. Комітет із нагляду за діяльністю видавництв і розповсюдженням друкованих видань було ліквідовано, а натомість створено Комітет у справах друку Наркомторгу УСРР, який 27 січня 1930 р. реорганізували у Комітет у справах друку при РНК УСРР. Положення про Комітет у справах друку при РНК УСРР передбачало: планування та регулювання видавничої діяльності, координацію роботи паперової й поліграфічної промисловості, розповсюдження продукції видавничої галузі.

Комітет був безпосередньо підпорядкований РНК УСРР. Питання, які вимагали рішення в загальному масштабі, вирішувались через Комітет у справах друку при РНК СРСР у Москві, а також через постійне представництво УСРР при РНК СРСР. 8 січня 1933 р. постановою РНК УСРР Комітет було ліквідовано, а його функції передано Бюро друку при Держплані УСРР. Кооперативні та приватні видавництва дозвіл на друк отримували від ЦУДу, особливо це стосувалося видань із “чорного списку”.

Із метою об’єднання всіх видів цензури друкованих видань у РСФРР, а згодом і в Україні було створено окремий орган – Головне управління у справах літератури і видавництва (Головліт) при Міністерстві народного просвітництва (6 червня 1922 року). Орган із такими ж повноваженнями було створено і в Ук-

раїні постановою РНК УСРР від 11 серпня 1922 року – Центральне управління у справах друку при Головному управлінні політичної просвіти Наркомату просвіти УСРР та його місцеві органи при губполітпросвітах.

До завдань Центрального управління у справах друку (Укрголовліту) і його місцевих органів належали: "попередній перегляд усіх призначених до опублікування чи поширення творів як рукописних, так і друкованих, видань періодичних і неперіодичних, знімків, малюнків, карт тощо; видача дозволів на право видання окремих творів, а також органів друку, періодичних і неперіодичних; видача дозволів на запровадження приватних друкарень, їх реєстрація та подальше спостереження за їхніми діями; складання списків і визначення творів, заборонених до друку, репродукції, продажу й поширення; видання правил, розпоряджень, інструкцій у справах друку, обов'язкових для всіх органів друку, видавництв, поліграфічних підприємств, бібліотек, читалень, книжкових магазинів і складів". Серед заборонених до друку і поширення видань зазначались ті, що "розголошують військові таємниці республіки".

Головліт забороняв видання та розповсюдження творів, які б агітували проти радянської влади, розголошували військову таємницю республіки, збуджували громадську думку шляхом поширення неправдивих відомостей, провокації національних чвар; а також творів порнографічного характеру. Завідуючого Головлітом призначала Колегія Наркомосу, а його двох помічників – відповідно Реввоєнрада та ДПУ республіки. Місцеві органи Головліту відповідали центральним органам, хоча в губернських містах діяли цензори, які призначалися губернським відділом народної освіти, а затверджувалися Головлітом.

Маючи свого представника в Колегії ЦК КП(б)У, Головліт брав участь у розробленні партійних директив у сфері друку, набув ознак і функцій єдиного центрального цензурного органу. Головліт співпрацював із відділом преси ЦК КП(б)У, НКО, Головреперткомом, Головнаукою, а також діяв під загальним керівництвом ДПУ, яке контролювало надходження друкованої продукції із-за кордону. Упродовж другої половини 20-х рр. було значно розширено функціональні обов'язки Головного управління у справах літератури та видавництва. До зазначених вище додались такі: догляд за виконанням видавничих планів; розгляд питань про відкриття газет, часописів, книжкових видань; догляд за видавничою діяльністю; реєстрація окремих видань; вивчення книжкового ринку, літературних течій та змісту друкованих творів України; бібліографічна розро-

бка друкованої продукції УСРР і постачання книгосховищ республіки, що їх проводила Книжкова палата.

У Київській, Одеській, Катеринославській губерніях створювались губвідділи Центрального управління у справах друку. В усіх губернських містах запроваджувалась посада уповноваженого Центрального управління у справах друку, якого призначав Губполітпросвіт і затверджувало Центральне управління.

Штатним розкладом Організаційно-контрольного відділу Укрголовліту було передбачено посади "політконтролера з військової цензури", літературного відділу – "політконтролерів" із соціально-економічної та науково-технічної літератури. Такі співробітники, а також уповноважені Укрголовліту, котрі працювали безпосередньо в редакціях часописів, у своїй діяльності із запобігання витоку таємних відомостей через друковані органи керувались спеціальним переліком відомостей, що становили державну таємницю. Категорії відомостей, заборонених до відкритого опублікування, були визначені "Положенням про Військову цензуру", затвердженим декретом РНК РФСРР від 13 жовтня 1921 року; 14 квітня 1924 року цей перелік відомостей було оновлено й уведено в дію наказом РНК.

Боротьба з поширенням друкованих видань, не дозволених Укрголовлітом, покладалась на органи ДПУ. Вони також здійснювали нагляд за типографіями й іншими поліграфічними підприємствами, митними і прикордонними пунктами, вели боротьбу з поширенням підпільних видань, перевезенням через кордон для розповсюдження забороненої до обігу літератури; вилучали книги, які не були дозволені Центральним управлінням у справах друку і його органами відповідно до спеціальних списків. Виконання цих завдань входило до функціональних обов'язків служби політконтролю, керівництво якою здійснював відділ політконтролю секретного оперативного управління ОДПУ. Крім наведених вище функцій, відділ політконтролю з метою збереження військової, політичної й економічної таємниць радянської держави, виявлення і попередження злочинної діяльності "ворожих елементів" проводив негласний перегляд кореспонденції осіб, котрі становили оперативний інтерес для органів ОДПУ.

Верховним політичним куратором усієї цензурної системи в республіці був ЦК КП(б)У. До цензурних органів цього періоду слід віднести Колегію відділу преси. Активну "цензорську роботу" проводив Державний науково-методичний комітет, який складався із двох секцій: науково-педагогічного комітету та методичного комітету профосвіти. Увесь книговидавничий приватний сектор був

ліквідований, а кооперативні видавництва відповідно до постанови РНК УСРР від 21 серпня 1930 р. перейшли до Державного видавничого об'єднання України.

Отже, з метою захисту інформації про диктатуру в УСРР у 1930 році поступово сформувалася структура органів політичної цензури та певні інститути, які здійснювали контроль за найрізноманітнішими сферами духовного життя суспільства й інформацією, яка в ньому циркулювала.

2.3.3. Організація захисту рішень партії

Чимало уваги в зазначений період держава приділяла захисту інформації, яка містилася в рішеннях ЦК РКП(б), оскільки вже із 20-х років партія робила спроби підпорядкувати своєму курсу все суспільно-політичне та економічне життя країни. Звісно, щоб імітувати активну роботу, зв'язок із масами та демократичність рішень партії, ЦК РКП(б) змушений був публікувати їх в офіційному партійному виданні. У силу того, що при тоталітарному режимі демократія розвиватися не могла, частину своїх рішень партія була змушена засекречувати.

Перша спроба навести порядок у сфері оброблення й збереження секретних документів була започаткована 30 серпня 1922 року. Тоді Секретаріат ЦК РКП(б) прийняв Постанову "Про порядок збереження і руху секретних документів". У цьому документі вперше було зафіксовано, що для організації й ведення секретного діловодства необхідне створення секретних частин.

У листопаді того ж року Оргбюро ЦК РКП(б) ухвалило Постанову "Про порядок збереження секретних постанов ЦК РКП(б)". Постанова Політбюро ЦК РКП(б) про створення при ДПУ спеціального міжвідомчого бюро з дезінформації (Дезінформбюро) у складі представників від ДПУ, ЦК РКП(б), НКІС, Штабу РСЧА датована 11 січня 1923 р.

Основними завданнями бюро були: облік відомостей, які надходять у ДПУ і Розвідуправління й інші установи, про ступінь поінформованості іноземних розвідок про Росію; облік і характеристика відомостей, які цікавлять противника; виявлення ступеня поінформованості противника про СРСР; складання і технічне виготовлення низки помилкових відомостей і документів для уведення противника в оману; постачання противника вказаними вище матеріалами й документами через відповідні органи ДПУ та Розвідуправління. Так була започаткована багаторічна практика численних ефективних операцій із дезінформації

противника. Крім цього, відомості про рівень поінформованості противника дозволяли органам контррозвідки оперативно виявляти факти витоку секретної інформації й нейтралізувати ворожих агентів.

Отже, внутрішній розвиток країни та зовнішня обстановка зумовили необхідність захисту певних видів інформації, а це змушувало державу реагувати й уживати адекватних заходів, у тому числі створювати відповідні органи, що реалізували її політику із захисту інформації. Зміни пріоритетів у цій сфері приводили до коригування державної політики, наслідком чого було виникнення або ліквідація певних органів, зміна їхньої структури та функціональних обов'язків.

У цей період у СРСР і Україні було закладено основи системи захисту секретної інформації, яка розвивалась та ефективно діяла упродовж кількох наступних десятиліть. Зокрема були створені суб'єкти захисту інформації, повноваження яких на той час відповідали чинним вимогам. Оскільки секретна інформація була об'єктом спрямувань розвідувальних органів противника, закономірно, що із самого початку такі повноваження було покладено на контррозвідувальні підрозділи органів державної безпеки. Згодом оперативні заходи було поєднано із заходами щодо організації та контролю за дотриманням режимно-секретних вимог на підприємствах, в установах та організаціях.

Отже, органи й підрозділи державної безпеки захист секретної інформації здійснювали шляхом проведення контррозвідувальних заходів, організації режимно-секретної діяльності, військової цензури тощо. Крім діяльності спецслужби, роль якої у збереженні секретної інформації була визначальною, було створено механізм захисту від розголошення секретної інформації через друковані органи. Закладена в ті часи структура проіснувала протягом усього радянського періоду й була успадкована незалежною Україною.

2.3.4. Правові основи забезпечення захисту інформації органами ДПУ УСРР

В умовах тоталітарного політичного режиму захист інформації з обмеженим доступом набуває гіпертрофованих форм, супроводжується масовими порушеннями прав людини. Однак у той же час система захисту державної таємниці характеризується певною ефективністю і її окремі елементи, якщо вони не суперечать нормам чинного законодавства, можуть бути використані сьогодні.

У 1924–1925 рр. на органи ДПУ УСРР був покладений контроль за додержанням режиму таємності та веденням шифрувальної справи. Постановою Ради Народних Комісарів (РНК) УСРР від 10 вересня 1924 р. при ДПУ УСРР був створений спеціальний відділ. На нього покладались обов'язки щодо керування шифрувальною роботою у всіх наркоматах і центральних установах УСРР (крім загальносоюзних), розроблення та облік шифрів, підбір і облік особового складу шифрувальних апаратів, загальний нагляд за додержанням конспірації в шифрувальній роботі. Спеціальний відділ при ДПУ УСРР був організований на базі шифрувального бюро ДПУ УСРР. Постановою РНК УСРР від 24 листопада 1924 р. було затверджено штат спеціального відділу ДПУ УСРР у кількості п'яти осіб.

Постановою РНК УСРР від 6 грудня 1924 р. була затверджена інструкція, яка надавала органам ДПУ УСРР право контролю та нагляду за додержанням установленого порядку прийому, розсилки й зберігання таємного листування в центральних установах УСРР, у тому числі в загальносоюзних і об'єднаних наркоматах. Цією ж інструкцією до відання органів ДПУ УСРР був віднесений облік осіб, які вели роботу з таємною документацією. Керівники установ повинні були відбирати в останніх підписку про суворе дотримання службової таємниці та оформляти низку інших документів, направляючи їх до органів ДПУ УСРР.

Перелік цих документів і порядок погодження з органами ДПУ допуску осіб до роботи з таємною, шифрувальною та мобілізаційною кореспонденцією був конкретизований у подальших циркулярах ДПУ УСРР і спеціальних міжвідомчих нормативних актах. Згідно з циркуляром ДПУ УСРР від 12 квітня 1927 р. на всіх осіб, яких передбачалося залучати до таємного та мобілізаційного діловодства в спецвідділ ДПУ УСРР і окружні відділи ДПУ на місцях, мали направлятися заповнена анкета, рекомендації двох членів КП(б)У зі стажем роботи не менше п'яти років, завірені партійним осередком або райкомом; завірена фотокартка.

Інструкцією з таємного діловодства, затвердженою 30 травня 1928 р. начальником спецвідділу Об'єднаного державного політичного управління (ОДПУ), всім особам, які вели таємну та мобілізаційну роботу, заборонялось відвідувати іноземні місії й представництва, а також підтримувати стосунки зі співробітниками цих установ. Установлений порядок допуску осіб до таємного й мобілізаційного діловодства поширювався на всі державні, партійні, професійні та громадські установи й організації.

Органи ДПУ УСРР у цей період також займалися визначенням переліку відомостей, листування з яких відносилось до категорії таємного, цілком таємного або такого, що не підлягає розголошенню. У березні 1924 р. шифр-бюро ДПУ УСРР уведений у дію циркуляр спецвідділу ОДПУ № 23981/С від 22 грудня 1923 р., який установив подібний перелік у військовій, економічній, політичній та інших сферах державного життя.

Він періодично змінювався й доповнювався новими пунктами. У вересні 1926 р. спецвідділом при ОДПУ був розроблений новий орієнтовний перелік питань таємного, цілком таємного і такого, що не підлягає розголошенню, листування; у лютому 1928 р. директивою ДПУ УСРР доопрацьовано перелік фінансово-економічних питань таємного характеру тощо. Всі суперечки між установами стосовно втаємничення матеріалів або зняття з них грифу таємності відповідно до циркуляру ДПУ УСРР № 106644 від 4 листопада 1927 р. мав розглядати спецвідділ ДПУ УСРР.

Пересилання таємної кореспонденції всіх категорій здійснювали виключно органи ДПУ УСРР. Ця функція покладалась на спеціально сформований у 1922 р. фельд'єгерський корпус (ФК) ДПУ УСРР.

У березні 1926 р. НКФ УСРР звернувся з проханням до начальника спецвідділу ДПУ УСРР у зв'язку з незадовільним станом таємного діловодства у фінансових відділах провести обстеження стану таємного діловодства через окрвідділи ДПУ і про його результати доповісти НКФ УСРР. Обстеження стану таємного діловодства в НКФ Автономної Молдавської СРР (АМСРР) і окружних фінансових відділах було завершено наприкінці травня 1926 р.

Органи ДПУ також вивчали стан таємного діловодства і мобілізаційного документування також в інших державних установах і на підприємствах.

Під контролем органів ДПУ в цій сфері діяльності перебували й партійні установи, їхні осередки в державних органах і громадських організаціях. На підставі постанови Секретаріату ЦК КП(б)У від 6 вересня 1927 р. і циркуляру ДПУ УСРР № 047493 від 5 травня 1928 р. передбачалося провести обстеження порядку ведення таємного діловодства, зберігання таємних матеріалів; перевірку осіб, які здійснюють таємне листування в міських районних комітетах КП(б)У. Проведення перевірки мало попередньо погоджуватися з окружними комітетами КП(б)У.

6 березня 1928 р. ДПУ УСРР надіслало директиву всім своїм окрвідділам щодо перевірки порядку ведення й зберігання таємного та цілком таємного листування фракцій КП(б)У у всіх професійних і громадських організаціях.

29 жовтня 1929 р. Секретаріат ЦК КП(б)У доручив спеціальному відділу ДПУ УСРР систематично вивчати стан таємного та шифрувального діловодства й поводження з конспіративними матеріалами ЦК КП(б)У в усіх окружних партійних комітетах (ОПК), а висновки подавати на розгляд Секретаріату ЦК КП(б)У.

Обстеження стану таємного й мобілізаційного листування здійснювали інспектор спеціального відділу ДПУ УСРР і представники місцевих територіальних та спеціалізованих органів ДПУ УСРР за спеціальними мандатами, завізованими у відповідних органах ДПУ УСРР. За результатами перевірки складалися акти обстеження, у яких констатувалися основні недоліки, виявлені під час обстеження, і пропонувались конкретні заходи із їхнього усунення. Найбільш поширеними порушеннями були: допуск осіб до таємних робіт без узгодження їх кандидатури в органах ДПУ УСРР, відправлення на цих осіб до органів ДПУ неповного переліку необхідних документів або неправильне оформлення останніх; зберігання таємних документів у непередбачених для цього місцях; засекречення нетаємних матеріалів; відправлення таємних матеріалів звичайною поштою тощо.

Циркуляром ДПУ УСРР від 31 травня 1927 р. контроль і нагляд за виконанням указівок зазначеного акта покладався на відповідні окрвідділи ДПУ, які проводили обстеження. Всі підприємства, установи та організації після отримання акта обстеження мали провести у визначений у заключній частині документа термін заходи щодо усунення недоліків і повідомити про це окрвідділ ДПУ. Органи ДПУ натомість періодично доповідали про наслідки обстежень у партійні установи. Усі випадки порушення нормативно-правових актів, які регламентували режим таємності, розслідували органи ДПУ УСРР. Отже, в середині 20-х рр. до компетенції органів ДПУ УСРР був віднесений комплекс функцій у сфері забезпечення режиму таємності – визначення переліку відомостей закритого характеру, допуск осіб до роботи з таємною інформацією, встановлення правил роботи з таємною документацією, організація таємного листування, обстеження стану таємного діловодства в державних і партійних установах; розслідування правопорушень тощо.

Монополізація органами ДПУ УСРР повноважень щодо забезпечення режиму таємності певною мірою сприяла посиленню службової дисципліни, поліпшенню стану захисту державної таємниці, зменшенню кількості правопорушень у цій сфері. У той же час, в умовах згортання непу та формування адміністративно-командної системи створена впродовж 1924–1928 рр. нормативно-правова база стала формально-юридичною основою проведення органами ДПУ УСРР масових репресивно-каральних заходів.

2.3.5. Організація захисту військової інформації

Велику увагу в СРСР приділяли захисту військової інформації, особливо напередодні Другої світової війни. З цією метою було видано кілька розпорядчих документів щодо порядку забезпечення охорони військової інформації. Це зокрема "Настанова з мобілізаційної роботи у військових частинах, управліннях, установах і закладах РСЧА", уведена в дію наказом Наркомвоєнмору СРСР № 070 від 25 вересня 1930 року. Відповідно до наказу НКО СРСР № 024 набувало чинності "Положення про центральну військову цензуру РУ". Приділяли увагу в РСЧА й збереженню в таємниці інформації про дислокацію військ. Ці питання регулювали накази НКО СРСР № 0043 "Про основи й організацію прихованого керування військами", № 0105 "Про заходи щодо зашифровки найменувань військових частин і збереження в таємниці дислокаційних відомостей" (1937 рік) та ін. Вже на початку Другої світової війни наказом НКО СРСР № 0150 від 4 вересня 1939 року уведено в дію "Настанову із секретного діловодства в РСЧА". Головне її призначення полягало в запобіганні витоку військової інформації.

У повоєнний період і добу протистояння двох систем практично вся інформація була державною таємницею, а військова – одним із її видів. Тому забезпечення її охорони здійснювалося відповідно до загальнодержавних, а також внутрішньовідомчих інструкцій, які регулювали ці питання.

2.4. РОЗВИТОК РАДЯНСЬКОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ в 40–80-х рр. XX ст.

2.4.1. Організаційно-правові основи забезпечення охорони державної таємниці органами КДБ

У післявоєнний час держава не залишає турботу про забезпечення охорони державної таємниці, що підтверджує Постанова РМ СРСР від 8 червня 1947 р. "Про встановлення переліку відомостей, що складають державну таємницю, розголошення яких карається за законом" та Указ Президії Верховної Ради СРСР від 9 червня 1947 р. "Про відповідальність за розголошення державної таємниці й за втрату документів, що містять державну таємницю".

Фактично щороку перероблялися та вдосконалювалися нормативно-правові акти з питань забезпечення охорони державної таємниці. Таким чином створювалася її система. Постановою Ради Міністрів СРСР від 1 березня 1948 р. затверджений "Перелік найголовніших відомостей, що складають державну таємницю" та "Інструкція із забезпечення охорони державної таємниці в установах і на підприємствах СРСР". В Інструкції 1948 р. установлено три ступеня секретності ("таємно", "цілком таємно", "особливої важливості"); порядок визначення ступеня секретності відомостей; проведено уніфікацію назв секретних органів. У цьому переліку відомості розбиті на такі види: "мобілізаційні питання і відомості про резерви; відомості військового характеру; відомості економічного характеру про промисловість, корисні копалини, сільське господарство, транспорт і зв'язок; фінанси; зовнішню політику і зовнішню торгівлю; питання науки і техніки – атомна енергія, радіолокаційна техніка, реактивна техніка; відкриття й винаходи; відомості з картографії, геології, гідрології; відомості про Арктику тощо".

У березні 1954 р. після утворення КДБ при Раді Міністрів СРСР йому було передано й функції забезпечення охорони державної таємниці. Вже в 1956 р. Головою КДБ при РМ СРСР була затверджена Інструкція із забезпечення охорони державної таємниці в установах і на підприємствах СРСР. У ній викладено завдання секретних відділів, секретних частин; описано вимоги до приміщень секретних відділів і частин та їх охорони; визначено допуск осіб до документів й інформації "особливої важливості", "цілком таємної" і "таємної"; обов'язки осіб, які допущені до роботи з документами з цими грифами; чітко визначено ступінь секретності. Документ регулював ведення документації з грифами "особливої важливості", "цілком таємно" і "таємно", розроблення, облік і розмноження, збереження креслень і технічної документації з грифами "особливої важливості", "цілком таємно" і "таємно"; розмноження видань із грифами у друкарнях; ведення грифованого діловодства; складання і проходження шифротелеграм; користування "особливої важливості", "цілком таємними" і "таємними" відомостями у відрядженнях; визначав правила проведення нарад із різними грифами; створення та функціонування бібліотек і зберігання в них видань із грифами "цілком таємно" й "таємно" тощо. Основні положення цього документа свідчать про вмілу організацію органами КДБ забезпечення захисту одного з найважливіших видів інформації з обмеженим доступом – державної таємниці.

2.4.2. Організаційно-правові основи діяльності цензури та технічного захисту інформації

Діяльність Головліту в 40-60-х рр. XX ст. була спрямована на забезпечення охорони інформації в пресі; фактично цей орган займався цензурою видань. Так, із метою уніфікації усієї видавничої справи і недопущення витоку інформації про СРСР у ЗМІ 21 грудня 1987 р. Головлітом були затверджені "Єдині правила друкування несекретних видань". 25 березня 1988 року Головліт затвердив "Положення про порядок підготовки матеріалів, призначених для відкритого опублікування і видання з грифом "ККК користування" (Положення-88). Відповідно до цих документів і здійснювався захист інформації в пресі. Головним управлінням з охорони державної таємниці у пресі (ГУОТ) при Раді Міністрів СРСР були затверджені "Методичні рекомендації з охорони відомостей, що підлягають захисту від розголошення в пресі й інших засобах масової інформації".

Наприкінці 50–60-х років у процесі забезпечення охорони інформації брала активну участь і КПРС разом із РМ СРСР, "умовним" законодавчим органом. Про це свідчить низка постанов, спрямованих на забезпечення охорони державної таємниці, зокрема Постанова ЦК КПРС "Про заходи із збереження державної таємниці" 1958 року; Постанова ЦК КПРС і РМ СРСР "Про посилення режиму секретності проведених робіт" 1963 року; Постанова ЦК КПРС і РМ СРСР "Про заходи посилення режиму таємності" 1970 року; Постанова ЦК КПРС "Про заходи протидії іноземним технічним розвідкам" 1973 року; Постанова ЦК КПРС і Ради Міністрів СРСР № 941-323 від 15 листопада 1976 року "Про заходи з подальшого удосконалювання системи збереження державних секретів".

Важливим етапом цього періоду став технічний прогрес. Створювалися новітні на той час технічні засоби, за допомогою яких можна було знімати важливу інформацію, зокрема таку, що містила державну таємницю. Крім того, протидіяти технічним розвідкам іноземних держав на етапі "гонки озброєнь" стало одним із найважливіших державних завдань і однією із складових заходів із забезпечення державної та службової таємниці. Тому 18 грудня 1973 р. було створено Державну технічну комісію з протидії іноземним технічним розвідкам (Держтехкомісія СРСР). Саме на неї були покладені функції протидіяти витоку інформації технічним шляхом. Очолив її Н.В.Недогарков, а в період із 1977–1989 рр. –

В.М.Бабанов, у 1989–1992 рр. – Ю.А.Яшин. За час функціонування цієї комісії сформовані концептуальні, організаційні, науково-методологічні й нормативні основи технічного захисту інформації в СРСР. У 80-ті роки завдання та можливості Держтехкомісії значно розширюються, удосконалюється нормативна база, методи й засоби захисту інформації.

До початку 90-х років відбулися якісні зміни у військово-політичній і науково-технічній сферах, що зумовило перегляд державної політики в галузі захисту інформації в цілому. Це було викликано передусім зміною інформаційних технологій, процесів оброблення та передання інформації, яка обертається в технічних засобах. У зв'язку із розпадом СРСР у Росії було зруйновано державну монополію на інформаційні ресурси, зокрема конституційно закріплено право громадян збирати, одержувати й поширювати інформацію. Крім того, став неприйнятним і неефективним адміністративний механізм управління захистом інформації. Також у кінці 80-х рр. завершилася гостра військово-політична конфронтація між СРСР і країнами НАТО, натомість виникла співпраця з цими державами з питань захисту державної таємниці. Більше того, відпала потреба в режимно-обмежувальних заходах, що полегшували захист інформації, наприклад у системі регіонів, закритих для іноземного відвідування.

Важливим елементом радянської системи захисту інформації з обмеженим доступом стало прийняття "Інструкції з забезпечення режиму секретності в міністерствах, відомствах, на підприємствах, в установах і організаціях СРСР", яка була уведена в дію Постановою Ради Міністрів СРСР № 556-126 від 12 травня 1987 р. У цій інструкції захист інформації з обмеженим доступом на підприємствах і в установах покладався на режимно-секретні органи, які створювалися на правах структурних підрозділів. До складу структурних підрозділів входили підрозділ режиму і підрозділ секретного діловодства. Крім того, інструкція конкретизувала забезпечення охорони інформації з обмеженим доступом в організаціях та установах. Фактично саме за цією інструкцією здійснювався захист інформації з обмеженим доступом аж до розпаду СРСР і створення на його теренах незалежних держав, які почали формувати свої системи захисту інформації.

Зазначимо, що у СРСР діяла адміністративно-правова система захисту державної таємниці. При цьому існували дві системи таємниці: державна і партійна. Традиційні стереотипи верховенства влади над правом зумовили політико-правову ситуацію, коли секретність виступала як соціальний інститут, який стояв над багатьма соціальними інститутами. Проблема визначення державної

таємниці розв'язувалася на рівні не закону, а урядових ухвал. Засекречувані відомості підрозділялися на державну та службову (військову) таємницю. З метою запобігання розголошенню державної таємниці у пресі діяла тотальна цензура всіх підготовлених до друку публікацій.

Незнання широкою громадськістю організаційно-правових основ, юридичних і адміністративно-технічних засобів захисту інформації в державі породжувало міфи та спотворене уявлення про цю сферу діяльності. Тому питання необхідності правового регулювання інформаційних відносин і режиму секретності в СРСР вперше було піднято в 1988 році В.А.Рубановим на сторінках журналу "Комуніст". Саме йому належала теза, що інформаційна безпека, стан захисту й використання інформаційних ресурсів – це показник інформаційної культури суспільства. Потім обговорення цієї проблеми висвітлило багато недоліків правового регулювання тогочасних інформаційних відносин. У радянському суспільстві почало розвиватися свідоме розуміння того, що в системі захисту інформації держави основну роль повинні відігравати не методи адміністративного тиску, а правові механізми.

2.5. ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ в 90-х рр. XX ст.

2.5.1. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Забезпечення охорони державної таємниці в Україні в 90-х роках XX ст. було покладено на Держкомсекретів України – спеціально уповноважений центральний орган виконавчої влади, який діяв у період із 1993 до середини 1999 років.

Із метою реалізації державної політики національної безпеки України у сфері охорони державної таємниці відповідно до постанови Кабінету Міністрів України № 327 від 4 травня 1993 року було створено спеціально уповноважений центральний орган державної виконавчої влади – Держкомсекретів України. Уже через рік, у травні 1994 року, в його складі згідно з "Положенням про Держкомсекретів України", затвердженим постановою Кабінету Міністрів України № 458 від 16 червня 1993 року, було утворено колегію Держкомсекретів України.

На колегію Держкомсекретів України були покладені такі завдання: "...розгляд та погоджене вирішення найважливіших питань діяльності Держкомсекретів України із забезпечення, у межах своїх повноважень, проведення державної політики з охорони державної таємниці у сферах оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку, організації, координації і контролю режимно-секретної діяльності державних органів, органів місцевого та регіонального самоврядування, підприємств, установ, організацій, незалежно від форми власності".

Колегія Держкомсекретів України була утворена як постійно діючий колегіальний дорадчий орган у складі Держкомсекретів України. До її складу відповідно до постанови Кабінету Міністрів України № 458 від 16 червня 1993 року входили Голова Держкомсекретів України, його заступники за посадами та інші посадові особи Держкомсекретів України. Затвердження членів колегії Держкомсекретів України здійснювалося в персональному порядку Кабінетом Міністрів України.

Колегія Держкомсекретів України розглядала питання щодо:

- програм і планів заходів із здійснення політики держави стосовно охорони державної таємниці у сферах оборони, економіки України, її міжнародних відносин, безпеки та правопорядку;
- розроблення концептуальних основ державної політики охорони державної таємниці, створення й удосконалення системи охорони державної таємниці, її організаційної та правової основи;
- організаційного й методичного керівництва системою охорони державної таємниці України та забезпечення її функціонування;
- забезпечення контролю за режимом секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах та організаціях незалежно від форми власності;
- організації взаємодії з державними експертами з питань таємниць, надання їм методичної допомоги в здійсненні покладених на них функцій щодо охорони державної таємниці;
- здійснення керівництва уповноваженими Держкомсекретів України на місцях, надання їм практичної допомоги у вирішенні покладених на них завдань, визначення стану службової діяльності структурних підрозділів Держкомсекретів України та заходів щодо її удосконалення;

- розроблення й обговорення проектів законів України, указів і розпоряджень Президента України й нормативних актів Кабінету Міністрів України, які готувались Держкомсекретів України;
- роботи з кадрами, організації підготовки спеціалістів для роботи у сфері охорони державної таємниці тощо.

У цілому колегія Держкомсекретів України провела 19 засідань, розглянула понад 75 питань, ухваливши відповідні рішення. Робота колегії спрямовувала діяльність Держкомсекретів України та визначала шляхи вирішення найважливіших питань у сфері охорони державної таємниці.

На початку своєї діяльності колегія Держкомсекретів України визначила, що станом на 1994 рік нової ефективної системи охорони державної таємниці не існувало, а старою не можливо було користуватися.

Тому було прийнято низку нових нормативно-правових актів України – Закон України "Про інформацію", Постанова Кабінету Міністрів України № 658 від 20 серпня 1993 року "Про запобігання відтоку таємної інформації під час користування системами електронної пошти", Постанова Кабінету Міністрів України № 149 від 2 березня 1993 року "Про заходи щодо забезпечення обслуговування органами внутрішніх справ об'єктів, залучених до виконання важливих оборонних програм", – які тільки частково окреслили питання захисту охорони державної таємниці. Крім цього, діяли нормативні акти колишнього СРСР відповідно до Постанови Верховної Ради України № 1545 від 12 вересня 1991 року "Про порядок тимчасової дії на території України окремих актів законодавства Союзу РСР".

Основним документом, який безпосередньо регламентував порядок охорони державної таємниці, на той час була "Інструкція із забезпечення режиму секретності в міністерствах, відомствах, на підприємствах, в установах і організаціях СРСР" № 0126 – 1987 року.

Фахівцями Держкомсекретів України за відповідними рішеннями колегії було безпосередньо розроблено та забезпечено уведення в дію низки загальнодержавних нормативно-правових актів, зокрема: Закону України "Про державну таємницю"; Указу Президента України № 185/94 від 23 квітня 1994 р. "Про Положення про державного експерта з питань таємниць"; Постанови Кабінету Міністрів України № 278 від 29 квітня 1994 р. "Про затвердження Положення про порядок і механізм формування та опублікування Зводу відомостей, що становлять державну таємницю"; Постанови Кабінету Міністрів України № 414

від 15 червня 1994 р. "Про види, розміри і порядок надання компенсації громадянам у зв'язку з роботою, яка передбачає доступ до державної таємниці"; Постанови Кабінету Міністрів України № 426 від 20 червня 1994 р. "Про затвердження Положення про порядок і умови надання органам державної виконавчої влади, підприємствам, установам і організаціям дозволу на здійснення діяльності, пов'язаної з державною таємницею, та про особливий режим цієї діяльності"; Постанови Кабінету Міністрів України № 779 від 16 листопада 1994 р. "Про встановлення письмової форми трудових договорів з працівниками, діяльність яких пов'язана з державною таємницею"; Постанови Кабінету Міністрів України № 878 від 30 липня 1996 р. "Про затвердження Положення про порядок надання, скасування та переоформлення допуску громадян України до державної таємниці"; Постанови Кабінету Міністрів України № 609 від 4 серпня 1995 р. "Положення про режимно-секретні органи в міністерствах, відомствах, уряді Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах, в установах і організаціях"; Постанови Кабінету Міністрів України № 558 від 22 травня 1996 р. "Про затвердження Інструкції про порядок охорони державної таємниці, а також іншої інформації з обмеженим доступом, що є власністю держави, під час прийому іноземних делегацій, груп та окремих іноземців і проведення роботи з ними".

Із метою запобігання витоку секретної інформації Держкомсекретів України в 1997 році розроблено та затверджено Указом Президента України № 423/97 від 13 травня 1997 р. "Положення про порядок оформлення дозволів за розпорядженнями Президента України на передачу іншій державі інформації, що становить державну таємницю, та матеріальних носіїв такої інформації", а також Указом Президента України № 1229/97 від 1 листопада 1997 р. "Положення про порядок підготовки міжнародних договорів України про взаємну охорону державних таємниць".

Що стосується нормативно-правового забезпечення технічного захисту секретної інформації Держкомсекретів України, була затверджена постановою Кабінету Міністрів України "Концепція технічного захисту інформації", яка стала фундаментом для розроблення усього спектра нормативних документів у цій галузі. Так, Головним управлінням технічного захисту інформації Держкомсекретів України напрацьовано та подано на затвердження державні стандарти системи технічного захисту інформації: ДСТУ 3396.0-96 "Основні положення";

ДСТУ 3396.1-96 “Порядок проведення робіт”; ДСТУ 3396.2-97 “Терміни та визначення” тощо.

Усього станом на 1998 рік в Україні за участю Держкомсекретів України було уведено в дію близько 60 нормативних актів, які регулювали відносини у сфері охорони державної таємниці. Держкомсекретів України безпосередньо видав понад 15 відомчих нормативно-правових актів, роз’яснень, методик тощо, які були обов’язковими для виконання в усіх державних органах, підприємствах і установах, що проводили діяльність пов’язану з державною таємницею.

2.5.2. Забезпечення контролю за режимом секретності в органах державної влади, місцевого самоврядування, на підприємствах, в установах та організаціях

Згідно з Указом Президента України № 179/96 від 12 березня 1996 р. набуло чинності “Типове положення про міністерство та інші центральні органи державної виконавчої влади”. Цим положенням державні органи зобов’язали здійснювати контроль за станом охорони державної таємниці як у центральних апаратах, так і на підпорядкованих їм підприємствах, установах і організаціях. Указом Президента України № 760/95 від 21 серпня 1995 р. на обласні, Київську та Севастопольську міські державні адміністрації було покладено функції державного контролю за дотриманням підприємствами, установами й організаціями законодавства про державну таємницю незалежно від форм власності.

За “Положенням про державного експерта з питань таємниць”, затвердженим Указом Президента України № 185/94 від 23 квітня 1994 р., повноваження щодо окремих контрольних функцій були покладені на державних експертів із питань таємниць.

Функція контролю за станом охорони державної таємниці на підприємствах, в установах та організаціях, яку повинні були здійснювати керівники всіх рівнів, а також режимно-секретних органів (РСО), визначалась Постановою Кабінету Міністрів України № 609 від 4 серпня 1995 р. “Про затвердження Положення про режимно-секретні органи в міністерствах, відомствах, уряді Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах, в установах і організаціях”.

Крім того, механізм реалізації контрольних функцій регламентувала "Інструкція із забезпечення режиму секретності в міністерствах, відомствах, на підприємствах, в установах і організаціях СРСР" № 0126 – 1987 року.

Отже, напрацьована в 90-ті роки минулого століття в державі нормативна база забезпечувала контроль за станом охорони державної таємниці на всіх напрямах діяльності, де створювались, використовувались та зберігались матеріальні носії секретної інформації.

Усі відомства здійснювали охорону державної таємниці відповідно до нормативно-правових актів держави та відомчих розпоряджень. Контролював їхню роботу на цьому напрямі Держкомсекретів України.

Зокрема загальна кількість перевірок міністерствами і відомствами стану охорони державної таємниці на підприємствах, в установах і організаціях згідно з показниками статистичної звітності за 1997 рік становила близько п'яти тисяч. Оскільки такі перевірки часто виявляли незадовільне забезпечення охорони державної таємниці, Держкомсекретів регулював роботу відомств у цій сфері.

Із метою підвищення ефективності системи контролю за станом охорони державної таємниці в Україні колегія Держкомсекретів України сприяла зміцненню апарату уповноважених Держкомсекретів у регіонах, налагодженню тісних стосунків із міністерствами, відомствами, обласними держадміністраціями, іншими структурами, зміцненню інституту державних експертів із питань таємниць, підвищенню ефективності їхньої роботи; організовувала підготовку та перепідготовку кадрів; здійснювала контроль за станом охорони державної таємниці на всіх підприємствах, в установах і організаціях та надавала їм практичну допомогу в усуненні виявлених недоліків.

2.5.3. Забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва

Із початку 90-х років XX століття значно розширилися міжнародні зв'язки України з іншими державами. Тому виникла необхідність подальшого зміцнення правової основи функціонування системи охорони державної таємниці. Держкомсекретів України спільно з іншими зацікавленими державними органами здійснював роботу з підготовки законодавчих та інших нормативних актів у сфері охорони державної таємниці під час міждержавних стосунків.

Із розвитком міждержавних відносин незалежної України постало питання забезпечення охорони міждержавних секретів, насамперед у галузі військово-технічного співробітництва. Вперше така необхідність виникла в рамках програми "Партнерство заради миру". Структури НАТО вимагають від країн, із якими вони співпрацюють, надійності захисту інформації, якою вони обмінюються. Із цією метою фахівцями Офісу безпеки НАТО було вивчено систему охорони державної таємниці в Україні. За їхніми висновками, створена система відповідала світовим стандартам.

Підписання Угоди про безпеку між урядом України й НАТО в березні 1995 року в м. Брюсселі визначило актуальні питання співробітництва з НАТО у сфері захисту секретної інформації. Дорученням Президента України згідно із ст. 4 цієї Угоди Держкомсекретів України було визначено державним органом, який відповідав за забезпечення охорони інформації з обмеженим доступом, обмін якою відбувався в межах співробітництва з Альянсом.

Угоди про взаємний захист секретної інформації, у підготовці яких брали участь фахівці Держкомсекретів України, були підписані із Словацькою Республікою, Федеративною Республікою Німеччиною, Ізраїлем (1998 р.); Республікою Узбекистан, Французькою Республікою (1999 р.). Держкомсекретів України розглянув та погодив проекти угод між Міністерством оборони України та Міністерством оборони Грузії про співробітництво між Військово-повітряними силами України й Військово-повітряними силами Грузії; Меморандуму про взаєморозуміння між Міністерством оборони Федеративної Республіки Німеччини і Міністерством оборони України щодо збереження та використання технічної інформації тощо. Фахівці Держкомсекретів України підготували міжурядову угоду зі Словацькою Республікою про взаємний захист секретної інформації.

Значна увага Держкомсекретів України приділялась підготовці Угоди із США про взаємний захист секретної інформації. Одночасно готувались проекти угод між Міністерством оборони США і Міністерством оборони України та Міністерством у справах науки і технологій України щодо обміну інформацією у сфері досліджень та розробок.

Крім участі в підготовці міжнародних угод із питань охорони державної таємниці під час здійснення міжнародного співробітництва, представники Держкомсекретів України були задіяні на засіданнях робочої групи Ради Європи з питань захисту персональних даних у м. Страсбурзі. За результатами їхньої роботи в цій групі розроблено та направлено пропозиції до МЗС України щодо

доцільності приєднання України до "Конвенції про захист прав фізичних осіб у зв'язку з автоматизованою обробкою персональних даних Ради Європи".

Міжнародні договори України про взаємну охорону державних секретів укладалися від імені України. У випадку, коли сторони не доходили згоди про укладання таких міжнародних договорів від імені держави, міжнародні договори України про взаємну охорону державних секретів укладались від імені Кабінету Міністрів України. При цьому контроль за виконанням зобов'язань, узятих згідно з міжнародними договорами про взаємну охорону державних секретів, здійснював Держкомсекретів України відповідно до "Положення про порядок підготовки міжнародних договорів України про взаємну охорону державних таємниць", затвердженого Указом Президента України від 1 листопада 1997 року.

2.6. ФОРМУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ в 1991–2008 рр.

2.6.1. Характеристика законодавства України, яке визначило систему захисту інформації з обмеженим доступом

Після проголошення незалежності України в 1991 році розпочалося формування системи захисту інформації. Спочатку готувалася нормативно-правова база, яка регламентувала створення системи та органів із захисту інформації з обмеженим доступом. Так, було прийнято низку нормативно-правових актів, які регулювали суспільні інформаційні відносини в нашій державі, зокрема закони України "Про інформацію", "Про державну таємницю", "Про державну статистику", "Про науково-технічну інформацію", "Про захист інформації в інформаційно-комунікаційних системах", "Про Національну програму інформатизації", "Про основи національної безпеки України", "Про Державну службу спеціального зв'язку та захисту інформації".

Зазначимо, що саме в Законі України "Про інформацію" розкрито поняття інформації. Він закріпив право громадян України на інформацію, заклав правові основи інформаційної діяльності, визначив інформаційний суверенітет України й розкрив правові форми міжнародного співробітництва в цій сфері.

Стаття 5 цього Закону визначає основні принципи інформаційних відносин:

- гарантованість права на інформацію;
- відкритість, доступність інформації та свобода її обміну;
- об'єктивність, достовірність інформації;
- повнота й точність інформації;
- законність одержання, використання, поширення та зберігання інформації.

Стаття 6 цього Закону вперше визначила державну інформаційну політику як сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації.

Головними напрямами й способами державної інформаційної політики стали:

- забезпечення доступу громадян до інформації;
- створення національних систем і мереж інформації;
- зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;
- забезпечення ефективного використання інформації;
- сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
- створення загальної системи охорони інформації;
- сприяння міжнародному співробітництву в галузі інформації й гарантування інформаційного суверенітету України.

Відповідно до зазначеного нормативно-правового акта державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

Визначено в цьому Законі й право громадян на інформацію: усі громадяни України, юридичні особи й державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Тут слід зазначити, що законодавче закріплення права громадян на інформацію було значним кроком не лише в правовій розбудові системи захисту інформації, а й у демократичних завоюваннях посттоталітарного режиму. При цьому реалізація права на інформацію громадянами, юридичними особами й державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи й законні інтереси інших громадян,

права та інтереси юридичних осіб. Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Наступним кроком на шляху нормативно-правового закріплення системи та органів захисту інформації з обмеженим доступом стало прийняття Закону України "Про державну таємницю", який регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Фактично цей Закон визначив органи, які стали забезпечувати охорону одного з найважливіших видів інформації з обмеженим доступом – державної таємниці. Ним стала Служба безпеки України.

Крім того, цей Закон уперше визначив низку понять, зокрема:

- державна таємниця (далі – 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 України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;
- віднесення інформації до державної таємниці – процедура прийняття (державним експертом із питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього;
- гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації;
- державний експерт із питань таємниць – посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування;
- допуск до державної таємниці – оформлення права громадянина на доступ до секретної інформації;

- доступ до державної таємниці – надання уповноваженою посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;
- засекречування матеріальних носіїв інформації – уведення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;
- Звід відомостей, що становлять державну таємницю – акт, у якому зведено переліки відомостей, що згідно з рішеннями державних експертів із питань таємниць становлять державну таємницю у визначених цим Законом сферах;
- категорія режиму секретності – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях;
- криптографічний захист секретної інформації – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) із метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;
- матеріальні носії секретної інформації – матеріальні об'єкти, зокрема фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів і т. ін.;
- охорона державної таємниці – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;
- режим секретності – встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;
- розсекречування матеріальних носіїв секретної інформації – зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

- спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, – експертиза, що проводиться з метою визначення в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для провадження діяльності, пов'язаної з державною таємницею;
- ступінь секретності ("особливої важливості", "цілком таємно", "таємно") – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;
- технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Характеризуючи цей Закон, доходимо висновку, що він заклав правове підґрунтя формування системи та органів захисту одного з видів інформації з обмеженим доступом – державної таємниці.

Ще одним нормативно-правовим актом, який сформулював правову основу системи та органів захисту інформації з обмеженим доступом, став Закон України "Про державну статистику", який регулює правові відносини у сфері державної статистики, визначає права і функції органів державної статистики, організаційні засади державної статистичної діяльності з метою отримання всебічної та об'єктивної статистичної інформації щодо економічної, соціальної, демографічної й екологічної ситуації в Україні та її регіонах і забезпечення нею держави та суспільства.

Оскільки в державних статистичних органах циркулює чимало інформації, яка може вплинути на національну безпеку України, цей нормативно-правовий акт значною мірою сприяв процесу формування системи та органів захисту інформації з обмеженим доступом. Адже саме в цьому Законі наведені визначення:

- адміністративні дані – дані, отримані на підставі спостережень, проведених органами державної влади (за винятком органів державної статистики), органами місцевого самоврядування та іншими юридичними особами відповідно до законодавства та з метою виконання адміністративних обов'язків і завдань, віднесених до їхньої компетенції;
- державна статистика – централізована система збирання, опрацювання, аналізу, поширення, збереження, захисту та використання статистичної інформації;
- конфіденційна інформація – статистична інформація, яка належить до інформації з обмеженим доступом і знаходиться у володінні, користуванні або

розпорядженні окремого респондента та поширюється тільки за його згодою відповідно до погоджених із ним умов;

- статистична інформація (дані) – офіційна державна інформація, яка характеризує масові явища та процеси, що відбуваються в економічній, соціальній та інших сферах життя України та її регіонів.

Звичайно, важливу роль у системі інформації держави відіграє науково-технічна інформація. Закон України "Про науково-технічну інформацію" визначив основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного й соціального прогресу країни. Метою цього Закону стало створення в Україні правової бази для одержання та використання науково-технічної інформації. Законом регулюються правові й економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій сфері.

Крім того, цей Закон розкрив такі важливі поняття, як:

- науково-технічна інформація – це документовані або публічно оголошувані відомості про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані під час науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності;
- науково-інформаційна діяльність – це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави в науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні;
- інформаційні ресурси науково-технічної інформації – це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксоване на паперових чи інших носіях;
- довідково-інформаційний фонд – це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб;

- довідково-пошуковий апарат – це сукупність упорядкованих вторинних документів, створюваних для пошуку першоджерел;
- інформаційні ресурси спільного користування – це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання;
- аналітично-синтетична обробка науково-технічної інформації – це процес обробки інформації шляхом аналізу і синтезу змісту документів із метою одержання необхідних відомостей, а також шляхом їх класифікації, оцінки, співставлення й узагальнення;
- інформаційний ринок – це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

У зв'язку з розвитком сучасних інформаційно-телекомунікаційних систем і збільшенням циркуляції інформації в автоматизованих системах постало питання належного юридичного оформлення, поширення та використання її через ці засоби. Тому метою Закону України "Про захист інформації в автоматизованих системах" стало установлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України та юридичних осіб на інформацію і права доступу до неї, права власника інформації на її захист, а також установленого чинним законодавством обмеження на доступ до інформації.

Саме тому цей Закон уперше визначив, що:

- автоматизована система (АС) – система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення;
- інформація в АС – сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення;
- обробка інформації – вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних;

• захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією;

• несанкціонований доступ – доступ до інформації, що здійснюється з порушенням установлених в АС правил розмежування доступу;

• розпорядник АС – фізична або юридична особа, яка має право розпоряджання АС за угодою з її власником або за його дорученням;

• персонал АС – фізичні особи, яких власник АС або уповноважена ним особа чи розпорядник АС визначили для здійснення функцій управління та обслуговування АС;

• користувач АС – фізична або юридична особа, яка має право використання АС за угодою із розпорядником АС;

• порушник – фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо АС та інформації в ній;

• витік інформації – результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

• втрата інформації – дія, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;

• підробка інформації – навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС;

• блокування інформації – дії, наслідком яких є припинення доступу до інформації;

• порушення роботи АС – дії або обставини, які призводять до спотворення процесу обробки інформації.

Доповнює проаналізований вище нормативно-правовий акт Закон України "Про Національну програму інформатизації". Він визначає, наприклад, що інформаційний суверенітет держави – це її здатність контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави.

У цьому Законі також визначені поняття:

• база даних – іменована сукупність даних, що відображає стан об'єктів та їх відношень у визначеній предметній галузі;

• база знань – масив інформації у формі, придатній до логічної і смислової обробки відповідними програмними засобами;

• геоінформаційні системи – сучасні комп'ютерні технології, що дають можливість поєднати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо);

• засоби інформатизації – електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі й мережі зв'язку, що використовуються для реалізації інформаційних технологій;

• інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

• інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами;

• інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

• інформаційний продукт (продукція) – документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

• інформаційний ресурс – сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо);

• локалізація програмних продуктів – приведення програмних продуктів, які використовуються в Україні, у відповідність до законів України та інших нормативно-правових актів, стандартів, норм і правил, що діють в Україні;

• нерезиденти – юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням за межами України, які створені й діють відповідно до законодавства іноземної держави, у тому числі юридичні особи та інші суб'єкти підприємницької діяльності, створені за участю юридичних і фізичних осіб;

- окреме завдання – комплекс проектів інформатизації, взаємопов'язаних і взаємопогоджених за термінами реалізації, складом виконавців та спрямованих на досягнення конкретних цілей;
- проект інформатизації – комплекс взаємопов'язаних заходів, як правило, інвестиційного характеру, що узгоджені за часом, використанням певних матеріально-технічних, інформаційних, людських, фінансових та інших ресурсів і мають на меті створення заздалегідь визначених інформаційних і телекомунікаційних систем, засобів інформатизації та інформаційних ресурсів, які відповідають певним технічним умовам і показникам якості;
- резиденти – юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням на території України, які здійснюють свою діяльність відповідно до законодавства України.

Закон України "Про основи національної безпеки України" – це ще один нормативно-правовий акт, який становить вагомий внесок у правове підґрунтя формування системи та органів захисту інформації. Цей Закон, серед іншого, визначає загрози національній безпеці в інформаційній сфері:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

Цивільний кодекс України (стаття 1 "Відносини, що регулюються цивільним законодавством") теж регулює відносини у сфері обігу інформації з обмеженим доступом. Цивільне законодавство регулює особисті немайнові та майнові відносини (цивільні відносини), засновані на юридичній рівності, вільному волевиявленні, майновій самостійності їх учасників. Об'єктами цивільних прав виступають речі, у тому числі гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація,

а також інші матеріальні й нематеріальні блага. “Інформацією є документовані або публічно оголошені відомості про події та явища, що мали або мають місце в суспільстві, державі та навколишньому середовищі. Суб’єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової й моральної шкоди, завданої такими правопорушеннями. Порядок використання інформації та захисту права на неї встановлюється законом”.

Господарський кодекс України (стаття 88 “Права й обов’язки учасників господарського товариства”) визначає, що учасники господарського товариства мають право одержувати інформацію про діяльність товариства. На вимогу учасника товариство зобов’язане надати йому для ознайомлення річні баланси, звіти про фінансово-господарську діяльність товариства, протоколи ревізійної комісії, протоколи зборів органів управління товариства тощо.

Завданням Кодексу України про адміністративні правопорушення є охорона прав і свобод громадян, власності, конституційного ладу України, прав та законних інтересів підприємств, установ і організацій, установленого правопорядку, зміцнення законності, запобігання правопорушенням, виховання громадян у дусі точного й неухильного додержання Конституції і законів України, поваги до прав, честі й гідності інших громадян, до правил співжиття, сумлінного виконання своїх обов’язків, відповідальності перед суспільством.

Адміністративним правопорушенням (проступком) визнається протиправна, винна (умисна або необережна) дія чи бездіяльність, яка посягає на громадський порядок, власність, права і свободи громадян, на встановлений порядок управління і за яку законом передбачено адміністративну відповідальність (стаття 212-2 “Порушення законодавства про державну таємницю”, стаття 212-3 “Порушення права на інформацію”; Кримінальний кодекс України, стаття 329 “Втрата документів, що містять державну таємницю”, стаття 330 “Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави”).

Низка нормативно-правових актів Президента, Уряду теж спрямовані на формування системи та органів захисту інформації з обмеженим доступом. Зокрема це укази Президента України “Про порядок здійснення криптографічного захисту інформації в Україні” № 505/98 від 22 травня 1998 р. (визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі); “Про технічний захист інформації в Україні” № 1229/99 від 27 вересня 1999 р.

(визначає правові та організаційні засади технічного захисту важливої для держави, суспільства й особи інформації, охорона якої забезпечується державою відповідно до законодавства. Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних сил України та інших військових формувань, утворених згідно із законодавством України; відповідних підприємств, установ, організацій).

Ухвалені й відповідні постанови Кабінету Міністрів України. Зокрема це "Концепція технічного захисту інформації в Україні" № 1126 від 8 жовтня 1997 р. (визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами). Технічний захист інформації (далі – ТЗІ) є складовою забезпечення національної безпеки України. Концепція має забезпечити єдність принципів формування і проведення такої політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо) й бути підставою для створення програм розвитку сфери ТЗІ. Відповідно до постанови Уряду № 1772 від 16 листопада 2002 р. "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах" зазначений порядок увів в обіг такі поняття:

- інформаційна система – організаційно-технічна система обробки інформації за допомогою технічних і програмних засобів;
- комплексна система захисту інформації – сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації;
- несанкціоновані дії – доступ або спроба такого доступу до державних інформаційних ресурсів в інформаційних та телекомунікаційних системах без відповідно оформленого власником або уповноваженою ним особою дозволу, вірусне ураження, вчинення інших дій, які можуть призвести до порушення цілісності, доступності та конфіденційності цих ресурсів;
- телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання (випромінювання) або приймання сигналів, знаків, звуків, рухомих чи нерухомих зображень або іншим способом.

Багато постанов Уряду було направлено на забезпечення формування системи захисту інформації в Україні: "Про деякі питання захисту інформації, охорона якої забезпечується державою" № 281 від 13 березня 2002 р. (уповноважено Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки здійснювати управління захистом інформації в автоматизованих системах відповідно до Закону України "Про захист інформації в автоматизованих системах)"; "Державна програма створення, розвитку та забезпечення функціонування Національної системи конфіденційного зв'язку" (ККК користування) № 1520 від 11 жовтня 2002 р.; "Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави" № 1893 від 27 листопада 1998 р. (визначала обов'язковий для всіх центральних органів виконавчої влади, Ради Міністрів Автономної Республіки Крим, місцевих органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності порядок обліку, зберігання, використання та знищення документів, справ, видань, магнітних й інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави тощо. Переліки конфіденційної інформації, що є власністю держави та якій надається гриф обмеження доступу "ККК користування", розробляють і вводять у дію міністерства, інші центральні органи виконавчої влади, Рада Міністрів Автономної Республіки Крим, обласні, Київська та Севастопольська міські державні адміністрації, в яких утворюються або у володінні, користуванні чи розпорядженні яких перебувають ці відомості.

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

Таким чином, після проголошення Україною незалежності протягом 1991–2005 рр. було прийнято низку нормативно-правових актів, які заклали засади для формування, становлення та розвитку системи й органів захисту інформації в Україні.

2.6.2. ВІДОМЧІ НОРМАТИВНО-ПРАВОВІ АКТИ З ПИТАНЬ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Значний внесок у нормотворчий процес створення системи та органів захисту інформації в Україні зробила і Служба безпеки України, оскільки саме на цей орган виконавчої влади покладено забезпечення охорони одного з видів інформації з обмеженим доступом – державної таємниці. Протягом зазначеного періоду були прийняті: "Інструкція про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, в установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави", затверджена наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 45 від 22 жовтня 1999 р., зареєстровано в Міністерстві юстиції України 29 листопада 1999 р. за № 817/4110 (визначає конкретні вимоги щодо режиму безпеки, який повинен бути створений при проведенні робіт із криптографічного захисту конфіденційної інформації, що є власністю держави); "Положення про контроль за функціонуванням системи технічного захисту інформації", затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 61 від 22 грудня 1999 р., зареєстровано в Міністерстві юстиції України 11 січня 2000 р. за № 10/4231 (установлює правові та організаційні засади контролю за функціонуванням системи технічного захисту інформації, який здійснюється згідно з Положенням про технічний захист інформації в Україні, затвердженим Указом Президента України № 1229/99 від 27 вересня 1999 р.); "Положення про державну експертизу у сфері технічного захисту інформації", затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 62 від 29 грудня 1999 р., зареєстровано в Міністерстві юстиції України 24 січня 2000 р. за № 40/4261 (державна експертиза у сфері технічного захисту інформації проводиться з метою оцінки захищеності інформації, яка обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, приміщеннях, інженерно-технічних спорудах тощо та підготовки обґрунтованих висновків для прийняття відповідних рішень);

"Порядок інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади", затверджений наказом Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України № 327/225 від 25 листопада 2002 р., зареєстровано в Міністерстві юстиції України 29 грудня 2002 р. за № 1021/7309 (визначає процедуру інформаційного наповнення Єдиного вебпорталу органів виконавчої влади (далі – Єдиний вебпортал). Здійснення інформаційного наповнення має на меті інтеграцію до Єдиного вебпорталу вебсайтів, інших електронних інформаційних систем органів виконавчої влади).

Отже, протягом 1991–2005 рр. фактично було сформовано національну системи захисту інформації: ухвалено нормативно-правові акти, а також створено органи, які безпосередньо займаються захистом інформації в межах держави на підприємствах, в установах та організаціях усіх форм власності.

Система захисту інформації в нашій державі утворює комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню інформації з обмеженим доступом та втратам її матеріальних носіїв.

Забезпечення охорони найважливішого виду інформації здійснює Служба безпеки України, зокрема два її підрозділи – охорони державної таємниці й Департамент спеціальних телекомунікаційних систем та захисту інформації. У міністерствах, на підприємствах, в установах та організаціях усіх форм власності створені відповідно режимно-секретні органи, на які покладено ці функції.

В організаціях усіх форм власності, де не циркулює державна таємниця, а є інші види інформації з обмеженим доступом – банківська, адвокатська, комерційна, лікарська, персональні дані тощо, – створені підрозділи, які займаються захистом інформації. Із розвитком інформаційних технологій буде удосконалюватися й система захисту інформації.

2.7. ГАРМОНІЗАЦІЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ІНФОРМАЦІЇ В УКРАЇНІ ВІДПОВІДНО ДО КРИТЕРІЇВ І ЦІННОСТЕЙ КРАЇН – ЧЛЕНІВ НАТО

2.7.1. Характеристика етапів відносин України із структурами НАТО

Відносини Організації Північноатлантичного договору (НАТО) з Україною почали розвиватися невдовзі після отримання країною незалежності в 1991 році. Україна не забарилася з приєднанням до Ради Північноатлантичного співробітництва і залишалась активною учасницею протягом усієї історії існування цього органу.

Правове підґрунтя курсу України на євроатлантичну інтеграцію було закладене “Основними напрямами зовнішньої політики України” та Концепцією (основами державної політики) національної безпеки України, а також нормативними актами Президента України, Кабінету Міністрів України, іншими документами.

У схвалених Верховною Радою 2 липня 1993 р. “Основних напрямах зовнішньої політики України” зазначається, що “в умовах зникнення блокового протистояння в Європі пріоритетного значення набуває проблема створення загальноєвропейської системи безпеки на базі таких міжнародних інститутів, як Рада з питань безпеки та співробітництва в Європі (сучасна Організація з питань безпеки та співробітництва в Європі – ОБСЄ з 1995 року), Рада Північноатлантичного співробітництва (сучасна Рада Євроатлантичного партнерства – РЄАП з 1997 року), НАТО та Західноєвропейський Союз (ЗЄС). Безпосереднє й повне членство України в такій структурі створюватиме необхідні зовнішні гарантії її національної безпеки. З огляду на кардинальні зміни, які відбулися після розпаду СРСР і визначили сучасне геополітичне становище України, проголошений нею свого часу намір стати нейтральною та позаблоковою державою має бути адаптований до нових умов і не може уважатися перешкодою її повномасштабній участі в загальноєвропейській структурі безпеки”. Для забезпечення національної безпеки держави Концепція (Основи державної політики) національної безпеки України передбачала зокрема входження в наявні та створювані системи

універсальної й регіональної безпеки. У червні 2003 року Верховна Рада України прийняла оновлений і значно докладніший документ – "Закон про основи національної безпеки". Саме ці документи наголошують на реформуванні усієї системи національної безпеки, а не лише збройних сил.

У затвердженій Верховною Радою України 19 жовтня 1993 року "Воєнній доктрині України" передбачено, що участь нашої держави в таких системах універсальної та загальноєвропейської безпеки є "важливим компонентом" її національної безпеки.

Україна приєдналась до програми "Партнерство заради миру" (ПЗМ) у 1994 році. Ця програма є важливою ініціативою, яку НАТО запропонувало на січневому 1994 року Брюссельському саміті Північноатлантичної ради з метою зміцнення стабільності та безпеки в усій Європі. Запрошення приєднатися до "Партнерства заради миру" було надіслано усім державам – учасницям Ради Євроатлантичного партнерства та іншим країнам, що беруть участь у ОБСЄ (55 європейських держав, а також США й Канада) та які мають бажання і можливості зробити свій внесок у програму.

Президент Л.Кучма відвідав НАТО 1 червня 1995 року, зустрівся з Генеральним секретарем і повідомив про бажання підняти відносини між НАТО й Україною на новий рівень. Через три місяці, 14 вересня 1995 р., міністр закордонних справ Удовенко відвідав НАТО для офіційного прийняття "Індивідуальної програми партнерства України" і провів зустріч із питань європейської безпеки з членами Північноатлантичної ради. НАТО й Україна оприлюднили Спільну заяву для преси, в якій були висловлені загальні принципи відносин НАТО – Україна в ПЗМ та інших галузях.

Подальші зустрічі проводились на різних рівнях у 1996 та 1997 роках. Була створена українська місія при НАТО, до якої увійшов і військовий представник. Україна також представлена в Центрі координації партнерства, розташованому в Монсі (Бельгія). Згідно з рішенням, прийнятим Комісією НАТО – Україна на засіданні 29 травня 1998 року в Люксембурзі офіцера по зв'язках НАТО було призначено в Київ для сприяння широкомасштабній участі України в ПЗМ та вдосконалення співпраці між військовим керівництвом НАТО і України в цілому. Україна бере активну участь у заходах ПЗМ як у штаб-квартирі НАТО, так і в державах – членах Альянсу і партнерах, влаштовувала низку навчань у рамках ПЗМ на своїй території. Ратифікація українським парламентом Угоди про статус

сил "Партнерства заради миру" (SOFA) дає змогу більш повно використовувати цей потенціал, включно з Яворівським полігоном на заході країни, який із березня 1999 року є офіційно визнаним навчальним центром ПЗМ. У рамках співпраці з НАТО Україна провела широкомасштабні навчання "Кооператив партнер – 2003" поблизу міста Одеси за участю 5 тис. військовослужбовців, 43 кораблів, включаючи підрозділи з 14 різних держав. Під час навчань було відпрацьовано ситуації із доставки вантажів гуманітарної допомоги та відновлення правопорядку після землетрусу й повені. Група українських фахівців брала участь у навчаннях із ліквідації наслідків цивільного надзвичайного стану "Дакія – 2003", які проходили в Пешті з 7 до 10 жовтня і були організовані у співпраці з Євроатлантичним центром координації реагування на катастрофи (ЄАЦКРК).

Ще один важливий документ, який підписала Україна з НАТО, – "Хартія про Особливе партнерство". Під час липневого саміту глав держав та урядів НАТО 1997 року в Мадриді керівники НАТО й президент України Л.Кучма підписали "Хартію про особливе партнерство між НАТО та Україною", яка була парафована кількома тижнями раніше в Сінтрі (Португалія). Базовим політико-правовим документом, який регулює комплекс двосторонніх відносин між Україною та НАТО, є "Хартія про особливе партнерство", підписана 9 липня 1997 року в Мадриді. З метою реалізації її положень Указом Президента України була затверджена Державна програма співробітництва України з НАТО, яка забезпечує співпрацю між нашою державою й Альянсом на двосторонньому рівні та в рамках РЄАП. Обидва документи спрямовані на здійснення Україною політики євроатлантичної інтеграції.

У цій Хартії країни – члени НАТО підтвердили свою підтримку суверенітету та незалежності України, її територіальної цілісності демократичного розвитку, економічного процвітання й статусу без'ядерної держави, а також принципу недоторканності кордонів. Ці чинники є ключовими для стабільності та безпеки в Центральній і Східній Європі та на континенті загалом.

НАТО тепло вітало рішення України про підтримку необмеженої пролонгації Договору про непоширення ядерної зброї (ДНЯЗ) та її внесок у виведення й знищення ядерних озброєнь, розташованих на її території. Схвалювались і запевнення, надані Україні як неядерній учасниці ДНЯЗ усіма п'ятьма ядерними державами, які також є учасницями ДНЯЗ. У грудні 1997 року між НАТО та Україною підписаний Меморандум про домовленість із питань планування на випадок надзвичайних ситуацій і готовність до катастроф.

На додаток до цього Меморандуму, за яким планування на випадок надзвичайних ситуацій є головною сферою співпраці, є низка інших спільних програм, які торкаються широкого спектра питань. Консультації та співробітництво між Україною і НАТО через семінари, робочі групи та спільні програми стосуються широкого кола питань. До них належать планування на випадок надзвичайних ситуацій та готовність до катастроф; стосунки між військовими й цивільними, демократичний контроль над збройними силами, оборонна реформа в Україні; оборонне планування і складання бюджету, політика, стратегія та концепція національної безпеки; конверсія оборонної промисловості; військова співпраця між НАТО й Україною та сумісність; військова підготовка й навчання; економічні аспекти безпеки; наука і технологія; питання екологічної безпеки, зокрема ядерної безпеки; аерокосмічні науково-технічні розробки; координація дій військових і цивільних органів; управління повітряним рухом та контроль за повітряним простором. Для забезпечення роботи в цьому напрямі була створена Спільна робоча група НАТО – Україна (СРГ) з оборонної реформи.

Україна бере участь і в Комісії НАТО – Україна. Північноатлантична рада періодично (принаймні двічі на рік) проводить свої засідання за участю представників України на форумі, створеному згідно з Хартією, який називається “Комісія НАТО – Україна”. Комісія оцінює хід виконання Хартії та обговорює шляхи поліпшення і подальшого розвитку співпраці.

У квітні 1999 року у Вашингтоні відбулася зустріч у верхах між НАТО і Україною, а в березні 2000 року Комісія НАТО – Україна вперше провела засідання в Києві. Політичний комітет НАТО відвідав Україну тричі в 1997 – 2000 роках і провів різноманітні консультації та обміни інформацією в Києві й інших містах України.

Крім того, згідно з Хартією про особливе партнерство між Україною й НАТО створено формат відносин “19+1”. Головним його механізмом є Комісія Україна – НАТО, що працює на рівні глав держав та урядів, міністрів закордонних справ і оборони, послів. Хартією передбачаються широкі можливості розвитку практичного співробітництва на двосторонній основі з НАТО – в рамках засідань комітетів НАТО у форматі “19+1”, діяльності спільних робочих груп на різних напрямах. Фактично, ці механізми дуже схожі з механізмами, передбаченими Планом дій щодо членства в НАТО.

У штаб-квартирі НАТО працює українська місія, у складі якої діють повномасштабні політичне та військове представництва. З огляду на вимоги під-

готовки до членства в НАТО, кадрове наповнення місії постійно зростає і зараз перебуває на рівні багатьох держав-аспірантів. На нашу думку, механізми та формати співробітництва України з НАТО є цілком достатніми для забезпечення процесу євроатлантичної інтеграції нашої держави. Головне – ефективно їх використовувати.

Утім, підготовка держави до членства в НАТО не обмежується зовнішньополітичними та дипломатичними аспектами. Ключове значення має реформування політичної, економічної й військової сфер життя країни відповідно до євроатлантичних стандартів. Ця робота здійснюється в рамках Плану дій та Цільового плану Україна – НАТО, розроблених на основі вимог Плану дій щодо членства в НАТО. Безумовно, узгодження з НАТО Плану дій – це ще не залучення до офіційних програм підготовки до членства, якими є Інтенсифікований діалог і План дій щодо членства в НАТО. На саміті у Празі у 2002 році було ухвалено План дій Україна – НАТО.

Етап імплементації Плану дій є лише перехідним у розвитку відносин з Альянсом. Однак, враховуючи те, що Цільовий план за форматом, змістом і характером звітування ідентичний Плану дій щодо членства в НАТО, офіційне приєднання України до цієї програми стане насамперед політичним кроком. Тому ефективність процесу підготовки держави до членства в НАТО більше залежить від якості виконання конкретних завдань, ніж від назви програми, в рамках якої здійснюється процес підготовки.

Зазначені вище позитивні події допомогли закласти міцну основу майбутньої співпраці й чітко вказують на галузі, в яких вдалося досягти прогресу. Активна участь у заходах ПЗМ, серед яких програми практичної діяльності з оборонних питань, у яких беруть участь більшість країн – членів НАТО і партнерів, дала змогу Україні порівняти свої оборонні структури з тими, які мають її європейські сусіди, і більш ефективно визначити свою роль у європейській безпеці. Участь України в роботі Ради Євроатлантичного партнерства доповнює цей процес.

Візит Північноатлантичної ради в Україну в березні 2000 року надав новий поштовх Особливому партнерству між НАТО і Україною, яке було започатковано в червні 1997 року в Мадриді. Засідання Комісії НАТО – Україна в Києві (цей орган, який направляє Партнерство, вперше зібрався в Україні) стало нагодою для 19 країн – членів НАТО й України переглянути весь спектр своєї співпраці. Це стало значним кроком у напрямі наближення України до євроатлантичної спільноти націй.

Підписання в 1997 році в Мадриді "Хартії про особливе партнерство" підняло співпрацю між НАТО й Україною на новий рівень і забезпечило офіційне визнання значення незалежної, стабільної й демократичної України для всієї Європи. Хартія відповідає задекларованій Україною стратегії більш активного приєднання до європейських та трансатлантичних структур. Вона є основою для консультацій між НАТО й Україною в контексті євроатлантичної безпеки і стабільності та в таких галузях, як запобігання конфліктів, урегулювання криз, підтримка миру і гуманітарні операції.

Семінари, засідання спільних робочих груп та інші спільні програми зосереджені на таких питаннях, як оборонна реформа й перебудова оборонної галузі, стосунки між цивільними та військовими, бюджети і планування ресурсів. Проводяться також семінари з перепідготовки звільнених у запас офіцерів та скорочення збройних сил і конверсії.

Спільна робота з планування на випадок надзвичайних ситуацій і готовності до катастроф стала тією сферою співпраці, яка приносить пряму користь Україні. На вересень 2000 року були заплановані навчання з ліквідації наслідків катастроф у Закарпатській області України, на яких відпрацьовувались процедури гуманітарної допомоги на випадок повеней.

Іншою потужною сферою співпраці стала наука, де НАТО виділяє гранти на підтримку українських науковців, економічні аспекти безпеки та навчання. У контексті останньої діяльності започатковано програму навчання англійській мові близько 100 українських офіцерів.

Центр інформації та документації НАТО, відкритий у травні 1997 року Генеральним секретарем Альянсу, став центром інформаційної діяльності, спрямованої на пояснення широкому загалу української громадськості переваг Особливого партнерства з НАТО. Це перший центр такого типу, який НАТО відкрило в країні-партнері. З того часу Центр відіграє провідну роль у поясненні політики Альянсу і подоланні хибних поглядів на організацію.

У грудні 1998 року був підписаний Меморандум про згоду, за яким два офіцери НАТО по зв'язках можуть прибути до Києва для сприяння широкомасштабній участі України в програмі "Партнерство заради миру". У 1999 році був створений Офіс по зв'язках з НАТО, на який покладено завдання сприяти контактам між НАТО й цивільними та військовими відомствами, які мають стосунок до участі України в Партнерстві заради миру і виконанні робочого плану КУН.

До інших позитивних подій належать ратифікація 1 березня 2000 року українським Парламентом Угоди про статус сил "Партнерства заради миру" та додаткового протоколу до неї. Парламент також схвалив виконання Україною договору "Відкрите небо", чим зробив важливий внесок у прозорість питань контролю за озброєннями. Крім того, створено низку інших органів, які співпрацюють із НАТО.

8 липня 2002 року Президент України відповідно до ст. 107 Конституції України своїм Указом увів у дію рішення Ради національної безпеки й оборони України від 23 травня 2002 року "Про Стратегію України щодо Організації Північноатлантичного договору (НАТО)". Це рішення суттєво розширило параметри інтеграційних процесів, учасницею яких є Україна, – просування до ЄС, СОТ, активна участь у діяльності інших міжнародних структур (Центральноєвропейська ініціатива, СНД, Вишеградська четвірка, ГУУАМ та ін.). Кожен із цих напрямів має свої особливості, перспективи, а всі вони мають єдину мету – становлення України як рівноправного члена міжнародної спільноти.

У документі зокрема зазначається, що спрямування політики України на повномасштабне приєднання до європейських і євроатлантичних структур викликане необхідністю рахуватися з об'єктивними реаліями європейської та світової політики; продиктоване національними інтересами України. Для ефективного забезпечення цього курсу розроблено Стратегію України щодо Організації Північноатлантичного договору, яка окреслює політико-правові засади та кінцеву мету курсу України на євроатлантичну інтеграцію, бачення нею моделі загальноєвропейської системи безпеки, національні інтереси стосовно НАТО, цілі та рамки відносин із цією організацією на сучасному етапі й на перспективу.

На думку України, загальноєвропейська система безпеки має бути кооперативною і формуватися на основі наявних організацій і структур: НАТО, ОБСЄ, Європейського Союзу (ЄС) та інших політико-військових механізмів. Україна виступає за певну структуризацію в рамках цієї системи, уважаючи водночас, що вона має ґрунтуватися на засадах відкритості для нових членів. Основними принципами її функціонування повинні стати взаємодія наявних у Європі структур безпеки на основі взаємодоповнення й партнерства та створення ефективного механізму гарантування безпеки європейських держав.

Виходячи з політичних реалій сьогодення, Україна розглядає НАТО як основу майбутньої загальноєвропейської системи безпеки і підтримує процес її розширення. Україна вважає, що розширення НАТО має бути еволюційним, транспарентним процесом, відкритим для співробітництва з іншими державами,

який сприятиме зміцненню європейської стабільності та безпеки в контексті загальноєвропейського інтеграційного процесу. Україна розглядає НАТО як військово-політичну організацію, що об'єднує демократичні держави Європи й Північної Америки з високим рівнем соціально-економічного розвитку і не несе в собі загрози національній безпеці нашої держави.

З огляду на роль НАТО в підтриманні європейської безпеки й стабільності та розвитку співробітництва держав регіону, виходячи із взаємопов'язаності процесів розширення НАТО та ЄС і тісної взаємодії цих організацій у формуванні системи європейської безпеки, враховуючи військові й політичні можливості НАТО та досвід держав-членів у формуванні демократичного суспільства, ефективної економіки й оборонної сфери, євроатлантична інтеграція України з майбутнім членством в Альянсі надасть можливість для розв'язання таких важливих проблем:

- отримання надійних гарантій державного суверенітету, політичної незалежності, територіальної цілісності та непорушності державних кордонів, створення сприятливих умов для економічного розвитку України як невід'ємної частини єдиного європейського економічного простору, зміцнення регіональної та європейської стабільності й безпеки;
- забезпечення національної безпеки в найефективніший із політичного, військового, економічного та фінансового поглядів спосіб;
- отримання надійних гарантій незворотності утвердження в Україні засад громадянського суспільства, верховенства права та ефективної ринкової системи;
- підвищення ступеня відповідальності нашої держави перед спільнотою розвинутих демократій, що дозволить їй стати повноправною стороною процесу прийняття важливих для Європейського континенту політико-військових рішень;
- сприяння входженню України в інші європейські та світові структури;
- надання суттєвого імпульсу процесу інтеграції до Європейського Союзу;
- завершення реформування Збройних сил України, включаючи створення ефективної системи демократичного контролю над ними, формування прозорого оборонного бюджету та раціонального використання коштів на оборонні цілі.

Пріоритети наукової співпраці між Україною й НАТО були започатковані під час засідання Спільної робочої групи Україна – НАТО з питань співпраці у галузі науки та довкілля, яке проходило в Києві 25 червня 2003 року. Саме тоді було визначено п'ять галузей, що становлять найбільший інтерес для України: інформа-

ційні технології; біологія клітини та біотехнології; нові матеріали й речовини; охорона довкілля та раціональне використання ресурсів. На цій зустрічі також було представлено нову наукову програму "Безпека шляхом науки".

Започаткована співпраця між Україною та НАТО у сфері охорони кордонів. Цей напрям, на нашу думку, буде активно розвиватися в майбутньому, що наочно показала "тузлинська" проблема в листопаді 2003 року. У липні 2003 року Робочу групу Україна – НАТО з питань охорони кордонів приймала в Будапешті Служба охорони кордонів Угорщини. Під час цієї зустрічі фахівці з України та держав НАТО дійшли згоди про те, що основні зусилля слід зосередити на виробленні загальної стратегії, якою Прикордонні війська України мають керуватися в процесі реформування.

30 вересня 2003 року новопризначений міністр закордонних справ України К.Грищенко відвідав штаб-квартиру НАТО, де провів двосторонню зустріч із Генеральним секретарем НАТО лордом Робертсоном. Робертсон високо оцінив відносини України з НАТО: "Відносини між Україною та НАТО сьогодні у доброму стані. Вони і надалі розвиватимуться паралельно із процесом реформ – економічних, політичних, військових, – які мають втілюватися в Україні". 20 жовтня лорд Робертсон з прощальним візитом відвідав Київ, оскільки наприкінці поточного року він залишив пост Генерального секретаря, поступившись посадою міністру закордонних справ Нідерландів Яапу де Хооп Схефферу. Під час цього візиту Робертсон зустрівся з міністрами закордонних справ та оборони України, Президентом України, секретарем Ради національної безпеки та оборони, Прем'єр-міністром та Головою Верховної Ради України. Крім того, він узяв участь в установчому засіданні загальноукраїнського об'єднання громадських організацій Ліги "Україна – НАТО". На всіх цих зустрічах Генеральний секретар відзначав успішність виконання зобов'язань, узятих Україною в Празі.

Таким чином, в аспекті вступу України до НАТО її національні інтереси мають визначатися місцем і роллю Альянсу в підтриманні миру, міжнародної стабільності й безпеки на планеті, просуванні стандартів демократії, громадянського суспільства, ринкової економіки; в боротьбі з міжнародним тероризмом, створенні нової системи регіональної безпеки в Європі, вирішенні проблем роззброєння та контролю над озброєннями, нерозповсюдження зброї масового знищення.

Крім того, повноправне членство в НАТО дозволить значно підвищити рівень гарантій політичної незалежності, територіальної цілісності та непоруш-

ності кордонів нашої держави, активно сприятиме її участі у створенні нової архітектури безпеки на євроатлантичному просторі. Особливо актуалізувалося це питання зараз, коли навколо України, на всіх її кордонах (окрім молдовського), розташовані держави, що перебувають у різних воєнно-політичних координатах.

Протягом кількох років, ще на етапі "партнерства" з НАТО, ми набували загальноєвропейського досвіду і зараз широко використовуємо його в опрацюванні політичних, економічних, безпекових і правових аспектів входження до євроатлантичної спільноти, усвідомлюючи необхідність відновлення своєї європейської ідентичності.

Значного поштовху цим процесам надало підписання у 2002 р. Плану дій Україна – НАТО та Цільового плану Україна – НАТО на 2003, 2004, 2005, 2006 рр. Цими документами ми не лише взяли на себе серйозні зобов'язання, а й створили реальні механізми контролю їх виконання спільно з країнами-членами НАТО.

Більше того, в Україні з'явилася та почала функціонувати довгоочікувана цілісна, структурована система державних органів із чітким розподілом завдань і зобов'язань на чолі з Державною радою з питань європейської та євроатлантичної інтеграції.

На 2006 рік до НАТО входило 26 країн. Ще 20, зокрема й Україна, є країнами – партнерами НАТО.

2.7.2. Загальна характеристика законодавства про інформаційну безпеку країн – членів НАТО

Охарактеризуємо питання становлення та розвитку законодавства про інформаційну безпеку країн – членів НАТО. Зазначимо, що йдеться про організацію захисту інформації з обмеженим доступом, що не становить державної таємниці. Це дуже важливо в контексті євроатлантичної інтеграції нашої держави, оскільки, задекларувавши вступ до НАТО, країна повинна гармонізувати національну законодавчу базу відповідно до світових стандартів.

Законодавство у сфері захисту інформації цих країн передусім визначає об'єкти правової охорони в інформаційній сфері, порядок реалізації права власності на інформаційні об'єкти, права й обов'язки власників, правовий режим

функціонування інформаційних технологій; категорії доступу окремих суб'єктів до певних видів інформації, установлює категорії секретності, поняття "конфіденційної інформації" та межі його правового застосування.

Разом із тим, слід наголосити, що інформація в цих країнах може бути захищена за допомогою правових засобів захисту інтелектуальної власності і взагалі вона розглядається як об'єкт права інтелектуальної власності, навіть коли йдеться про масову інформацію.

Персональна інформація в цих країнах розглядається відповідно до концепції "*privacy*". Зокрема в Канаді був прийнятий Стандарт CSA, а в травні 1996 року Міжнародною організацією стандартизації (ISO) – Резолюція щодо розвитку міжнародних стандартів приватності, яка базувалася на Стандарті CSA. Цей стандарт містить такі принципи регулювання суспільних відносин, що виникають із приводу персональних даних:

1. *Відповідальність.* Організація відповідальна за ті персональні дані, що перебувають під її контролем, і має призначати особу або осіб, які відповідають за відповідність дій організації принципам законодавства.

2. *Ідентифікація мети*. Мета, задля якої збирається інформація, має бути ідентифікована організацією до початку процесу збирання інформації.

3. *Згода.* Усвідомлення та згода особи на збирання інформації про неї є обов'язковою умовою збирання, використання чи поширення (розкриття) персональних даних, крім випадків, де це недоречно.

4. *Обмежене збирання.* Збирання персональної інформації має бути обмежене тією метою, яка визначена (ідентифікована) організацією. Інформація може збиратися лише для справедливої та законної мети.

5. *Обмежене використання, поширення, зберігання*. Персональна інформація не повинна використовуватись або поширюватись не з тією метою, для якої вона була зібрана, крім випадків згоди особи або вимоги закону. Персональна інформація не повинна зберігатися довше, ніж це необхідно для досягнення зазначеної мети.

6. *Точність.* Персональна інформація має бути точною, повною та сучасною, якою необхідно бути для досягнення мети, задля якої її було зібрано.

7. *Безпека*. Персональна інформація має бути захищена за допомогою забезпечення такого рівня безпеки, який відповідає вимогам "чутливості" (sensitivity) інформації.

8. *Відкритість*. Організація має зробити доступною для особи специфічну інформацію про її (організації) політичне та практичне відношення до управління персональною інформацією.

9. *Особистий доступ.* На вимогу особи, яка має бути проінформована про існування, використання та поширення її персональної інформації, їй має бути наданий доступ до цієї інформації. Особа має бути в змозі перевірити точність та повноту інформації, виправити таку інформацію, якщо є потреба.

10. *Перевірка відповідності*. Особа повинна мати можливість направити завдання з перевірки стосовно відповідності принципам законодавства особам чи особі, відповідальним за відповідність діяльності організацій принципам законодавства.

Закріплюючи законодавчо забезпечення захисту персональних даних та захисту особи від впливу за допомогою інформації (інформаційна безпека особи), Канада планує досягти установлення балансу між використанням інформації для потреб бізнесу та потребою окремих осіб (споживачів) бути проінформованими про те, як використовується інформація про них, бути впевненими в безпеці такої інформації.

У 1995 році Європейським Союзом була прийнята Директива щодо захисту особистості з дотриманням режиму персональних даних та вільного руху таких даних, спрямована на впорядкування практики захисту інформації в межах Європейського Союзу. Однією з вимог, адресованих державам-учасникам, є вимога прийняти закони щодо захисту персональної інформації як у публічному, так і в приватному секторі. Такі закони мають також включати тимчасове блокування переміщення інформації до держав – нечленів Європейського Союзу, які не встановили належного рівня захисту інформації.

Як доповнення цієї Директиви в 1996 році була прийнята Директива, яка забезпечує гармонізацію в державах-членах умов, необхідних для того, щоб гарантувати еквівалентний рівень захисту фундаментальних прав та свобод, зокрема специфічного права на секретність стосовно оброблення персональних даних у секторі телезв'язку; вільний рух таких даних, обладнання телезв'язку і послуг у Співдружності (Законом України "Про інформацію" до основних персональних даних віднесено національність, освіту, сімейний стан, релігійність, стан здоров'я, а також адресу, дату і місце народження. Офіційним тлумаченням окремих статей цього Закону такий перелік доповнено ще й майновим станом).

Ця Директива не повинна звертатися до дій, які не підпадають під можливості законодавства Співдружності, на кшталт передбачених Правилами V та VI Угоди щодо Європейського Союзу, та в будь-якому випадку до дій щодо забезпечення безпеки, коли дії стосуються питань державної безпеки та дій держави у сфері кримінального закону. Ця Директива має стосуватися оброблення персональних даних у зв'язку з публічно доступними послугами телезв'язку в громадських мережах телезв'язку Співдружності, через об'єднані послуги цифрового зв'язку та громадські цифрові пересувні мережі (ст. 3). Держави-учасники повинні гарантувати за допомогою національних інструкцій конфіденційність повідомлень у громадських мережах телезв'язку та публічно доступних послуг телезв'язку. Зокрема, вони містять заборони на прослуховування, виявлення, зберігання та інші види перехоплення або спостереження за повідомленнями осіб, які не є абонентами, без згоди зацікавлених абонентів, крім випадків, коли особи уповноважені на такі дії законом (ст. 5).

Положення Директиви регламентують також порядок оброблення інформації, надання інформації на запити. Передбачається обов'язкове знищення інформації або надання їй характеру анонімної після вимоги її на запит чи після досягнення іншої мети, погодженої з абонентом. Оброблення даних щодо рахунків може тривати лише до закінчення періоду, протягом якого по рахунках має бути сплачено. Можливість оброблення торгівельних даних та інформації розрахунків має бути обмежена діяльністю осіб, які діють відповідно до повноважень постачальників публічно доступного обслуговування телезв'язку, запитами клієнта, виявленням шахрайства і вдосконаленням управління послугами телезв'язку. Під час такої діяльності можливість оброблення інформації має відповідати належному рівню для досягнення установленої мети. Персональні дані, що містяться в друкованих або електронних довідниках абонентів, які є доступним для громадськості чи можуть стати доступними шляхом запиту, мають бути обмежені тією інформацією, яка дозволяє ідентифікувати конкретного абонента, якщо останній не дав згоди на публікацію додаткової інформації. Держави-учасники можуть дозволити операторам мереж зв'язку вимагати платню від абонентів, які бажають, щоб інформація щодо адреси або статі не була внесена до довідника, у тому випадку, якщо встановлена сума буде помірною та не заважатиме здійсненню такого права. Держави-учасники можуть обмежити застосування цього положення до абонентів. Із метою реалізації чинної Ди-

рективи держави-учасники мають гарантувати, що для обладнання зв'язку не встановлені жодні примусові вимоги щодо певних технічних особливостей, які б могли перешкоджати вільному розміщенню обладнання на ринку та його обігу між державами-учасниками.

Відповідно до Директиви щодо захисту особистості з дотриманням режиму персональних даних та вільного руху таких даних (Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data), 95/46/EC, та конкретизуючої її Директиви від 1996 року були внесені зміни до національного законодавства держав-учасників Європейського Союзу.

Згідно із загальними принципами Акта захисту інформації в телекомунікаціях (Teleservices Data Protection Act-TDPA) збирання, оброблення та використання інформації дозволяється лише у випадках, коли воно дозволене законом або здійснюється за наявності згоди користувача обслуговування. Інформація може бути лише зібрана, оброблена або використана окремо для різних послуг, яких потребує один і той самий користувач. Згода користувача не може бути зроблена умовою для надання послуг. Інформація за договором може бути зібрана, оброблена та використана в обсязі, необхідному для виконання договору. Дані використання та бухгалтерського обліку не повинні передаватися третім особам. Утім, деякі із зазначених вище типів даних можуть бути передані з певною метою обслуговування постачальників від постачальників, через яких здійснений доступ до послуг. Дані використання та бухгалтерського обліку повинні бути знищені негайно, як тільки потреба в них відпаде. Кожен постачальник повинен запропонувати анонімне використання послуг та їх відкриту оплату. Він також має вжити заходів для того, щоб гарантувати, що інформація використовується відповідно до правил, наведених вище. Крім того, користувач має бути проінформованим стосовно типу, можливостей, місця та мети збирання, оброблення й використання його даних і він також повинен мати можливість перервати зв'язок у будь-який момент.

Істотним фактором, що гальмує міжнародний інформаційний обмін та ускладнює належний захист інформації, є невідповідність категорій розмежування доступу до інформації в різних країнах. По-перше, інформаційні законодавства можуть передбачати різну побудову ієрархічної структури режиму дос-

тупу до інформації. По-друге, одні й ті самі терміни в різних державах можуть застосовуватись для позначення не ідентичної за режимом доступу інформації.

У країнах НАТО напрацьована значна нормативно-правова база, яка регулює питання забезпечення захисту інформації з обмеженим доступом, що становить державну таємницю. Захист інформації в НАТО регламентується великою кількістю документів, які кожна нова країна-член організації повинна імплементувати у своїй державі. Ці нормативно-правові акти регулюють основні вимоги до систем забезпечення фізичної, персональної, процедурної й технічної безпеки.

Доступ до засекреченої інформації НАТО надається особі лише після отримання відповідного сертифіката допуску персоналу, визначення необхідних для її роботи меж обізнаності та інструктажу з питань процедур безпеки НАТО і підтвердження її зобов'язань стосовно безпеки.

Питання захисту інформації між Україною і НАТО регулює "Угода про безпеку між урядом України і Організацією Північноатлантичного Договору" від 12 вересня 2002 року. Вона складена з урахуванням того, що Україна є учасницею Ради Північноатлантичного співробітництва (РПАС) та програми "Партнерство заради миру". Між Україною і НАТО проводяться консультації з політичних та безпекових питань, а також розширюється й інтенсифікується політичне й військове співробітництво в Європі. Крім того, відбувається обмін таємною та конфіденційною інформацією між сторонами.

Саме тому сторони домовилися "захищати інформацію та матеріали іншої Сторони; докладати всіх зусиль для забезпечення того, щоб у разі, якщо інформація та матеріали мають гриф секретності, така інформація та матеріали зберігали грифи секретності, встановлені будь-якою Стороною стосовно інформації й матеріалів, що надаються такою Стороною, і зберігати таку інформацію та матеріали відповідно до узгоджених спільних стандартів; не використовувати отриману в результаті обміну інформацію та матеріали в цілях, відмінних від тих, що встановлені в рамках відповідних програм, а також рішень та резолюцій, що стосуються таких програм; не надавати таку інформацію та матеріали третім сторонам без згоди Сторони-джерела" (ст. 1).

Згідно з цим нормативно-правовим документом Уряд України узяв на себе зобов'язання надавати відповідний допуск усім своїм громадянам, які під час виконання службових обов'язків потребують або можуть мати доступ до ін-

формації чи матеріалів, отриманих за програмами РПАС або ПЗМ; до одержання доступу до такої інформації та матеріалів. Установлено й процедуру отримання допуску, яка відповідає тому, щоб визначити, чи може особа, зважаючи на її лояльність і можливість їй довіряти, мати доступ до інформації з обмеженим доступом без ризику для безпеки цієї інформації (ст. 2).

Відповідальними органами за домовленості в галузі безпеки з метою захисту таємної інформації, обмін якою відбувся в рамках співробітництва РПАС/ПЗМ, є Управління безпеки НАТО (УБН), Військовий комітет НАТО (ст. 3).

Крім того, перед обміном будь-якою таємною інформацією між Урядом України та НАТО відповідальні органи безпеки досягають спільної домовленості, що Сторона-отримувач готова до захисту інформації, яку вона отримує, відповідно до вимог Сторони-джерела.

Запитання і завдання для самоперевірки

1. Розкрийте питання організації захисту інформації на території України в XVII-XIX ст.

2. Охарактеризуйте організацію захисту інформації в російській армії (XIX – початок XX ст.).

3. Визначте зусилля уряду з питань організації захисту інформації в добу Центральної Ради.

4. Розкрийте питання організації захисту інформації в Українській державі гетьмана П.Скоропадського.

5. Дайте характеристику організації захисту інформації в період Директорії.

6. Покажіть специфіку та особливості організації захисту інформації в Західноукраїнській Народній Республіці.

7. Визначте специфіку захисту інформації органами МВС Державного центру УНР в екзилі.

8. Порівняйте спільні та особливі риси захисту інформації урядами в період національного відродження 1917–1921 рр.

9. Розкрийте еволюцію формування української радянської системи захисту інформації (1920–1930 рр.).

10. Охарактеризуйте питання організації захисту державної таємниці в 1920–1930 рр.

11. Як організовувався захист інформації в пресі та видавничій галузі?

12. Охарактеризуйте правові основи забезпечення захисту інформації органами ДПУ УСРР.

13. Охарактеризуйте організаційно-правові основи забезпечення охорони державної таємниці органами КДБ у 40–90-х рр. XX ст.

14. Визначте організаційно-правові основи діяльності цензури та технічного захисту інформації в 40–90-х рр. XX ст.

15. Розкрийте питання нормативно-правового забезпечення діяльності органів охорони державної таємниці в 90-х роках XX ст.

16. Опишіть проблеми забезпечення контролю за режимом секретності в органах державної влади, місцевого самоврядування, на підприємствах, в установах та організаціях у 90-х роках XX ст.

17. Окресліть питання забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва в 90-х роках XX ст.

18. Дайте характеристику законодавства України, яке визначило систему захисту інформації з обмеженим доступом.

19. Охарактеризуйте відомчі нормативно-правові акти з питань організації захисту інформації з обмеженим доступом.

20. Розкрийте етапи відносин України із структурами НАТО.

21. Дайте загальну характеристику законодавства про інформаційну безпеку країн – членів НАТО.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрієвський В. З минулого / В.Андрієвський. – Берлін : Укр. слово, 1923. – Т. 2. – 310 с.

2. Андрощук Г.А. Экономическая безопасность предприятия: защита коммерческой тайны : моногр. / Г.А.Андрощук , П.П.Крайнев – К. : Издательский Дом “Ин Юре”, 2000. – 400 с.

3. Антисоветская интервенция и ее крах. 1917–1922 гг. – М. : Политиздат, 1987. – 208 с.

4. Антонов-Овсеенко В. Записки о гражданской войне / В.Антонов-Овсеенко. – М., 1924–1933.

5. Апанович О. Розповіді про запорізьких козаків / О.Апанович. – К., 1991.

6. Аршинов П. История махновского движения (1918–1921 гг.). / П.Аршинов. – Берлин : Изд-во “Группы русских анархистов в Германии”, 1923. – 258 с.

7. Ауссем В.К. К истории повстанчества на Украине / В.К.Ауссем // Летопись революции. – 1926. – № 5.

8. Багатопартійна українська держава на початку XX ст. : програмні документи перших українських політичних партій. – К. : Україна, 1992. – 96 с.

9. Батурин Ю.М. Компьютерная безопасность / Ю.М.Батурин, А.М.Жодзишский. – М. : Юрид. лит., 1991. – С. 101.

10. Белое дело : избр. произведения : в 16 кн. – М. : Голос, 1993.

11. Биншюк М. Николаевское подполье / М.Биншюк // Летопись революции. – 1926. – № 3–4.

12. Білас І. Репресивно-каральна система в Україні 1917–1953 : суспільно-політичний та історико-правовий аналіз : у 2 кн. / І.Білас. – К. : Либідь-Військо України, 1994.

13. Бойко О.Д. Історія України / О.Д.Бойко. – К., 2004. – 655 с.

14. Бонч-Бруевич М. Вся власть советам. Воспоминания / М.Бонч-Бруевич. – М., 1958.

15. Бородиєвич Є. В чотирикутнику смерті (причини до трагедії УГА на Великій Україні) / Є.Бородиєвич. – Львів : Нове життя, 1921. – 86 с.

16. Борьба с преступностью в Украинской ССР : в 2 т. – К. : ВШ МООП УССР, 1966. – Т. 1. – 454 с.; 1967. – Т. 2. – 952 с.

17.Брайко П.Е. Партизанская война / П.Е.Брайко, И.Г.Старинов. – М. : В/ч 64510, 1983. – 335 с.

18.Брилинський М. Хресний вогонь (воєнні нариси) / М.Брилинський. – Львів : Червона Калина, 1929. – 148 с.

19.Бурнацюв Г. Генерал-хорунжий Юрій Тютюнник. Чекістська “Справа № 39” / Г.Бурнацюв. – Івано-Франківськ, 1996. – 71 с.

20.Бычков Л. ВЧК в годи гражданской войны / Л.Бычков. – М. : Госвоениздат, 1940. – 77 с.

21.Велика історія України : у 2 т. – К. : Глобус, 1993. – Т. 1. – 352 с.; Т. 2. – 400 с.

22.Верстюк В. Українська Центральна Рада : навч. посіб. / В.Верстюк. – К. : Заповіт, 1997. – 344 с.

23.Верстюк В.Ф. Махновщина: селянський повстанський рух на Україні (1918–1921 рр.) / В.Ф.Верстюк. – К. : Наукова думка, 1991. – 368 с.

24.Верстюк В.Ф. Україна від найдавніших часів до сьогодення : хронологічний довідник / В.Ф.Верстюк, О.М.Дзюба, Б.Ф.Репринцев. – К. : Наукова думка, 1995. – 685 с.

25.Вєдєнєєв Д. З досвіду побудови дипломатичної служби України / Д.Вєдєнєєв // Розбудова держави. – 1993. – № 3.

26.Вєдєнєєв Д. З історії розвідки і військової дипломатії України / Д.Вєдєнєєв // Розбудова держави. – 1993. – № 9.

27. Вєдєнєєв Д. Крила волі / Д.Вєдєнєєв // Військо України. – 1995. – № 5–6.

28.Вєдєнєєв Д. Листування між українськими та французькими масонами / Д.Вєдєнєєв // Розбудова держави. – 1996. – № 5.

29.Винниченко В. Відродження нації : у 3 ч. / В.Винниченко. – К. : Політвидав України, 1990. – 542 с.

30.Висоцький І. Розвідча служба / І.Висоцький // Українська Галицька Армія. – Т. 1. – С. 354–359.

31.Вісник Генерального секретаріату УЦР. – 1917–1918.

32.Вісник державних законів для всіх земель УНР. – 1919–1920.

33.Вісник державних законів Західної області УНР. – 1919.

34. Вісник державного Секретаріату Військових Справ. – Станіславів, 1918–1919.

35.Вісник Народного Міністерства Внутрішніх Справ УНР. – 1919–1920.

36.Вісник Українського Військового Генерального Комітету. – 1917.

37.Волков Ф.Д. Крах английской политики интервенции и дипломатической изоляции Советского государства / Ф.Д.Волков. – М. : Госполитиздат, 1954. – 400 с.

38.Волков Ф.Д. Тайны Уайт холла и Даунинг-стрит / Ф.Д.Волков. – М. : Мысль, 1980. – 462 с.

39.Ґалаґан М. З моїх споминів: 20-ті роки до Світової війни : у 3 ч. / М.Ґалаґан. – Львів : Червона Калина, 1930. – 202 с.

40.Ганжа О. При применении расстрелов бить на психику неторопливым приготовлением к жеребьевке / О.Ганжа // Віче. – 1994. – № 1.

41.Гладков Т.К. Медведєв / Т.К.Гладков. – М. : Молодая гвардия, 1985. – 304 с.

42.Голіченко В. Вартові революції: короткий нарис з історії чекістських органів України від часу їх утворення до 1922 р. / В.Голіченко. – К. : Політвидав України, 1966. – 163 с.

43.Голобуцький В. Запорізьке козацтво / В.Голобуцький. – К., 1994.

44.Голубєв В.О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В.О.Голубєв, В.Д.Гавловський, В.С.Цимбалюк ; за ред. Р.А.Калюжного. – Запоріжжя : Просвіта, 2001. – С. 52.

45. Гончаренко В. Історія держави і права України : хрестоматія / В.Гончаренко, А.Рогожин. – К., 1997.

46.Гопинков Д.Л. Крушение антисоветского подполья в СССР : в 2 кн. / Д.Л.Гопинков. – М. : Политиздат, 1986. – Кн. 1. – 333 с.; Кн. 2. – 397 с.

47.Горбулін В. Взаємовідносини Україна – НАТО в контексті євроатлантичних інтеграційних процесів / В.Горбулін // Національна безпека і оборона. – 2003. – № 7. – С. 5–7.

48.Горяева Т. Политическая цензура в СССР 1917–1991 гг. / Т.Горяева. – М. : РОССПЗН, 2002. – 400 с.

49.Гражданская война и иностранная интервенция в СССР : энциклопедия. – М.–Л. : Сов. энциклопедия, 1987. – 720 с.

50.Гражданськая война на Украине 1918-1920 гг. : сб. докум. и матер. : в 3 т. – 1967.

51.Грушевокий М. Хто такі українці і чого вони хочуть / М.Грушевокий . – К. : Т-во "Знання" України, 1991. – 240 с.

52.Гудь Б. Нелегка дорога до порозуміння. До питання ґенези українсько-польського військово-політичного співробітництва 1917–1921 рр. / Б.Гудь, В.Голубко. – Львів : Українські технології, 1997. – 67 с.

53.Гуз А.М. З історії зафронтової діяльності органів держбезпеки України в період Великої Вітчизняної війни / А.М.Гуз, О.А.Штоквиш // Історія в школі. – К., 2002. – № 7. – С. 17–19.

54.Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу : курс лекцій / А.М.Гуз. – К. : Вид-во НА СБ України, 2006. – 208 с.

55.Гуз А.М. Как защищать коммерческую тайну / А.М.Гуз, А.І.Марущак // В мире спецслужб. – К., 2006. – № 1 (13). – С. 74–80.

56.Гуз А.М. Організація партизанського руху органами держбезпеки на території України (1941–1942 рр.) / А.М.Гуз, О.А.Штоквиш // Історія в школі. – К., 2001. – №11–12. – С.14–19.

57.Гуз А.М. Програма Курсу "Вступ до спеціальності організація захисту інформації з обмеженим доступом" / А.М.Гуз, А.І.Марущак. – К. : Вид-во НА СБ України, 2004. – 13 с.

58.Гуз А.М. Роль органів держбезпеки в організації партизанського руху на території України на початковому етапі війни (1941–1942 рр.). / А.М.Гуз, О.А.Штоквиш // Збірник наукових праць НА СБ України. – К., 2002. – № 5. – С. 153–159.

59. Гуковський О. Французька інтервенція на Україні / О.Гуковський. – Х. : Пролетарій, 1929. – 63 с.

60.Гуржий О. Право в українській козацькій державі другої пол. XVII–XVIII ст. / О.Гуржий. – К., 1994.

61.Державна програма співробітництва України з Організацією Північно-Атлантичного Договору (НАТО) на період до 2001 року, затверджена Указом Президента України № 1209/98 від 4 листопада 1998 р. // Правова база НАУ, версія 8.3.1.0.

62.Державна програма створення, розвитку та забезпечення функціонування Національної системи конфіденційного зв'язку" № 1520 від 11 жовтня 2002 р.

63.Джексон Брюс. Майбутнє України визначать наступні одинадцять місяців / Джексон Брюс // Національна безпека і оборона. – 2003. – № 7. – С. 12–14.

64.Дорошенко Д. Нарис історії України / Д.Дорошенко. – К., 1992. – Т. 2.

65.Доступ до інформації та електронне урядування / [авт.-упоряд. М.С.Демкова, М.В.Фігель]. – К. : Факт, 2004. – 336 с.

66.Зленко А. Україна – і невід'ємна частина євроатлантичної спільноти / А.Зленко // Національна безпека і оборона. – 2003. – № 7. – С. 3.

67.Інструкція про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави, затверджено Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 45 від 22 жовтня 1999 р., зареєстровано в Міністерстві юстиції України за № 817/4110 від 29 листопада 1999 р.

68.Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави № 1893 від 27 листопада 1998 р.

69.История цензуры (органов по охране тайн в печати) (История Главлита) //http://www.vif.ru/users/offtopic/vio/VIO/IST32.HTM.

70.Історія України / [за ред. В.А.Смолія]. – К., 1997. – 424 с.

71.Концепція (основи державної політики) національної безпеки України (втратила чинність) // Правова база НАУ, версія 8.3.1.0.

72.Концепція технічного захисту інформації в Україні № 1126 від 8 жовтня 1997 р.

73.Курушин В.Д. Компьютерные преступления и информационная безопасность / В.Д.Курушин, В.А.Минаев. – М. : Новый Юрист, 1998.

74.Мельник Л. Конституція П.Орлика / Л.Мельник // Вісник Київського університету. Історико-філологічні науки. – 1999. – № 2.

75.Меморандум про взаєморозуміння між урядом України та НАТО, підписаний у Києві 7 травня 1997 р. // Правова база НАУ, версія 8.3.1.0.

76.Меньшиков А.А. Правові питання передачі "ноу-хау" в міжнародній торгівлі / А.А.Меньшиков. – ІГПАН СРСР, 1983. – 324 с.

77.Мицик Ю. Нові дані до історії українсько-кримських зносин у середині XVII ст. / Ю.Мицик // Пам'ять століть. – 1999. – № 5.

78.Мицик Ю. Спадкоємець Богдана Хмельницького / Ю.Мицик // Пам'ять століть. – 1999. – № 1.

79.Мицик Ю. Як козаки воювали: історичні розповіді про запорізьких козаків / Ю.Мицик. – Дніпропетровськ, 1990.

80.Нариси з історії дипломатії України / [за ред. В.А.Смолія]. – К., 2001. – 736 с.

81.Окіпнюк В.Т. Правові основи забезпечення режиму таємності органами ДПУ УСРР (20-ті – початок 30-х рр. XIX ст.) / В.Т.Окіпнюк // З архівів ВУЧК-ГПУ-НКВД-КГБ СССР. – 2001. – № 2 (17). – С. 317–325.

82.Партнерство заради миру // Довідник НАТО. – Брюссель, 2001. – С. 69–80.

83.Партнерство НАТО з Україною // Довідник НАТО. – Брюссель, 2001. – С. 90–93.

84.Підлісний А.І. Роль колегії державного комітету з питань державних секретів та технічного захисту інформації України у формуванні національної системи охорони державної таємниці / А.І.Підлісний, С.О.Князєв, О.А.Колєснік. – К. : Вид-во НА СБ України, 2003. – 52 с.

85.План заходів щодо інформаційного забезпечення співробітництва України з НАТО на 2003 рік, затверджений розпорядженням Кабінету Міністрів України № 525-р від 21 серпня 2003 р. // Правова база НАУ, версія 8.3.1.0.

86.Положение о Всеукраинской и местных чрезвычайных комиссиях // ЦДАВОВ. – Ф. 1. – Оп. 1. – Спр. 15. – С. 160.

87.Положение о Центральном Управлении по делам печати при Главполитпросвете Наркомпроса УССР // ЦДАВОВ. – Ф. 2. – Оп. 2. – Спр. 378. – С. 58.

88.Положение об Особом отделе при Всеукраинском Чрезвычайном Комитете // Центральний державний архів вищих органів влади і управління України (ЦДАВОВ). – Ф. 1738. – Оп. 1. – Спр. 13. – С. 229.

89.Положение об отделе пропаганды и агитации Ц.И.К.С.У // ЦДАВОВ. – Ф. 1. – Оп. 1. – Спр. 15. – С. 211.

90.Положення про Державне політичне управління Української Соціалістичної Радянської Республіки // ЦДАВОВ. – Ф. 1. – Оп. 2. – Спр. 1542. – С. 299.

91.Положення про державну експертизу у сфері технічного захисту інформації, затверджено Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 62 від 29 грудня 1999 р., зареєстровано в Міністерстві юстиції України за № 40/4261 від 24 січня 2000 р.

92. Положення про контроль за функціонуванням системи технічного захисту інформації, затверджено Наказом Департаменту спеціальних телекомуні-

каційних систем та захисту інформації Служби безпеки України № 61 від 22 грудня 1999 р., зареєстровано в Міністерстві юстиції України за № 10/4231 від 11 січня 2000 р.

93. Постанова Верховної Ради України "Про Воєнну доктрину України" // Відомості Верховної Ради України. – 1993. – № 43. – Ст. 409.

94. Постановление Всеукраинского Центрального Исполнительного Комитета от 5 мая 1919 г. // ЦДАВОВ. – Ф. 1738. – Оп. 1. – Спр. 13. – С. 194.

95. Постановление Всеукраинского Центрального Исполнительного Комитета от 5 мая 1919 г. о централизации Издательского дела // ЦДАВОВ. – Ф. 1738. – Оп. 1. – Спр. 13. – С. 193.

96. Постановление Всеукраинской Центральной Исполнительной Комиссии от 22 марта 1922 г. // ЦДАВОВ. – Ф. 1. – Оп. 2. – Спр. 518. – С. 30.

97. Постановление СНК УССР от 16 января 1924 г. "Об организации при Государственном Политическом Управлений УССР "Специального отдела" // ЦДАВОВ. – Ф. 1. – Оп. 2. – Спр. 2238. – С. 18.

98. Порядок інформаційного наповнення та технічного забезпечення Єдиного вебпорталу органів виконавчої влади, затверджено Наказом Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України № 327/225 від 25 листопада 2002 р., зареєстровано в Міністерстві юстиції України.

99. Про деякі питання захисту інформації, охорона якої забезпечується державою № 281 від 13 березня 2002 р.

100. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах № 1772 від 16 листопада 2002 р.

101. Про порядок здійснення криптографічного захисту інформації в Україні № 505/98 від 22 травня 1998 року.

102. Про технічний захист інформації в Україні № 1229/99 від 27 вересня 1999 року.

103. Практика защиты коммерческой тайны в США. – М., 1996.

104. Приказ по Всеукраинской Чрезвычайной Комиссии № 20/114 от 6 мая 1921 г. // ЦДАВОВ. – Ф. 2. – Оп. 2. – Спр. 116. – С. 1 .

105. Про Основні напрями зовнішньої політики України // Відомості Верховної Ради України. – 1993. – № 37. – Ст. 379.

106. Про стратегію України щодо організації Північноатлантичного договору (НАТО) // Політика і час. – 2002. – № 9. – С. 84–86.

107. Сідак В. З історії української розвідки та контррозвідки (нариси) / В.Сідак. – К., 1995.

108. Сідак В. Національні спецслужби в період Української революції 1917–1921 рр. (невідомі сторінки історії) / В.Сідак. – К., 1998.

109. Сідак В.С. З історії української розвідки та контррозвідки / В.С.Сідак, В.С.Степанков. – К., 1994. – 201 с.

110. Сідак В.С. Історія української розвідки та контррозвідки (нариси) / В.С.Сідак, В.С.Степанков. – К., 1994. – 402 с.

111. Сідак В.С. Спецслужби України часів національної революції 1917–1920 рр. : навч. посіб. / В.С.Сідак. – К., 1994. – 184 с.

112. Слюсаренко А. Історія української конституції / А.Слюсаренко, М.Томенко. – К., 1993.

113. Смолій В. Українська козацька держава: витоки та шляхи історичного розвитку / В.Смолій. – К., 1994.

114. Стан роботи Управління по справах літератури та видавництв (Укрголовліт) за 1925/26 рр. // ЦДАВОВ. – Ф. 166. – Оп. 6. – Спр. 724. – С. 988.

115. Уривчасте просування вперед // Новини НАТО. – 2003. – № 3. – С. 12.

116. Чертопруд С. Зарождение и становление системы защиты государственной тайны / С.Чертопруд // http:// www. agentura. ru/press/cenzura/secret-ussr/.

117. Шерр Джеймс Від документів до дій: чи можна подолати прірву? / Шерр Джеймс // Національна безпека і оборона. – 2003. – № 7. – С. 76–77.

РОЗДІЛ 3

ПОНЯТТЯ ТА ЗМІСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

3.1. ЗМІСТ ПОНЯТТЯ "ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ"

Визначення поняття "інформація з обмеженим доступом" має не лише наукові цілі. Чітке розуміння цього терміна сприятиме більш раціональному законотворчому процесу й дасть змогу розмежувати нерідко протилежні інтереси суб'єктів відповідних відносин.

Відповідно до ст. 28 Закону України "Про інформацію" інформація поділяється на відкриту та з обмеженим доступом. Статтею 30 цього Закону визначено, що до таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству й державі. На сьогодні термін "інформація з обмеженим доступом" законодавчо не визначений. Лише в Угоді між Кабінетом Міністрів України та Урядом Республіки Білорусь про співробітництво в галузі технічного захисту інформації (ст. 1) закріплено: "Інформація обмеженого доступу – інформація, право доступу до якої обмежено відповідно до національних законодавств держав Сторін".

Визначаючи зміст поняття "інформація з обмеженим доступом", необхідно враховувати й положення чинного законодавства України, які закріплюють правові підстави та процедури обмеження доступу до інформації певних категорій. Адже всі громадяни України, юридичні особи та державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення й зберігання відомостей, необхідних їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій. При цьому кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України. Натомість гарантіями охорони права на інформацію є норми, закріплені в ст. 47 Закону України "Про інформацію", згідно з якими відповідальність за порушення законодавства про інформацію несуть особи, винні в необґрунтованому віднесенні окремих видів інформації до категорії відомостей з обмеженим доступом.

Звичайно, реалізація права на інформацію громадянами, юридичними особами й державою не повинна порушувати громадянські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи й законні інтереси інших громадян, права та інтереси юридичних осіб. Однак віднесення певних відомостей до інформації з обмеженим доступом у будь-якому випадку має бути правомірним, тобто здійсненим чітко у відповідності й на підставі чинних правових нормативів.

Крім того, громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною за власні кошти або такою, яка є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу й не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Слід зазначити, що положення Закону України "Про інформацію" були доповнені Законом від 3 квітня 2003 р. № 676-IV нормою такого змісту: "Інформація з обмеженим доступом може бути поширена без згоди власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист". Питання практичного застосування зазначеної норми доволі проблематичне. Якщо предмет громадського інтересу ще можна визначити з певною часткою імовірності, то переважання права громадськості знати інформацію з обмеженим доступом над правом її власника на захист такої інформації визначається не так легко. У будь-якому випадку лише органи судової влади повноважні приймати остаточне рішення стосовно співвідношення цих прав.

Отже, інформація з обмеженим доступом – це відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, які визнані такими відповідно до установлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей.

3.2. ВИДИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ТА ЇХНІ ОСОБЛИВОСТІ

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну й таємну. Слід зазначити, що в багатьох підзаконних нормативно-правових актах використовується саме термін "конфіденційна інформація".

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Таке визначення закріплене Законом України "Про інформацію", хоча й має певні недоліки. По-перше, у перелік суб'єктів права власності конфіденційної інформації не включено державу, яка також володіє відомостями конфіденційного характеру. По-друге, визначення слід після слова "відомості" доповнити конструкцією "що не становлять передбаченої законом таємниці". Це пов'язано із установленим законодавством поділом інформації з обмеженим доступом на таємну та конфіденційну.

Таємна інформація – це інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (банківську, комерційну, службову, професійну, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству й державі.

Конфіденційну інформацію можна поділяти на таку, яка є власністю держави і яка не належить державі. Правовий режим конфіденційної інформації, що є власністю держави, значною мірою визначається положеннями Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затвердженої Постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893.

Відповідно до цієї Інструкції переліки конфіденційної інформації, що є власністю держави і якій надається гриф обмеження доступу "ККК користування" (далі – гриф "ККК користування"), розробляються і вводяться в дію міністерствами, іншими центральними органами виконавчої влади, Радою Міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською міськими державними адміністраціями, в яких утворюються або у володінні, користуванні чи розпорядженні яких перебувають ці відомості.

До видів таємної інформації, які передбачені чинним законодавством, відносимо:

- державну таємницю;
- комерційну таємницю;
- службову таємницю;
- професійну таємницю;

- військову таємницю;
- банківську таємницю;
- адвокатську таємницю;
- лікарську таємницю;
- таємницю страхування,
- таємницю усиновлення;
- таємницю голосування;
- таємницю нотаріальних дій;
- таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції.

На законодавчому рівні чітко регламентовані такі види таємної інформації, як державна, комерційна, банківська, професійна таємниці. Поняття службової таємниці хоча і має своє законодавче визначення, однак зміст та правові ознаки цього виду інформації з обмеженим доступом ще не достатньо регламентовані й потребують законодавчого закріплення відповідно до вимог ст. 30 Закону України "Про інформацію".

Поняття "службова таємниця" та "професійна таємниця" близькі за змістом. Службова таємниця – це склад і обсяг відомостей, що є в розпорядженні конкретного органу державної контрольно-ревізійної служби або її посадової особи стосовно об'єктів контролю, контрольних, правоохоронних та інших державних органів, їх працівників, способів досягнення визначених законодавством завдань, що необхідні для якісного проведення контрольно-ревізійних дій, забезпечення відповідної їх раптовості, ефективності і які з цієї причини на певний період не підлягають зовнішньому чи внутрішньому розголошенню.

Професійна таємниця – стан збереження матеріалів, документів, інших відомостей, якими користуються посадові особи Рахункової палати та особи, котрі залучаються до здійснення функцій Рахункової палати під час проведення перевірок, ревізій, обслідувань, і які забороняється розголошувати у будь-якій формі до моменту прийняття рішення Рахунковою палатою.

Інше визначення професійної таємниці закріплено в Законі України "Про фінансові послуги та державне регулювання ринків фінансових послуг" (ст. 1): професійна таємниця – матеріали, документи, інші відомості, якими користуються в процесі та у зв'язку з виконанням своїх посадових обов'язків посадові особи державних органів, що здійснюють регулювання ринків фінансових пос-

луг, та особи, які залучаються до здійснення цих функцій, і які забороняється розголошувати у будь-якій формі до моменту прийняття рішення відповідним уповноваженим державним органом.

Особливості правового статусу державної таємниці визначаються Законом України "Про державну таємницю", відповідно до якого державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані такою (державною таємницею) у порядку, встановленому Законом України "Про державну таємницю", і підлягають охороні державою.

Статтею 505 Цивільного кодексу України визнано, що комерційна таємниця – це інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Правовий статус банківської таємниці визначено Законом України "Про банки і банківську діяльність", зокрема главою 10 "Банківська таємниця та конфіденційність інформації", а також Цивільним кодексом України. Банківська таємниця – це інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин із ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної або моральної шкоди клієнту.

Одним із специфічних видів інформації з обмеженим доступом є конфіденційна інформація про особу. Її правовий статус визначається Законом України "Про інформацію", а офіційне тлумачення викладене в Рішенні Конституційного Суду України № 5-зп від 30 жовтня 1997 року (справа К.Г.Устименка). Зокрема зазначається, що ч. 4 ст. 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.

До конфіденційної інформації про особу належать такі свідчення про неї: освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані. На визначення змісту конфіденційної інформації про особу спрямовані й інші нормативно-правові акти, зокрема органів судової влади. Їхній аналіз дає підстави віднести до конфіденційної інформації про особу також дані про інтимні сторони життя, захворювання, непорядні вчинки тощо.

Крім того, Постанова Пленуму Верховного Суду України визначає відомості, що ганьблять потерпілого або близьких йому осіб. Це такі дійсні чи вигадані дані про них, їхні дії й дії, учинені щодо них, які потерпілий бажає зберегти в таємниці та розголошення яких, на його думку, скомпрометує або принизить честь і гідність його чи близьких йому осіб.

Погроза розголосити такі відомості – це погроза повідомити про них особам (або особі), яким вони невідомі й чиє ознайомлення з ними небажане для потерпілого.

Окремими видами таємної інформації передбачені законодавством таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, таємниця заповіту тощо, про які ітиметься далі.

Банківською таємницею зокрема є:

1) відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку України;

2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

3) фінансово-економічне становище клієнтів;

4) системи охорони банку та клієнтів;

5) інформація про організаційно-правову структуру юридичної особи-клієнта, її керівників, напрями діяльності;

6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

8) коди, що використовуються банками для захисту інформації.

Інформація про банки чи клієнтів, котру збирають під час проведення банківського нагляду, теж становить банківську таємницю.

Банки зобов'язані забезпечити збереження банківської таємниці шляхом:

1) обмеження кола осіб, котрі мають доступ до інформації, яка становить банківську таємницю;

2) організації спеціального діловодства з документами, що містять банківську таємницю;

3) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;

4) використання застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком та клієнтом.

Службовці банку при призначенні на посаду підписують зобов'язання щодо збереження банківської таємниці. Керівники та службовці банків зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні службових обов'язків.

Приватні особи та організації, які під час виконання своїх функцій або надання послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати її та не використовувати на свою користь чи на користь третіх осіб.

У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їхніх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовують винні органи. Особи, винні в порушенні порядку розкриття та використання банківської таємниці, несуть відповідальність згідно із законами України.

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 виконанні професійних обов'язків.

Наразі в Україні триває нормотворча робота у сфері правового регулювання конфіденційної інформації про особу, зокрема прийнято проект Закону України про захист персональних даних (реєстр. № 2618), на який Президент наклав вето.

3.3. МІСЦЕ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ

Інформаційні ресурси та інформаційна інфраструктура відіграють дедалі більшу роль у міждержавній боротьбі за світове лідерство й досягнення політичних, економічних, військових цілей. Отже, стійке функціонування інформаційної інфраструктури, забезпечення інтересів особи, суспільства й держави в цій сфері виступають важливим чинником збалансованого розвитку будь-якої країни.

У статті 17 Конституції України закріплена норма, відповідно до якої забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, справою всього українського народу. Наголошуємо: саме держави, а не громадянина чи окремих суб'єктів господарської діяльності.

Конкретизує конституційну норму положення, закріплене у ст. 28 Закону України "Про інформацію", а саме: "держава здійснює контроль за режимом доступу до інформації". При цьому завдання контролю за режимом доступу до інформації полягає в забезпеченні дотримання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом.

Державний контроль за додержанням установленого режиму здійснюють спеціальні органи, які визначають Верховна Рада й Кабінет Міністрів України. У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти про їхню діяльність із забезпечення інформацією зацікавлених осіб (кількість випадків відмови в наданні доступу до інформації із зазначенням мотивів таких відмов; чисельність та обґрунтування застосування режиму обмеженого доступу до окремих видів інформації; кількість скарг на неправомірні дії посадових осіб, які відмовили в доступі до інформації, та вжиті щодо них заходи тощо).

Так, ст. 5 Закону України "Про основи національної безпеки України" серед принципів забезпечення національної безпеки передбачає "проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм... у інформаційній та інших сферах". Натомість ст. 7 указаного Закону визначає, що на сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві в інформаційній сфері є, серед інших, "розголошення

інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави".

Зазначена загроза, як бачимо, закріплена на найвищому – законодавчому рівні. Причому зауважимо, що увага акцентується на фактах розголошення не лише державної, а й іншої передбаченої законом таємниці, а також конфіденційної інформації. Йдеться, звичайно, про комерційну, банківську таємницю, інші види інформації з обмеженим доступом, яка належить фізичним та юридичним особам.

Насамперед розглянемо зміст поняття "захист інформації з обмеженим доступом". Поняття "захист інформації" закріплено в Законі України "Про захист інформації в автоматизованих системах" як "сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованим системам та особам, які користуються інформацією". Таке ж визначення містять підзаконні акти.

Поняття "захист інформації" визначається також у міжнародно-правових угодах зокрема як "комплекс заходів, спрямованих на запобігання небажаним впливам на об'єкт захисту інформації, а також її неконтрольованому поширенню". Нормативно закріплені визначення суміжних понять. Так, комплексна система захисту інформації – це сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації. Закон України "Про державну таємницю" дає таке визначення поняття "охорона державної таємниці": комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

З огляду на ці визначення, керуючись змістом поняття "інформація з обмеженим доступом", зазначимо, що захист інформації з обмеженим доступом – це сукупність організаційно-правових, інженерно-технічних та криптографічних заходів, які вживають власник інформації з обмеженим доступом або інші особи за його замовленням із метою запобігання заподіянню шкоди інтересам власника інформації та неконтрольованому поширенню останньої.

Важливість захисту інформації з обмеженим доступом для належного забезпечення національної й державної безпеки підтверджується багатьма законодавчими й підзаконними нормативно-правовими актами. Їхній аналіз дає підстави для висновку, що на сьогодні захист інформації з обмеженим доступом, його законодавча регламентація, встановлення відповідних гарантій для власників такої інформації є важливими завданнями держави й відповідних органів.

3.4. ПРАВОВІ ОСОБЛИВОСТІ ОБІГУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У ДІЯЛЬНОСТІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Зміни в політичному житті й економіці України стали підґрунтям для появи значної кількості недержавних підприємств і організацій, які стали самостійними суб'єктами господарювання. Їхній новий статус серед інших спричинив проблему захисту належної їм інформації з обмеженим доступом економічного характеру (комерційної, банківської таємниці та конфіденційної інформації).

В умовах планової економіки СРСР протиправні посягання на економічну інформацію підприємств і організацій із боку вітчизняних суб'єктів підприємницької діяльності були виключені в силу їхньої безпідставності. Захист цієї інформації від посягань іноземних організацій цілком забезпечували вітчизняні спецслужби.

Поряд із традиційними загрозами у сфері формування, зберігання й поширення інформаційних ресурсів зростає небезпека несанкціонованого втручання в роботу інформаційних систем не тільки з метою отримання закритої інформації, а й для порушення її цілісності та знищення, дезорганізації інформаційної системи держави, суб'єктів підприємництва тощо. Реаліями сучасності стали інформаційна експансія, інформаційна зброя, інформаційна війна. Все це зумовлює не тільки застосування традиційних, практично перевірених заходів охорони інформаційних ресурсів, що містять відомості, віднесені до інформації з обмеженим доступом, а й розроблення та впровадження заходів і засобів правового, організаційного, інженерно-технічного й криптографічного захисту вказаної інформації.

У 1990 році в СРСР була здійснена спроба визначення комерційної таємниці та відповідальності за її розголошення в ст. 33 Закону СРСР "Про підприємства", який повинен був визначати загальноправові, економічні й соціальні основи організації підприємств різних форм власності та їхню діяльність в умовах "розвитку товарно-грошових відносин і регульованого ринку". При цьому комерційною таємницею підприємства визначались пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою його діяльністю відомості, що не є державними таємницями, розголошення (передавання, витік) яких може завдати шкоди його інтересам.

Нині в Україні, як і в інших державах світу, у процесі підприємницької діяльності, при створенні нових технологій, у результаті інтелектуальної праці виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, що становлять комерційну цінність. Це можуть бути методики робіт, перспективні технічні рішення, результати маркетингових досліджень тощо, спрямовані на досягнення підприємницького успіху.

Проблема захисту комерційної таємниці має багато аспектів. Серед них найважливішими є визначення правових ознак комерційної таємниці як соціального ресурсу, юридичне закріплення права на комерційну таємницю та створення правових гарантій реалізації цього права, регулювання відносин, які виникають у сфері обігу комерційної таємниці.

У світі немає єдиного підходу до визначення інформації, яка становить комерційну цінність. Застосовуються різні поняття: "ділові секрети", "виробничі секрети", "торговельні секрети", "конфіденційна інформація", "комерційна таємниця" тощо.

Згідно зі ст. 155 Господарського кодексу України та ст. 420 Цивільного кодексу України серед об'єктів прав інтелектуальної власності у сфері господарювання визнається комерційна таємниця. Досягнення успіху в підприємницькій діяльності дуже часто пов'язане з комерційною таємницею й неможливістю її використання конкурентами. Виділяють такі причини неправомірного використання комерційної таємниці конкурентами:

- для поліпшення виробничої та комерційної діяльності організації (конкурента), що протиправно заволоділа комерційною таємницею, підвищення конкурентоспроможності продукції та ефективності виробництва, вибору оптимальної стратегії реалізації продукції й торгових переговорів;
- для завдання шкоди власнику комерційної таємниці, протидії реалізації продукції, руйнуванню виробничих та торгівельних зв'язків останнього; зриву торгівельних переговорів й угод; зниження інвестиційних можливостей, підготовки та поширення неправдивих відомостей про власника комерційної таємниці тощо.

Сьогодні втраті комерційної таємниці в Україні "сприяє" безсистемність її захисту, роз'єднаність зусиль держави й приватних підприємців у забезпеченні цілісності інформації, відсутність у власників комерційної таємниці організаційного досвіду щодо її захисту, недостатність правової підготовки та інформаційної культури. При застосуванні організаційно-правового механізму захисту

комерційної таємниці виділяють низку невирішених питань, серед яких відсутність: чіткого визначення поняття "комерційна таємниця" з урахуванням інтересів як юридичних, так і фізичних осіб; механізму здійснення прав власності на інформацію, віднесену до комерційної таємниці; методики визначення її вартості; органу державної виконавчої влади, що буде формувати й реалізовувати державну політику щодо охорони прав на комерційну таємницю тощо.

Здійснюється також обмеження доступу до архівних документів. Стаття 16 Закону України "Про Національний архівний фонд та архівні установи" визначає можливості обмеження доступу до документів Національного архівного фонду, що належать державі, територіальним громадам. Так, архівні установи мають право обмежити доступ до таких документів на строк до одного року у зв'язку з їх науково-технічним опрацюванням, перевіркою наявності та стану або реставрацією. У разі проведення великого обсягу таких робіт термін обмеження може бути продовжений із дозволу центрального органу виконавчої влади у сфері архівної справи й діловодства, але не більше, ніж на один рік.

Архівні установи мають право відмовити в доступі до документів Національного архівного фонду неповнолітнім, особам, визнаним судом недієздатними, та особам, які грубо порушували порядок користування архівними документами. В інтересах охорони інформації, віднесеної до державної або іншої передбаченої законом таємниці, що міститься в документах Національного архівного фонду, доступ до цих документів обмежується відповідно до закону до моменту скасування рішення про віднесення інформації до державної або іншої таємниці.

Доступ до документів Національного архівного фонду, що містять конфіденційну інформацію про особу, а також створюють загрозу для життя чи недоторканності житла громадян, обмежується на 75 років від часу створення цих документів, якщо інше не передбачено законом. Раніше зазначеного строку доступ здійснюється з дозволу громадянина, права та законні інтереси якого можуть бути порушені, а в разі його смерті – з дозволу спадкоємців.

У разі передання за договором до державних архівних установ, архівних відділів міських рад документів Національного архівного фонду, що не належали державі, територіальним громадам, умови подальшого користування ними визначаються з колишніми власниками цим договором. Такий порядок може бути встановлено також у випадках передавання документів на зберігання без зміни права власності на них.

Стаття 17 Закону України "Про Національний архівний фонд та архівні установи" визначає обмеження доступу до документів Національного архівного фонду, що належать іншим власникам (окрім держави, територіальних громад). Архівні підрозділи об'єднань громадян, релігійних організацій, а також підприємств, установ і організацій, заснованих на приватній формі власності, архівні установи, засновані фізичними особами, мають право обмежити доступ до документів Національного архівного фонду з метою забезпечення їх схоронності й захисту прав та законних інтересів їхніх власників або інших осіб. Обмеження встановлюються на вимогу власника документів чи інших зацікавлених осіб із письмовим повідомленням центрального органу виконавчої влади у сфері архівної справи і діловодства.

Визначені законом обмеження (ч. 4, 5 ст. 16 й ч. 1 ст. 17 Закону України "Про Національний архівний фонд та архівні установи") не поширюються на працівників державних архівних установ, суду, правоохоронних, контрольно-ревізійних та податкових органів, які виконують службові завдання, у передбачених законом випадках, а саме:

- коли йдеться про доступ до конфіденційної інформації про особу;
- передання за договором до державних архівних установ, архівних відділів міських рад документів Національного архівного фонду, що не належали державі, територіальним громадам;
- коли архівні установи, засновані на приватній формі власності, обмежили доступ до документів Національного архівного фонду з метою забезпечення збереженості документів і захисту прав та законних інтересів власників документів або інших осіб.

Законом можуть бути передбачені інші випадки, коли зазначені обмеження не застосовуються.

Важливість визначення співвідношення права громадськості знати інформацію з обмеженим доступом та права її власника на захист такої інформації має не лише теоретичне, а й практичне значення. Це пов'язано з тим, що зазначена процедура стосується захисту прав громадян, адже ст. 47-1 Закону України "Про інформацію" передбачено звільнення особи від відповідальності "за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно значимою". Проблема в застосуванні наведених норм Закону України "Про інформацію" полягає в тому, що на сьогодні чинним законодавством не встановлено порядок надання інформації статусу суспільно значущої.

Запитання і завдання для самоперевірки

1. Дайте визначення поняття “інформація з обмеженим доступом”.
2. У яких випадках інформація з обмеженим доступом може бути поширена без згоди її власника?
3. Назвіть види інформації з обмеженим доступом.
4. Що таке конфіденційна інформація?
5. Дайте визначення поняття “таємна інформація”.
6. Назвіть види конфіденційної інформації.
7. Які види таємної інформації передбачені чинним законодавством України?

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про інформацію”.
2. Марущак А.І. Свобода слова та інформація з обмеженим доступом: співвідношення понять / А.І.Марущак // Бюлетень Мін’юсту України. – 2005. – № 6 (44). – С. 44–49.
3. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. / А.Б.Стоцький, А.М.Гуз, А.І.Марущак та ін. ; за заг. ред. В.С.Сідака. – К. : Вид-во Європейського ун-ту, 2006. – 232 с.
4. Порядок надання послуг конфіденційного зв’язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям, затверджений постановою Кабінету Міністрів України від 11 жовтня 2002 р. № 1519.
5. Рішення Конституційного Суду України № 5-зп від 30 жовтня 1997 року (справа К.Г.Устименка) у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру”.
6. Цивільний кодекс України.

РОЗДІЛ 4

ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

Входження України до євроатлантичних структур, прагнення вступу до Всесвітньої торговельної організації, а також намагання створити регіональну систему безпеки, яка стала б основою загальноєвропейської системи безпеки, потребують дієздатних органів виконавчої влади. З огляду на це, а також з урахуванням важливих внутрішньополітичних функцій держави постає питання правового й організаційного забезпечення інформаційної безпеки органів виконавчої влади. Інформаційне забезпечення органів виконавчої влади є однією із складових загальної системи забезпечення державного управління.

Важливим елементом забезпечення інформаційної безпеки держави й національної безпеки загалом, реалізації функцій управління в органах державної влади виступає режим охорони державної таємниці в Україні.

4.1. ПРАВОВИЙ СТАТУС ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

Проблема урегулювання суспільних відносин у сфері охорони державної таємниці на сучасному етапі була вирішена в розвинених країнах шляхом прийняття відповідних законів. Однак у СРСР та донедавна в Україні не було закону не тільки про державну таємницю, але й про інформацію загалом. Відносини, що виникали у сфері охорони державної таємниці, регулювались на рівні урядових рішень, які в більшості випадків мали закритий характер. Із ними не могли ознайомитися ні вчені-юристи, ні широкі верстви населення.

Із прийняттям Закону України “Про державну таємницю” на законодавчому рівні було врегульовано суспільні відносини, пов’язані з віднесенням інформації до державної таємниці, її засекречуванням та охороною з метою захисту життєво важливих інтересів України у сфері оборони, економіки, зовнішніх відносин, державної безпеки й охорони правопорядку.

Насамперед розкриємо поняття “державна таємниця” та ознаки, які його характеризують. Це дасть змогу правильно установлювати коло відомостей, котрі потрібно охороняти, розподіляти зусилля з організації охорони, вирішувати питання про відповідальність осіб за порушення законодавства, уникати витра-

чання сил та засобів на охорону несекретної інформації, визначати й аналізувати можливі шляхи витоку інформації тощо.

Законодавство України дає чітке визначення поняття "державна таємниця". Це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому законом, державною таємницею й підлягають охороні державою. Отже, слід виокремити та дослідити ознаки, які характеризують це поняття.

Перша ознака полягає в тому, що державна таємниця є видом таємної інформації, правове регулювання якої здійснюється відповідним законом. Закон України "Про інформацію" вперше на законодавчому рівні закріпив необхідність урегулювання правових відносин у сфері охорони державної таємниці на рівні спеціального закону, прийняття якого було першим кроком на шляху раціонального та демократичного підходу до регулювання зазначених вище суспільних відносин. До речі, законодавче врегулювання останніх здійснюється й у таких країнах, як США, Сполучене Королівство Великої Британії та Північної Ірландії, Польща та інші.

Закон України "Про інформацію" визначив місце державної таємниці серед іншої інформації. За режимом доступу інформація поділяється на відкриту та з обмеженим доступом. Остання за своїм правовим режимом буває конфіденційна й таємна. Одним із видів таємної інформації є державна таємниця.

Отже, перша ознака державної таємниці полягає в тому, що суспільні відносини, які виникають під час визначення такої інформації, її охорони та обігу, врегульовано на рівні окремого закону.

Другою ознакою державної таємниці є те, що до неї відносять лише відомості у сфері оборони, економіки, зовнішніх відносин, науки і техніки, державної безпеки й охорони правопорядку. На законодавчому рівні закріплено не всі сфери життєдіяльності держави, які може охоплювати державна таємниця, а лише найважливіші, пов'язані із забезпеченням національної безпеки. Слід зазначити, що не вся інформація в цих сферах може становити державну таємницю, оскільки визначаються відповідні її категорії. У зв'язку з цим до державної таємниці можуть бути віднесені конкретні відомості лише за умови, що вони належать до цих категорій.

Із усього інформаційного простору вирізняють державні інтереси та інтереси суспільства й громадян. Щодо останніх законом установлено перелік відомостей, які забороняється відносити до державної таємниці:

- про стан довкілля, 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 та свобод людини і громадянина;
- про незаконні дії органів державної влади, місцевого самоврядування та їхніх посадових осіб;
- іншу інформацію, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена.

Третя ознака полягає в тому, що розголошення державної таємниці може завдати шкоди національній безпеці України. Справді, немає сенсу приховувати інформацію, розголошення якої не завдасть шкоди. Як бачимо, шкода національній безпеці України є однією з матеріальних ознак цього поняття. Протиправний вихід державної таємниці з володіння правомочних суб'єктів пов'язується з об'єктивним заподіянням або можливістю заподіяння шкоди. Під шкодою розуміються як економічні збитки, так і інші тяжкі наслідки. Економічно шкода визначається матеріальними збитками в кількісному (вартісному) вираженні, які завдані чи яких завдадуть унаслідок розголошення конкретних відомостей, що становлять державну таємницю у сферах оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку. Щодо інших тяжких наслідків, то вони пов'язуються з негативними змінами у зазначених сферах (здебільшого у зовнішніх відносинах, державній безпеці й охороні правопорядку), які відбулися чи можуть відбутися через розголошення конкретних відомостей, що становлять державну таємницю, і які не піддаються економічному обрахунку у вартісному вираженні. Обґрунтування шкоди національній безпеці в разі розголошення державної таємниці України здійснює державний експерт із питань державних таємниць під час віднесення інформа-

ції до державної таємниці. Він також бере участь у розробленні критеріїв визначення шкоди, яку може бути завдано розголошенням такої інформації.

Наступна ознака державної таємниці – створення на законодавчому рівні механізму віднесення інформації до державної таємниці та її засекречування. Як уже зазначалося, є категорії інформації, яка становить державну таємницю. Відповідно до цих категорій формується Звід відомостей, що становлять державну таємницю (ЗВДТ). Це єдина форма реєстрації таких відомостей в Україні. Із моменту опублікування Зводу держава забезпечує захист і правову охорону зареєстрованих у ньому відомостей. Служба безпеки України формує ЗВДТ на підставі рішень державних експертів із питань таємниць та публікує його в офіційних виданнях. Інформація уважається державною таємницею з моменту включення її до ЗВДТ. Реєстрація відомостей у Зводі є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифу секретності, установленого для них у ЗВДТ. На підставі та в межах ЗВДТ із метою конкретизації даних про інформацію, яка віднесена до державної таємниці, органи державної влади України можуть створювати відповідні розгорнуті переліки таких відомостей. Ці переліки повинні бути затверджені державними експертами з питань таємниць та погоджені СБ України; вони не можуть суперечити ЗВДТ. Віднесення інформації до державної таємниці та її засекречування – вольовий акт із боку держави, який залежить від внутрішньо- та зовнішньополітичної обстановки, економічного розвитку, політичного режиму тощо.

Ознакою державної таємниці є те, що її охорону здійснює держава. На відміну від інших видів інформації (банківської, комерційної), фінансування діяльності, пов’язаної з державною таємницею, в бюджетних установах і організаціях має здійснюватися за рахунок Державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати повинні передбачатися у відповідних бюджетах окремим рядком. Такі витрати інших установ і організацій, а також підприємств належать до валових витрат виробника продукції, виготовлення якої пов’язано з державною таємницею. Витрати, пов’язані з державною таємницею, на недержавних підприємствах, в установах, організаціях згідно із Законом України “Про державну таємницю” фінансуються на підставі договору із замовником відповідних робіт.

Підприємствам, установам і організаціям, які проводять діяльність, пов’язану з державною таємницею, можуть надаватися податкові та інші пільги в порядку, встановленому законом.

4.2. ЗМІСТ ПОНЯТТЯ “ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ”

Охорона державної таємниці України – це складний соціально-правовий процес, який відображає багатоаспектну діяльність держави в соціально-політичній, економічній, правовій та інших сферах суспільного життя. Комплексний характер здійснюваних при цьому заходів зумовлює необхідність активної участі в охороні державної таємниці різних органів держави.

Охорона державної таємниці є однією із складових забезпечення національної безпеки України. Суб’єкти, на яких покладено функції забезпечення національної безпеки, тією чи іншою мірою забезпечують й охорону державної таємниці. Охорона державної таємниці – це комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації і втратам її матеріальних носіїв.

Основні організаційно-правові заходи щодо охорони державної таємниці полягають у впровадженні:

- єдиних вимог до виготовлення, користування, збереження, передавання, транспортування та обліку матеріальних носіїв секретної інформації;
- дозвільного порядку проведення органами державної влади, місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов’язаної з державною таємницею;
- обмеження оприлюднення, передавання іншій державі або поширення іншим шляхом секретної інформації;
- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування й переміщення об’єктів і технічних засобів, що їм належать;
- умов здійснення органами державної влади їхніх функцій щодо органів державної влади, місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов’язана з державною таємницею;
- режиму секретності органів державної влади, місцевого самоврядування, підприємств, установ і організацій, що проводять діяльність, пов’язану з державною таємницею;
- спеціального порядку допуску та доступу громадян до державної таємниці;
- технічного й криптографічного захисту секретної інформації.

Правову основу створення й функціонування системи охорони державної таємниці в Україні закладено в Законі України "Про державну таємницю", який регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням та охороною її матеріальних носіїв. Важливість діяльності з охорони державної таємниці полягає в тому, що діяння, які посягають на збереження останньої, кваліфікуються як злочини. Кримінальний кодекс України визначає такі злочини, предметом яких є державна таємниця:

- державна зрада (ст. 111);
- шпигунство (ст. 114);
- розголошення відомостей, що становлять державну таємницю (ст. 328);
- втрата документів, що містять державну таємницю (ст. 329);
- розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422).

У Кримінально-процесуальному кодексі України зафіксовано, що у справах про злочини, передбачені названими статтями Кримінального кодексу України, досудове слідство проводять слідчі органів Служби безпеки України. Чинне законодавство України передбачає закритий розгляд справ у всіх судах у разі потреби забезпечення охорони державної таємниці.

Закони України "Про державну таємницю", "Про Службу безпеки України", "Про оперативно-розшукову діяльність", "Про контррозвідувальну діяльність", "Про розвідувальні органи" визначають організацію охорони державної таємниці в Україні. Це основні, хоча й не всі акти Верховної Ради України, які стосуються питань забезпечення охорони державної таємниці. На основі положень законів та на їх виконання ухвалюються укази Президента України, постанови Кабінету Міністрів України й інші нормативно-правові акти центральних органів виконавчої влади. Їхньою метою є конкретизація та реалізація приписів законів. Отже, всі названі вище акти є підзаконними і не можуть суперечити вимогам законів.

У статті 35 Закону України "Про державну таємницю" зазначено, що технічний та криптографічний захист секретної інформації здійснює в порядку, установленому Президентом України. На виконання положень цієї статті видано такі укази Президента України: "Положення про технічний захист інформації в Україні" (від 27 вересня 1999 року № 1229), "Положення про порядок здійснення криптографічного захисту інформації в Україні" (від 22 травня 1998 року № 505)

і “Положення про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України” (від 6 жовтня 2000 року № 1120).

Функції державного експерта з питань таємниць у державних органах (крім Верховної Ради України), Національній академії наук України, на підприємствах, в установах і організаціях покладаються Президентом України на конкретних посадових осіб за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій. Перелік таких посадових осіб затверджено Указом Президента України від 18 жовтня 2000 року № 1144.

Згідно зі ст. 19 Закону України “Про державну таємницю” єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передавання та транспортування матеріальних носіїв секретної інформації установлює Кабінет Міністрів України.

Дозвільний порядок провадження діяльності, пов’язаної з державною таємницею, регламентується ст. 20 Закону України “Про державну таємницю”, в якій зазначається, що порядок надання, переоформлення, зупинення дії або скасування дозволу на провадження діяльності, пов’язаної з державною таємницею, форма акта спеціальної експертизи щодо наявності умов для провадження діяльності, пов’язаної з державною таємницею, форма дозволу на провадження діяльності, пов’язаної з державною таємницею, та категорії режиму секретності установлені в нормативно-правових актах Кабінету Міністрів України.

4.3. ЗВІД ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ ДЕРЖАВНУ ТАЄМНИЦЮ

Згідно із Законом України “Про державну таємницю” віднесення інформації до державної таємниці є процедурою прийняття державним експертом із питань таємниць рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їхньої секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України в разі розголошення цих відомостей, включенням цієї інформації до ЗВДТ, із його опублікуванням чи внесенням змін до нього.

Закон України “Про державну таємницю” визначає категорії інформації, яка може бути віднесена до державної таємниці у сферах оборони, економіки, науки і техніки, зовнішніх зносин, державної безпеки й охорони правопорядку. З урахуванням цього, на підставі рішень державних експертів із питань таємниць Служба безпеки України формує та публікує в офіційних виданнях ЗВДТ (головний документ у країні, від якого залежить обсяг секретної інформації). Чинний Звід відомостей, що становлять державну таємницю, затверджено наказом Служби безпеки України від 12 серпня 2005 р. № 440, зареєстровано в Міністерстві юстиції України 17 серпня 2005 р. за № 902/11182.

Зміни до Зводу відомостей, що становлять державну таємницю, публікуються не пізніше трьох місяців із дня одержання Службою безпеки України відповідного рішення чи висновку державного експерта з питань таємниць. На підставі та в межах ЗВДТ із метою конкретизації й систематизації даних про секретну інформацію органи державної влади створюють галузеві або відомчі (а також міжгалузеві чи міжвідомчі) розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що проводять діяльність, пов’язану з державною таємницею, за ініціативою та погодженням із замовником відповідних робіт можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються зі Службою безпеки України, затверджуються державними експертами з питань таємниць та реєструються в Службі безпеки України. Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити ЗВДТ.

Нині в Україні створено демократичний порядок віднесення інформації до державної таємниці, результатом якого є відображення ЗВДТ в офіційно опублікованому виданні.

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлює державний експерт із питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого установлює Служба безпеки України, та інших обставин. Він не може перевищувати для інформації із ступенем секретності “особливої важливості” – 30 років, “цілком таємно” – 10 років, “таємно” – 5 років.

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров’ю й безпеці населення.

4.4. ПОНЯТТЯ ДОПУСКУ ТА ДОСТУПУ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Спеціальний порядок допуску й доступу громадян до державної таємниці є складовою комплексу заходів, спрямованих на запобігання витоку секретної інформації. Наявність такого порядку зумовлюється необхідністю вивчення та обмеження кола осіб, діяльність яких буде пов'язана з державною таємницею. Порядок надання, переоформлення й скасування громадянам допуску до державної таємниці передбачений ст. 22-29 Закону України "Про державну таємницю" і встановлюється Кабінетом Міністрів України.

Допуск до державної таємниці – це оформлення права громадянина на доступ до секретної інформації. Доступ до державної таємниці – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею; або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Залежно від ступеня секретності інформації установлюються такі форми допуску до державної таємниці:

- форма 1 – для роботи із секретною інформацією, що має ступені секретності "особливої важливості", "цілком таємно" й "таємно";
- форма 2 – для роботи з секретною інформацією, що має ступені секретності "цілком таємно" й "таємно";
- форма 3 – для роботи із секретною інформацією, що має ступінь секретності "таємно";

а також такі терміни дії допусків:

- для форми 1 – 5 років;
- для форми 2 – 10 років;
- для форми 3 – 15 років.

Допуск до державної таємниці зі ступенями секретності "особливої важливості", "цілком таємно" й "таємно" надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання, наказом чи письмовим розпорядженням керівника органу державної влади, місцевого самоврядування, підприємства, установи або організації, де працює, перебуває на службі або навчається громадянин.

У окремих випадках, які визначають міністерства, інші центральні органи виконавчої влади, за погодженням із Службою безпеки України громадянам України віком від 16 років може надаватися допуск до державної таємниці із ступенями секретності "цілком таємно" й "таємно", а віком від 17 років – також до державної таємниці із ступенем секретності "особливої важливості".

Відповідно до ст. 27 Закону України "Про державну таємницю" доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання. Рішення про надання доступу до конкретної секретної інформації та її матеріальних носіїв приймають у формі наказу або письмового розпорядження керівники органів державної влади, місцевого самоврядування, підприємств, установ і організацій, у яких виконуються роботи, пов'язані з державною таємницею, чи зберігаються матеріальні носії секретної інформації.

Відмова надати громадянинові України доступ до конкретної секретної інформації та її матеріальних носіїв можлива лише в разі відсутності підстав, передбачених вище.

Президентові України, Голові Верховної Ради України, Прем'єр-міністрові України, Голові Верховного Суду України, Голові Конституційного Суду України, Генеральному прокурору України, Голові Служби безпеки України доступ до державної таємниці усіх ступенів секретності надається за посадою після взяття ними письмового зобов'язання щодо збереження державної таємниці.

Іноземцям та особам без громадянства доступ до державної таємниці надається у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

4.5. ПОВНОВАЖЕННЯ ОРГАНІВ, КОТРІ ЗАБЕЗПЕЧУЮТЬ ОХОРОНУ ДЕРЖАВНОЇ ТАЄМНИЦІ ВІДПОВІДНО ДО ЗАКОНОДАВСТВА УКРАЇНИ

Стаття 5 Закону України "Про державну таємницю" визначає компетенцію органів державної влади, місцевого самоврядування та їхніх посадових осіб у сфері охорони державної таємниці. Всі суб'єкти забезпечення охорони державної таємниці діють виключно в межах повноважень, визначених Конституцією, законами й іншими нормативно-правовими актами України.

Розглянемо повноваження Верховної Ради України, Президента України, Ради національної безпеки і оборони України та Кабінету Міністрів України у сфері охорони державної таємниці.

Провідну роль у сфері охорони державної таємниці відіграє Верховна Рада України як єдиний орган законодавчої влади в нашій державі; її повноваження закріплені в ст. 85 Конституції України та ст. 4 Закону України "Про державну таємницю", а саме:

- визначення державної політики щодо державної таємниці як складової засад внутрішньої та зовнішньої політики;
- прийняття законодавчих актів, які забезпечують функціонування системи охорони державної таємниці, обмежують права і свободи людини й громадянина в зазначеній сфері;
- ухвалення законодавчих актів, що визначають правовий статус органів, які забезпечують охорону державної таємниці;
- ратифікація міжнародних договорів про взаємний захист секретної інформації;
- визначення правопорушень у сфері охорони державної таємниці та встановлення відповідальності, яка настає за їх учинення (кримінальна, адміністративна, дисциплінарна);
- здійснення нагляду й контролю за забезпеченням охорони державної таємниці через спеціально утворені парламентські структури.

Президент України як глава держави відповідно до ст. 106 Конституції України та Закону України "Про державну таємницю":

- забезпечує національну безпеку України, здійснює керівництво у сферах національної безпеки й оборони;
- підписує закони, прийняті Верховною Радою України, та має право вето щодо них із подальшим поверненням на повторний розгляд;
- на основі та на виконання Конституції й законів України видає укази і розпорядження з питань охорони державної таємниці, які є обов'язковими до виконання на території України;
- утворює, реорганізовує та ліквідовує за поданням Прем'єр-міністра України міністерства й інші центральні органи виконавчої влади, діючи в межах коштів, передбачених на їх утримання;
- покладає виконання функцій державних експертів із питань таємниць на посадових осіб органів державної влади (ст. 9 Закону України "Про державну таємницю");
- може установлювати більш тривалі строки дії рішень державних експертів із питань таємниць про віднесення інформації до державної таємниці (ст. 13 Закону України "Про державну таємницю");
- дозволяє надавати доступ до державної таємниці іноземцям та особам без громадянства шляхом видання письмового розпорядження, а передавати секретну інформацію іноземній державі чи міжнародній організації – письмового мотивованого розпорядження з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України (ст. 27, 32 Закону України "Про державну таємницю");
- установлює порядок технічного й криптографічного захисту секретної інформації (ст. 35 Закону України "Про державну таємницю").

Координаційним органом із питань національної безпеки і оборони при Президентові України виступає Рада національної безпеки і оборони (РНБО України), яка координує і контролює діяльність органів виконавчої влади у сфері національної безпеки й оборони. Головою РНБО України є Президент України, який формує її персональний склад. До складу РНБО України за посадою входять Прем'єр-міністр України, Міністр оборони України, Голова Служби безпеки України, Міністр внутрішніх справ України, Міністр закордонних справ України. У засіданнях РНБО України може брати участь Голова Верховної Ради України. Рішення РНБО України уводяться в дію указами Президента України,

функції та повноваження – визначені в Законі України "Про Раду національної безпеки і оборони України". На РНБО України покладено такі функції:

- внесення пропозицій Президентові України щодо реалізації засад внутрішньої й зовнішньої політики у сфері національної безпеки та оборони;
- координація і здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки й оборони в мирний час.

Важливу роль у забезпеченні охорони державної таємниці відіграє вищий орган у системі виконавчої влади – Кабінет Міністрів України. Уряд України розробляє та вживає безпосередні заходи щодо охорони державної таємниці. До його повноважень відповідно до ст. 116 Конституції України та чинного законодавства належить:

- забезпечення реалізації державної політики щодо державної таємниці;
- забезпечення виконання законів України шляхом визначення порядку здійснення загальнодержавних заходів охорони державної таємниці;
- установлення порядку функціонування загальної системи охорони державної таємниці (визначення напрямів та форм взаємодії центральних органів виконавчої влади, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею, та органів Служби безпеки України).

Міністерство внутрішніх справ України бере участь у здійсненні заходів з організації охорони й оборони внутрішніми військами та Державною службою охорони МВС України (за договорами й згідно з переліком, затвердженим КМ України) об'єктів, діяльність яких пов'язана з державною таємницею. Підрозділи у справах громадянства, імміграції та реєстрації фізичних осіб органів внутрішніх справ беруть участь у визначенні фактичної обізнаності з відомостями, що становлять державну таємницю, осіб, які порушили клопотання про виїзд на постійне проживання за кордон.

Міністерство закордонних справ України задіяне в підготовці міжнародних договорів України про взаємну охорону (захист) секретної інформації, координує дії щодо розміщення дипломатичних представництв іноземних держав.

Міністерство юстиції України здійснює експертну оцінку та реєстрацію нормативно-правових актів із питань охорони державної таємниці.

Міністерство транспорту та зв'язку України проводить регулювання у сфері фельд'єгерського і спеціального поштового зв'язку.

Державна служба експортного контролю готує та узгоджує в установленому порядку пропозиції щодо надання суб'єктам зовнішньоекономічної діяльності України повноважень на право здійснення експорту, імпорту товарів військового призначення та товарів, котрі містять відомості, що становлять державну таємницю, веде облік суб'єктів зовнішньоекономічної діяльності України, яким надано такі повноваження, видає їм відповідні засвідчувальні документи, забезпечує контроль за використанням наданих повноважень, готує пропозиції щодо їх зупинення, скасування, готує та подає в установленому порядку матеріали про надання дозволів на передавання іншій державі інформації, що становить державну таємницю, та матеріальних носіїв цієї інформації, здійснює в межах своєї компетенції контроль за виконанням порядку оформлення дозволів на передавання іншій державі інформації, що становить державну таємницю, та матеріальних носіїв такої інформації.

Обов'язок центральних органів виконавчої влади – забезпечувати охорону державної таємниці – передбачено в Загальному положенні про міністерство, інший центральний орган державної виконавчої влади України. Визначені законодавством функції виконавчої влади у сфері охорони державної таємниці на місцевому територіальному рівні здійснюють державні адміністрації та місцеві (територіальні) органи (підрозділи) міністерств й інших центральних органів виконавчої влади. Для виконання указаних функцій в усіх обласних, Київській та Севастопольській міських державних адміністраціях відповідно до Примірного переліку управлінь, відділів та інших структурних підрозділів обласної державної адміністрації створюються самостійні структурні підрозділи (відділи) з питань режимно-секретної роботи.

У забезпеченні охорони державної таємниці беруть участь органи судової влади та прокуратура. Органи судової влади забезпечують охорону державної таємниці своїми специфічними засобами й методами, а саме:

- здійснюють правосуддя шляхом розгляду кримінальних справ, справ щодо спорів, котрі виникають із цивільних, трудових, адміністративно-правових відносин, справ про адміністративні правопорушення, пов'язані з державної таємницею;
- забезпечують охорону державної таємниці під час здійснення правосуддя при розгляді зазначених справ;

• здійснюють судовий захист прав і свобод громадян, інтересів органів державної влади, підприємств, установ, організацій у зв'язку з їх діяльністю щодо охорони державної таємниці України.

Органи прокуратури здійснюють нагляд за дотриманням Конституції та законів України у сфері забезпечення охорони державної таємниці всіма суб'єктами держави відповідно до своїх повноважень. Допуск та доступ посадових осіб, які здійснюють нагляд, до відомостей, що становлять державну таємницю, відбуваються згідно із Законом України "Про державну таємницю".

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в органах державної влади, місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на їхніх керівників. Із цією метою в таких структурах створюються на правах окремих підрозділів режимно-секретні органи (далі – РСО), основне завдання яких полягає в розробленні та здійсненні заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням.

До складу РСО входять підрозділи режиму, секретного діловодства та інші підрозділи, які безпосередньо забезпечують охорону державних таємниць, залежно від специфіки діяльності органу державної влади, місцевого самоврядування, підприємства, установи й організації. Передання функцій РСО будь-яким іншим підрозділам не допускається.

На сьогодні становлення ефективної державної влади є пріоритетним напрямом у загальній стратегії розвитку України; інформаційне забезпечення органів виконавчої влади є основою такого розвитку. Таємна інформація, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може зашкодити національній безпеці України, підлягає охороні державою. Особливості охорони державної таємниці розкриті в Постанові Кабінету Міністрів України "Про затвердження Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях" від 2.10.2003 року № 1561.

Запитання і завдання для самоперевірки

1. Проаналізуйте компетенцію Верховної Ради України у сфері охорони державної таємниці.
2. Розкрийте повноваження Президента України у сфері охорони державної таємниці.
3. Які повноваження РНБО України та Кабінету Міністрів України у сфері охорони державної таємниці?
4. Визначте повноваження центральних органів виконавчої влади у сфері охорони державної таємниці.
5. Яким чином забезпечують охорону державної таємниці органи судової влади та прокуратури?
6. Розкрийте систему нормативно-правових актів, що регулюють суспільні відносини у сфері охорони державної таємниці.
7. Розкрийте роль Служби безпеки України як спеціально уповноваженого органу державної влади у сфері забезпечення охорони державної таємниці.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про державну таємницю”.
2. Збірник нормативно-правових актів України у сфері охорони державної таємниці та конфіденційної інформації, що є власністю держави. – К. : Вид-во “НІКС”, 2007. – 460 с.
3. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12 серпня 2005 р. № 440, зареєстрований у Міністерстві юстиції України 17 серпня 2005 р. за № 902/11182 // Офіційний вісник України. – 2005. – № 34. – Ст. 2089.
4. Кодекс України про адміністративні правопорушення.
5. Кримінальний кодекс України.
6. Кримінально-процесуальний кодекс України.
7. Макаренко В.В. Адміністративна відповідальність за порушення законодавства про державну таємницю / В.В.Макаренко // Право України. – 2001. – № 2. – С. 114–118.
8. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. / А.Б.Стоцький, А.М.Гуз, А.І.Марущак та ін.; за заг. ред. В.С.Сідака. – К. : Вид-во Європейського ун-ту, 2006. – 232 с.
9. Постанова Кабінету Міністрів України “Про затвердження Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях” від 02.10.2003 року № 1561.

РОЗДІЛ 5

ОРГАНІЗАЦІЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ТА КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

5.1. ВИДИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ НА ПІДПРИЄМСТВІ

В умовах конкуренції між суб'єктами господарювання інформація стає цінним об'єктом, оскільки володіння нею в ринковій економіці необхідне для конкурентоспроможної господарської діяльності. Проведення економічної реформи в Україні й розвиток підприємництва привели до значного збільшення обсягів комерційної таємниці суб'єктів господарювання.

Унаслідок посилення економічної конкуренції в умовах розвитку ринкових відносин в Україні комерційна таємниця суб'єктів господарювання та її охорона набувають пріоритетного значення. Натомість якщо в країнах із розвиненою ринковою економікою комерційна таємниця захищається законодавством як цінний товар, то в Україні дотепер відсутній повноцінний правовий механізм захисту такої інформації.

Деякі консультативні організації пропонують структурувати інформацію суб'єктів господарювання з метою визначення режимів доступу до неї. Так, можна визначити, що інформацією про підприємство є сукупність відомостей, що закріплені в документах або на інших носіях та містять інформацію про будь-які події й факти, пов'язані з діяльністю відкритого акціонерного товариства (підприємства); підприємство здійснює свою діяльність на основі принципів прозорості й відкритості.

Інформація, що отримується, обробляється, зберігається, поширюється та використовується на підприємстві, є його власністю, якщо інше не передбачено чинним законодавством або договором. За режимом доступу інформація про підприємство поділяється на відкриту та з обмеженим доступом.

Відкриту інформацію становлять будь-які відомості про підприємство, які є у його володінні, користуванні або розпорядженні та не віднесені до категорії інформації з обмеженим доступом. Відкрита інформація вільно поширюється серед акціонерів та осіб, котрі не є учасниками.

Підприємство забезпечує доступ до відкритої інформації шляхом:

- публікації в офіційних друкованих виданнях;

- поширення через засоби комунікації;
- надання інформації на запит зацікавлених осіб (акціонерів та осіб, що не є учасниками).

Інформація з обмеженим доступом відповідно до “Положення про інформацію на підприємстві та порядок її надання” поділяється на конфіденційну й таємну (комерційну таємницю).

Конфіденційна інформація – це відомості технічного, фінансового та комерційного характеру, що перебувають у володінні, користуванні чи розпорядженні підприємства, не є загальнодоступними та поширення яких відбувається за бажанням підприємства відповідно до порядку, встановленого його внутрішніми документами. Перелік конфіденційних відомостей, а також перелік осіб, котрі мають доступ до конфіденційної інформації, встановлюється спостережною радою за поданням правління підприємства та зберігається в правлінні підприємства. Конфіденційна інформація надається за рішенням правління за умови письмового попередження таких осіб про обов’язок збереження конфіденційної інформації.

Посадові особи підприємства зобов’язані не допускати розголошення підприємствами, установами, організаціями – діловими партнерами підприємства, а також працівниками підприємства, особами, що закінчили трудові відносини з ним, та претендентами на роботу на підприємстві конфіденційної інформації, що стала їм відома під час переговорів, співбесід, сумісної діяльності.

Інформація, що є конфіденційною, надається на підставі чинного законодавства України, рішення органів управління підприємства чи запиту зацікавленої особи (заявника). Особа, котра її отримує, повинна підписати відповідне зобов’язання про нерозголошення конфіденційної інформації, яке засвідчується головою правління або уповноваженою ним посадовою особою та зберігається на підприємстві.

Надання конфіденційної інформації учасникам, їхнім представникам та передбаченим чинним законодавством державним органам, що контролюють діяльність підприємств, здійснюється безоплатно, з відшкодуванням витрат на виготовлення копій документів та пересилання їх поштою.

Інформація не вважається конфіденційною, якщо вона:

- є загальновідомою;
- стала загальновідомою не з вини особи, якій вона надана;
- стала відомою з будь-яких інших джерел до або після надання її особі;
- згідно з чинним законодавством не може бути віднесена до конфіден-

ційної.

Таємна інформація (комерційна таємниця) не підлягає наданню учасникам та особам, що не є учасниками, за винятком випадків, передбачених чинним законодавством України й рішеннями органів управління підприємства. Доступ до таємної інформації (комерційної таємниці) мають лише посадові особи та працівники підприємства, зазначені у відповідному переліку.

Порядок розроблення, зберігання, поширення, знищення та розмноження конфіденційної або таємної інформації регулюється спеціальними внутрішніми нормативними актами. Положенням про інформацію на підприємстві та порядок її надання також визначено, що посадові особи підприємства в межах наданої їм компетенції повинні забезпечувати своєчасну та якісну підготовку, публікування й надання інформації. Посадові особи несуть передбачену чинним законодавством відповідальність за повноту та достовірність поширюваної інформації.

Посадові особи, відповідальні за збереження інформації з обмеженим доступом, несуть матеріальну, дисциплінарну, адміністративну та кримінальну відповідальність за розголошення такої інформації, якщо воно сталося з їхньої вини й завдало матеріальної та іншої шкоди підприємству.

5.2. КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ ПРО ОСОБУ НА ПІДПРИЄМСТВІ

На сучасному етапі демократичних перетворень Україна визнає людину, її життя та здоров'я, честь і гідність, недоторканність та безпеку найвищою соціальною цінністю. При цьому стаття 21 Конституції визначає, що "усі люди є вільні і рівні у своїй гідності та правах. Права і свободи людини є невідчужуваними та непорушними".

Кожний має право на вільний розвиток своєї особистості, якщо при цьому не порушуються права і свободи інших людей; має обов'язки перед суспільством, у якому забезпечується вільний і всебічний розвиток особистості (стаття 23 Конституції України).

До конституційних основ правового статусу людини як учасника інформаційних відносин належить і стаття 34 Конституції України: "Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, захисту репутації або прав інших людей, запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету й неупередженості правосуддя.

Стаття 23 Закону України "Про інформацію" дає визначення поняття "інформація про особу" – це сукупність документованих або публічно оголошених відомостей про особу. Основними даними про особу (*персональними даними*) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Джерела документованої інформації про особу – видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого й регіонального самоврядування в межах своїх повноважень.

Обмеження доступу до інформації про особу здійснюється на підставі такої норми ст. 23 Закону України "Про інформацію": "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.

Конфіденційна інформація про особу є одним із специфічних видів інформації з обмеженим доступом. Її правовий статус визначається Законом України "Про інформацію", а офіційне тлумачення викладене у Рішенні Конституційного Суду України № 5-зп від 30 жовтня 1997 року (справа К.Г.Устименка). Зокрема зазначається, що 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.

До конфіденційної інформації про особу зокрема належать такі свідчення про неї:

- освіта;
- сімейний стан;
- релігійність;
- стан здоров'я;
- дата й місце народження;
- майновий стан;
- інші персональні дані.

Конституцією України встановлено головні засади механізму захисту особи від втручання в її особисте й сімейне життя, зокрема гарантовано таємницю

листування, телефонних розмов, телеграфної та іншої кореспонденції. Для іноземців та осіб без громадянства в Україні визначено національний режим захисту цих прав. Законодавство України містить також кримінально-правову заборону порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Цивільним кодексом України це право віднесено до особистих немайнових прав та передбачено судовий порядок його захисту від протиправних посягань; визначено право власності адресата на надіслані на його адресу листи, телеграми тощо. Хоча на їхню публікацію повинна дати згоду й особа, яка їх надіслала. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи. Визначено також, що кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи, якщо в ній містяться докази, що мають значення для вирішення справи. Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню.

Право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції може бути обмежено рішенням суду за наявності підстав, передбачених ст. 6 Закону України "Про оперативно-розшукову діяльність", із метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо. За забезпеченням законності цих обмежень здійснюється прокурорський нагляд. Законодавство зобов'язує операторів, провайдерів телекомунікацій уживати відповідно до законодавства технічних та організаційних заходів із захисту поштових відправлень, телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж і відомості, що передаються цими мережами.

Стан здоров'я особи також включено до переліку персональних даних, які підлягають захисту. Механізми правового захисту такої інформації встановлено ст. 286 Цивільного кодексу України. Фізична особа має право на таємницю про стан свого здоров'я, факт звернення по медичну допомогу, діагноз, а також про відомості, одержані при її медичному обстеженні. Чинним законодавством заборонено вимагати й надавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи. Фізична особа зобов'язана утримуватися від поширення такої інформації, яка стала їй відома у зв'язку з виконанням службових обов'язків або з інших джерел.

Офіційним тлумаченням окремих статей Закону України "Про інформацію" до основних персональних даних віднесено майновий стан особи. Таємність ін-

формації про майновий стан особи та факти розпорядження нею своїм майном захищена також інститутом таємниці вчинення нотаріальних дій. Так, за ст. 8 Закону України "Про нотаріат" нотаріуси, інші посадові особи, які вчиняють нотаріальні дії, та особи, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням службових обов'язків, зобов'язані додержуватися таємниці цих дій, у зв'язку із чим довідки про вчинені нотаріальні дії та документи видаються тільки громадянам і юридичним особам, за дорученням яких або щодо яких вчинялися нотаріальні дії.

Закон допускає видачу довідок про вчинювані нотаріальні дії на письмову вимогу компетентних державних органів у зв'язку з кримінальними, цивільними або господарськими справами, що перебувають у їхньому провадженні, чи в разі необхідності визначення правильності стягнення державного мита та цілей оподаткування.

Порушення права фізичної особи на конфіденційну інформацію може бути підставою для захисту такою особою своїх прав у судовому порядку. Такі судові розгляди, безумовно, становлять загрозу для діяльності суб'єкта господарювання. Розуміння вищим менеджментом і співробітниками безпекових підрозділів підприємства організаційно-правових нормативів стосовно конфіденційної інформації фізичної особи сприятиме нейтралізації подібних потенційних загроз.

5.3. РЕЖИМ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

У Стародавньому Римі діяв закон, що передбачав покарання у вигляді штрафу за примушування чужих рабів до видачі таємниць свого хазяїна. Традиція вести торговельні книги, таємниця яких була різновидом комерційної таємниці, побутувала ще в античному світі. Торговці й банкіри були зобов'язані вести такі книги, відображаючи в них свою діяльність. Дані торговельних книг були конфіденційними й розкривалися тільки для уточнення податків, у справах про спадкування майна, у випадках настання банкрутства або з метою правосуддя. Таким чином, держави ще на ранніх стадіях свого розвитку створювали закони, які захищали інтереси підприємств, їхніх засновників й учасників від можливого витоку секретів.

Історично комерційно важливу інформацію позначали різними термінами. У поняття "виробнича таємниця" включали внесення чого-небудь нового в процес створення благ; під "фабричною таємницею" розуміли як предмет патенту (першими увели Велика Британія, Франція й Німеччина), так і будь-яку особливість виробництва (еквівалент сучасного поняття "ноу-хау"); "торговельну таємницю" становили, наприклад, система місць реалізації товарів, списки постачальників і т. д.

Закони Російської імперії містили норми, що передбачали охорону фабричного секрету, торговельної таємниці й таємниці кредитних установ. Порушенням, пов'язаним із розголошенням таємниці, запобігали забороною службовцям оголошувати відомі їм таємниці підприємства, недопущенням сторонніх до торговельних книг та іншими заходами. Законодавство передбачало й застосування кримінальних покарань або стягнення збитків по цивільних позовах за подібні порушення.

Правове регулювання системи захисту виробничої й комерційної таємниці царської Росії було скасовано радянською владою в листопаді 1917 року. У СРСР на державному рівні комерційна таємниця довгий час не сприймалася як така і вважалася рудиментом капіталістичного ладу. Уперше про комерційну таємницю й право на її захист згадувалося в статті 33 Закону СРСР "Про підприємства в СРСР".

В умовах планової економіки протиправні посягання на економічну інформацію підприємств і організацій із боку вітчизняних суб'єктів підприємницької діяльності були виключені в силу їх безпідставності. Захист цієї інформації від посягань іноземних організацій цілком забезпечували вітчизняні спецслужби.

У 1990 році в СРСР була здійснена спроба визначення комерційної таємниці та відповідальності за її розголошення (ст. 33 Закону СРСР "Про підприємства"). Цей закон повинен був установити загальноправові, економічні та соціальні основи організації підприємств різних форм власності та їхньої діяльності в умовах "розвитку товарно-грошових відносин і регульованого ринку". При цьому комерційною таємницею визначались відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, які не є державними таємницями, розголошення (передавання, витік) яких може завдати шкоди його інтересам.

Із здобуттям Україною незалежності починає формуватися окремий правовий інститут комерційної таємниці. У останні роки зміни в політичному житті й економіці держави стали підґрунтям появи численних недержавних підприємств і організацій – самостійних суб'єктів господарювання. Їхній новий статус серед інших спричинив проблему захисту належної їм інформації економічного характеру з обмеженим доступом (комерційної, банківської таємниці та конфіденційної інформації).

Поряд із традиційними загрозами у сфері формування, зберігання й поширення інформаційних ресурсів зростає небезпека несанкціонованого втручання в роботу інформаційних систем із метою не тільки отримання закритої інформації, а й порушення її цілісності та знищення, дезорганізації інформаційної системи держави, суб'єктів підприємництва тощо. Реаліями сучасності стали "інформаційна експансія", "інформаційна зброя", "інформаційна війна". Все це вимагає не тільки застосування традиційних, перевірених на практиці заходів охорони інформаційних ресурсів, що містять відомості, віднесені до інформації з обмеженим доступом, а й розроблення та впровадження заходів і засобів правового, організаційного, інженерно-технічного й криптографічного захисту вказаної інформації.

Нині в Україні, як і в інших державах світу, у процесі підприємницької діяльності, при створенні нових технологій, у результаті інтелектуальної праці виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, що становлять комерційну цінність. Це можуть бути методики робіт, перспективні технічні рішення, результати маркетингових досліджень тощо, спрямовані на досягнення підприємницького успіху.

Проблема захисту комерційної таємниці має багато аспектів. Серед них найважливішими є визначення правового становища комерційної таємниці як соціального ресурсу, юридичне закріплення права на комерційну таємницю та створення правових гарантій реалізації цього права, регулювання відносин у сфері обігу комерційної таємниці.

У країнах, де використовуються інформаційні об'єкти, які становлять комерційну цінність, немає єдиного підходу до визначення поняття такої інформації (ділові секрети", "виробничі секрети", "торговельні секрети", "конфіденційна інформація", "комерційна таємниця" тощо).

Згідно із статтею 505 Цивільного кодексу України комерційною таємницею виступає інформація, секретна в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Згідно зі статтями 155 Господарського кодексу України та 420 Цивільного кодексу України комерційна таємниця виступає об'єктом прав інтелектуальної власності у сфері господарювання. Стаття 506 Цивільного кодексу України майновими правами інтелектуальної власності на комерційну таємницю визначає: право на використання комерційної таємниці; виключне право дозволяти використання комерційної таємниці; виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці; інші майнові права інтелектуальної власності, встановлені законом. Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною таємницею, якщо інше не встановлено договором.

Досягнення успіху в підприємницькій діяльності дуже часто пов'язане з використанням комерційної таємниці й неможливістю її застосування конкурентами. Виділяють такі причини неправомірного використання комерційної таємниці конкурентами:

- для поліпшення виробничої та комерційної діяльності організації (конкурента), що протиправно заволоділа комерційною таємницею, підвищення конкурентоспроможності продукції й ефективності виробництва, вибору оптимальної стратегії реалізації продукції та торгових переговорів;
- для завдання шкоди власнику комерційної таємниці, протидії реалізації продукції, руйнування виробничих та торгівельних зв'язків; зриву торгівельних переговорів й угод; зниження інвестиційних можливостей, підготовки та поширення неправдивих відомостей про власника комерційної таємниці тощо.

На сьогодні втратам комерційної таємниці в Україні сприяє безсистемність її захисту, роз'єднаність зусиль держави й приватних підприємців у забезпеченні

цілісності інформації, відсутність у власників комерційної таємниці організаційного досвіду щодо її захисту, недостатність правової підготовки та інформаційної культури. При застосуванні організаційно-правового механізму захисту комерційної таємниці виділяють низку невирішених питань, серед яких відсутність чіткого визначення поняття "комерційна таємниця" з урахуванням інтересів як юридичних, так і фізичних осіб; нерозроблення механізму здійснення прав власності на інформацію, віднесену до комерційної таємниці; методики визначення її вартості; невизначення органу державної виконавчої влади з формування й реалізації державної політики щодо охорони прав на комерційну таємницю тощо.

Стаття 155 Господарського кодексу України також частково визначає особливості комерційної таємниці, включаючи останню до об'єктів прав інтелектуальної власності. При цьому ст. 162 Господарського кодексу України установлює повноваження суб'єктів господарювання щодо комерційної таємниці. Зокрема "суб'єкт господарювання, що є володільцем технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів до охорони її конфіденційності".

Акцентуємо увагу на тому, що строк правової охорони комерційної таємниці обмежується часом дії сукупності зазначених вище умов.

Відповідно до Постанови Кабінету Міністрів України від 9.08.1993 р. № 611 комерційну таємницю не становлять:

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
- інформація за всіма установленими 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.

Підприємства зобов'язані надавати перелічені в зазначеній Постанові відомості органам державної виконавчої влади, контролюючим і правоохоронним структурам, іншим юридичним особам відповідно до чинного законодавства за їхньою вимогою.

Зважаючи на зазначені вище положення, цілком логічно буде виокремити такі правові ознаки комерційної таємниці:

- секретність інформації, яка виступає комерційною таємницею, полягає в тому, що вона є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить;
- інформація, яка визнається комерційною таємницею, має комерційну цінність, тобто певну цінову визначеність (вартість);
- комерційна таємниця – склад і обсяг відомостей, що визначені суб'єктом господарювання або уповноваженим на це органом;
- при визначенні складу й обсягу комерційної таємниці має враховуватись Постанова Кабінету Міністрів України від 9.08.1993 р. № 611 "Про перелік відомостей, що не становлять комерційної таємниці";
- володілець інформації повинен уживати належних заходів з охорони інформації, яка є комерційною таємницею;
- строк правової охорони комерційної таємниці обмежується часом дії сукупності факторів, коли така інформація має комерційну цінність, невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів щодо її схоронності.

Комерційна таємниця відповідно до ст. 30 Закону України "Про інформацію" належить до інформації з обмеженим доступом. Для того, щоб економічно важливі відомості мали статус саме комерційної таємниці, їх необхідно оформити відповідним чином. Наявність комерційної таємниці бажано обумовити в установчих документах підприємця, включивши, наприклад, в установчий договір й (або) статут підприємства розділ, що регламентує захист комерційної таємниці.

При формуванні переліку відомостей, що становлять комерційну таємницю підприємця, доцільно діяти в такий спосіб. Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві створюється спеціальна комісія, яка займається групуванням і уточненням інформації для цього переліку.

Чисельність такої комісії не повинна перевищувати чотирьох-п'яти осіб – найбільш кваліфікованих і компетентних фахівців основних підрозділів та представників служби безпеки підприємства, ознайомлених як із діяльністю підприємства в цілому, так і з роботою окремих підрозділів. До її складу бажано включити:

- фахівця, який володіє фінансовими питаннями, кон'юнктурою ринку та інформацією щодо діяльності конкуруючих фірм (як правило, це фінансовий менеджер);
- фахівця, який досконало знає систему організації роботи підприємства, її особливості;
- фахівця з питань зв'язків з іншими підприємствами, а також з укладення контрактів і договорів;
- фахівця, який володіє всіма відомостями про продукцію, що випускається, її технологічний цикл і виробництво, про проходження усіх видів інформації (усної, документальної, у вигляді зразків, вузлів, блоків, готової продукції).

Якщо підприємство досить велике або виготовлена продукція має різнорідний характер, можна створити кілька таких груп: одну – головну з метою координації та узагальнення результатів роботи, інші – залежно від необхідності по кожній ділянці. Утім, не виключено, що підприємство може складатися з кількох осіб, особливо на початкових етапах розвитку. Тоді це питання здатен вирішити один керівник за умови, що він буде володіти всією необхідною інформацією. Однак, щоб уникнути суб'єктивних помилок, краще розглядати ці питання щонайменше удвох.

Як уже було сказано, у групі повинні бути провідні фахівці, які володіють повним обсягом даних, що можуть бути віднесені до комерційної таємниці. Однак це не означає, що варто обов'язково ознайомлювати всіх залучених експертів із конкретною інформацією, яка може становити комерційну таємницю, якщо раніше вони її не знали. Здебільшого достатньо, щоб хоча б один із них був детально обізнаний із питанням, що розглядається, а інші мали про нього загальне уявлення. Такий підхід зробить роботу групи більш раціональною й виключить уже на першому етапі передумови до необґрунтованого поширення комерційної таємниці.

Насамперед із усього переліку інформації, з якою працює підприємець і яка циркулює на підприємстві, необхідно виключити відомості, що становлять державну таємницю (якщо суб'єкт господарювання з такою працює), а також ту інформацію, що не є комерційною таємницею відповідно до постанови КМУ від 9.08.1993 р. № 611.

Однозначно, до комерційної таємниці повинні бути віднесені різні види ноу-хау; відомості про винаходи й раціональні пропозиції, які не захищені авторським або патентним правом; інформація про факти укладання договорів і їхній зміст.

Отже, перед групою експертів необхідно поставити комплекс питань у такій послідовності:

а) виділити всі види діяльності підприємства, що приносять прибуток на цей момент;

б) на основі наявних даних про ринок збуту оцінити, чи перевищує рівень прибутку від цього виду діяльності аналогічні показники на інших підприємствах;

в) визначити ймовірну перспективу рентабельності цієї діяльності.

Якщо з економічної точки зору зазначений вид діяльності відповідає цілям підприємства і на цей момент, і в перспективі, а прибуток вищий, ніж у конкуруючих фірм, експерти повинні визначити, що саме такий вид діяльності дає змогу отримувати прибуток. Відповідь на це питання й буде комерційною таємницею підприємства.

Особливу увагу необхідно приділити розробленню положення про комерційну таємницю на підприємстві. Таке положення є основним у системі правового захисту інформації від несанкціонованого доступу. У ньому розкриваються загальні положення у сфері захисту інформації, принципи й процедури розмежування доступу до такої інформації, порядок прийому, реєстрації, інвентаризації та обліку носіїв інформації, що містить комерційну таємницю. У цьому положенні прописується також механізм забезпечення схоронності інформації, що є комерційною таємницею, зокрема деталізуються процедури забезпечення доступу до комерційної таємниці сторонніх осіб (включаючи перевірні органи). Рекомендується закріплювати правило, згідно з яким сторонні особи допускаються до ознайомлення з документами, що містять комерційну таємницю, з дозволу керівника за обов'язкової наявності письмового запиту. При цьому такі особи повинні видати розписку про нерозголошення комерційної таємниці або укласти угоду з підприємством про таке нерозголошення. У положенні рекоме-

ндується прописати порядок поширення комерційної таємниці, а також процедуру виключення інформації з переліку комерційної таємниці.

Аналіз чинного законодавства дає підстави стверджувати, що законодавець, визначаючи засоби захисту комерційної таємниці, застосовує два підходи:

1) абсолютного захисту, що захищає комерційну таємницю як об'єкт інтелектуальної власності від посягань будь-яких третіх осіб;

2) відносного захисту, що передбачає захист нелегкодоступної та незагальновідомої комерційної інформації, щодо якої вжито заходів збереження її таємності, від актів недобросовісної конкуренції.

Саме такою концепцією слід керуватися при побудові системи інформаційної безпеки на підприємстві. Хоча маємо доволі незвичний об'єкт захисту – об'єкт інтелектуальної власності з обмеженим доступом, неможливо не помітити переваг, зумовлених дуалістичною природою комерційної таємниці, а саме комплексності та всебічності її захисту, що випливає з такого:

- захист комерційної таємниці як інформації з обмеженим доступом забезпечується за допомогою встановлення й реалізації режиму таємності (ст. 30 Закону України "Про інформацію");
- захист комерційної таємниці як об'єкта інтелектуальної власності здійснюється судом із використанням спеціальних правових засобів, у тому числі оприлюднення в засобах масової інформації факту посягання на комерційну таємницю та розміщення в друкованому офіційному виданні відповідного судового рішення (ст. 432 ЦК України);
- різнорідність суб'єктів посягання на комерційну таємницю:

а) конкуренти підприємства – суб'єкта господарювання або особи, які їм допомагають (ст. 16 "Неправомірне збирання комерційної таємниці", ст. 18 "Схилення до розголошення комерційної таємниці", ст. 19 "Неправомірне використання комерційної таємниці" Закону України "Про захист від недобросовісної конкуренції", ч. 2, 4, 5 ст. 36 "Неправомірне збирання, розголошення та використання відомостей, що є комерційною таємницею" Господарського кодексу України, ч. 3 ст. 164-3 "Недобросовісна конкуренція" Кодексу України про адміністративні правопорушення, ст. 231 "Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю" Кримінального кодексу України);

б) особи, яким комерційна таємниця відома на законних підставах (ст. 17 "Розголошення комерційної таємниці", ч. 3 ст. 36 Господарського кодексу України,

ст. 232 “Розголошення комерційної або банківської таємниці” Кримінального кодексу України, ч. 3 ст. 164-3 “Недобросовісна конкуренція” Кодексу України про адміністративні правопорушення);

в) суб’єкти промислового шпигунства (ст. 231 “Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю” Кримінального кодексу України).

Очевидно, коли йдеться про працівників підприємства, то в більшості випадків ми маємо на увазі потенційних суб’єктів посягання, яких віднесено до другої групи. Умови, за яких працівник буде уважатися таким, якому комерційна таємниця відома на законних підставах, такі:

а) працівник є керівником підприємства або виконуючим обов’язки керівника підприємства. В такому разі йому на підставі статуту належить бути обізнаним в інформації з обмеженим доступом;

б) працівник створив на підставі трудового договору інформацію, яка є комерційною таємницею підприємства;

в) виконання трудових обов’язків працівника вимагає його обізнаності в інформації з обмеженим доступом (із певного питання, в частині або в цілому), тому його допущено до комерційної таємниці, про що є розпорядження керівника підприємства, а від працівника отримано зобов’язання про нерозголошення комерційної таємниці. Поряд із цим, не потрібно забувати, що працівник може стати потенційним конкурентом або вже бути таким унаслідок володіння корпоративними правами конкуруючого підприємства. Можлива також ситуація, коли працівник не має допуску до комерційної таємниці, але зацікавлений у тому, щоб отримати в будь-який спосіб таку інформацію.

У будь-якому випадку система захисту комерційної таємниці в трудових правовідносинах повинна бути спрямована на те, щоб:

1) працівники, яким довірено комерційну таємницю, не розголошували її третім особам;

2) працівники, яким не довірено комерційну таємницю, але відомо про її існування, не збирали її з метою неправомірного використання.

З огляду на зазначене, рекомендується включати норму про нерозголошення комерційної таємниці в трудовий договір (контракт) як керівника підприємства, так і інших співробітників.

На керівника організації повинні бути покладені обов’язки із забезпечення схоронності комерційної таємниці підприємця. У контракт керівника із власником

підприємства доцільно включити відповідні положення з цього питання. Зокрема необхідно зобов'язати керівника зберігати комерційну таємницю організації й не використовувати її для заняття будь-якою іншою діяльністю на шкоду підприємству. У контракті варто зазначити, що керівник організації несе персональну відповідальність за створення необхідних умов для забезпечення схоронності комерційної таємниці підприємства. Зрозуміло, що він, як і члени трудового колективу, повинен бути попереджений про відповідальність за порушення режиму комерційної таємниці й про те, що наслідками цього може бути настання передбаченої законом юридичної відповідальності й розірвання контракту.

Зобов'язання про нерозголошення інформації може бути оформлене як записом безпосередньо в тексті трудового договору (контракту), так і у вигляді окремого документа, що є додатком до трудового договору (контракту). Форма та зміст відповідного розділу трудового договору (контракту) або окремого додатка до нього в частині, що стосується збереження інформації, яка становить комерційну таємницю, мають велике значення. У випадку розголошення працівником інформації, що становить комерційну таємницю, ці документи становитимуть юридичну основу для притягнення такого працівника до відповідальності й відшкодування заподіяного збитку.

У договір (контракт) працівника, що допускається до комерційної таємниці підприємця, або в додаток до нього можуть бути включені такі зобов'язання:

- не розголошувати інформацію, що становить комерційну таємницю, яка буде йому довірена або стане відома по роботі;
- виконувати вимоги наказів, інструкцій і положень із забезпечення схоронності комерційної таємниці;
- зберігати інформацію, що становить комерційну таємницю тих підприємців, із якими є ділові відносини;
- не передавати третім особам і не розкривати привселюдно інформацію, яка становить комерційну таємницю, без згоди керівництва підприємства;
- у випадку спроби сторонніх осіб одержати від працівника інформацію, що становить комерційну таємницю підприємства, негайно сповістити про це відповідну посадову особу;
- не використовувати інформацію, що становить комерційну таємницю підприємства, для заняття іншою діяльністю, яка як конкурентна дія може завдати шкоди підприємству;
- негайно повідомляти відповідну посадову особу підприємства про

втрату або недостачу носіїв інформації, що становить комерційну таємницю, ключів від режимних приміщень, сховищ, сейфів, особистих печаток і про інші факти, які можуть призвести до розголошення комерційної таємниці, а також про причини й умови можливого витоку інформації, що становить комерційну таємницю підприємства;

- у випадку звільнення всі носії інформації, що становить комерційну таємницю, які перебували в розпорядженні працівника у зв'язку з виконанням ним службових обов'язків під час роботи на підприємстві, слід передати відповідній посадовій особі організації.

Сьогодні підприємницька діяльність має чимало прикладів, коли працівників поряд із підписанням додатків до договору (контракту) про нерозголошення й недопущення неправомірного використання комерційної таємниці змушують підписувати зобов'язання про відмову працювати після звільнення з підприємства на підприємствах-конкурентах протягом певного періоду. Така практика є неправомірною. Чинне законодавство України гарантує особі право на працю (ст. 43 Конституції України), що включає можливість заробляти собі на життя працею, яку вона вільно обирає або на яку вільно погоджується. Тому додатковий превентивний захист комерційної таємниці (власне її комерційної цінності) шляхом обмеження права працівника на працю вважаємо недоцільним. Якщо працівник неправомірно використає відомості, що становлять комерційну таємницю підприємства, навіть після звільнення з нього він нестиме відповідальність, у тому числі передбачену кримінальним законодавством.

Працівник під розписку повинен бути попереджений про відповідальність за невиконання взятих на себе зобов'язань. У трудовому договорі (контракті) або його невід'ємній частині (зобов'язанні про нерозголошення інформації, що становить комерційну таємницю) варто передбачити порядок ознайомлення працівника з чинними на підприємстві положеннями й інструкціями із забезпечення схоронності комерційної таємниці.

На підприємстві слід розробити спеціальний договір про збереження комерційної таємниці. Дотримання цієї рекомендації дасть змогу представникам підприємця почуватися впевнено при проведенні перевірок органами контролю. Перевіряльники повинні дотримуватися всіх процедур, які встановлені на підприємстві для одержання доступу до комерційної таємниці. Підписавши документ про нерозголошення комерційної таємниці, такі особи не мають права використати отриману інформацію у своїй діяльності без згоди керівництва підприємства.

Правила внутрішнього розпорядку й посадові інструкції осіб, котрі працюють із комерційною таємницею, а також інструкції про ведення переговорів, про роботу з документами теж повинні містити застереження про комерційну таємницю. Можливе й розроблення окремої інструкції з дотримання режиму нерозголошення комерційної таємниці співробітниками підприємця.

Комбінація зазначених вище документів, що закріплюють комерційну таємницю, може бути різною залежно від роду діяльності й характеру "таємності" підприємства.

Суб'єкт підприємницької діяльності (підприємець) як власник відомостей, що становлять комерційну таємницю, – це юридична особа, а також фізична особа – підприємець. Склад і обсяг відомостей, що становлять комерційну таємницю, порядок роботи з ними та їхнього захисту визначаються підприємцем самостійно. Він має право вибудовувати власну систему захисту комерційної таємниці. При цьому важливо, щоб відповідна інформація була невідомою й важкодоступною для сторонніх осіб.

Персонал підприємства має право користуватися відомостями, що становлять комерційну таємницю, для виконання своїх трудових обов'язків. Підприємець самостійно встановлює ступінь доступу кожного з працівників до такої інформації, скажімо, залежно від займаної посади й функціональних обов'язків; може моделювати категорії доступу до інформації: I категорія – для керівного складу, II – для менеджерів середнього рівня, III – для низової ланки працівників тощо.

Для того, щоб економічно цінні відомості становили саме комерційну таємницю, їх необхідно оформити відповідним чином.

Про існування комерційної таємниці бажано згадати в установчих документах, включивши, наприклад, в установчий договір і (або) статут підприємства розділ, що регламентує захист комерційної таємниці. Такий розділ сприятиме розподілу владних повноважень суб'єктів управління підприємства стосовно створення й затвердження переліку відомостей, що становлять його комерційну таємницю, та їхнього захисту.

Правила внутрішнього розпорядку й посадові інструкції осіб, котрі працюють із комерційною таємницею, а також інструкції про ведення переговорів, про роботу з документами теж повинні містити застереження про комерційну таємницю. Можливе й розроблення окремої інструкції з дотримання режиму нерозголошення (збереження та охорони) комерційної таємниці співробітниками.

Документальне забезпечення правового статусу комерційної таємниці на підприємстві сприятиме надійному її захисту як у випадку розголошення відповідних відомостей працівниками підприємства, так і в разі цілеспрямованих дій конкурентів щодо її викрадення. Проте чи не основним заходом запобігання витоку конфіденційної інформації через працівників фахівці уважають створення сприятливої атмосфери на підприємстві. Це пояснюється тим, що притягнути працівника до адміністративної чи кримінальної відповідальності за розголошування комерційної таємниці дуже складно. Однак якщо узяти всі доступні способи запобігання порушенням, виходить цілком ефективний комплекс заходів, продумана реалізація якого може стати надійним захистом від "розбазарювання" конфіденційної інформації працівниками підприємства.

Американський психолог А.Маслоу виокремив п'ять груп основних потреб індивіда: фізіологічні; у гарантуванні безпеки; спілкуванні й контактах з іншими людьми; суспільному визнанні своєї значущості (отриманні високого соціального статусу); самореалізації. Знаючи цей науково установлений факт, можна передбачити, що, забезпечивши на підприємстві умови для задоволення працівниками потреб у реалізації їхніх здібностей і потенціалу, в суспільному визнанні значущості їхніх успіхів, можна створити сприятливий соціально-психологічний клімат, знизити плинність кадрів, сформувати "фірмовий патріотизм".

Домогтися такої пропорції в колективі й таким чином мінімізувати витік конфіденційної інформації найлегше на підприємстві, де:

- створено дієву систему матеріальних стимулів;
- кожен працівник забезпечений довготривалою роботою;
- до підлеглих ставляться як до самостійних індивідів;
- є перспектива участі в прибутку підприємства;
- створено можливості для просування по службі;
- забезпечена участь усього персоналу у виробленні рішень.

Більшість дослідників визначають такі причини розголошування комерційних секретів:

1. Балакучість працівників, особливо пов'язана з уживанням алкоголю й спілкуванням у дружніх компаніях, – 32 %.

2. Прагнення працівників заробити гроші в будь-який спосіб (принцип "гроші не пахнуть") – 24 %.

3. Відсутність служби безпеки фірми – 14 %.

4. "Радянська" звичка персоналу ділитися досвідом, давати поради – 12 %.

5. Безконтрольне використання інформаційних і копіювальних засобів на фірмі – 10 %.

6. Психологічні конфлікти між працівниками, між працівниками й керівництвом – 8 %.

На сьогодні в менеджменті немає методів роботи з персоналом, які повністю виключали б можливість розголошування комерційної таємниці й конфіденційної інформації про компанію. Найефективніший превентивний захід, на думку фахівців, – це формувати відданий компанії колектив, оскільки збереження корпоративних таємниць ґрунтується виключно на високій лояльності працівників. Тому необхідно створити і впровадити прозору та зрозумілу персоналу програму мотивації, так званий соціальний пакет, та систему винагороди персоналу. Як показує досвід, чинниками, які сприяють формуванню відданості працівників, можуть бути: залежність заробітної плати від стажу роботи в компанії, можливість підвищення своєї кваліфікації, отримання позики на купівлю автомобіля чи нерухомості, медичне страхування та інші соціальні й матеріальні блага. Це стосується і планування кар'єри працівників: кожен має чітко розуміти перспективу свого зростання: пропрацювавши в компанії певний час і досягши високих результатів, він може розраховувати на просування по службі.

Важливо знати міру при визначенні адміністративних заходів із захисту комерційної таємниці. Особливо небезпечне впровадження режиму тотального контролю за діями працівників, аж до відстеження їхньої електронного листування і телефонних переговорів. Такий підхід врешті-решт призводить до численних конфліктів усередині підприємства, а іноді й до деградації та руйнування компанії. Треба бути обережним і вживаючи заходи щодо можливих порушників. Зазвичай до публічних розглядів справа не доходить – якщо людина відчуває себе винною, щоб уникнути розвитку конфлікту, вона зазвичай звільняється "за власним бажанням". Сама по собі підозра в розголошуванні працівником комерційної таємниці не може бути підставою для його звільнення і застосування до нього передбачених законодавством санкцій. Якщо ж звільнений з ініціативи компанії працівник уважатиме, що його звільнили необґрунтовано, він може оскаржити дії керівництва в суді, причому в цьому випадку ймовірність його відновлення на роботі й призначення йому компенсацій за незаконне звільнення буде доволі великою.

Таким чином, комбінація зазначених вище заходів і документів, що закріплюють комерційну таємницю, може бути різною залежно від виду діяльності й

характеру "таємності" підприємства. Тому пропонований алгоритм дій із збереження комерційної таємниці є модельним і може варіюватися.

Режим комерційної таємниці має будуватись на організаційно-правових засадах, визначених у юридичних документах підприємства. Важливо зазначити, що процес оформлення та реалізації режиму обмеженого доступу до комерційної таємниці має бути економічно та юридично обґрунтованим, відбуватись у декілька етапів, які логічно витікають один з одного.

Основними кроками оформлення правового режиму комерційної таємниці є:

- визначення відомостей, які будуть віднесені до комерційної таємниці;
- застосування технічних засобів захисту цих відомостей;
- визначення переліку посад, які мають повний та обмежений доступ до комерційної таємниці;
- організація роботи з документами, які містять комерційну таємницю;
- встановлення та реалізація відповідальності персоналу щодо дотримання режиму таємності комерційної таємниці;
- вжиття заходів захисту комерційної таємниці як об'єкта інтелектуальної власності (авторське право, патентування).

Необхідно зауважити, що чіткого нормативного регламентування процесу організації та реалізації режиму комерційної таємниці немає. Як уже зазначалось, є тільки імперативна вказівка на те, що комерційна таємниця має бути "предметом адекватних обставинам заходів збереження її секретності".

Порядок поширення інформації випливає з режиму й визначається її власником. Відповідно до ч. 4 ст. 14 Закону України "Про інформацію" поширення інформації – це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації. Керівник підприємства вирішує всі питання щодо поширення власними силами, оприлюднення через ЗМІ та реалізації права на розпорядження комерційною таємницею.

Способи розголошення відомостей, що становлять комерційну таємницю, можуть бути різними: повідомлення зазначених відомостей іншим особам, зокрема конкурентам; надання іншим особам для ознайомлення документів, що містять комерційну таємницю; повідомлення інформації, що є комерційною таємницею, в засобах масової інформації тощо.

Слід звернути увагу на те, що правові засади захисту комерційної таємниці від актів недобросовісної конкуренції передбачені ст. 36 ГК України та

деталізуються у ст. 16–19 Закону України "Про захист від недобросовісної конкуренції", де дається така кваліфікація:

1) неправомірне збирання комерційної таємниці (ст. 16);

2) розголошення комерційної таємниці (ст. 17);

3) схилення до розголошення комерційної таємниці (ст. 18);

4) неправомірне використання комерційної таємниці (ст. 19).

У цих нормативно-правових актах установлюються підстави для юридичної відповідальності особи, яка посягає на комерційну таємницю, а саме склад юридичного правопорушення. Юридична відповідальність є засобом захисту комерційної таємниці, який має каральний (адміністративна) чи компенсаційний (цивільно-правова) характер, але практика підказує, що такий підхід неефективний, оскільки засоби захисту комерційної таємниці підприємства мають виконувати превентивну функцію.

Юридичні особи, винні у скоєнні вказаних вище актів недобросовісної конкуренції, несуть відповідальність у вигляді штрафу в розмірі до двох тисяч неоподатковуваних мінімумів доходів громадян, який накладає на них Антимонопольний комітет України, його територіальні відділення (ст. 22 Закону). Громадяни, вину яких у вчиненні названих правопорушень доведено і які займаються підприємницькою діяльністю без створення юридичної особи, несуть також адміністративну відповідальність. Стягнення за вказані правопорушення визначені ч. 3 ст. 164-3 Кодексу України про адміністративні правопорушення: це штраф від п'яти до дев'яти неоподатковуваних мінімумів доходів громадян. Відповідно до ст. 23 Закону адміністративну відповідальність несуть також особи, які не є підприємцями і вчинили порушення комерційної таємниці в інтересах третіх осіб.

Крім того, Кримінальний кодекс України містить дві статті, які визначають кримінальну відповідальність за посягання на комерційну таємницю (ст. 231 "Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю" і ст. 232 "Розголошення комерційної або банківської таємниці").

Так, ст. 231 КК України умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей; а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, – караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян, або обмеженням волі на строк до п'яти років, або позбавленням волі

на строк до трьох років. Злочин, передбачений ст. 231 КК України, уважається закінченим із моменту вчинення дій, спрямованих на незаконне збирання відомостей, що містять комерційну таємницю. Тобто дії особи згідно з цією статтею уважаються злочинними ще задовго до того моменту, коли вона отримала відомості, що містять комерційну таємницю, оскільки склад злочину утворюють лише дії із збирання такої інформації.

У сучасній науковій літературі трапляється термін "промислове шпигунство". Шпигунство (економічне, промислове, комерційне, науково-технічне) означає активні дії, спрямовані на збирання або розкрадання цінної інформації, закритої для доступу сторонніх осіб (передача або збирання з метою передачі – ст. 114 КК України).

Відповідно до західної теорії промислове шпигунство – це добування законним і незаконним шляхом у конкуруючих фірм відомостей чи інформації у сфері наукових досліджень, виробництва продукції із застосуванням найбільш перспективних технологій, а також персональних даних із метою їх використання в конкурентній боротьбі або корисливих цілях.

Економічне шпигунство – ширше поняття, яке охоплює такі підвиди, як промислове, виробниче, науково-технічне, комерційне. Якщо таємницею володіє одна особа, це викликає інтерес до неї іншої особи, для задоволення якого чиняться дії, спрямовані на отримання нею певної матеріальної або іншої вигоди. Особа, котра бере участь у подібній діяльності, має загальновідому назву "шпигун". У підприємництві конкурентна боротьба неможлива без отримання інформації. Прагнення одержати відомості в умовах закритого до них доступу законним шляхом неминуче породжує недобросовісну конкуренцію, тобто об'єктивну потребу шпигувати за конкурентом. Без володіння інформацією про дії конкурента, передбачуваний попит на продукцію, перспективні наукові розробки важко, а інколи й неможливо бути конкурентоспроможним. Тому, з одного боку, підприємець змушений виступати захисником своїх таємниць (цінної інформації); з іншого – із метою конкуренції він має здобувати (красти, купувати) чужі захищувані секрети.

Умисне розголошення комерційної або банківської 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, карається штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян із поз-

бавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років, або позбавленням волі на той самий строк (ст. 232 КК України).

Слід звернути увагу, що за цією ж статтею відповідальність може нести лише обмежене коло осіб – суб'єкти, яким такі відомості стали відомі у зв'язку з їхньою професійною чи службовою діяльністю і які згідно з чинним законодавством повинні їх зберігати. До таких суб'єктів можуть належати працівники органів державної податкової служби, банків, правоохоронних структур, особи, яким комерційну таємницю було довірено її власником, та інші суб'єкти, які згідно з чинним законодавством мають право на ознайомлення з відомостями, що становлять комерційну таємницю, або мають доступ до таких відомостей по службі.

Із норм законів, які установлюють правовий статус, призначення та компетенцію державних органів, випливає, що в деяких із них діє прямо передбачене право державних органів на отримання інформації, що містить комерційну таємницю (наприклад, п. 17 ч. 1 ст. 11 Закону України "Про міліцію" від 20 грудня 1990 р. № 565-XII). Але більшість законів містять норми загального характеру, в яких передбачено право органів державної влади на отримання інформації та документів. При цьому не конкретизується, що така інформація підлягає розкриттю також у випадках, якщо вона містить комерційну таємницю.

Запитання і завдання для самоперевірки

1. Види інформації з обмеженим доступом на підприємстві.
2. Конфіденційна інформація на підприємстві.
3. Конфіденційна інформація про особу на підприємстві.
4. Суть і значення комерційної таємниці.
5. Правові аспекти комерційної таємниці.
6. Механізм створення переліку інформації, що становить комерційну таємницю.
7. Налагодження охорони комерційної таємниці.
8. Юридична відповідальність за розголошення комерційної таємниці.
9. Поняття промислового шпигунства.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бондарчук Ю.В. Безпека бізнесу: організаційно-правові основи : наук.-практ. посіб. / Ю.В.Бондарчук, А.І.Марущак. – К. : Вид. дім "Скіф", 2008. – 369 с.

2. Господарський кодекс України № 436-IV від 16.01.2003 р.

3. Гуз А. Как защитить коммерческую тайну / А.Гуз, А.Марущак // В мире спецслужб. – К., 2006. – № 1.

4. Економічна безпека підприємств, організацій, установ : навч. посіб. / В.Л.Ортинський, І.С.Керницький, З.Б.Живко та ін. – К. : Правова єдність, 2009. – 544 с.

5. Закон СРСР "Про підприємства".

6. Закон України "Про захист від недобросовісної конкуренції" // Відомості Верховної Ради України. – 1996. – № 36. – Ст. 164.

7. Закон України "Про інформацію" // Відомості Верховної Ради України. – 1992. – № 48, № 650.

8. Закон України "Про захист від економічної конкуренції" // Відомості Верховної Ради України. – 2001. – № 12. – Ст. 64.

9. Клименко П.М. Інформація як об'єкт інтелектуальної власності, що потребує охорони / П.М.Клименко // Недержавна система безпеки підприємництва як суб'єкт національної безпеки України : зб. матер. наук.-практ. конф., Київ, 16 – 17 травня 2001 року. – К. : Вид-во Європ. ун-ту, 2003. – С. 283–289.

10. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. із змінами від 8 грудня 2004 р. : офіц. вид. – К. : Вид. дім "Ін Юре", 2006.

11. Кримінальний кодекс України від 01.09.2001 р.

12. Марущак А.І. Правові основи захисту інформації з обмеженим доступом : навч. посіб. / А.І.Марущак. – К. : Наук.-вид. відділ НА СБ України, 2007. – 245 с.

13. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. / [за заг. ред. В.С.Сідака]. – К. : Вид-во Європейського ун-ту, 2006. – 232 с.

14. Ткачук И.Б. Коммерческая тайна: организация защиты, расследование посягательств / И.Б.Ткачук. – М. : Изд-во "Щит-М", 2000. – 168 с.

15. Цивільний кодекс України № 435-IV від 16.01.2003 р.

РОЗДІЛ 6

ПРАВОВІ ЗАСОБИ ОХОРОНИ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

6.1. ЗМІСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК ОБ'ЄКТА ОХОРОНИ ТА ПЕРЕЛІК ПРАВОВИХ МЕХАНІЗМІВ ЇХНЬОГО ЗАХИСТУ

Правову основу функціонування персональних даних як виду інформації з обмеженим закріплено статтею 32 Конституції України наступним чином: "Ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених Конституцією України. 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". Для контролю за цим процесом кожному громадянину гарантовано Конституцією право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації визнано ст.182 Кримінального кодексу України злочином.

Право особи на обмеження доступу до своїх персональних даних задекларовано і на міжнародному рівні, зокрема у ратифікованій Україною у 1997 році Конвенції про захист прав і основних свобод людини 1950 року. Статтею 8 названої Конвенції закріплено, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Таким чином, право людини на недоторканість приватного життя передбачає правовий захист відомостей про неї, при якому об'єктом правовідносин є дані про особу або персональні дані.

Законом України «Про захист персональних даних» закріплено визначення персональних даних як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Цим же законом всім персональним даним, крім знеособлених надано статус інформації з обме-

женим доступом». Аналогічне визначення персональних даних як «будь-якої інформації, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною» закріплено у ст. 2 ратифікованої Україною Конвенції Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” (відома як Конвенція № 108, згідно з порядком нумерації Європейських договорів).

Законом України «Про захист персональних даних» також дещо звужено розуміння персональних даних як об’єкта захисту для фізичних осіб, які претендують зайняти чи займають виборну посаду (у представницьких органах) або посаду державного службовця першої категорії, вивівши їх персональні дані із класу інформації з обмеженим доступом, за винятком інформації, яка визначена такою відповідно до закону.

Безсумнівно таке широке визначення персональних даних як об’єкта охорони повинно сприяти досягненню цілей цих нормативних актів, які покликані гарантувати захист персональних даних під час їх обробки, що здійснюється не власниками цієї інформації, а іншими особами, які несуть зобов’язання щодо захисту наданої їм інформації.

Крім такої узагальненої характеристики змісту персональних даних Законом України «Про інформацію» виділено перелік основних даних про особу, які ототожнено з терміном «персональні дані», це національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Цим же законом встановлено заборону на збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом. Проте названий закон не називає цю інформацію конфіденційною, а наділяючи фізичних осіб правом на конфіденційну інформацію, Закон веде мову про право власника інформації «професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаної на власні кошти, або такої, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці», самостійно визначати режим доступу до неї, включаючи належність її до категорії конфіденційної. Здійсненим у 1997 році Конституційним Судом України офіційним тлумаченням названих положень Закону України «Про інформацію» встановлено перелік персональних даних як основної інформації про особу, ці дані оголошено «конфіденційною інформацією про особу», закріплено заборону не тільки на збирання, а і на зберігання, використання та поширення цих даних та доповнено їх перелік майновим станом із «розкриттям» цього переліку доповненням «та інші персональні дані».

При цьому варто зазначити, що персональні дані будучи за своєю природою конфіденційною інформацією, у разі їх переходу у користування визначених законодавством осіб можуть набувати статусу таємної інформації.

Взагалі інформація про особу має унікальну властивість перебувати у режимах охорони різних видів таємної інформації, зокрема таких її видів як: та-

ємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, банківська таємниця, адвокатська таємниця, лікарська таємниця, таємниця усиновлення, таємниця страхування, таємниця голосування, таємниця нотаріальних дій.

Персональні дані можуть належати і до державної таємниці, на що натякає офіційне тлумачення закону України «Про інформацію», стверджуючи що дійсно за законом кожна особа дійсно має право на ознайомлення із інформацією зібраною про неї, але якщо така інформація не становить державної таємниці.

Як бачимо, правовий статус персональних даних і спосіб їх захисту залежить від виду правовідносин у які вони потрапляють. Якщо інформація здобута оперативним шляхом - це державна таємниця, якщо цю саму інформацію про особу отримав адвокат - це адвокатська таємниця, якщо її отримав лікар - то це лікарська таємниця. А з самої своєї появи ці ж персональні дані одночасно могли отримати статус таємниці усиновлення.

Виходячи із наведених положень робимо висновок, що чинним законодавством фізичним особам надано право на обмеження доступу до всієї інформації, яка їх стосується, що підкріплено статтею 63 Конституції України, якою фізичних осіб звільнено від відповідальності за відмову давати показання або пояснення щодо себе. Необхідність надання у розпорядження інших суб'єктів такої інформації пов'язана із вступом фізичних осіб у різні види правовідносин. Так для здійснення багатьох видів правочинів фізична особа зобов'язана надати паспортні дані (здійснення правочинів, що підлягають нотаріальному посвідченню), дані про стан здоров'я (донорство крові) або дані щодо майнового стану (отримання субсидій при оплаті комунальних послуг) чи освітнього рівня (вступ до вищих навчальних закладів). Питання в тому, щоб отримуючи, використовуючи чи зберігаючи дані про фізичних осіб усі уповноважені суб'єкти усвідомлювали обов'язок і мали можливості належним чином захищати цю інформацію від несанкціонованого доступу.

6.2. ПОРЯДОК ФУНКЦІОНУВАННЯ БАЗ ПЕРСОНАЛЬНИХ ДАНИХ

Частково це питання вирішено шляхом правового регулювання створення та функціонування баз персональних даних, яке закріплено у 2010 році Законом України «Про захист персональних даних» та ратифікованою Україною Конвенцією Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" (відома як Конвенція № 108, згідно порядку нумерації Європейських договорів).

Відповідно до названого закону мета обробки персональних даних у базах має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця бази персональних даних, та відповідати законодавству про захист персональних даних. Склад та зміст персональних даних у базі визначаються умовами згоди суб'єкта персональних даних або відповідно до закону і мають бути відповідними та не надмірними стосовно визначеної мети їх обробки.

Законом заборонено обробку даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Статтею 9 Конвенції Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" також допускаються обмеження у правах фізичних осіб, якщо це стосується державної чи суспільної безпеки, фінансової стабільності, боротьби зі злочинністю, захисту прав та законних інтересів інших осіб.

Законом «Про захист персональних даних» забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя.

Ця заборона не застосовується, якщо обробка персональних даних:

- здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних чи стосується даних, які були оприлюднені суб'єктом персональних даних;
- необхідна для здійснення прав та виконання обов'язків у сфері трудових правовідносин відповідно до закону;
- необхідна для захисту інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;
- здійснюється релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;
- необхідна для обґрунтування, задоволення або захисту правової вимоги;
- необхідна в цілях охорони здоров'я, для забезпечення піклування чи лікування за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних;
- стосується обвинувачень у вчиненні злочинів, вироків суду, здійснення державним органом повноважень, визначених законом, щодо виконан-

ня завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом.

передачі персональних даних за запитами Фізичній особі як суб'єкту персональних даних законом «Про захист персональних даних» надано право:

- знати про місцезнаходження бази персональних даних, яка містить його персональні дані, її призначення та найменування, місцезнаходження та / або місце проживання (перебування) володільця чи розпорядника цієї бази або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані, що містяться у відповідній базі персональних даних;
- на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних;
- отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також отримувати зміст його персональних даних, які зберігаються;
- пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних органами державної влади, органами місцевого самоврядування при здійсненні їхніх повноважень, передбачених законом;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником цієї бази, якщо ці дані обробляються незаконно чи є недостовірними;
- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- звертатися з питань захисту своїх прав щодо персональних даних до органів державної влади, органів місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних;
- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних

Про передачу персональних даних третій особі володілець бази персональних даних протягом десяти робочих днів зобов'язаний повідомити суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом.

Повідомлення, не здійснюються у разі:

- при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;
- виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;
- здійснення обробки персональних даних в історичних, статистичних чи наукових цілях (у таких випадках відповідно до цього ж закону обробка даних допускається лише у знеособленому виді).

Статтею 12 Конвенції Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" закріплено, що транскордонні потоки даних мають здійснюватися за умов забезпечення захисту персональних даних. Допускається обмеження цієї вимоги у разі, коли національне законодавство передбачає особливий порядок упорядкування суспільних інформаційних відносин та визначення окремих видів персональних даних у зв'язку із специфічністю деяких відомостей, крім випадків, коли законодавство іншої держави – члена має аналогічний ступінь захисту.

6.3. ПЕРЕЛІК ТА ОСНОВНИЙ ЗМІСТ ІНСТИТУТІВ ІНФОРМАЦІЙНОГО ПРАВА, ЯКІ ЗАДІЯНІ В ЗАХИСТІ ПЕРСОНАЛЬНИХ ДАНИХ

Тепер звернемось до порядку захисту персональних даних в режимах таємної інформації. Конституцією України гарантовано таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Відповідно до Закону України „Про правовий статус іноземців" для іноземців та осіб без громадянства в Україні встановлено національний режим захисту цих прав. Статтею 146 Кримінального кодексу України встановлена також кримінально-правова заборона порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Цивільним Кодексом України це право віднесено до особистих немайнових прав та передбачено судовий порядок його захисту від протиправних посягань. Цим кодексом також визначено право власності адресата на надіслані на його адресу листи, телеграми тощо. Проте на їх публікацію повинна дати згоду і особа, яка їх надіслала. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи. Визначено також, що кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи лише у разі, якщо в ній містяться докази, що мають значення для вирішення справи. Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню.

Право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції може бути обмежено рішенням суду за наявності підстав, передбачених ст.6 Закону України "Про оперативно-розшукову діяльність" з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної

справи, якщо іншими способами одержати інформацію неможливо. За забезпеченням законності цих обмежень згідно з Законом України “Про прокуратуру” здійснюється прокурорський нагляд. Законодавство також зобов’язує операторів, провайдерів телекомунікацій вживати відповідно до законодавства технічних та організаційних заходів із захисту поштових відправлень, телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Стан здоров’я особи також включено до переліку персональних даних, які підлягають захисту. Механізми правового захисту такої інформації встановлено ст. 286 Цивільного кодексу України та «Основами законодавства України про охорону здоров'я». Фізична особа має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні. Чинним законодавством заборонено вимагати та подавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи. Службові особи зобов'язані утримуватися від поширення цієї інформації, яка стала їй відома у зв'язку з виконанням службових обов'язків або з інших джерел.

Відповідно до «Основ законодавства України про охорону здоров'я» 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.

Проте саму особу зобов’язують під час медичного обстеження, що проводиться перед даванням крові повідомити відповідну посадову особу установи чи закладу охорони здоров'я відомі їй дані про перенесені та наявні в неї захворювання, а також про вживання нею наркотичних речовин та властиві їй інші форми ризикованої поведінки, що можуть сприяти зараженню донора інфекційними хворобами, які передаються через кров, і за наявності яких виконання донорської функції може бути обмежено. Згідно з законом України „Про донорство крові та її компонентів” зазначена інформація засвідчується особистими підписами особи, яка виявила бажання здати кров або її компоненти, та посадової особи установи чи закладу охорони здоров'я і становить лікарську таємницю. Відповідно до закону України „Про трансплантацію органів та інших анатомічних матеріалів людині” захисту підлягають також дані про реципієнтів донорських органів, а також про осіб, які заявили про свою згоду або незгоду стати донорами у разі смерті. Такі дані також віднесені чинним законодавством до лікарської таємниці.

Медична інформація, тобто свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для

життя і здоров'я, за своїм правовим режимом належить до конфіденційної, тобто інформації з обмеженим доступом. Лікар зобов'язаний на вимогу пацієнта, членів його сім'ї або законних представників надати їм таку інформацію повністю і в доступній формі.

В особливих випадках, як і передбачає частина третя статті 39 Основ законодавства України про охорону здоров'я, коли повна інформація може завдати шкоди здоров'ю пацієнта, лікар може її обмежити. У цьому разі він інформує членів сім'ї або законного представника пацієнта, враховуючи особисті інтереси хворого. Таким же чином лікар діє, коли пацієнт перебуває у непритомному стані.

У випадках відмови у наданні або навмисного приховування медичної інформації від пацієнта, членів його сім'ї або законного представника згідно з офіційним тлумаченням відповідних положень закону України «Про інформацію» вони можуть оскаржити дії чи бездіяльність лікаря безпосередньо до суду або, за власним вибором, до медичного закладу чи органу охорони здоров'я.

Коло осіб, яким у силу виконання службових обов’язків стають відомі факти особистого життя людини не обмежується лікарями. До них також належать адвокати, яким особи довіряють таку інформацію у зв’язку із необхідністю отримання правової допомоги. Адвокат зобов'язаний зберігати адвокатську таємницю. Відповідно до закону України „Про адвокатуру” **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.

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. Забороняється будь-яке втручання в адвокатську діяльність, вимагання від адвоката, його помічника, посадових осіб і технічних працівників адвокатських об'єднань відомостей, що становлять адвокатську таємницю. З цих питань вони не можуть бути допитані як свідки.

Документи, пов'язані з виконанням адвокатом доручення, не підлягають оглядові, розголошенню чи вилученню без його згоди. Забороняється прослуховування телефонних розмов адвокатів у зв'язку з оперативно-розшуковою діяльністю без санкції Генерального прокурора України, його заступників, прокурорів Республіки Крим, області, міста Києва.

У нормативно затвердженому тексті присяги адвоката є зобов’язання суворо зберігати адвокатську таємницю. За порушення присяги адвокат рішенням дисциплінарної палати кваліфікаційно-дисциплінарної комісії до адвоката можуть бути застосовані такі дисциплінарні стягнення:

- попередження;
- зупинення дії свідоцтва про право на заняття адвокатською діяльністю на строк до одного року;

- анулювання свідоцтва про право на заняття адвокатською діяльністю.

Крім того, статтею 397 Кримінального кодексу України встановлено кримінально-правову заборону на вчинення в будь-якій формі перешкод до здійснення правомірної діяльності захисника чи представника особи по наданню правової допомоги або порушення встановлених законом гарантій їх діяльності та професійної таємниці.

Офіційним тлумаченням окремих статей закону України "Про інформацію" до основних персональних даних віднесено **майновий стан особи**. Захист цієї інформації зокрема забезпечено інститутом банківської таємниці. Відповідно до ст. 1076 Цивільного кодексу України банки зобов'язані гарантувати таємницю банківського рахунку, операцій за рахунком і відомостей про клієнта. Детальний перелік відомостей, що відносяться до банківської таємниці наведено у ст.60 Закону України „Про банки і банківську діяльність". Зокрема до банківської таємниці відносять відомості про стан рахунків клієнтів, їх фінансово-економічний стан, у тому числі щодо операцій, які були проведені на користь чи за дорученням клієнта а також здійснені клієнтом угоди.

Інформація щодо фізичних осіб, яка містить банківську таємницю, розкривається банками лише на письмовий запит або з письмового дозволу власника такої інформації або на письмову вимогу суду чи за рішенням суду. Інші органи державної влади можуть отримати доступ до рахунків фізичної особи лише у тому випадку, коли вона зареєстрована підприємцем.

У разі розголошення банком відомостей, що становлять банківську таємницю, клієнт має право вимагати від банку відшкодування завданих збитків та моральної шкоди.

Відповідно до закону України „Про страхування" не підлягає також розголошенню конфіденційна інформація щодо діяльності та фінансового стану страхувальника - клієнта страховика, яка стала відомою йому під час взаємовідносин з клієнтом чи з третіми особами при провадженні діяльності у сфері страхування, розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Таку інформацію законом визнано таємницею страхування і вона надається страховиком лише на письмовий запит або з письмового дозволу власника такої інформації, за рішенням суду чи на запит органів досудового слідства у разі порушення кримінальної справи щодо клієнта страхувальника.

Таємність інформації про майновий стан особи та факти розпорядження нею своїм майном захищені також інститутом таємниці вчинення нотаріальних дій. Так ст.8 Закону України „Про нотаріат" нотаріуси, інші посадові особи, які вчиняють нотаріальні дії, та особи, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків, зобов'язані додержувати таємниці цих дій у зв'язку із чим довідки про вчинені нотаріальні дії та документи видаються тільки громадянам та юридичним особам, за дорученням яких або щодо яких вчинялися нотаріальні дії.

Названий закон допускає видачу довідок про вчинювані нотаріальні дії на письмову вимогу компетентних державних органів у зв'язку з кримінальними, цивільними або господарськими справами, що знаходяться у їх провадженні чи у зв’язку із необхідністю визначення правильності стягнення державного мита та цілей оподаткування.

Законом України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» також передбачено заходи щодо забезпечення нерозголошення даних про майновий стан особи. Так органи державної реєстрації зобов’язані забезпечувати захист інформації названого державного реєстру від несанкціонованого доступу. Законом також обмежено коло осіб, які мають право отримувати витяги з Державного реєстру прав на нерухоме майно. Такі документи видаються лише:

- власнику (власникам) нерухомого майна або їх уповноваженим особам;
- спадкоємцям (правонаступникам - для юридичних осіб) або їх уповноваженим особам;
- особам, в інтересах яких встановлено обтяження, або їх уповноваженим особам.

Інформаційну довідку з Державного реєстру прав на підставі письмового запиту мають також право отримувати суд, органи місцевого самоврядування, органи внутрішніх справ, органи прокуратури, органи державної податкової служби, органи Служби безпеки України та інші органи державної влади (посадові особи), якщо запит зроблено у зв'язку із здійсненням ними повноважень, визначених законом.

Аналогічні вимоги законодавства щодо забезпечення захисту баз персональних даних та розмежування доступу до них стосуються Державного реєстру виборців. Щодо Державного реєстру фізичних осіб-платників податків законом лише визнано відомості цього реєстру інформацією з обмеженим доступом, яку слід охороняти відповідно до чинного законодавства.

До інформації персонального характеру захистом якої уповноважені займатися державні органи відносять і **дані щодо всиновлення**. Так відповідно до ст.228 Сімейного кодексу України особи, яким у зв'язку з виконанням службових обов'язків доступна інформація щодо усиновлення (перебування осіб, які бажають усиновити дитину, на обліку, пошук ними дитини для усиновлення, подання заяви про усиновлення, розгляд справи про усиновлення, здійснення нагляду за дотриманням прав усиновленої дитини тощо), зобов'язані не розголошувати її, зокрема і тоді, коли усиновлення для самої дитини не є таємним. Відомості про усиновлення видаються судом лише за згодою усиновлювача, крім випадків, коли такі відомості потрібні правоохоронним органам, суду у зв'язку з цивільною чи кримінальною справою, яка є у їх провадженні. За розголошення таємниці усиновлення (удочеріння) всупереч волі усиновителя (удочерителя) статтею 168 Кримінального кодексу України передбачена кримінальна відповідальність. Задля забезпечення таємниці усиновлення ст.ст. 10, 265-4

ЦПК України дозволено закритий судовий розгляд цивільних справ за мотивованою ухвалою суду.

Конституцією України гарантовано свободу волевиявлення громадян у ході виборів до органів державної влади та органів місцевого самоврядування, референдумів та реалізації інших форм безпосередньої демократії. Для забезпечення цієї свободи законодавством України передбачено таємну форму голосування на виборах Президента України, народних депутатів України, депутатів органів місцевого самоврядування та у ході голосування на всеукраїнських та місцевих референдумах. Забезпечення свободи волевиявлення громадян доповнено кримінально-правовою забороною на умисне порушення таємниці голосування під час проведення передбачених законом України виборів, вчинене членом виборчої комісії або іншою службовою особою з використанням влади чи службового становища.

Розглядаючи механізми захисту персональних даних варто зауважити, що право особи на конфіденційність даних про себе є конкурентним із правом громадськості на доступ до інформації, яка є необхідною для забезпечення розвитку і безпеки суспільства. У зв'язку із цим окремі правозахисники та представники ЗМІ гостро критикували позиції національного законодавства зокрема зміст ст.182 Кримінального кодексу України, якою, на їх думку обмежено журналістську діяльність та зведено нанівець так звану „концепцію публічних осіб, обсяг конфіденційної інформації про яких має бути значно більш відкритим для громадськості, ніж про приватних осіб" та ставлять журналіста в положення, коли він „за результатами кожної своєї публікації поставати перед судом і відбиватися, посилаючись на те, що конфіденційна інформація зібрана й опублікована в інтересах, приміром, національної безпеки". З приводу таких закидів керівництвом Генеральної Прокуратури України у засобах масової інформації було надано роз'яснення, що ст.132 Кримінального кодексу України є лише логічним продовженням ст. 32 Конституції України, що має силу прямої дії. Вона змушує працівників ЗМІ і редакції більш виважено підходити до справі, щоб у результаті журналістських розслідувань не порушувались нічиї права й інтереси. При вирішенні питання про відповідальність у кожному конкретному випадку буде встановлюватися - чи законно збирався матеріал, чи йшла мова про конфіденційність, чи мала відношення інформація до приватного життя, чи була згода на її публікацію. Більше того, ст. 37 Закону України „Про телебачення і радіомовлення" на телерадіоорганізації покладено обов'язок не розголошувати інформацію про приватне життя громадянина без його згоди, за умови якщо ця інформація не є суспільно необхідною. Проте ні названим, ні іншими нормативними актами не визначено механізму віднесення інформації до суспільно необхідної. Крім цього, варто зауважити, що обмеження щодо збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не перешкоджає „четвертій владі" виконувати свій обов'язок із підтри-

мання демократичних засад функціонування держави, бо ці обмеження не стосуються інформації про діяльність посадових осіб та державних органів.

ЗАПИТАННЯ І ЗАВДАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Розкрийте зміст поняття "персональні дані".
2. В статусі яких видів інформації з обмеженим доступом можуть перебувати персональні дані?
3. Якими правами володіє фізична особа у зв'язку із обробкою її персональних даних?
4. Які підстави обмеження прав особи на конфіденційність її персональних даних?
5. Розкрийте зміст механізмів захисту інформації про стан здоров'я особи.
6. Розкрийте зміст механізмів захисту інформації щодо майнового стану особи.
7. Порядок задоволення запитів органів державної влади про отримання персональних даних.
8. Який порядок використання засобами масової інформації персональних даних?

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України // Відомості Верховної Ради України, 1996 р., N 30, ст. 141.
2. Конвенція Ради Європи "Про захист прав людини та основних свобод" (Рим, 04.09.1950 р.) та Протокол № 11 // Голос України. – 2001. – № 3 (2503). – С. 6–8.
3. Цивільний Кодекс України // Офіційний Вісник України 2003, N 11, ст. 461.
4. Кримінальний кодекс України // Офіційний Вісник України 2001, N 21, ст. 920.
5. Закон України "Про прокуратуру" // Відомості Верховної Ради України, 1991 р., N 53, ст. 793.
6. Закон України „Про адвокатуру" // Відомості Верховної Ради України 1993, N9 від 02.03.1993р.
7. Закон України „Про банки і банківську діяльність» від 07.12.2000р. // Офіційний Вісник України 2001,1-2 (частина 1) від 26.01.2001р.
8. Закон України „Про всеукраїнський та місцеві референдуми" // Відомості Верховної Ради України, 1991 р., N 33, ст. 443.
9. Закон України „Про донорство крові та її компонентів" від 23.06.95р.// Відомості Верховної Ради України, 1995 р., N 23, ст. 183.
10. Закон України „Про захист персональних даних» // Офіційний вісник України від 09.07.2010 - 2010 р., № 49, стор. 199, стаття 1604
11. Закон України „Про нотаріат" від 2.09.1993р. // Відомості Верховної Ради України 1993, N39 від 28.09.1993р.

12. Закон України „Про поштовий зв'язок” від 04.10.2001р. // Офіційний Вісник України 2001, N 43, ст. 1918.

13. Закон України „Про правовий статус іноземців” від 4.02.94р. // Відомості Верховної Ради України 1994, N23 від 07.06.94р.

14. Закон України „Про страхування” // Відомості Верховної Ради України, 1996 р., N 18, ст. 78

15. Закон України „Про телебачення і радіомовлення” // Відомості Верховної Ради України 1994, N10 від 09.03.94р.

16. Закон України „Про телекомунікації” від 18.11.2003р. // Офіційний Вісник України 2003, N 51, ст. 2644

17. Закон України „Про трансплантацію органів та інших анатомічних матеріалів людині” від16.07.99р.

18. Закон України «Про Державний реєстр виборців» від 21.09.2010р. // Голос України 2010, N 186 (4936) від 6.10.2010р.

19. Закон України «Про Державний реєстр фізичних осіб-платників податків та інших обов'язкових платежів» від 22.12.94 р. // Відомості Верховної Ради України, 1995 р., N 2, ст. 10

20. Основи законодавства України про охорону здоров'я від 19.11.92р. // Відомості Верховної Ради України 1993, N4 від 26.01.1993р.

21. Закон України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» від 11.02.2010 р. // Офіційний Вісник України 2010, 19 від 26.03.2010, ст. 823

22. Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» // Офіційний вісник України від 09.08.2010 - 2010 р., № 58, стор. 46, стаття 1994, код акту 52188/2010

23. 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) від 30.10.97р. // Офіційний Вісник України 1997,46 від 24.11.97р.

24. Інструкція про порядок вчинення нотаріальних дій нотаріусами України: затв. Наказом Міністерства Юстиції України від 03.03.2004 р. N 20/5 // Офіційний Вісник України, N 10, ст. 639.

25. Захаров Є. Без права на інформацію // Дзеркало тижня, 2003, № 30 (455).

26. Примаченко О. СБУ захищає права людини громадяни — опираються // Дзеркало тижня, 2003, № 26 (451).

27. Журналистские расследования вымрут как мамонты // Еженедельник 2000, 14.03.2002р. http://www.2000.net.ua/politic/ukraine/7026.html.

РОЗДІЛ 7

ФОРМУВАННЯ ТА ЕКСПЛУАТАЦІЯ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

7.1. ОСНОВНІ ПОЛОЖЕННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Еволюційний перехід суспільства від постіндустріальної до інформаційної фази розвитку зумовив широке впровадження інформаційних технологій в усі сфери життєдіяльності особи, суспільства та держави. Водночас, прогрес науки й техніки привів до розроблення методів та створення компактних і високоефективних технічних засобів, за допомогою яких можна легко отримати можливість несанкціонованого ознайомлення з інформацією.

Тому в загальному комплексі заходів щодо забезпечення національної безпеки держави важлива роль належить заходам, пов’язаним із безпосереднім захистом інформації від загроз, реалізація яких може завдати особі, суспільству, державі політичних, економічних, фінансових та інших збитків.

Серед загроз інформації за небезпечністю наслідків особливе місце посідає здобування технічними розвідками відомостей у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

Незважаючи на позитивні зміни в міжнародній обстановці стосовно України, діяльність технічних розвідок іноземних держав із здобування інформації триває. Проти України безперервно ведеться розвідка багатофункціональними космічними, повітряними, наземними, морськими системами та комплексами технічної розвідки. Провідні країни світу продовжують модернізувати свої розвідувальні служби, вдосконалюють технічну розвідку, нарощують її можливості.

Технічна розвідка сьогодні дає змогу забезпечити безперервне спостереження практично за всією територією України. У подальшому засоби технічної розвідки, зокрема космічної компоненти, будуть мати виключно високі характеристики.

Активізувалися несанкціоновані дії щодо інформації, яка обробляється та циркулює в інформаційних і телекомунікаційних системах, а також спеціальний вплив на інформацію з метою її спотворення, руйнування, знищення, порушення нормального функціонування систем оброблення інформації.

В умовах недостатньої номенклатури вітчизняних засобів оброблення інформації та програмного забезпечення в інформаційно-телекомунікаційних системах широко використовуються продукти іноземного виробництва, які здебільшого не мають об'єктивних оцінок механізмів захисту й створюють передумови упровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій. Останнє зумовило широке розгортання інформаційно-телекомунікаційних систем, різке зростання обсягів інформації, яка обробляється, зберігається в цих системах, значне збільшення кола користувачів, які мають безпосередній доступ до інформаційних ресурсів тощо.

При цьому за відсутності конкурентоспроможних вітчизняних зразків перевага надається інформаційним технологіям та технічним засобам оброблення інформації іноземного виробництва, які здебільшого не забезпечують захист інформації, а також створюють передумови неконтрольованого використання спеціальних програмних й апаратних засобів ("закладних пристроїв").

У світі зберігається тенденція зростання масштабів комп'ютерної злочинності, розповсюдження комп'ютерних вірусів, насамперед із використанням інтернету; істотно підвищується небезпека наслідків неправомірних дій, технічних і технологічних помилок та збоїв при застосуванні інформаційно-телекомунікаційних систем, що особливо актуально в умовах глобалізації вітчизняних інформаційно-телекомунікаційних систем.

Сусідні держави реалізують концепції "інформаційного протиборства" та "інформаційного впливу", які полягають у здійсненні заходів із спеціального впливу на інформаційну інфраструктуру з метою ураження (знищення) інформаційних ресурсів та руйнування системи управління у сферах оборони, економіки, безпеки, фінансів і т. ін.

Відбувається також витік інформації з обмеженим доступом технічними каналами внаслідок побічних електромагнітних випромінювань і наведень, здійснення акустичної та оптико-електронної розвідки в безпосередній близькості від об'єкта інформаційної діяльності.

У процесі інформаційної діяльності для зберігання, оброблення та передавання інформації, в тому числі з обмеженим доступом, широко використовуються технічні засоби різного призначення (обчислювальна, оргтехніка, засоби зв'язку, автоматизовані системи тощо). На об'єктах інформаційної діяльності обговорюються службові питання за різними напрямами діяльності установи і може озвучуватися інформація з обмеженим доступом. Певні фізичні процеси, що відбуваються в технічних засобах та під час обговорення інформації, інші фактори створюють об'єктивні передумови для появи технічних каналів витоку інформації, що зумовлює необхідність реалізації заходів зі створення комплексів (систем) технічного захисту інформації, спрямованих на запобігання витоку інформації цими каналами.

Розвиток співробітництва із закордонними державами в політичній, військовій, економічній та інших сферах приводить до активного відкриття в Україні іноземних дипломатичних, комерційних установ та представництв, розташування яких в безпосередній близькості від державних органів та установ створює передумови для добування технічними засобами розвідки інформації з обмеженим доступом, яка циркулює на об'єктах інформаційної діяльності, що є особливо актуальним внаслідок широкого використання незахищених імпортних технічних засобів оброблення інформації.

Всі ці фактори значно підвищують уразливість інформації, отже, визначають необхідність здійснення державою відповідних заходів. При цьому небезпека негативних наслідків реалізації загроз інформації, насамперед з обмеженим доступом, для національної безпеки зумовлює загальнодержавну важливість заходів попередження таких загроз, а також необхідність переходу від фрагментарного відомчого до комплексного підходу у формуванні й реалізації заходів із забезпечення технічного захисту інформації, залучення належного кадрового потенціалу, акумулювання необхідних ресурсів для вирішення проблеми захисту інформації.

У загальному випадку під захистом інформації розуміють сукупність технічних засобів, організаційних заходів та правових норм для уникнення завдання збитків інтересам власника інформації. При цьому використання засобів захисту інформації спрямовується на:

- запобігання знищенню або спотворенню інформації;
- унеможливлення несанкціонованого доступу до інформації;
- унеможливлення несанкціонованої модифікації інформації;
- зниження рівня електромагнітного випромінювання тощо.

Технічний захист інформації (ТЗІ) – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну й іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Для протидії зазначеним вище загрозам у державі створена, функціонує та розвивається *система технічного захисту інформації*, яка є сукупністю організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правовою та матеріально-технічною базою. Відповідно до Концепції технічного захисту інформації в Україні технічний захист інформації визначено складовою забезпечення національної безпеки України.

Метою *державної політики у сфері технічного захисту інформації* є створення правових, організаційних, економічних засад функціонування системи технічного захисту інформації.

Державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз інформації та здійснюється в напрямах нормативно-правового й організаційного забезпечення, науково-технічної та виробничої діяльності. Важливість для безпеки держави галузі ТЗІ, її наукоємність вимагає концентрації відповідних зусиль науково-технічного та виробничого потенціалу міністерств, інших органів виконавчої влади, наукових установ.

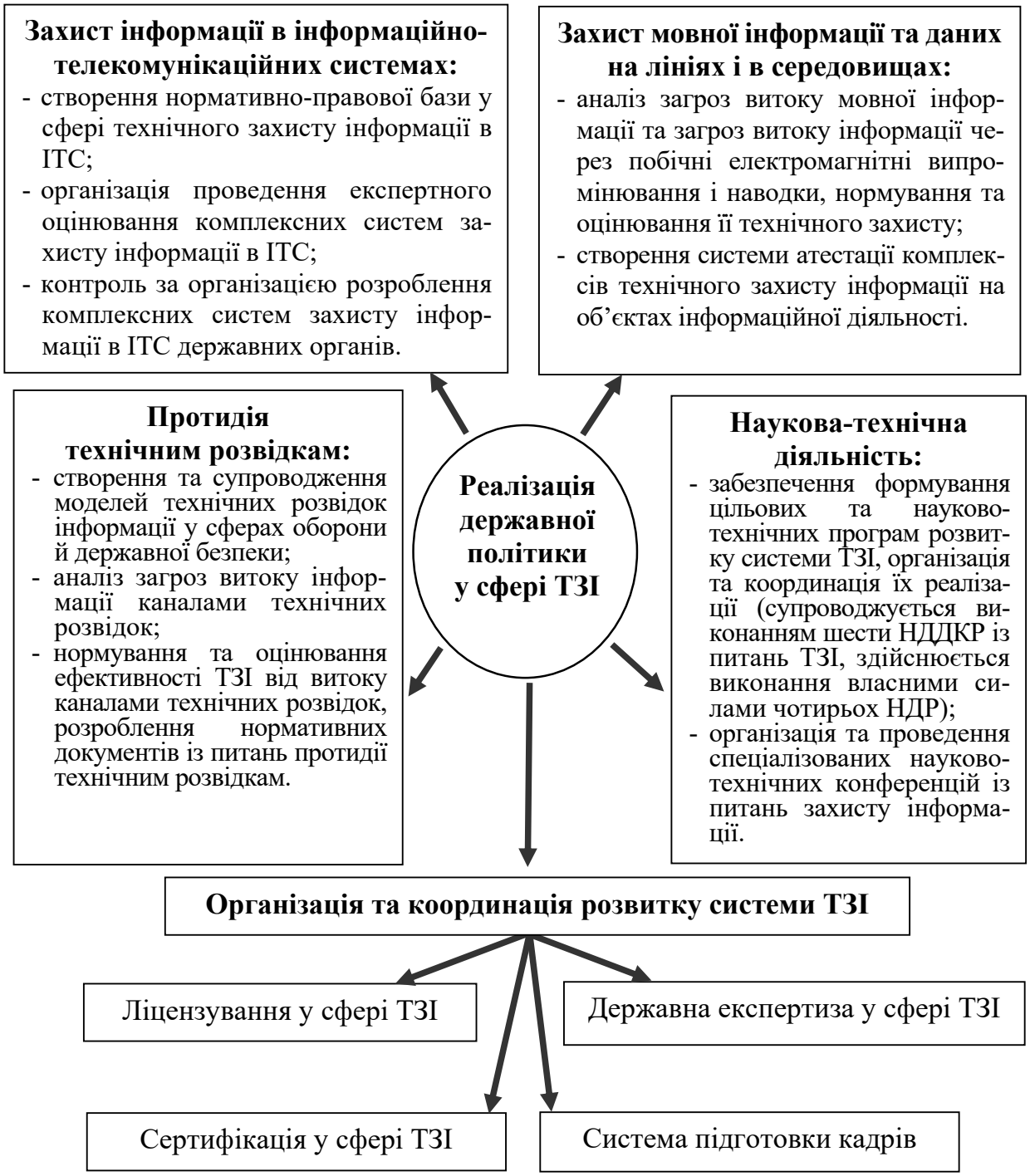

Рис. 7.1. Побудова й організаційна структура системи ТЗІ в Україні

Основними напрямами державної політики у сфері ТЗІ є:

1) нормативно-правове забезпечення:

• удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну й іншу передбачену законом таємницю, конфіденційної інформації, що належить державі;

• розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;

• удосконалення правових механізмів організаційного забезпечення технічного захисту інформації;

• удосконалення нормативно-правових актів щодо умов і правил проведення діяльності у сфері ТЗІ;

• розроблення нормативно-правових актів щодо визначення статусу головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій;

• удосконалення нормативно-правових актів щодо здійснення контролю за імпортом із метою впровадження в Україні іноземних інформаційних технологій захисту інформації та засобів забезпечення ТЗІ;

• розроблення нормативних документів із питань формування та розвитку моделі загроз інформації;

• розроблення нормативних документів із питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об’єктів, робота яких пов’язана з інформацією, що підлягає технічному захисту;

• удосконалення чинних та розроблення нових нормативних документів із питань ТЗІ в засобах обчислювальної техніки, автоматизованих системах, оргтехніці, мережах зв’язку, комп’ютерних мережах та приміщеннях, де циркулює інформація, що підлягає технічному захисту; під час створення, експлуатації та утилізації зразків озброєнь, військової й спеціальної техніки; проектування, будівництва і реконструкції військово-промислових, екологічно небезпечних та інших особливо важливих об’єктів;

2) організаційне забезпечення:

• забезпечення створення підрозділів ТЗІ в органах державної влади та місцевого самоврядування, академіях наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях усіх форм власності, діяльність яких пов’язана з інформацією, що підлягає технічному захисту;

• створення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ;

• підготовка кадрів для роботи у сфері ТЗІ;

• залучення до розв'язання проблем ТЗІ вітчизняних учених і висококваліфікованих спеціалістів;

• розвиток міжнародного співробітництва у сфері ТЗІ.

3) науково-технічна та виробнича діяльність:

• моніторинг і оцінка стану ТЗІ, підготовка аналітичних матеріалів та пропозицій щодо стратегії його розвитку;

• створення інформаційно-аналітичних моделей загроз інформації та методології їх прогнозування;

• обґрунтування критеріїв і показників рівнів ТЗІ;

• створення методології синтезу систем багаторівневого захисту інформації, адекватних масштабам загроз безпеці інформації та режиму доступу до неї;

• створення методології для визначення зниження ефективності продукції, зумовленого витоком інформації про неї, порушенням її цілісності чи блокуванням, та методології обґрунтування заходів ТЗІ;

• системне й поетапне розроблення сучасних засобів забезпечення технічного захисту інформації;

• пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ;

• створення умов для забезпечення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ науковим, контрольно-вимірювальним, випробувальним та виробничим обладнанням.

Першочерговими заходами реалізації державної політики у сфері ТЗІ є:

• створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

• визначення перспективних напрямів розроблення нормативних документів із питань ТЗІ на основі аналізу стану вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;

• визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку,

призначених для оброблення інформації з обмеженим доступом; інших засобів забезпечення ТЗІ в органах державної влади та місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ;

- налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;
- завершення створення та розвиток системи сертифікації вітчизняних і закордонних засобів забезпечення ТЗІ;
- визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців із питань ТЗІ.

Значущість забезпечення ТЗІ, його наукоємність вимагає концентрації зусиль науково-технічного та виробничого потенціалу міністерств, інших центральних органів виконавчої влади й наукових установ. Відповідно до цього визначено основні принципи й концептуальні засади організації забезпечення ТЗІ в Україні:

- додержання балансу інтересів особи, суспільства та держави, їхня взаємна відповідальність;
- єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;
- комплексність, повнота й безперервність заходів ТЗІ;
- гармонізація нормативно-правових актів та нормативних документів щодо ТЗІ з відповідними міжнародними договорами України й міжнародними стандартами;
- обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади, інших державних органах та органах місцевого самоврядування, у допоміжних органах і службах Президента України, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях;

- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту інформації, що є їхньою власністю, та відкритої інформації, важливої для особи й суспільства, якщо остання циркулює за межами державних організацій;
- покладання відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;
- ієрархічність побудови організаційної структури системи ТЗІ, суб'єкти якої належать до сфери управління або підпорядковані відповідній державній організації, керівництво діяльністю цих суб'єктів у межах повноважень, наданих нормативно-правовими актами;
- методичне керівництво спеціально уповноваженого центрального органу виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи технічного захисту інформації;
- фінансова забезпеченість системи ТЗІ за рахунок державного бюджету, бюджету Автономної Республіки Крим, місцевих бюджетів та інших джерел.

Організаційна структура системи ТЗІ має ієрархічну деревовидну будову з підлеглістю і підзвітністю від низу до верху по вертикалі та незалежністю суб'єктів одного рівня ієрархії.

Суб'єктами системи технічного захисту інформації є:

- Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку);
- органи, щодо яких здійснюється ТЗІ;
- державні наукові, науково-дослідні та науково-виробничі підприємства, установи й організації, що належать до системи Служби безпеки України і виконують завдання технічного захисту інформації;
- військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність із технічного захисту інформації за відповідними дозволами або ліцензіями;
- навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців із технічного захисту інформації.

До об'єктів, де здійснюються заходи ТЗІ, відносять:

- будівлі, споруди, приміщення, транспортні засоби, де відбувається діяльність, пов'язана з інформацією, що підлягає захисту, об'єкти спеціального зв'язку;

- інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, в яких здійснюється оброблення інформації, що підлягає захисту, системи спеціального зв'язку.

На відомчому рівні заходи із забезпечення ТЗІ здійснюють безпосередньо суб'єкти системи ТЗІ – міністерства й інші органи державної влади та підпорядковані їм підприємства, установи й організації, а відповідальність за організацію і стан захисту інформації покладається на їхніх керівників. Вони мають створювати або визначати підрозділи для оцінювання стану загроз інформації, розроблення та реалізації планів заходів щодо її захисту, координації діяльності інших суб'єктів у сфері підпорядкування, здійснення розрахунків потрібних для цього коштів.

На сьогодні нормативно-правовими актами повністю визначена правова основа функціонування всіх елементів організаційної структури системи технічного захисту інформації, завдання та функції суб'єктів ТЗІ, їхні права й обов'язки, порядок їх взаємодії і проведення ними діяльності, а також порядок функціонування таких основних елементів, як системи ліцензування та оцінювання продукції, підготовки й перепідготовки кадрів.

Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

- забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів із питань ТЗІ;
- підготовка в межах своїх повноважень нормативно-правових актів із зазначених питань;
- здійснення контролю за станом технічного захисту інформації.

Органи, щодо яких здійснюється ТЗІ, відповідно до покладених на них завдань:

- створюють або визначають підрозділи, на які покладається забезпечення технічного захисту інформації та контроль за його станом, узгоджують основні завдання й функції цих підрозділів;
- видають за погодженням із Держспецзв'язку та впроваджують нормативно-правові акти з питань технічного захисту інформації;
- погоджують із Держспецзв'язку проведення підприємствами, установами, організаціями здійснюваних за рахунок коштів державного бюджету науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток нормативно-правової та матеріально-технічної бази системи технічного захисту інформації;

- створюють або визначають за погодженням із Держспецзв'язку підприємства, установи та організації, які забезпечують технічний захист інформації;
- забезпечують підготовку, перепідготовку й підвищення кваліфікації кадрів із технічного захисту інформації;
- надають Держспецзв'язку за його запитами відомості про стан технічного захисту інформації.

Основними завданнями інших суб'єктів системи технічного захисту інформації є:

- дослідження загроз інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні;
- створення засобів забезпечення технічного захисту інформації;
- розроблення, впровадження, супроводження комплексів технічного захисту інформації;
- підвищення кваліфікації фахівців із технічного захисту інформації.

Одним із важливих напрямів технічного захисту інформації виступає протидія технічним розвідкам. Організація протидії, своєчасне розроблення та впровадження необхідних заходів покладається на керівника органу державної влади, органу місцевого самоврядування, органу управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України; підприємств, установ, організацій. Проведення заходів протидії покладається на створений або визначений наказом керівника органу (організації) штатний чи позаштатний підрозділ ТЗІ або призначену особу.

Протидія технічним розвідкам (ПДТР) є невід'ємною складовою систем охорони державної таємниці та захисту інформації з обмеженим доступом, яка є власністю держави (ІОДД), і проводиться шляхом упровадження заходів щодо запобігання порушенню конфіденційності ІОДД засобами технічної розвідки. Сукупність упроваджуваних організаційних й інженерно-технічних заходів, програмних і технічних засобів, які використовуються для забезпечення протидії, є частиною комплексу ТЗІ, спрямованого на приховування ІОДД та дезінформування технічних розвідок.

7.2. ЛІЦЕНЗУВАННЯ ДІЯЛЬНОСТІ В ГАЛУЗІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Один із суттєвих важелів регулювання діяльності у сфері ТЗІ – процедура ліцензування діяльності суб'єктів господарської діяльності. Механізм ліцензування діяльності у сфері ТЗІ діє в Україні з 1995 року. Метою провадження ліцензування є формування в Україні контрольованого ринку послуг із ТЗІ, виконання вимог нормативних документів із питань захисту інформації, розповсюдження систем і засобів технічного захисту інформації, що відповідають законодавству України, а також виключення:

- передумов застосування засобів ТЗІ в протизаконних та злочинних діях унаслідок їх неконтрольованого обігу в країні;
- можливості компрометації інформації з обмеженим доступом через надання некваліфікованих послуг та використання неякісних засобів ТЗІ, що може призвести до реальних загроз безпеці особи, суспільства та держави;
- розповсюдження засобів ТЗІ, що не відповідають вимогам нормативних документів, чи засобів низької якості, зокрема іноземного виробництва, що може призвести до знищення вітчизняної галузі розроблення та виробництва надійних, конкурентоспроможних засобів ТЗІ.

Таким чином, крім безпосередньо регулятивних і контрольних функцій, ліцензування діяльності спрямоване на розвиток матеріально-технічної бази системи технічного захисту інформації.

Усього в галузі ТЗІ підлягає ліцензуванню сім видів робіт, а саме:

- розроблення, упровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля, надання консультативних послуг;
- розроблення, упровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали, надання консультативних послуг;
- розроблення, виробництво, упровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інфор-

маційних системах, інформаційних технологій із захисту інформації від несанкціонованого доступу, надання консультативних послуг;

- виявлення та блокування витоку мовної й видової інформації через закладні пристрої на об'єктах інформаційної діяльності, надання консультативних послуг;
- виробництво засобів забезпечення технічного захисту інформації, носіями якої є акустичні поля;
- виробництво засобів забезпечення технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали;
- розроблення, упровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої виступають хімічні речовини, надання консультативних послуг.

У зв'язку з тим, що органи державної влади та місцевого самоврядування не є суб'єктами господарювання й не можуть отримувати ліцензії, для них визначено порядок одержання дозволів на проведення робіт із технічного захисту інформації для власних потреб. Держспецзв'язку надає органам державної влади й місцевого самоврядування такі дозволи, здійснює контроль за проведенням ними визначених видів робіт.

Система оцінювання продукції у сфері ТЗІ включає дві процедури – сертифікацію засобів ТЗІ та державну експертизу.

7.3. СЕРТИФІКАЦІЯ ЗАСОБІВ ТА ДЕРЖАВНА ЕКСПЕРТИЗА У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Об'єктом сертифікації є засоби ТЗІ, які можуть вироблятися як одиничні зразки, так і серійно. Сертифікації можуть підлягати й засоби імпортного виробництва. Процедура призначена надавати споживачу гарантії відповідності цих засобів нормативним документам після проведення певних організаційно-технічних заходів. Результатом сертифікаційних робіт є спеціальний документ установленого зразка – сертифікат відповідності.

Створення системи сертифікації засобів ТЗІ в Україні було розпочато ще в середині 90-х років XX ст. Раніше ні в СРСР, ні в Україні така сертифікація не проводилася, до того ж на той час бракувало необхідної для досягнення цієї мети нормативно-правової та матеріально-технічної бази.

Із березня 1999 року система сертифікації засобів ТЗІ почала функціонувати відповідно до Порядку проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення, який обов'язковий як для акредитованих у системі органів із сертифікації засобів ТЗІ та випробувальних лабораторій, так і для підприємств, установ й організацій, у тому числі іноземних, які виготовляють і (або) постачають засоби ТЗІ в державні й недержавні установи, де циркулює інформація, що підлягає захисту згідно із законодавством.

На сьогодні в нашій державі сертифікацію засобів ТЗІ здійснюють акредитовані в Українській державній системі сертифікації продукції (УкрСЕПРО) органи та випробувальні лабораторії. Зараз діють два такі органи й дві випробувальні лабораторії. За період функціонування системи сертифікації видано 94 сертифікати відповідності на 93 види засобів ТЗІ.

Уведення процедури експертного оцінювання комплексних систем захисту інформації в ІТС, технічних і програмно-апаратних засобів захисту інформації зумовлено логічною складністю сучасних програмно-апаратних комплексів, а також суттєвим впливом на безпеку інформації конкретних умов експлуатації ІТС. Іншими словами, такі об'єкти не повторюють один одного й кожний із них має тільки йому притаманні особливості. У випадках оцінювання програмно-апаратних засобів закордонного виробництва, як правило, відсутня необхідна для їхньої сертифікації технічна документація; практично неможлива оцінка умов виробництва, організація взаємодії органів сертифікації із закордонними виробниками засобів захисту.

Правову основу цієї процедури становить Закон України "Про наукову та науково-технічну експертизу", методологічну – експертиза технічних рішень і організаційних заходів, які базуються як на узагальненні висновків окремих експертів, так і на результатах інструментальних вимірювань та випробувань комплексу програмно-апаратних і технічних засобів захисту інформації.

Порядок проведення державної експертизи у сфері ТЗІ, основні функції й права її суб'єктів визначено "Положенням про державну експертизу у сфері технічного захисту інформації". Відповідно до законодавства у ньому визначено суб'єктів експертизи (замовник, організатор експертизи, експерт), основні функції ДСТСЗІ СБ України та суб'єктів експертизи, порядок їхньої взаємодії, документального оформлення результатів експертизи та видання Експертного ви-

сновку (для окремих засобів захисту інформації) й Атестату відповідності на комплексні системи захисту інформації в ІТС.

Позитивне рішення щодо засобу є підставою для його включення до Переліку засобів технічного захисту інформації загального призначення, які дозволені до використання з метою ТЗІ, а наявність атестату відповідності – підставою для одержання дозволу на оброблення в ІТС інформації, що підлягає захисту.

Система державної експертизи функціонує з 2000 року і за цей час стала одним із найбільш вагомих чинників реалізації державної політики в галузі, а її результати сприяли розвитку матеріально-технічної бази системи ТЗІ та наповненню ринку ефективними конкурентоспроможними програмно-апаратними засобами захисту інформації.

Науково-технічна діяльність у сфері ТЗІ полягає у формуванні, супроводженні та контролі за виконанням комплексних і цільових програм, метою яких є розвиток та удосконалення трьох складових системи ТЗІ. В 1994 році вперше в Україні було розроблено Науково-технічну програму “Розвиток системи технічного захисту інформації України” та Програму робіт з організації стандартизації й сертифікації в галузі технічного захисту інформації на 1995-1998 рр. Програми передбачали проведення науково-дослідних та дослідно-конструкторських робіт у рамках державного оборонного замовлення. Переліки запланованих НДДКР й обсяги їхнього фінансування визначали окремо на кожний рік, виходячи з можливостей державного бюджету й пріоритетності робіт.

Реалізація завдань цих документів мала забезпечити подальший розвиток та удосконалення технічного захисту інформації в Україні, поетапний перехід до використання вітчизняних технологій і засобів забезпечення технічного захисту інформації; сприяти подальшому розвитку науково-технічного та промислового потенціалу держави.

До системи підготовки фахівців у галузі ТЗІ входять вищі навчальні заклади усіх форм власності, що мають ліцензії на провадження освітньої діяльності у сфері захисту інформації, заклади післядипломної освіти, навчальні центри, органи управління освітою й наукою, органи науково-методичного управління підготовкою фахівців із захисту інформації відповідних міністерств, правоохоронних та інших державних органів, консультативно-дорадчі установи.

Оскільки завдання захисту інформації самі по собі є технологічно складними й наукоємними, потребують упровадження сучасних досягнень у сфері

інформаційних технологій, проведення теоретичних і прикладних досліджень, необхідною умовою для їх ефективного вирішення виступає наявність висококваліфікованих спеціалістів. В Україні упродовж останніх десяти років у вищих навчальних закладах діє система підготовки та перепідготовки спеціалістів у цій галузі.

Сьогодні система підготовки та перепідготовки фахівців із технічного захисту інформації переживає нову трансформацію і модернізацію з урахуванням сучасних вимог, що висуваються до захисту інформації і, як наслідок, до рівня підготовки фахівців.

7.4. ОСНОВНА ТЕРМІНОЛОГІЯ В ГАЛУЗІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

При проведенні діяльності, пов'язаної з ТЗІ, найчастіше використовується така термінологія:

- аналіз ризику – процес визначення загроз безпеці інформації та їх характеристик, слабких сторін захисту (відомих і ймовірних), оцінювання потенційних збитків від реалізації загроз та ступеня їх прийнятності;
- блокування інформації – унеможливлення санкціонованого доступу до інформації;
- витік інформації – результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та (або) юридичним особам, що не мають права доступу до неї;
- дезінформування – спосіб технічного захисту інформації, який полягає у формуванні свідомо неправдивої інформації для унеможливлення несанкціонованого доступу до істини;
- доступ до інформації – можливість одержання, оброблення інформації, її блокування та (чи) порушення цілісності;
- ефективність технічного захисту інформації – ступінь відповідності вжитих заходів щодо технічного захисту інформації встановленим вимогам;
- загроза для інформації – витік, можливість блокування чи порушення цілісності інформації;
- закладний пристрій – приховано установлюваний технічний засіб, який створює загрозу для інформації;

- засіб технічного захисту інформації – пристрій та (чи) програмний засіб, у якому функція захисту інформації від загроз є основною;
- інформація – відомості про суб'єктів, об'єкти, явища та процеси;
- інформація з обмеженим доступом – інформація, право доступу до якої обмежено установленими правовими нормами і (чи) правилами;
- інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів;
- інформативний сигнал – фізичне поле та (чи) хімічна речовина, що містять інформацію з обмеженим доступом;
- інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які в процесі оброблення інформації діють як єдине ціле;
- конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються фізичні чи юридичні особи або держава, і порядок доступу до якої встановлюють теж вони;
- модель загроз для інформації – формалізований опис методів та засобів здійснення загроз для інформації;
- модель технічної розвідки – формалізований опис методів, засобів та можливостей технічної розвідки;
- несанкціоновані дії щодо інформації в системі – дії з порушенням порядку доступу до інформації, установленого відповідно до законодавства;
- носій інформації – матеріальний об'єкт, що містить інформацію, яка підлягає захисту від загроз;
- оцінювання уразливості – дослідження об'єкта оцінювання з метою визначення можливості реалізації загроз;
- оцінювання безпеки інформації – процес, метою якого є визначення відповідності стану безпеки інформації установленим вимогам;
- побічне електромагнітне випромінювання й т. ін. – електромагнітне випромінювання тощо, що є побічним результатом функціонування технічного засобу та може бути носієм інформації;
- приховування інформації – спосіб технічного захисту інформації, який полягає в унеможливленні або суттєвому утрудненні несанкціонованого доступу до інформації;

- порушення цілісності інформації – спотворення інформації, її руйнування або знищення;
- рівень (технічного) захисту інформації – сукупність вимог (зокрема нормованих), що визначаються режимом доступу до інформації та загрозами її безпеці;
- спеціальний вплив – вплив на технічні засоби, що призводить до здійснення загрози для інформації;
- таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю;
- телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом її передавання, випромінювання або приймання у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;
- технічна розвідка – несанкціоноване здобування інформації за допомогою технічних засобів, її аналіз;
- технічний канал витоку – сукупність технічного засобу оброблення інформації, фізичного середовища її поширення та апаратури технічної розвідки.

7.5. ПЕРЕЛІК НОРМАТИВНО-ПРАВОВИХ АКТІВ ТА НОРМАТИВНИХ ДОКУМЕНТІВ, ЩО РЕГЛАМЕНТУЮТЬ ДІЯЛЬНІСТЬ У СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

- Конституція України, уведена в дію Законом України “Про прийняття Конституції України і введення її в дію” від 28.06.1996 р. № 254-96-ВР. Процитуємо деякі її статті.

Стаття 31. Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з’ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Стаття 32. 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...

Стаття 34. Кожний має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір...

- Закон України "Про інформацію", уведений у дію Постановою Верховної Ради України від 02.10.1992 р. № 2658-XII.

Установлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного й державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу й суспільство від неправдивої інформації.

Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя й діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

Регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Дія цього Закону поширюється на будь-яку інформацію, що обробляється в системах.

Закон визначає об'єкти захисту в системі та суб'єктів відносин, пов'язаних із захистом інформації в системах. Принципову вимогу становить те, що інформація, яка є власністю держави, або інформація з обмеженим доступом, захист якої установлений законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, установленому законодавством.

- Закон України "Про державну таємницю".

Регулює суспільні відносини у сфері охорони державних секретів. На його основі розроблено та уведено в дію низку загальнодержавних, відомчих нормативно-правових актів, що дало змогу в цілому створити систему охорони державної таємниці та забезпечити її функціонування.

- Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".

Визначає правові основи її організації та діяльності. Відповідно до нього Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування й розвитку

державної системи урядового зв'язку, національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації.

- Концепція (основи державної політики) національної безпеки України, схвалена Постановою Верховної Ради України від 16.01.1997 р. № 3/97-ВР.

Визначає основи політики захисту національних інтересів України та забезпечує єдність принципів її формування і проведення, поєднання підходів до створення відповідної законодавчої бази, підготовки доктрин, стратегій, концепцій, державних і відомчих програм у різних сферах національної безпеки.

- Указ Президента України від 6.12.2001 р. № 1193/2001 "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" визначає заходи із:

- створення проекту Концепції національної інформаційної політики та інформаційної безпеки України;

- створення організаційної структури системи забезпечення інформаційної безпеки;

- організаційно-методичного забезпечення системи захисту інформації у сферах взаємодії управлінь озброєння МО України з оборонно-промисловим комплексом;

- вирішення питань боротьби з комп'ютерною злочинністю та створення відповідного міжвідомчого центру;

- створення захищеної інформаційно-телекомунікаційної системи органів державної влади;

- створення та розгортання вітчизняного виробництва засобів захисту інформації, національної захищеної інформаційної системи, захищених систем електронного документообігу та електронного цифрового підпису, сертифікації технічних і програмних засобів інформатизації на відповідність вимогам інформаційної безпеки;

- розроблення проекту Закону України "Про захист інформації в інформаційно-телекомунікаційних системах";

- підготовки та перепідготовки спеціалістів у сфері інформаційної безпеки;

- створення Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при РНБО України.

- Указ Президента України від 27.09.1999 р. № 1229 "Про Положення про технічний захист інформації в Україні".

Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства й особи інформації, охорона якої забезпечується державою відповідно до законодавства. Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України; відповідних підприємств, установ, організацій.

Організація технічного захисту інформації в органах, стосовно яких здійснюється ТЗІ, покладається на їхніх керівників. Організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації, порядок контролю в цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації й експертизи комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

Нормативно-правові акти з технічного захисту інформації обов'язкові для виконання всіма суб'єктами системи технічного захисту інформації.

Положення визначає завдання суб'єктів ТЗІ, їхню взаємодію та відповідальність.

- Постанова КМ України від 8.10.1997 р. № 1126 "Про затвердження Концепції захисту інформації в Україні".

Концепція визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації є складовою забезпечення національної безпеки України.

Концепція забезпечує єдність принципів формування й проведення такої політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо) і слугує підставою для створення програм розвитку ТЗІ.

- Постанова КМ України від 29.03.2006 р. № 373 "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".

Правила визначають загальні вимоги та організаційні засади забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

- Наказ ДСТСЗІ СБ України від 23.02.2002 р. № 9 "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інфор-

мації для власних потреб”.

Положення визначає види та умови проведення робіт із технічного захисту інформації (далі – роботи з ТЗІ) для власних потреб, які виконуються за дозволами Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (далі – Департамент); установлює порядок надання дозволів, контроль та відповідальність під час проведення визначених видів робіт.

Вимоги Положення поширюються на органи державної влади, місцевого самоврядування (далі – державні органи), які мають намір проводити роботи з технічного захисту інформації для власних потреб, необхідність охорони якої визначена законодавством. За відсутності в державного органу дозволу на проведення робіт із ТЗІ для власних потреб зазначені роботи повинні виконуватись із залученням організацій, які мають ліцензії на право провадження господарської діяльності у сфері ТЗІ.

- Наказ Адміністрації Держспецзв’язку від 16.05.2007 р. № 87 “Про затвердження Положення про державний контроль за станом технічного захисту інформації”.

Визначає порядок організації та здійснення державного контролю за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої установлена законом. Державний контроль за станом технічного захисту інформації здійснює Державна служба спеціального зв’язку та захисту інформації України відповідно до законів України “Про Державну службу спеціального зв’язку та захисту інформації України” (3475-15), “Про захист інформації в інформаційно-телекомунікаційних системах” та “Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації”, затвердженого постановою Кабінету Міністрів України.

Дія Положення поширюється на всіх суб’єктів системи технічного захисту інформації.

- Наказ Адміністрації Держспецзв’язку від 16.05.2007 р. № 93 “Про затвердження Положення про державну експертизу в сфері технічного захисту інформації”.

Це Положення визначає порядок здійснення експертизи у сфері технічного захисту інформації. Державна експертиза у сфері технічного захисту інформації (далі – експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об’єктів експертизи щодо можливості їх використання для забезпечення

технічного захисту інформації.

Ліцензійні умови провадження господарської діяльності, пов'язаної з розробленням, виробництвом, упровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації, затверджені спільним наказом Держпідприємництва України та ДСТСЗІ СБ України від 29.12.2000 р. № 89/67 і зареєстровані в Міністерстві юстиції України 20.01.2001 р. за № 50/5241.

Ліцензійні умови визначають кваліфікаційні, організаційні, технологічні та інші вимоги до суб'єктів господарювання, виконання яких є обов'язковою умовою провадження певних видів робіт та надання певних видів послуг у межах господарської діяльності, пов'язаної з розробленням, виробництвом, упровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації.

Ліцензування господарської діяльності у сфері ТЗІ проводить Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Суб'єкт господарювання, який має намір проводити господарську діяльність у сфері ТЗІ та відповідає Ліцензійним умовам, подає до ДСТСЗІ СБ України заяву установленої форми про видачу ліцензії.

Державні стандарти та нормативні документи системи технічного захисту інформації

- ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення.

Установлює об'єкт, мету, основні організаційно-технічні положення щодо забезпечення технічного захисту інформації. Поширюється на підприємства, організації та установи усіх форм власності, органи державної власності усіх рівнів, які використовують та розпоряджаються інформацією з обмеженим доступом.

ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

Установлює вимоги до порядку проведення робіт із технічного захисту інформації. Поширюється на підприємства, організації та установи усіх форм власності, органи державної власності усіх рівнів, які використовують та розпоряджаються інформацією з обмеженим доступом.

- ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

Установлює терміни та визначення понять у сфері технічного захисту інформації. Поширюється на підприємства, організації та установи усіх форм власності, органи державної власності усіх рівнів, які використовують та розпоряджаються інформацією з обмеженим доступом.

У стандарті наведено абетковий покажчик українською, російською та англійською мовами.

- ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва, затверджені наказом Держкоммістобудування України від 2.09.1996 р. № 156, чинні від 1.01.1997 р.

Норми установлюють вимоги до забезпечення ТЗІ під час організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) підприємств, будівель та споруд.

Норми обов'язкові для застосування суб'єктами інвестиційної діяльності України й представництвами України за кордоном при виконанні проектних і будівельних робіт з урахуванням вимог технічного захисту інформації, яка містить відомості, що становлять державну та іншу передбачену законодавством України таємницю, а також конфіденційної інформації, що є державною власністю. Норми можуть бути використані суб'єктами, інвестиційна діяльність яких пов'язана з технічним захистом конфіденційної інформації, що не є власністю держави.

- Тимчасове положення про категоріювання об'єктів (ТПКО-95), затверджене наказом ДСТЗІ від 10.07.1995 р. № 35, призначене для організації робіт із категоріювання об'єктів.

Положення документа поширюються на центральні й місцеві органи державної виконавчої влади, органи виконавчої влади Автономної Республіки Крим, місцеві Ради народних депутатів та їхні органи, військові частини всіх військових формувань; на підприємства, установи й організації усіх форм власності, представництва України за кордоном і громадян, яки володіють, користуються та розпоряджаються інформацією з обмеженим доступом.

- Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ТЗІ-ПЕМВН-95), затверджені наказом ДСТСЗІ СБУ від 10.07.1995 р. № 25.

Документ призначений для організації захисту інформації з обмеженим доступом у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ПЕМВН).

- Тимчасові рекомендації з технічного захисту інформації в засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95), затверджені наказом ДСТЗІ від 10.07.1995 р. № 25.

Призначені для організації захисту інформації з обмеженим доступом від витоку каналами побічних електромагнітних випромінювань та наводок (ПЕМВН).

- Модель технічних розвідок (ТР – 2015).

Це керівний документ, у якому міститься формалізований опис систем і засобів технічних розвідок та інших засобів здійснення загроз для інформації. Наведені в Моделі тактико-технічні характеристики апаратури розвідки є вихідними даними для проведення розрахунків можливостей технічних розвідок за методиками, викладеними в “Методиках оцінки можливостей іноземної технічної розвідки (МВТР-87)”.

- НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12.12.2007 р. № 232.

Визначає основи організації й етапи виконання робіт щодо створення на об’єкті інформаційної діяльності органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації (далі – установа) комплексу, який має забезпечувати захист від витоку інформації з обмеженим доступом можливими технічними каналами.

- НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12.12.2007 р. № 232.

Визначає загальні вимоги до організації проведення на об’єкті інформаційної діяльності органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації випробувань щодо створення комплексу ТЗІ для захисту від витоку інформації з обмеженим доступом технічними каналами.

Установлює засади щодо проведення випробувань із метою перевірки (контролю) повноти та достатності реалізованих заходів із захисту інформації на ОІД, атестації комплексу ТЗІ, а також вимоги до розроблення висновків за результатами випробувань та їх програм і методик.

- НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.12.2007 р. № 232.

Визначає основні положення щодо проведення передпроектних робіт при створенні на об'єкті інформаційної діяльності органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації комплексу ТЗІ, який має забезпечувати захист від витоку інформації з обмеженим доступом (ІзОД) технічними каналами.

Установлює порядок та зміст проведення передпроектних робіт на ОІД, які вже функціонують або будуються (модернізуються), вимоги до оформлення акта обстеження на ОІД, а також вимоги до порядку розроблення й оформлення технічного завдання на створення комплексу ТЗІ.

- НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.12.2007 р. № 232.

Визначає порядок проведення робіт під час створення комплексу ТЗІ на об'єкті інформаційної діяльності органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації на етапі розроблення (проектування) й упровадження заходів із захисту від витоку інформації з обмеженим доступом технічними каналами.

Установлює вимоги до розроблення пояснювальної записки з ТЗІ, паспорта на комплекс ТЗІ та паспортів (як складових паспорта на комплекс ТЗІ) на приміщення, де ІзОД озвучується та (або) обробляється технічними засобами.

- НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення, затверджений наказом ДСТЗІ від 09.02.2001 р. № 2.

Установлює загальні вимоги до організацій атестації комплексів щодо повноти та якості робіт із ТЗІ. Призначений для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, підприємств, організацій, установ, діяльність яких пов'язана з інформацією, необхідність охорони якої визначено законодавством України, а також виконавців робіт із ТЗІ.

- НД ТЗІ 2.3-014-08 Захист інформації на об'єктах інформаційної діяльності. Методика оцінки ефективності зашумлення ліній електроживлення технічних засобів.
- НД ТЗІ 2.7-007-08 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки щодо зашумлення ліній електроживлення технічних засобів.
- НД ТЗІ 1.1-006-07 Протидія технічним розвідкам. Основні положення щодо організації та забезпечення комплексної протидії технічним розвідкам під час проведення навчань із застосуванням озброєння та військової техніки (без права публікації).
- НД ТЗІ 2.3-012-07 Протидія технічним розвідкам. Методика контролю ефективності комплексної протидії технічним розвідкам під час проведення навчань із застосуванням озброєння та військової техніки.
- НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги, затверджений наказом ДСТСЗІ СБ України від 13.06.2000 р. № 29, чинний із 1.07.2000 р.
- НД ТЗІ 2.4-005-07 Протидія технічним розвідкам. Рекомендації із забезпечення комплексної протидії технічним розвідкам під час проведення навчань із застосуванням озброєння та військової техніки.
- НД ТЗІ 2.2-006-07 Протидія технічним розвідкам. Норми протидії засобам радіорозвідки.
- НД ТЗІ 2.3-013-07 Протидія технічним розвідкам. Методика контролю ефективності протидії засобам радіорозвідки.
- НД ТЗІ 2.4-006-07 Протидія технічним розвідкам. Рекомендації із забезпечення протидії засобам радіорозвідки.

Поширюється на радіовиявлювачі (технічні засоби виявлення, ідентифікації та локалізації джерел електромагнітного випромінювання в галузі ТЗІ), а також на всі види комбінованих радіоелектронних засобів, до складу яких входять радіовиявлювачі, і встановлює для них обов'язкові технічні вимоги призначення. Його вимоги є обов'язковими для юридичних та фізичних осіб, які проводять свою діяльність у сфері ТЗІ згідно з чинним законодавством.

- НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань, затверджений наказом ДСТЗІ від 27.02.2001 р. № 5, чинний із 1.03.2001 р.

Поширюється на радіовиявлювачі вимірювальні й установлює єдині умови та методи їх випробувань на відповідність вимогам призначення; його вимоги є

обов'язковими для юридичних та фізичних осіб, котрі проводять свою діяльність у сфері ТЗІ згідно з чинним законодавством.

- НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБ України від 9.04.2001 р. № 12, чинний із 10.04.2001 р.

Поширюється на індикаторні радіовиявлювачі й установлює єдині умови та методи їх випробувань на відповідність вимогам призначення. Його вимоги обов'язкові для юридичних та фізичних осіб, котрі проводять свою діяльність у галузі ТЗІ згідно з чинним законодавством.

- НД ТЗІ 2.3-005-2001 Радіовиявлювачі панорамні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБ України від 11.09.2001 р. № 54, чинний із 30.09.2001 р.

Поширюється на радіовиявлювачі панорамні й установлює для них єдині умови та методи їх випробувань на відповідність вимогам призначення в діапазоні частот від 10 кГц до 18 ГГц. Вимоги НД є обов'язковими для юридичних та фізичних осіб, котрі проводять свою діяльність у галузі ТЗІ згідно з чинним законодавством.

- НД ТЗІ 2.3-006-2001 Радіовиявлювачі аналізувальні. Методи та засоби випробувань, затверджений наказом ДСТСЗІ СБ України від 6.11.2001 р. № 64, чинний із 15.11.2001 р.

Поширюється на радіовиявлювачі аналізувальні й установлює для них єдині умови та методи їх випробувань на відповідність вимогам призначення в діапазоні частот від 10 кГц до 18 ГГц. Вимоги НД обов'язкові для юридичних та фізичних осіб, котрі проводять свою діяльність у галузі ТЗІ згідно з чинним законодавством.

- НД ТЗІ 2.7-003-2000 Методичні вказівки щодо виявлення хімічних каналів витоку інформації з обмеженим доступом при створенні й упровадженні нових технологій і матеріалів, затверджений наказом ДСТСЗІ СБ України від 4.12.2000 р. № 052, чинний із 15.12.2000 р.

Установлює порядок і зміст робіт із виявлення хімічних каналів витоку інформації з обмеженим доступом (ІзОД) при створенні й упровадженні нових технологій і матеріалів, озброєння та воєнної техніки. Виявлення хімічних каналів витоку ІзОД при створенні й упровадженні нових технологій і матеріалів є першим етапом робіт при побудові системи технічного захисту ІзОД від витоку хімічними каналами.

НД становить методологічну основу для розроблення методик виявлення хімічних каналів витоку ІзОД на кожному етапі циклу створення й упровадження конкретних нових технологій та матеріалів.

- НД ТЗІ 2.7-004-2000 Інформаційно-аналітична модель мінімальних рівнів доступності інформації з обмеженим доступом у хімічних каналах, затверджений наказом ДСТСЗІ СБ України від 4.12.2000 р. № 052, чинний із 15.12.2000 р.

Вимоги нормативного документа, що містить інформаційні дані про засоби й методи хімічних розвідок, особливості хімічних речовин як носіїв інформації з обмеженим доступом, є обов'язковими для установ, організацій та підприємств, діяльність яких пов'язана з технічним захистом інформації та створенням і упровадженням нових технологій і матеріалів.

- НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, затверджений наказом ДСТСЗІ СБ України від 6.04.2001 р. № 11, чинний із 10.04.2001 р.

Визначає методи випробувань засобів технічного захисту мовної інформації з обмеженим доступом (ЗТЗІ) від її витоку через кінцеве обладнання симетричної аналогової абонентської телефонної лінії (АТЛ). Його вимоги обов'язкові для замовників, розробників, виготовлювачів, постачальників цих засобів та для випробувальних лабораторій (центрів), котрі здійснюють оцінку їхньої якості.

- НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань, затверджений наказом ДСТСЗІ СБ України від 6.04.2001 р. № 11, чинний із 10.04.2001 р.

Визначає методи випробувань засобів технічного захисту мовної інформації з обмеженим доступом (ЗТЗІ) від її витоку через кінцеве обладнання симетричної аналогової абонентської телефонної лінії (АТЛ). Його вимоги є обов'язковими для замовників, розробників, виготовлювачів, постачальників цих засобів та для випробувальних лабораторій (центрів), які здійснюють оцінку їхньої якості.

- НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та

віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань, затверджений наказом ДСТСЗІ СБ України від 6.04.2001 р. № 11, чинний із 10.04.2001 р.

Установлює порядок проведення випробувань засобів технічного захисту мовної інформації (ЗТЗІ) у симетричних абонентських телефонних лініях загального користування (АТЛ), призначених для визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки (ЗТР) до АТЛ.

Вимоги НД рекомендаційні для замовників, розробників, виготовлювачів, постачальників цих засобів та для випробувальних лабораторій (центрів), що здійснюють оцінку їхньої якості.

- НД ТЗІ 2.5-007-2007 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу “1”.
- НД ТЗІ 2.7-008-08 Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки.
- НД ТЗІ 2.3-017-08 Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами.
- НД ТЗІ 2.2-006-08 Захист інформації на об’єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і віброакустичному каналах витоку мовної інформації.

Установлює порядок визначення захищеності мовної інформації від порушення її конфіденційності за рахунок витоку акустичним і віброакустичним каналами на ОІД. Дія НД поширюється на комплекси ТЗІ таких ОІД: кабінетів, службових кімнат, аудиторій, залів тощо з внутрішнім об’ємом 20 – 5000 м^3, де не застосовується апаратура звукопідсилення. Вимоги документа є обов’язковими для підприємств, установ, організацій, діяльність яких пов’язана з інформацією з обмеженим доступом, що містить відомості, які становлять державну таємницю, а також із конфіденційною інформацією, що є власністю держави.

- НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація й загальні технічні вимоги. Рекомендації, затверджений наказом ДСТСЗІ СБ України від 4.09.2000 р. № 41.

Дія документа поширюється на технічні засоби активного захисту мовної інформації від витоку акустичним та віброакустичним каналами; містить класифікацію цих засобів і загальні технічні вимоги до них. Рекомендації

призначені для організацій на етапі розроблення засобів та їх експлуатації, а також для випробувальних лабораторій.

• НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22, чинний із 1.07.1999 р.

Визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних та методологічних документів, які регламентуватимуть питання:

- визначення вимог захисту комп'ютерних систем від несанкціонованого доступу;
- створення захищених комп'ютерних систем і засобів їхнього захисту від несанкціонованого доступу;
- оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

Відображає сучасний стан проблеми й підходів до її розв'язання. Із часом, як наслідок практичного застосування, а також із появою і розвитком нових тенденцій та підходів, у цей нормативний документ й інші нормативні та методологічні документи, що на ньому базуються, будуть уноситися відповідні корективи.

• НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22, чинний із 1.07.1999 р.

Установлює критерії оцінювання захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог із захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінювання захищеності інформації в комп'ютерних системах і придатності останніх для оброблення інформації, що підлягає захисту.

Критерії надають:

- порівняльну шкалу для оцінювання надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих у комп'ютерних системах;
- базу (орієнтири) для розроблення комп'ютерних систем, у яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно орієнтовані системи тощо.

- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22, чинний із 1.07.1999 р.

Установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу. Мета документа – надання нормативно-методологічної бази для вибору та реалізації вимог із захисту інформації в автоматизованій системі.

- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджені наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22, чинний із 1.07.1999 р.

Установлює вимоги до порядку розроблення, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передання інформації з обмеженим доступом або інформації, захист якої гарантується державою. Власники (користувачі) інформації, яка не є власністю держави або захист якої не гарантується державою, положення цього документа застосовують на свій розсуд. Зміни заходів, проведених раніше, відповідно до вимог чинних керівних документів не вимагається.

Нормативний документ розроблено в доповнення до чинних нормативних документів щодо створення об'єктів інформатики.

- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 4.12.2000 р. № 53, чинний із 15.12.2000 р.

Установлює єдиний підхід до визначення й формування завдань, функцій, структури, повноважень, організації робіт служби захисту інформації впродовж усього життєвого циклу АС в установах усіх форм власності, а також вимоги до структури та змісту нормативного документа, що регламентує діяльність служби захисту інформації в АС.

Призначений для суб'єктів інформаційних відносин, діяльність яких пов'язана з обробленням в АС інформації, що підлягає захисту, а також для ро-

зробників комплексних систем захисту інформації в АС.

- НД ТЗІ 2.5-007-2007 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу “1”.

Установлює згідно зі специфікаціями, визначеними НД ТЗІ 2.5-004-99, перелік функціональних послуг безпеки та рівнів їх реалізації в комплексі засобів захисту (КЗЗ) АС – так званий “стандартний функціональний профіль (СФП) захищеності”. Упровадження КЗЗ, у якому реалізовано СФП захищеності, є необхідною умовою для забезпечення захисту інформації, що становить державну таємницю, від загроз НСД при її обробленні в АС класу “1”, яка працює під управлінням операційної системи загального користування в певних умовах експлуатації АС.

- НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу “2”, затверджений наказом ДСТСЗІ СБ України від 13.12.2002 р. № 84, чинний із 20.12.2002 р.

Визначає вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в АС класу “2” і установлює згідно з визначеними НД ТЗІ 2.5-004 специфікаціями мінімально необхідний перелік функціональних послуг безпеки та рівнів їхньої реалізації в комплексах засобів захисту інформації (стандартний функціональний профіль захищеності).

Призначений для суб’єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов’язана з обробленням в АС конфіденційної інформації, розробників комплексних систем захисту інформації в автоматизованих системах, для постачальників компонентів АС, а також для фізичних та юридичних осіб, які здійснюють оцінювання захищеності АС на відповідність вимогам ТЗІ.

- НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 20.12.2000 р. № 60, чинний із 25.12.2000 р.

Установлює єдині вимоги до порядку створення, упровадження, супроводження та модернізації засобів ТЗІ від НСД у комп’ютерних системах і захищених від НСД компонентів обчислювальних систем (далі – засоби ТЗІ). Призначений для розробників та виробників (упроваджувальних організацій), споживачів (замовників, користувачів) засобів ТЗІ, а також для органів, що здійснюють функції оцінювання засобів ТЗІ на відповідність вимогам НД ТЗІ.

- НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 2.04.2003 р. № 33, чинний із 15.04.2003 р.

Установлює вимоги до технічних та організаційних заходів захисту інформації WEB-сторінки в Інтернеті. Згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями він установлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації в комплексах засобів захисту інформації WEB-сторінки від несанкціонованого доступу.

Призначений для суб'єктів інформаційних відносин (власників або розпорядників WEB-сторінки, операторів (провайдерів), користувачів), діяльність яких пов'язана з розробленням та експлуатацією WEB-сторінки, розробників комплексної системи захисту інформації та постачальників окремих її компонентів, а також для фізичних і юридичних осіб, які здійснюють оцінювання захищеності WEB-сторінки, на відповідність вимогам ТЗІ.

- Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України, призначений для використання суб'єктами системи ТЗІ під час розроблення, модернізації та упровадження комплексів ТЗІ на об'єктах інформаційної діяльності й комплексних систем захисту інформації в ІТС. Його формує та веде Держспецзв'язку.
- Перелік суб'єктів господарювання, котрі мають ліцензії на провадження господарської діяльності у сфері технічного захисту інформації.

Призначений для установлення виконавців робіт із ТЗІ під час розроблення, модернізації та упровадження комплексів ТЗІ на об'єктах інформаційної діяльності й комплексних систем захисту інформації в ІТС. Формує та веде Держспецзв'язку.

- Перелік засобів забезпечення технічного захисту інформації загального призначення, на які ДССЗЗІ України погоджено технічні умови.

Призначений для інформування суб'єктів системи технічного захисту інформації про технічні засоби із захисту інформації, засоби ТЗІ, засоби контролю за ефективністю ТЗІ та засоби виявлення й індикації загроз безпеці інформації, які розроблені в Україні та за певних умов можуть бути включені до Переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України. Формує й веде Держспецзв'язку.

Запитання і завдання для самоперевірки

1. Охарактеризуйте державну політику у сфері технічного захисту інформації.
2. Розкрийте суть ліцензування діяльності в галузі ТЗІ.
3. Охарактеризуйте необхідність сертифікації засобів ТЗІ та державної експертизи у сфері ТЗІ.
4. Розкрийте проблеми науково-технічної діяльності та системи підготовки й перепідготовки фахівців у сфері ТЗІ.
5. Охарактеризуйте нормативно-правові акти та нормативні документи, що регламентують діяльність у сфері ТЗІ.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
2. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
3. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12.12.2007 р. № 232.
4. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 12.12.2007 р. № 232.
5. НД ТЗІ 2.7-008-08 Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки.
6. НД ТЗІ 2.5-007-2007 Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробленні в автоматизованих системах класу “1”.

РОЗДІЛ 8

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У ПРОВІДНИХ КРАЇНАХ СВІТУ

8.1. КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У КРАЇНАХ НАТО ТА ЄС

Захист інформації з обмеженим доступом за всіх часів був однією з найважливіших функцій держави. От чому закони про обмеження доступу до певних видів інформації є майже в усіх європейських країнах. Ці обмеження стосуються інформації, пов'язаної з питаннями національної безпеки й міжнародних відносин, захисту приватного життя, комерційної інформації, правоохоронної діяльності та забезпечення суспільного порядку. У багатьох країнах документи, що подаються на розгляд парламентським комітетам і урядовим органам, виключаються зі списку відкритих для доступу аж до прийняття відповідних рішень. У міжнародній практиці також спостерігається тенденція підвищення рівня державного захисту персональної й комерційної інформації: держави розширюють свої зобов'язання щодо такого захисту.

У сучасному демократичному суспільстві більшість законів щодо обмеження доступу до інформації встановлюють рівень обмеження залежно від того, який збиток може виникнути в результаті несанкціонованого доступу до неї. При цьому переважно вимагається, щоб такий збиток був визначений ще до того, як буде прийняте рішення щодо обмеження.

Це пов'язано не лише з процесами демократизації й установлення вільного доступу до інформації, що відбуваються у світі, а й із тим, що захист інформації з обмеженим доступом вимагає значних, щораз більших фінансових витрат.

Як приклад можна навести відомості із щорічних офіційних звітів Служби інформаційної безпеки (Information Security Oversight Office – ISOO) Національної адміністрації архівів США (National Archives and Records Administration – NARA). Так, у зв'язку з подіями 11 вересня 2001 р. у порядку боротьби з тероризмом у США істотно зросла чисельність дій, пов'язаних із закриттям доступу до критичної інформації (від 8 млн процедур класифікації у

2001 році до 14 млн у 2005 році). Одночасно скорочується кількість процедур декласифікації: із 100 млн у 2001 році до 29 млн у 2005 році. У фінансовому вираженні це виглядає так: 4,5 млрд доларів на засекречування у 2001 році й 7,1 млрд доларів у 2004 році; на розсекречення 232 млн доларів у 2001 році й 48,3 млн доларів у 2004 році.

Суттєво те, що прийняття законів про захист інформації з обмеженим доступом в країнах – кандидатах на вступ до НАТО і ЄС відбувається на тлі боротьби громадськості за свободу доступу до урядової інформації, тобто синхронно із прийняттям законів про свободу доступу до інформації (див. таблицю 8.1). Цю боротьбу ведуть численні громадські організації, найбільш відомі з яких Суспільство свободи інформації (FOI – Freedom of Information) і Група "Статті 19" (Article 19 Group). Рух Суспільства свободи інформації за право цивільного контролю урядової інформації (right-to-know), розпочатий у США в 1966 р., нині охоплює 60 держав. Група "Статті 19" одержала свою назву за статтею 19 Загальної декларації про цивільні права, яка проголошує: "Кожний має право на свободу думок, право одержувати й передавати інформацію за допомогою будь-яких засобів масової інформації без обмежень". Заснована в 1987 р. у Великій Британії, ця група має міжнародні представництва в більшості країн Європи.

Таблиця 8.1

Польща	Закон "Про доступ до суспільної інформації", 2001 р.	Закон "Про захист класифікованої інформації", 1999 р.
Чехія	Закон "Про свободу доступу до інформації", 2000 р.	Закон "Про захист класифікованої інформації", 1998 р. (зміни від 2002 р.)
Угорщина	Закон "Про захист персональних даних та розкриття інформації, що становить суспільний інтерес", 1992 р.	Закон "Про державну таємницю", 1995 р. (зміни від 1999 р.)
Болгарія	Закон "Про доступ до суспільної інформації", 2000 р.	Закон "Про захист класифікованої інформації", 2002 р.
Румунія	Закон "Про доступ до інформації, що становить суспільний інтерес", 2001 р.	Закон "Про захист класифікованої інформації", 2002 р.
Словенія	Закон "Про доступ до інформації публічного характеру", 2003 р.	Закон "Про захист класифікованої інформації", 2001 р.; Закон "Про захист персональних даних", 1999 р.
Словаччина	Закон "Про вільний доступ до інформації", 2000 р.	Закон "Про захист класифікованих матеріалів", 2001 р.

У багатьох країнах вплив на рішення щодо обмеження доступу до інформації чинить омбудсмен, призначений парламентом. У різних державах така особа називається по-своєму (посередник, комісар, уповноважений). Поширення інституту омбудсмена в другій половині XX ст. пов'язано з розширенням управлінських функцій сучасної держави, зростанням його ролі в реалізації основних прав і свобод громадян. У результаті виникла необхідність доповнити судові й адміністративні гарантії цих прав особливою формою парламентського контролю. Вона є особливою тому, що акти й рішення, прийняті омбудсменом за скаргами чи подані громадянами за власною ініціативою, не володіють обов'язковою юридичною чинністю і ґрунтуються переважно на його авторитеті й сформованих традиціях.

З огляду на викладене, стає очевидним, що вивчення організаційно-правових основ захисту інформації з обмеженим доступом у ЄС і НАТО актуально зараз не тільки у зв'язку зі стратегічними намірами України щодо європейської та євроатлантичної інтеграції, а здебільшого унаслідок необхідності вивчення досвіду провідних країн світу в цій відповідальній і високовитратній сфері державної діяльності.

Інтеграція України до європейських структур становить стратегічний напрям діяльності держави на сучасному етапі її розвитку. Україна є учасницею Ради Євроатлантичного партнерства (РАЄП) та програми "Партнерство заради миру" (ПЗМ). Крім того, Україна підписала 13 березня 1995 р. Угоду про безпеку між Урядом України й Організацією Північноатлантичного Договору (Угода). Однак практичну імплементацію цього зовнішньополітичного вектора держави ускладнює низка об'єктивних та суб'єктивних чинників, зокрема проблеми у сфері захисту інформації з обмеженим доступом.

У міжнародних правовідносинах розрізняють норми міжнародного права (Rule of international law) і принципи міжнародного права (Standard of international law). Принципи міжнародного права – це такі норми міжнародного права, що мають обов'язковий характер для всіх суб'єктів. Слід зауважити, що принципи організаційно-правових основ захисту інформації з обмеженим доступом НАТО ще недостатньо досліджені на науковому рівні. Окремі аспекти цього питання розглядали провідні вітчизняні науковці М.Будаков, М.Галамба,

Б.Кормич, Г.Новицький та іноземні фахівці А.Роберт, К.Осакве, Т.Блентан, Д.Банісар та ін.

У монографії М.Будакова "Організаційно правові засади діяльності спеціальних служб держав НАТО" визначено поняття "спеціальні служби", виконано порівняльно-правовий аналіз законодавства провідних країн Північноатлантичного блоку у сфері регламентації функціонування спеціальних служб, здійснено класифікацію спеціальних служб за системою підпорядкування, установлено їхнє правове становище й організаційно-правові ознаки діяльності. У своїх публікаціях М.Будаков широко використовує терміни "організаційно-правові основи діяльності", "організаційно-правові основи функціонування". У той же час питання організаційно-правового регулювання захисту інформації з обмеженим доступом НАТО, актуальність яких набуває особливої важливості у зв'язку з інформаційними загрозами в сучасному світі, залишилися поза увагою цього фахівця.

У роботах відомого американського науковця, професора Нью-Йоркського університету А.Роберта, правника Організації свободи інформації (FOI), проаналізовано захисні функції безпеки НАТО. На основі аналізу нормативно-правових документів НАТО він уперше сформулював п'ять основних принципів політики безпеки Альянсу, але при цьому дослідник виступав із позицій правозахисника, що, безумовно, відбилося на його висновках.

У працях Б.Кормича, присвячених аналізу суспільних правовідносин, що виникають із приводу формування та функціонування системи інформаційної безпеки на сучасному етапі розвитку української державності в умовах прояву світових інформатизаційних та глобалізаційних тенденцій, уперше визначено правовий зміст:

• *національної безпеки* як стану захищеності гарантованих законодавством умов життєдіяльності держави, суспільства та особи від внутрішніх і зовнішніх загроз;

• *інформаційної безпеки* як важливої складової національної безпеки, що характеризує стан захищеності установлених законодавством норм і параметрів інформаційних процесів та відносин і забезпечує необхідні умови існування держави, людини та суспільства як суб'єктів цих процесів і відносин;

• *організаційно-правових основ* інформаційної безпеки як нерозривної єдності організаційних методів та правових норм регулювання суспільних відносин,

що виникають із приводу встановлення режимів і параметрів суспільного обігу інформації, правового статусу, поведінки та зв'язків суб'єктів інформаційних процесів.

Разом із тим, зосередившись на дослідженні регламентації правовідносин у галузі захисту інформаційних інтересів суспільства і людини, учений залишив поза увагою питання захисту інформації з обмеженим доступом з урахуванням організаційно-правових стандартів такого потужного воєнно-політичного блоку, як Північноатлантичний, та правотворчого досвіду країн – членів ЄС.

У роботах київської школи фахівців з інформаційної безпеки (М.Я.Швець, В.С.Цимбалюк та ін.) розкриваються джерела та витоки інформаційних загроз, що постають перед Україною й іншими державами в сучасному світі; значну увагу приділено проблемам, які пов'язані з використанням сучасних засобів комунікацій. Дослідники визначають, що саме *стандартизація* норм суспільних відносин формує законодавство у сфері захисту інформації з обмеженим доступом.

Захист інформації з обмеженим доступом Г.Новицький уважає головним завданням системи забезпечення національної безпеки України, насамперед підрозділів контррозвідки, що має лягти в основу побудови системи нормативно-правового регулювання забезпечення національної безпеки України.

8.2. ПОЛІТИКА БЕЗПЕКИ Й СУТНІСТЬ ОРГАНІЗАЦІЙНО-ПРАВОВИХ АСПЕКТІВ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У КРАЇНАХ НАТО ТА ЄС

На сучасному етапі розвитку юридичної науки й практики поняття сутності захисту інформації з обмеженим доступом отримало низку визначень, які не виходять за межі предмета того чи іншого наукового дослідження й охоплюють лише певні аспекти національних та міжнаціональних суспільних відносин.

Виходячи з того, що захист інформації є цілісною й комплексною системою, що потребує застосування організаційно-правових, технічних та інших засобів, для розкриття сутності захисту інформації з обмеженим доступом у ЄС та НАТО варто дослідити її основні ознаки та властивості.

Як свідчить аналіз, основні принципи захисту інформації з обмеженим доступом (у термінології НАТО – політика інформаційної безпеки SOI (Security Of Information Policy) регулюються документом C-M(2002)49 "Ключові питання інформаційної безпеки НАТО", C-M(2002)50 "Захист проти загроз тероризму" та C-M(2002)60 "Поводження з некласифікованою інформацією НАТО".

У НАТО є також категорії інформації, захист яких регламентують інші документи. Зокрема захист інформації категорії ATOMAL є предметом Договору між державами-членами НАТО про інформацію ATOMIC щодо ядерної зброї та компонентів для її виготовлення. Тут чинні документи C-M(64)39 та C-M(68)41. Захист інформації в межах Єдиного плану спільних дій США в межах НАТО (US-SIOP) регулюється документом C-M(71)27.

Під політикою інформаційної безпеки в документах ЄС та НАТО розуміються правила поводження з інформацією, у яких викладено питання філософії, стратегії й методів захисту інформації з обмеженим доступом. Політика безпеки дає змогу використовувати в конкретних обставинах такі методи і процедури, які здатні мінімізувати збитки в разі утрати або розкриття інформації з обмеженим доступом.

Аналіз документів Альянсу свідчить, що в термінології НАТО відсутнє поняття "інформація з обмеженим доступом". Навпаки, НАТО поділяє всі документи на "класифіковані" (classified), тобто такі, для яких визначено рівень обмеження доступу і які внесені до відповідних реєстрів, та "некласифіковані" (unclassified), які до відповідних реєстрів не внесені, але доступ до яких обмежується. Поводження з інформацією НАТО, яка має класифікацію "NATO Unclassified", регулюється документом C-M(2002)60. Крім того, Альянсу належить інформація, доступ до якої обмежується на тій підставі, що, на думку НАТО, "...нема офіційних причин для її поширення". Поводження з такою інформацією регулюється прийнятим у 2004 р. документом "Публічне поширення документів НАТО" (Public Disclosure of NATO Documents) і є предметом критики багатьох міжнародних організацій, наприклад FOI ("Freedom of Information").

Відповідно в ЄС також оперують поняттями "класифікована інформація" та "чутлива інформація".

У США досі триває дискусія стосовно такої інформації. "Чутлива" (sensitive), "чутлива некласифікована" (unclassified sensitive), "чутлива, але не-

класифікована” (sensitive but unclassified) – ось визначення для такої інформації. Втрата, неправильне використання, неправомірний доступ або модифікація такої інформації могли б негативно вплинути на національні інтереси чи виконання федеральних програм, але вона з тих, чи інших причин не увійшла до переліку, затвердженого Урядом або Конгресом США. Щодо окремих складових змісту цього визначення досі існують розбіжності між Міністерством оборони (DoD) та Агенцією з атомної енергії (NIST) США.

Історично політику SOI вперше в повному обсязі було викладено в документі, відомому як C-M(55)15(Final), який мав три компоненти. Перша та найстаріша з них була прийнята в січні 1950 р. як базова. Вона стала Додатком “A” документа C-M(55)15(Final). Друга компонента також була прийнята у 1950 р., проте потім неодноразово піддавалася суттєвому перегляду. Вона обумовила детальні процедури захисту таємної інформації НАТО та стала Додатком “C” документа C-M(55)15(Final). Третю компоненту було прийнято у 1955 р. Вона констатувала основні принципи та мінімальні стандарти, що стосуються національних систем захисту секретної інформації, незалежно від того, належить ця таємна інформації НАТО чи ні. Ця компонента стала Додатком “B” документа C-M (55) 15 (Final). Документ, який включав усі три компоненти, було прийнято в 1955 р.

Політика інформаційної безпеки НАТО у 1958 р. була доповнена Додатком “D”, який обумовлює захист промислової інформації. У 1961 р. ухвалено конфіденційні угоди щодо допуску персоналу до таємної інформації. На початку 80-х рр. XX ст. було прийнято Додаток “E”, присвячений боротьбі з тероризмом. Цей додаток було суттєво переглянуто у 2002 р.

Наприкінці 90-х рр. робоча група із фундаментального перегляду політики безпеки НАТО “Ad-Hoc” (Ad-Hoc Working Group for the Fundamental Review for NATO Security Policy) розпочала суттєвий перегляд документа C-M(55)15(Final). Документ, тепер відомий як C-M(2002)49, було прийнято 17 червня 2002 р., його структура дещо відмінна від структури C-M(55)15, що відображено у табл. 8.2.

Таблиця 8.2

Структури документів C-M(55)15 і C-M(2002)49

	C-M(55)15(Final)	C-M(2002)49
Додаток “A”	Угода про безпеку	Угода про безпеку
Додаток “B”	Основні принципи та мінімальні стандарти безпеки	Основні принципи безпеки
Додаток “C”	Процедури безпеки для захисту класифікованої інформації НАТО	Безпека персоналу
Додаток “D”	Промислова безпека	Фізична безпека
Додаток “E”	Заходи захисту проти* тероризму	Захист інформації*
Додаток “F”		INFOSEC**
Додаток “G”		Промислова безпека
* Основні принципи та мінімальні стандарти щодо захисту від тероризму в новій редакції було викладено в окремому документі C-M(2002)50. ** INFOSEC обумовлює захист інформації, яка обробляється, зберігається або передається в системах зв’язку, інформаційних та інших електронних системах.		

Наявність великої кількості документів, які регулюють поводження з таємною інформацією, невизначеність термінології, правових дефініцій стає на заваді дослідженню нормативної бази НАТО з питань захисту інформації з обмеженим доступом.

Згідно з дослідженнями професора А.Робертса документ C-M(2002)49, як і C-(55)15(Final), спирається на п’ять інституційних принципів, покликаних забезпечити високий рівень інформаційної безпеки. Ці принципи, за термінологією А.Робертса, такі:

- широта (Breadth);
- глибина (Depth);
- централізація (Centralization);
- контрольований доступ (Controlled Distribution);
- персональний контроль (Personnel Controls).

Проведений аналіз дає змогу стверджувати, що поняття захисту інформації НАТО з обмеженим доступом має базуватися на таких або аналогічних принципах. Додаткові дослідження дозволяють трансформувати наведені вище принципи в певну систему, яка адекватно відображає сутність захисту інформації НАТО з обмеженим доступом:

- *принцип уніфікації* рівнів класифікації інформації в НАТО й національних системах захисту інформації країн-учасниць;
- *принцип варіативності,* який полягає в тому, що НАТО не нав'язує країнам-членам норми і способи захисту інформації з обмеженим доступом, надаючи їм право обирати власні шляхи, виходячи з економічних можливостей та політико-історичних реалій за умов досягнення ними бажаних кінцевих результатів, транспарентності й відкритості;
- *принцип автентичності* надання рівня класифікації інформації з обмеженим доступом;
- *принцип збереження* рівня класифікації інформації;
- *принцип доцільності* надання доступу до інформації НАТО фізичним особам;
- *принцип перевірки* благонадійності фізичних осіб для надання їм допуску до інформації з обмеженим доступом;
- *принцип інституційного моніторингу* системи забезпечення захисту інформації з обмеженим доступом у НАТО і країнах-учасницях.

Принцип відповідності норм захисту інформації з обмеженим доступом у НАТО і національному законодавстві країн-учасниць означає, що держави – члени НАТО зобов'язуються регулювати на основі єдиних стандартів доступ не лише до інформації, яка належить НАТО, а й до всіх видів інформації, обов'язки щодо захисту якої бере на себе держава-учасник. Ця вимога чинна на тій підставі, що держави – члени НАТО мають бути впевнені, що кожна із них спроможна забезпечити високі стандарти захисту інформації. Цей принцип приблизно відповідає *принципу широти (Breadth)* у класифікації А.Робертса.

На принципі уніфікації рівнів класифікації інформації в НАТО й національних системах захисту інформації країн-учасниць базується вся система надання грифів секретності інформації Альянсу. Цей принцип приблизно відповідає *принципу глибини (Depth)* у класифікації А.Робертса. Відповідно до політики безпеки НАТО, викладеній в історичному документі C-M(55)15(Final), а потім підтвердженій у документі C-M(2002)49 від 2002 р., визначають такі рівні класифікації документів НАТО за ступенем таємності:

- NATO TOP SECRET (NTS);
- NATO SECRET (NS);

- NATO CONFIDENTIAL (NC);
- NATO RESTRICTED (NR).

Ця класифікація неодноразово була предметом дискусії в НАТО. Зокрема, ще в 50-х рр. минулого сторіччя штаб-квартира організації почала поширювати документи під грифом COSMIC, COSMIC TOP SICRET, COSMIC SICRET, які оброблялися особливо ретельно, розсилалися тільки зашифрованими, у спеціальних контейнерах, за подвійними печатками. Ініціатором такого нововведення був Воєнний комітет НАТО. Однак у 1954 р. було ухвалено рішення обмежити застосування грифа COSMIC. Унаслідок цього було затверджено порядок, відповідно до якого встановлено такі ступені секретності:

- COSMIC TOP SECRET (CTS) – несанкціоноване розкриття інформації з таким грифом може завдати надзвичайно великої шкоди НАТО;
- NATO SECRET (NS) – несанкціоноване розкриття інформації з таким грифом може завдавати дуже великої шкоди НАТО;
- NATO CONFIDENTIAL (NC) – несанкціоноване розкриття інформації з таким грифом може завдати шкоди НАТО;
- NATO RESTRICTED (NR) – несанкціоноване розкриття інформації з таким грифом може завдати шкоди інтересам або ефективності діяльності НАТО.

Як правила поводження з документами з грифом COSMIC TOP SECRET було затверджено порядок, прийнятий раніше для інформації з грифом NATO TOP SECRET. Однак і зараз серед документів найголовнішого члена НАТО США можна знайти такі, що мають гриф TOP SECRET або ABOVE TOP SECRET (надабсолютно секретно).

Суттєвим є те, що в національному законодавстві країн Центральної та Східної Європи – нових членів НАТО – відсутня категорія COSMIC TOP SECRET (див. таблицю 8.3).

Для інформації категорії NATO ATOMAL установлені грифи:

- COSMIC TOP SECRET ATOMAL;
- NATO SECRET ATOMAL;
- NATO CONFIDENTIAL ATOMAL.

Таблиця 8.3

Ступені секретності відповідно до національних правових актів країн – членів НАТО

НАТО	Cosmic top secret	Secret	Confidential	Restricted
Чехія	Přísnú tajné	Tajné	Dòvúrné	Vyhrazené
Словенія	Strogo tajno	Tajno	Zaupno	Interno
Румунія	Strict secret de importanta deosebita	Strict secret	Secret	Secrete de serviciu
Угорщина	Szigoruan titkos	Titkos	Bizalmas	–

Принцип автентичності надання рівня класифікації інформації з обмеженим доступом полягає в тому, що лише той орган країни – члена НАТО, який є автором документа, має право надавати йому ступінь секретності або – у термінології НАТО – рівень класифікації. Залежно від того, як інші члени НАТО виконують узяті на себе зобов'язання щодо захисту інформації, кожна країна визначає, яку інформацію вона зробить доступною іншим членам Альянсу, а яку – ні. Таким чином, будь-яка відмова одного або кількох членів Альянсу належним чином виконати зазначені зобов'язання може призвести до скорочення кількості та зниження якості переданої їм інформації. Наявність такого принципу вимагає від кожної країни – кандидата у члени НАТО приділяти особливу увагу якості функціонування власної системи захисту інформації з обмеженим доступом.

При цьому до рівня таємності в національному законодавстві різних країн висуваються різні вимоги. Наприклад, у законі про захист інформації, прийнятому Словаччиною, найнижчий рівень таємності – RESTRICTED – надається інформації, розкриття якої могло б завдати шкоди діяльності або перешкодити виконанню функцій окремими агентствами й установами. В аналогічному чеському законі рівень RESTRICTED надається інформації, втрата якої створить несприятливі умови для держави в цілому.

Відповідно до принципу збереження рівня класифікації інформації з обмеженим доступом жоден документ не може бути знижений у рівні таємності або розсекречений без згоди сторони, від якої він отриманий. У НАТО ці два

принципи уважаються фундаментальними. У класифікації А.Робертса вони окремо не виділені.

Принцип доцільності надання доступу до інформації фізичним особам у НАТО також називають фундаментальним. У термінології НАТО він зветься як *потреба знати (need-to-know)* і полягає в тому, що фізичні особи повинні мати доступ до класифікованої інформації, лише якщо вони її потребують для виконання прямих службових обов'язків, і доступ ніколи не має надаватися тільки тому, що особа обіймає певну службову посаду.

Принцип перевірки благонадійності фізичних осіб для надання їм допуску до інформації з обмеженим доступом передбачає правила щодо відбору осіб, які мають право одержати такий доступ. Відповідно до цього принципу контроль заснований на перевірці благонадійності (характеру та способу життя) кандидатів стосовно доступу до класифікованої інформації. Кандидати повинні демонструвати лояльність, певний характер, звички та спосіб життя, які без сумніву заслуговують на довіру. Важливою є вимога установити ступінь відповідальності за неправомірне розкриття класифікованої інформації. При цьому предметом розгляду національного законодавства країн-кандидатів є такі питання:

- чи будуть секрети НАТО розглядатися як державна таємниця;
- чи буде будь-яка особа, яка винна в розкритті секретів НАТО, переслідуватися в судовому порядку незалежно від того, чи є вона членом уряду, посадовцем або пересічним громадянином;
- чи буде особа, яка навмисно розкрила таємну інформацію НАТО, переслідуватися за законом із тією ж суворістю, що й особа, яка зробила це через необачність;
- чи може особа, яка розкрила державну таємницю або таємницю НАТО, переслідуватися в судовому порядку в країні за порушення, учинене за її межами;
- чи може держава в судовому порядку переслідувати іноземця, який розкрив таємницю НАТО на її території.

В основу політики країн-засновників НАТО у сфері персонального контролю покладено принцип *перевірки благонадійності (positive vetting),* що з'явився ще за часів адміністрації президента Г.Трумена. Зміст цих перевірок полягає у збиранні інформації, що може свідчити про нелояльність, наявність підозрілих зв'язків і дефектів характеру, які можуть зробити особу уразливою до впливів, що можуть завдати шкоди безпеці НАТО.

Із часом такі перевірки були визнані неефективними, такими, що суперечать принципам *гуманності (repugnant),* і такими, що порушують права людини. Ініціатива виходила від уряду Великої Британії, котрий запропонував використовувати принцип "перевірки неблагонадійності" (negative vetting), який на практиці зводився лише до перевірки осіб за наявними файлами спецслужб. Однак адміністрація президента Ейзенхауера перешкодила уведенню цього принципу у правове поле НАТО. У той же час і принцип "перевірки благонадійності" (positive vetting) не було повністю уведено в правове поле. Було зазначено, що він обов'язково набуває чинності лише при проведенні персонального контролю особливо важливих осіб. Останнім часом у зв'язку із прийняттям Йоганнесбурзької угоди громадськість у країнах-членах НАТО знову повернулася до цього питання. Адже відповідно до принципів НАТО можливо отримати відмову в доступі до класифікованої інформації, яка заснована не на фактах неблагонадійності, а лише на припущеннях та підозрах. У цьому вбачається порушення принципів 5 і 20 Йоганнесбурзької угоди. Проте положення щодо персонального контролю в НАТО зберігається до сьогодні тією мірою, якою залишаються чинними документи DC 2/1 і DC 2/7 (Revision of the North Atlantic Treaty Organization Security System, as approved by Cou*cil Deputies Final).

Принцип інституційного моніторингу системи забезпечення захисту інформації з обмеженим доступом у НАТО і країнах-учасницях означає вимогу мати в кожній такій державі інституційний національний уповноважений орган або урядове бюро національної безпеки (national security organization – NSO), яке відповідатиме за інформаційну безпеку й персонал, а також за збір і реєстрацію відомостей щодо шпигунства, підривної діяльності. Цей орган також має бути наділений повноваженнями контролювати стан захисту інформації з обмеженим доступом в усіх державних і недержавних інституціях, аналогічно тим, які в Україні мають назву "режимно-секретні органи" (РСО); організовувати методичну та дослідну роботу, проводити сертифікацію засобів захисту інформації.

Безпосередньо в НАТО діють установи, завданням яких є моніторинг результатів та якості захисту інформації з обмеженим доступом у країнах-учасницях. У 1955 р. було створено Бюро безпеки (нині – Офіс безпеки НАТО (NOS), що відповідає за повну координацію питань інформаційної безпеки в Альянсі). NOS доводить до NSO інформацію щодо застосування принципів і стандартів та виконує моніторинг національних систем захисту інформації.

Основні принципи, покликані забезпечувати високий рівень інформаційної безпеки в НАТО, неодноразово піддавалися ревізії. Зокрема повноваження Управління безпеки НАТО (NOS) спочатку були сформульовані так: NOS відповідальний за періодичну інспекцію заходів щодо захисту оборонної інформації НАТО в міжнародних та національних цивільних організаціях (for periodic inspection of security arrangements for the protection of North Atlantic Treaty defense information within international and national civil organizations). Пізніше, у 1954 році, це положення переглянули. NOS одержав ширші повноваження проводити періодичну перевірку системи забезпечення безпеки в національних та міжнародних цивільних агентствах (periodical examinations of the security system in national and international civil agencies). Остаточну редакцію було затверджено у зв'язку з ревізією, яка була зумовлена приєднанням до Альянсу ФРН у серпні 1955 р. Відповідно до цієї редакції NOS здійснює загальне керівництво утіленням повної системи безпеки, яка має забезпечувати належний захист як національної, так і тієї інформації, що належить НАТО (to provide guidance in setting up an overall security system that would safeguard national information as well as NATO).

Ревізії піддавався навіть такий фундаментальний принцип, як *потреба знати (need-to-know).* Наприклад, у США у зв'язку з подіями 11 вересня 2001 р. був виданий документ, що встановлює коло осіб, які одержують доступ до класифікованої інформації лише за посадою.

В історії НАТО також неодноразово піднімалося питання щодо спрощення системи класифікації секретних документів. Зокрема Норвегія і Данія виступили у 50-х рр. минулого сторіччя зі спільною заявою, пропонуючи виключити рівень RESTRICTED із класифікації, оскільки "...наявна класифікація занадто складна, забезпечення безпеки класифікованих так документів ускладнене, і скоріше це може призвести до конфузів, ніж до реального внеску до загальної безпеки НАТО" (this grading was superfluous, and governing the safeguarding of document so graded were so vague that they might lead to confusion instead of contributing to overall NATO security). Утім, гриф RESTRICTED у документах США застосовувався ще з 1940 р., і тому було прийнято рішення зберегти цю систему класифікації. У той же час, рівень NATO RESTRICTED не зовсім відповідає класифікації US RESTRICTED, тому документи, позначені як "NATO RESTRICTED", згідно з документами USSAN Instruction 1-69 (United States Security Authority for NATO) у США мають захищатися як такі, що мають гриф "виключно ККК користування (For Official Use Only)".

Законодавчі документи у сфері захисту інформації з обмеженим доступом приймає кожна країна ще до вступу в НАТО. У наш час прийняття законів щодо захисту інформації з обмеженим доступом у країнах, котрі прагнуть вступити до НАТО, відбувається в умовах демократизації, боротьби за цивільні права та свободу доступу до інформації або, у сучасній термінології, прозорості (transparency) інформації. Тому основні принципи і правові механізми, тобто *сутність* захисту інформації з обмеженим доступом, у цих країнах є предметом дискурсу між урядами та громадськими організаціями. Унаслідок цього в законодавстві таких країн ураховано не лише культурно-історичні, соціально-економічні особливості державного устрою, закріплені конституційно, але й результати цього дискурсу. Проте всі вони підкоряються певній моделі, прийнятій країнами-засновниками НАТО ще в 1949 р. і закріпленій у документі НАТО C-M(2002)49 у 2002 р.

Відповідно в ЄС 19.03.2001 року було прийнято Інструкцію безпеки Ради Європейського Союзу (2001/264/ЄС). Інструкція містить основні принципи та мінімальні стандарти захисту інформації з обмеженим доступом у ЄС. У таблиці 8.4 наведено порівняльні дані документів C-M(2002)49 НАТО та 2001/264/ЄС.

Таблиця 8.4

Порівняння структур основоположних документів ЄС та НАТО у сфері захисту інформації з обмеженим доступом

C-M(2002)49	2001/264/ЄС
Угода про безпеку	Рішення від 19.03.2001 р. про прийняття Інструкції безпеки ЄС
Основні принципи безпеки	Основні принципи та мінімальні стандарти безпеки
	Організація безпеки
Безпека персоналу	Безпека персоналу
Фізична безпека	Фізична безпека
Захист інформації	
INFOSEC	Безпека інформації (INFOSEC)
Промислова безпека	

Аналіз таблиці свідчить про деякі розбіжності між акцентами ЄС та НАТО у сфері захисту інформації, що зумовлено тим, що НАТО, на відміну від ЄС, є військово-політичним союзом. Натомість порівняння, наприклад рівнів класифікації інформації, свідчить про збіг основних засад забезпечення захисту інформації в ЄС та НАТО (табл. 8.5).

Таблиця 8.5

Рівні класифікації інформації в ЄС та НАТО

НАТО	ЄС
COSMIC TOP SECRET (CTS) – несанкціоноване розкриття інформації з таким грифом може завдавати надзвичайно великої шкоди НАТО	TRÈS SECRET UE/EU TOP SECRET – ця класифікація повинна застосовуватися тільки до такої інформації й матеріалів, несанкціоноване розкриття яких може завдати винятково серйозного збитку істотним інтересам ЄС або одній чи кільком державам-членам
NATO SECRET (NS) – несанкціоноване розкриття інформації з таким грифом може завдавати дуже великої шкоди НАТО	SECRET UE – ця класифікація повинна застосовуватися тільки до інформації й матеріалів, несанкціоноване розкриття яких може серйозно зашкодити істотним інтересам ЄС або одній чи більшій кількості держав-членів
NATO CONFIDENTIAL (NC) – несанкціоноване розкриття інформації з таким грифом може завдати шкоди НАТО	CONFIDENTIEL UE – ця класифікація повинна застосовуватися тільки до інформації й матеріалів, несанкціоноване розкриття яких може зашкодити істотним інтересам ЄС або одній чи більшій кількості держав-членів
NATO RESTRICTED (NR) – несанкціоноване розкриття інформації з таким грифом може завдати шкоди інтересам або ефективності діяльності НАТО	RESTREINT UE ця класифікація повинна застосовуватися до інформації й матеріалів, несанкціоноване розкриття яких може бути невигідним для інтересів ЄС або однієї чи кількох держав-членів

Як основні принципи політики безпеки ЄС проголошується таке:

- заходи безпеки повинні поширюватися на усіх осіб, які мають доступ до класифікованої інформації, на носії, що містять класифіковану інформацію, на усі приміщення, що містять таку інформацію, і важливі спорудження;
- мають застосовуватися засоби виявлення й запобігання доступу неуповноважених осіб у приміщення, що містять класифіковану інформацію, або на територію охоронюваних споруджень;
- мають застосовуватися засоби, що перешкоджають доступу будь-яких неуповноважених осіб до класифікованої інформації й споруджень, що охороняються;
- має гарантуватися, що доступ до класифікованої інформації надається винятково на основі принципу необхідності, що є фундаментальним для всіх аспектів безпеки (need-to-know);
- має забезпечуватися гарантія цілісності[1] й готовності[2] всієї інформації (як класифікованої, так і некласифікованої), особливо такої, що зберігається, обробляється чи передається в електромагнітній формі.

Суттєвим є те, що Рада Євросоюзу по телекомунікаціях у 2003 році, а потім Єврокомісія та Європарламент схвалили створення Європейської агенції з інформаційної безпеки. Ця структура займається питаннями забезпечення кібернетичної безпеки країн-членів й інститутів Євросоюзу. Штаб-квартира агенції розташована в Брюсселі.

Відповідно до рішень Євросоюзу був створений Комітет із безпеки, який очолює Генеральний секретар. До складу Комітету з безпеки Ради Європи входять представники національних агентств по безпеці (NSA). Представники регіональних агентств Євросоюзу можуть запрошуватися на засідання Комітету, якщо розглядається питання, яке їх стосується. Засідання Комітету проводяться відповідно до затвердженого плану, за рішенням Генерального секретаря чи за вимогою національних агентств NSA. Комітет має право аналізувати проблеми безпеки, що стосуються слухань Євросоюзу, і надавати відповідні рекомендації Раді.

У розпорядженні Генерального секретаря в складі Генерального секретаріату (GCS) знаходиться Офіс безпеки GCS для координування, спостереження і здійснення заходів безпеки. Глава Офісу безпеки GSC є основним радником Генерального секретаря ЄС із питань безпеки і діє як секретар Комітету безпеки. Глава Офісу безпеки GSC разом із відповідними національними агентствами безпеки NSA відповідає за акредитацію інформаційно-комунікаційних мереж,

[1] Запобігання несанкціонованій зміні, порушенню чи видаленню інформації.
[2] Надання безвідмовного доступу уповноваженим особам.

що належать GSC, регіональним агентствам ЄС, третім країнам і міжнародним організаціям, які мають справу з класифікованою інформацією ЄС.

Відповідно до установлених правил кожна держава – член ЄС створює національне агентство безпеки (NSA), у сферу відповідальності якого входить:

(a) забезпечення безпеки класифікованої інформації ЄС, що перебуває в розпорядженні будь-яких національних органів та агентств, суспільних чи приватних організацій;

(в) організація регістрів інформації, класифікованої як TRES SECRET UE/EU TOP SECRET;

(c) періодичний контроль заходів захисту класифікованої інформації ЄС;

(d) забезпечення гарантій того, що громадяни, які мають доступ до інформації, класифікованої як TRES SECRET UE/EU TOP SECRET, SECRET UE чи CONFIDENTIEL UE, мали відповідним чином оформлений допуск (сертифікат безпеки);

(e) створення таких планів безпеки, що гарантовано запобігають потраплянню класифікованої інформації ЄС до рук неуповноважених осіб.

Угода з безпеки ЄС передбачає проведення періодичних взаємних перевірок правил і порядку забезпечення захисту інформації з обмеженим доступом у державах-членах ЄС. Ці перевірки проводяться спільно та за взаємною згодою Офісом безпеки GSC і зацікавленим агентством національної безпеки NSA.

Між ЄС і НАТО в березні 2003 року була укладена Угода про безпеку, яка проголошує, що представник Генерального секретаря уповноважений передавати НАТО відповідно до інструкцій безпеки Ради класифіковану інформацію й документи, напрацьовані в Раді Європейського Союзу, що стосуються європейської безпеки й інших питань, які підпадають під юрисдикцію Угоди про безпеку між НАТО і ЄС.

8.3. ЗМІСТ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ОСНОВ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У КРАЇНАХ НАТО І ЄС

Зміст захисту інформації з обмеженим доступом визначається стандартами НАТО. Мінімальні стандарти НАТО щодо захисту інформації з обмеженим доступом викладено в додатку В документа C-M(2002)49, який спирається на такі директиви:

- AC/35-D/2000 – Директива з питань безпеки персоналу;
- AC/35-D/2001 – Директива з питань фізичної безпеки;
- AC/35-D/2002 – Директива з питань безпеки інформації;
- AC/35-D/2003 – Директива з питань промислової безпеки;
- AC/35-D/2004 – Директива стосовно INFOSEC;
- AC/35-D/2005 – Директива з питань управління INFOSEC для систем зв'язку та інформаційних систем.

Перші чотири директиви були затверджені Радою НАТО, а решта – дві (AC/35-D/2004 і D/2005) – ухвалені Комітетом безпеки НАТО і відділом С3 НАТО, який відповідає за безпеку в інформаційно-комунікаційних мережах.

Відповідно до вимог Альянсу кожна країна, яка вступає до НАТО, має взяти на себе зобов'язання привести власні нормативно-правові документи у сфері захисту інформації з обмеженим доступом у відповідність до стандартів НАТО. Тому вивчення та систематизація стандартів НАТО у сфері захисту інформації з обмеженим доступом – обов'язкова умова на шляху інтеграції України до Альянсу.

Суттєвим є те, що в НАТО під стандартизацією розуміють процес формулювання, узгодження, застосування та удосконалення угод (стандартів) із метою підвищення ефективності діяльності. Цим вона суттєво відрізняється від системи стандартів, яка діяла в Радянському Союзі.

Аналіз організаційно-правових документів показує, що політика безпеки НАТО спирається на розгалужену систему стандартів. В Альянсі діє система стандартів STANAG (Standardization Agreement), більшість із яких загалом повторюють стандарти військового відомства США – MILStandard. STANAG містить три види стандартів: матеріальні, операційні та адміністративні.

Стандартизація матеріальної частини включає розроблення практичних посібників та технічних умов на перспективну й наявну техніку, в тому числі на засоби і системи, що забезпечують захист інформації з обмеженим доступом. У наш час стандартизація матеріальної частини в нових країнах-членах НАТО певним чином стримується економічними й політичними факторами. Стандартизація нематеріальної частини розвивається успішно. НАТО щорічно ратифікує значну кількість міжнародних угод у цій галузі.

Стандарти STANAG на нематеріальну частину підрозділяються на операційні (operational) та адміністративні (administrative).

Операційні стандарти STANAG поширюються на тактичні концепції, доктрини, методи, матеріально-технічне забезпечення, навчання особового складу, організаційні питання тощо. Термін "операційний" застосовується в НАТО в широкому розумінні й охоплює усі нематеріальні аспекти підготовки і ведення військових операцій або забезпечення взаємодії систем, частин та видів озброєння. Мета цих стандартів – мінімізувати технічні, процедурні та операційні труднощі, які можуть виникнути між союзними військами під час бойових дій.

Адміністративні стандарти STANAG частіше стосуються термінології. Вони використовуються як в операційній, так і матеріальній сферах. Ця категорія включає воєнні та невоєнні стандарти, які можуть бути корисними для поліпшення взаємодії в адміністративній роботі.

Кожна країна НАТО ратифікує STANAG та імплементує його до національної системи стандартів. Це робиться для того, щоб кожний член Альянсу міг використовувати у воєнних цілях склади та технічну підтримку будь-якої іншої країни-члена НАТО.

Відповідно до прийнятих зобов'язань кожна країна-член НАТО повинна створити національне агентство зі стандартизації НАТО (NATO Standardisation Agency – NSA). NSA – це єдиний інтегративний орган, відповідальний перед Комітетом зі стандартизації НАТО (NATO Standardisation Committee – NSC). NSC встановлює процедури, планує та реалізує функції, що стосуються стандартизації у всіх членах Альянсу. NSC несе відповідальність за організацію роботи національних агентств, тобто NSA, проведення нарад на рівні NCSREPs та NSSG, загальне адміністрування STANAG та публікації з питань стандартизації НАТО (Allied Publications – APs).

NSA також забезпечує функціонування об'єднаних і спеціальних служб (Joint and Single Service Boards), кожна з яких має повноваження, делеговані Військовим комітетом НАТО, у тому числі розроблення доктрини стандартизації у своїй галузі. Ці служби (Service Boards) відповідають за розроблення процедур стандартизації на національному рівні. У ролі повноважних органів вони забезпечують розповсюдження публікацій Альянсу з питань стандартизації (AP) та прийняття стандартів системи STANAG як Військовим командуванням НАТО (NATO Military Commands), так і в країнах-членах Альянсу.

Органами безпеки НАТО є:

- офіс безпеки НАТО (NOS);
- органи безпеки у військових структурах НАТО (NAMILCOM);
- національні уповноважені органи з безпеки НАТО (NSA).

Структура органів безпеки НАТО наведена на рис. 8.1.

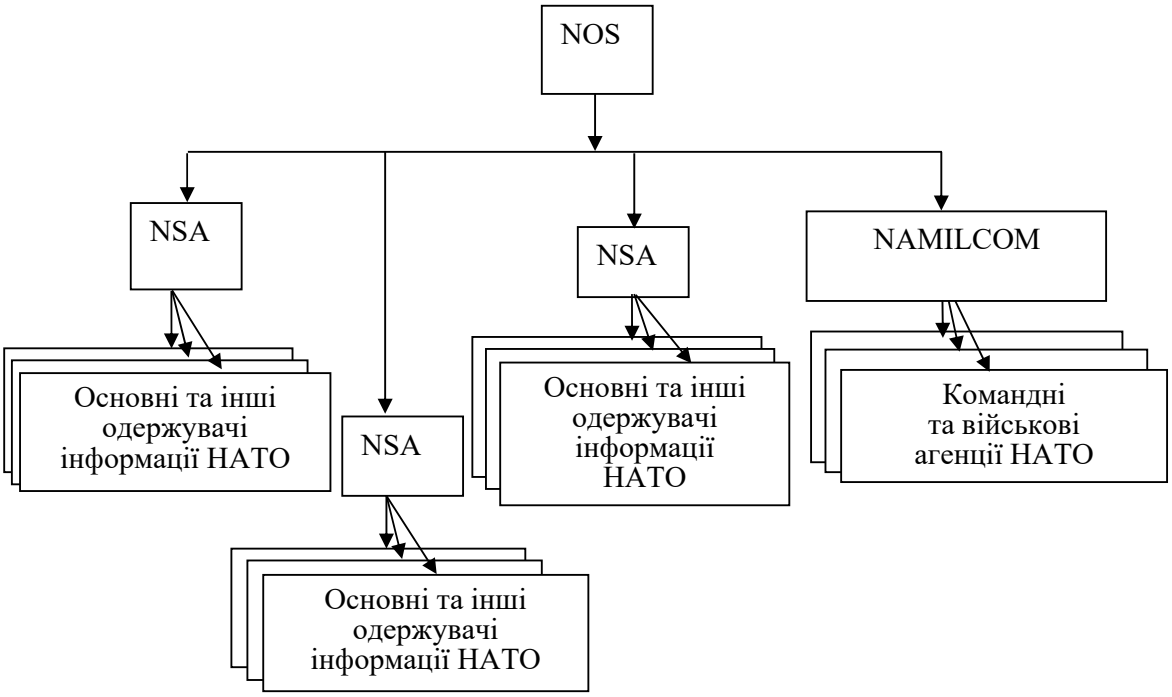

Рис. 8.1. Органи безпеки НАТО

Національний уповноважений орган із безпеки інформації (NSA) зобов'язаний забезпечувати:

- безпеку інформації з обмеженим доступом у військових і цивільних органах і структурах у країні та за її кордонами;
- керівництво створенням або ліквідацією режимно-секретних органів (РСО), про відповідні дії щодо таких органів повідомляється NOS;
- проведення спільно із NOS періодичних інспекцій із перевірки виконання правил захисту інформації з обмеженим доступом у національних організаціях усіх рівнів, як військових, так і цивільних;
- перевірку відповідно до правил НАТО благонадійності всіх громадян своєї країни, які за родом діяльності допущені до інформації з обмеженим доступом;
- розроблення планів захисту інформації в надзвичайних обставинах для запобігання нелегітимному використанню інформації з обмеженим доступом, потраплянню її до чужих рук або до противника.

Структура і функції NOS наведені на рис. 8.2.

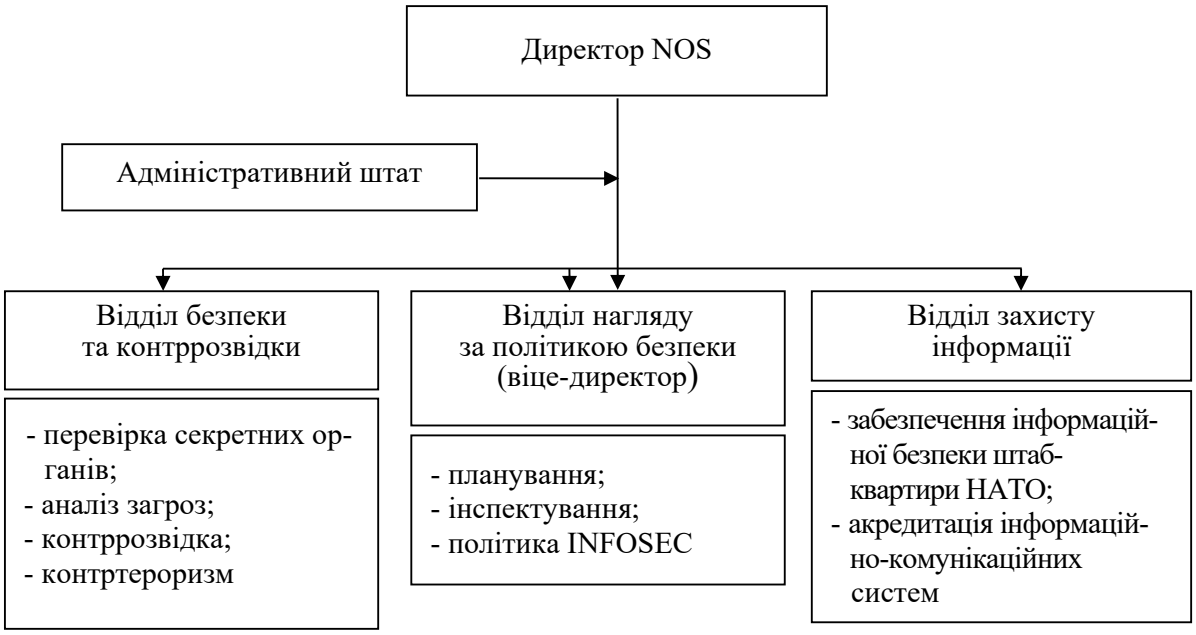

Рис. 8.2. Структура NOS

Статус національного уповноваженого органу з безпеки (NSA) в національних структурах влади залежить від обумовленої конституцією кожної країни загальної структури безпеки. Відповідно до цього уповноважений орган із безпеки інформації може входити до структур міністерств силового блоку або стояти над ними. У США, скажімо, цей орган підпорядкований безпосередньо президентові країни. У деяких державах керівником уповноваженого органу з безпеки є прем'єр-міністр, міністр оборони або міністр внутрішніх справ. При цьому спільне тільки те, що в країні призначається єдиний відповідальний уповноважений із безпеки інформації, функції якого можуть змінюватися залежно від сил і засобів, безпосередньо йому підлеглих. На обсяг функцій відповідального уповноваженого впливають чисельність населення, географічне положення, політичне й соціально-економічне становище країни, розподіл повноважень між органами вищої влади.

Найчастіше більша частина функцій відповідального уповноваженого делегується міністерству оборони. Так, у Бельгії відповідальним уповноваженим із безпеки інформації є заступник начальника Генерального штабу. У США це Міністерство оборони (DoD), Німеччині – Міністерство внутрішніх справ (MoI).

У США партнерами NSA (DoD) є Державний департамент (Міністерство іноземних справ) та ЦРУ, Німеччині – BfN і BSI, Франції – DGA та DST.

Базові принципи й мінімальні стандарти політики безпеки НАТО стосуються таких питань:

- створення системи надійних органів безпеки;
- організація захисту інформації, виробів, територій та споруд;
- забезпечення доступу до класифікованої інформації лише ретельно перевіреного персоналу.

До складу додатка В документа C-M(2002)49, який проголошує мінімальні стандарти НАТО у сфері захисту інформації з обмеженим доступом, входять такі розділи:

- цілі й наміри;
- застосування;
- повноваження;
- основні принципи;
- фізична безпека;
- безпека персоналу;
- захист інформації;
- INFOSEC;
- промислова безпека;
- відповідальність за безпеку;
- національний орган безпеки (NSA);
- повноважний орган безпеки (DSA);
- комітет безпеки НАТО (NSC);
- офіс безпеки НАТО (NOS);
- військовий комітет NAMILCOM та військові організації НАТО;
- цивільні організації НАТО.

Позиції 5 – 16 цього переліку дають змогу аналізувати зміст заходів щодо захисту інформації з обмеженим доступом відповідно до мінімальних стандартів НАТО.

Заходи фізичної безпеки НАТО (Physical Security) передбачають:

- захист приміщень та споруд;
- захист інформації усередині приміщень і споруд;
- контроль доступу до приміщень та споруд;

- захист проти візуального спостереження й прослуховування.

При визначенні, який саме ступінь фізичної безпеки в кожному конкретному випадку необхідний, беруться до уваги такі фактори:

- рівень класифікації й категорія інформації;
- кількість і форма збереження інформації;
- сертифікат допуску та необхідний для роботи рівень обізнаності персоналу;
- оцінка на місцевості загроз із боку спецслужб інших держав, терористичної або іншої кримінальної діяльності.

Програми фізичної безпеки базуються на принципі "оборона в глибині", який передбачає визначення таких зон безпеки:

1. Зона безпеки НАТО класу I, де забезпечується зберігання інформації з грифом "НАТО/Таємно" і вище усіма доступними засобами.
2. Зона безпеки НАТО класу II, де забезпечується зберігання інформації з грифом "таємно" й вище з використанням засобів внутрішнього контролю.
3. Адміністративна зона, де забезпечується зберігання інформації з грифом не вище "НАТО/Конфіденційно".

Заходи забезпечення фізичної безпеки визначені такі:

1. Огорожа по периметру та система охоронного освітлення.
2. Система виявлення порушника (IDS), у тому числі система відеоспостереження (CCTV).
3. Система контролю входів і виходів (електронна, електромеханічна або фізична, тобто така, що здійснюється спеціально підготовленими охоронцями).

Фізична безпека визначає засоби захисту класифікованої інформації від технічних атак, наприклад прослуховування. Офіси або територія, у яких регулярно озвучується класифікована інформація із грифом "SECRET" і вище, захищаються від пасивного та активного прослуховування за допомогою надійних заходів фізичної безпеки з урахуванням виправданого ризику. Відповідальність за визначення такого ризику покладається на органи з питань безпеки й узгоджується з технічними спеціалістами. Тут також наголошується на необхідності сертифікації та затвердження списків обладнання, які ухвалюються для захисту класифікованої інформації НАТО за різноманітних специфічних обставин та умов.

Заходи щодо безпеки персоналу (Personnel Security) полягають у тому, що особи, котрим санкціоновано доступ до інформації з грифом "таємно" й вище, повинні пройти відповідну перевірку на допуск персоналу (Personnel Security

Control – PSC), яку проводить орган національної безпеки або інший уповноважений орган. Процедури видання сертифіката допуску здійснюються з урахуванням політики безпеки НАТО й відповідних директив.

Процедури безпеки персоналу розробляються з метою оцінювання того, чи може особа, враховуючи її лояльність і надійність, мати допуск до інформації з обмеженим доступом, не піддаючи безпеку жодному ризику. Усі особи, цивільні або військові, які потребують доступу або чиї обов'язки чи функції дозволяють доступ до інформації з грифом "таємно" (CONFIDENTIAL) і вище, мають бути відповідно перевірені перед тим, як цей доступ буде санкціоновано. Особи мають доступ лише до такої засекреченої інформації НАТО, яка передбачена їхніми функціональними обов'язками (принцип "need-to-know").

Сертифікат допуску не вимагається для доступу до інформації з грифом "ККК користування" (RESTRICTED); особи лише мають бути попереджені про їхню відповідальність щодо охорони такої інформації. Дозвіл на отримання сертифіката допуску персоналу розглядається як кінцевий етап у процесі перевірки безпеки персоналу; крім того, вимагається гарантія постійної придатності особи щодо доступу до класифікованої інформації НАТО. Це досягається через постійне оцінювання осіб, котрі мають допуск, керівництвом і менеджерами з питань безпеки; а також шляхом навчання з питань безпеки й знання програм, які нагадують особам про їхню відповідальність щодо безпеки й потребу доповідати інформацію, яка може впливати на стан безпеки, своїм менеджерам або відповідальним за безпеку співробітникам.

Особи в державах – членах НАТО, цивільних та військових організаціях Альянсу мають доступ лише до такої засекреченої інформації, яка їм необхідна для роботи. Жодна особа не має права тільки завдяки своїй посаді, чину або сертифікату допуску мати доступ до засекреченої інформації НАТО.

Безпека інформації (Information Security) передбачає нормування процедур поводження з документованою інформацією, які виникають при її:

- маркіруванні;
- класифікації;
- підготовці;
- обігу, включаючи розповсюдження (release);
- переданні на відстань;
- знищенні.

За процедурами безпеки інформації автор відповідає за визначення рівня класифікації безпеки й початкове поширення інформації. Рівень класифікації інформації НАТО не може змінюватися або понижуватися, інформація також не може бути декласифікована без погодження з автором. Під час її створення автори мають визначити, у яких випадках та на яку дату чи подію можна знижувати рівень класифікації або декласифіковувати інформацію НАТО.

Згідно зі стандартами НАТО інформація з грифом “ONFIDENTIAL” і вище повинна переглядатися її автором кожні п’ять років. Такий перегляд не обов’язковий у тих випадках, коли автор передбачив зниження грифа автоматично через кожні два роки після його присвоєння. Документи, кваліфіковані як “CONFIDENTIAL” і вище, повинні мати кваліфікаційні відмітки на кожній сторінці (див. рис. 8.3). Автори класифікованої інформації можуть використовувати додаткові позначки для обмеження її поширення.

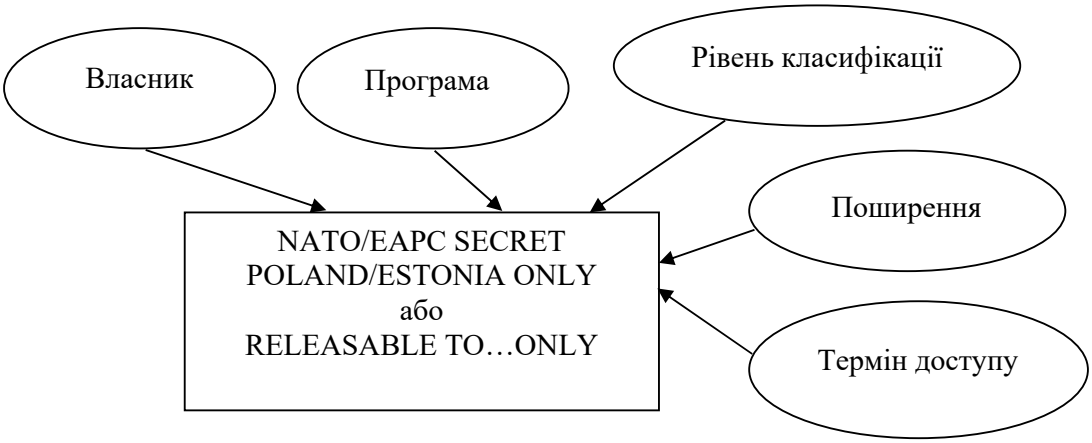

Рис. 8.3. Система маркування класифікованих документів НАТО

Головною метою стандарту є установлення відповідальності за порушення дисципліни поводження з класифікованою інформацією. Тут діють вимоги відслідковувати доступ до підзвітної інформації (хто має, потенційно має або ж мав доступ до підзвітної інформації, хто намагався отримати цей доступ), знати місцезнаходження підзвітної інформації й стежити за рухом підзвітної інформації в межах НАТО й територій держав – членів Альянсу.

Про всі факти порушення політики безпеки потрібно негайно доповідати відповідному органу безпеки. Після цього призначається розслідування факту

порушення, яке проводять особи з досвідом контррозвідувальної роботи й незалежні від тих, хто безпосередньо пов'язаний із фактом порушення.

Наявні такі форми розповсюдження (release)[1] інформації НАТО:

- спорадичне розповсюдження (case by case);
- регулярне (планове) розповсюдження.

Нерегулярне надання інформації здійснюватися щодо спеціально відмічених документів. Регулярне надання інформації може стосуватися наявних документів або тих, які будуть створені. Це надання стосується не конкретних документів, а лише їхніх категорій. Однак категорії документів мають бути визначені з максимальною точністю (предмет, рівень класифікації, джерело тощо).

Кожна держава – член НАТО створює Центральну реєстратуру для інформації з грифом "НАТО/COSMIC. Особливої важливості", яка діє як головний отримуючий і відправляючий державний орган. Крім Центральної реєстратури, в міністерствах, на підприємствах, в агенціях можуть створюватися реєстраційні та контрольні пункти, які діють як відповідальні за внутрішній розподіл інформації з грифами "НАТО/COSMIC. Особливої важливості" та "НАТО/Цілком таємно" і для утримання записів усіх підзвітних документів, що наявні в цих реєстратурах або контрольних пунктах. Вони можуть створюватися в міністерстві, відділі або командних рівнях.

Для інформації з грифами "НАТО/Таємно" і "НАТО/ККК користування" не вимагається реєстрація через систему реєстрації, якщо тільки це не обумовлено Державними правилами й положеннями з питань безпеки.

Військовий комітет НАТО (NAMILCOM) створив систему підзвітності, контролю й розподілу криптографічного матеріалу. Матеріал, який передається через цю систему, не вимагає підзвітності в системі реєстрації.

INFOSEC регулює процедури захисту конфіденційності, цілісності, готовності та звітності щодо інформації, яка передається й обробляється за допомогою інформаційно-комунікаційних технологій. "Попередня директива з INFOSEC", опублікована Комітетом безпеки НАТО й Комітетом політики з питань консультації, командування і контролю, вимагає створення національної організації, відповідальної за заходи фізичної та персональної безпеки в

[1] В оригіналі застосовується термін *release,* що в дослівному перекладі означає "розповсюдження" й приблизно відповідає терміну "доступ", який застосовується в Україні. Однак "розповсюдження" має ширше значення, яке передбачає як регулярне, так і спорадичне ("case by case") надання інформації.

комп'ютерних і комунікаційних мережах. Безпека комунікаційних мереж передбачає криптографічний захист та захист від витоків інформації через випромінювання або еманацію (TEMPEST).

Органами INFOSEC в структурі НАТО є:

1. Управління С3 НАТО.
2. Робоча група INFOSEC у складі NCS.
3. Підкомітет INFOSEC.
4. Командування NACOSA/INFOSEC (відповідає за криптографічний захист та захист від витоків інформації через випромінювання або еманацію – TEMPEST).
5. Установа INFOSEC з акредитації комунікаційного обладнання НАТО – SAA (Security Accreditation Authority).

Національними органами INFOSEC у кожній країні НАТО мають бути:

- національне управління з інформаційно-комунікаційних систем;
- національне представництво з безпеки комунікаційних мереж – NCSA (National Communication Security Authority);
- національне представництво з дистрибуції – NDA (National Distribution Authority);
- національне управління з акредитації комунікаційного обладнання (SAA), визнане НАТО.

Кожна держава – член НАТО установлює Національний орган безпеки комунікаційних систем (NCSA), основні завдання якого полягають у:

- контролі за криптографічною технічною інформацією, яка стосується захисту інформації НАТО в межах власної держави;
- забезпеченні гарантії, що криптографічні системи, продукти та механізми для захисту інформації НАТО ефективно та раціонально відібрані, керовані й підтримувані;
- повідомленні про безпеку комунікаційних систем НАТО та споріднені технічні справи INFOSEC, як цивільні, так і військові, відповідному органу НАТО або державному органу.

Під час передання засобами інформаційно-комунікаційних технологій інформація із грифом "НАТО/Цілком таємно" й вище захищається за допомогою криптографічних методів або продуктів, затверджених Військовим комітетом НАТО (NAMILCOM); із грифом "НАТО/Таємно" і "НАТО/ККК користування"

– із використанням криптографічних методів або продуктів, затверджених Військовим комітетом НАТО (NAMILCOM) чи державою-членом НАТО, за винятком випадків, коли такий метод або продукт спільно консолідований (затверджується NAMILCOM).

Під час передання класифікованої інформації в мережах комунікаційних систем тих держав, які не є членами НАТО, але співпрацюють із ним (NNN/IO), конфіденційність засекреченої інформації з грифом "НАТО/Цілком таємно" й вище захищається за допомогою затверджених Військовим комітетом НАТО криптографічних методів або продуктів. Під час передання в мережах комунікаційних систем NNN/IO конфіденційність засекреченої інформації з грифами "НАТО/Таємно" та "НАТО/ККК користування" захищається з використанням оцінених і затверджених відповідним органом криптографічних методів або продуктів. Таким органом може бути Військовий комітет НАТО, Орган безпеки національних комунікаційних систем держави-члена НАТО або рівнозначний орган NNN/IO, який гарантує, що NNN/IO володіє структурами, процедурами, обладнанням, адекватним для оцінки, відбору, сертифікації й контролю таких методів або продуктів. Такі структури, правила і процедури узгоджуються між НАТО й NNN/IO.

Для захисту від компрометації інформації з грифом "НАТО/Таємно" і вище внаслідок ненавмисного електромагнітного випромінювання передбачається використання заходів безпеки, які мають відповідати ризику використання й точному характеру інформації.

Вимоги щодо промислової безпеки (Industrial Security) унормовують порядок виконання промислових контрактів за замовленнями НАТО, а саме:

1) умови проведення переговорів й отримання дозволу на укладання засекречених контрактів із НАТО;

2) вимоги безпеки щодо класифікованих контрактів НАТО;

3) порядок оприлюднення наявної в контрактах класифікованої інформації НАТО;

4) порядок перевірки промислової безпеки для контрактів НАТО;

5) умови отримання підприємством ліцензій (FSC) на виробництво продукції та послуг за контрактами НАТО;

6) порядок отримання сертифікатів допуску для персоналу підприємств, які виконують контракти з НАТО;

7) умови міжнародного транспортування класифікованих матеріалів за контрактами з НАТО;

8) порядок виконання міжнародних візитів за контрактами з НАТО;

9) порядок залучення позаштатного персоналу для виконання проектів та програм НАТО.

Індустріальна безпека на додаток до стандартних засобів безпеки вимагає створення національних органів індустріальної безпеки, класифікації контрактів з організаціями НАТО, сертифікації обладнання з приводу безпеки, уведення спеціальних заходів для забезпечення безпеки транспортування класифікованих матеріалів та міжнародних візитів. Велика роль при цьому надається національним органам безпеки (NOS), які керують організаціями з виробництва та логістики НАТО (NPLOs) і промисловими проектами НАТО з питань безпеки.

Виконавчими органами NPLO є 12 цивільних агенцій, серед яких CEPMA (центральна європейська система трубопроводів), NAPMA (виробник літаків Авакс), NETMA (виробник літаків Торнадо), NHMO (виробник ракет типу Хаук), NC3A (виробник та консультант з телекомунікаційних систем), NACMA (виробник радарних систем) тощо.

NOS наглядає за упровадженням у ці проекти політики та процедур безпеки, інспектує обладнання для захисту класифікованої інформації у промислових проектах, пов’язаних із НАТО.

Кожна країна – член НАТО, крім NOS, має заснувати необхідну кількість довірчих агенцій безпеки DSA, підпорядкованих NOS і відповідальних за певні галузі у виробництві. NOS та DSA відповідають за впровадження політики безпеки в промисловості, здійснюють лідерство і надають допомогу в питаннях безпеки.

НАТО проводить класифікацію контрактів, що витікають із проектів, замовником яких є структури НАТО. Більшість таких контрактів передбачають наявність субконтрактів, виконавцями яких є численні контрактори. Ці субконтракти також вимагають класифікації, а отже, захисту.

Класифіковані контракти та субконтракти в обов’язковому порядку містять спеціальні інструкції з безпеки – PSI (Project Security Instruction), що визначають повний комплект засобів захисту, які перешкоджають несанкціонованому витоку інформації за межі проекту.

Допуск фізичних осіб до інформації, яка пов'язана з класифікованим промисловим контрактом, здійснює комітет директорів проекту – BOD (Board of Directors).

Перед тим, як підприємство або його службовці, менеджери чи власники отримують доступ до класифікованої інформації або їм буде запропоновано встановлювати ціни, вести переговори і діяти згідно з цим контрактом чи працювати над дослідженнями, які передбачають доступ до інформації з грифом "НАТО/ТАЄМНО" й вище, підприємство має отримати сертифікат допуску (FSC), виданий Національним органом безпеки (NOS). Для контрактів із грифом "НАТО/ККК користування" такий сертифікат не вимагається, якщо тільки це спеціально не обумовлено національними правилами та приписами (положеннями, інструкціями).

Документ C-M(2002)60 (NATO/Unclassified) установлює норми поводження з несекретною інформацією НАТО. Відповідно до політики безпеки НАТО така інформація поділяється на дві категорії:

а) "НАТО/некласифікована, але чутлива" (NATO/Unclassified but sensitive);

б) "НАТО/некласифікована" (NATO/Unclassified).

Згідно з документом C-M(2002)60 до NATO/Unclassified but sensitive належить інформація, що не має ступеня секретності, але має адміністративний гриф або гриф обмеження розповсюдження. Така інформація НАТО може використовуватися лише з офіційною метою й тільки особами, органами або організаціями, яким вона необхідна для офіційних цілей НАТО.

Адміністративні грифи можуть застосовуватися до документів тільки автором, де це необхідно, з метою ідентифікації типу інформації, що міститься в них, та зазначення потреби в обмеженому доступі. Адміністративні грифи НАТО може мати така інформація:

Комерційна (commercial)	Інформація про комерційну власність, наприклад, отримана внаслідок поставки продукції за контрактами НАТО.
Управлінська (management)	Інформація щодо управління та планування, яка має вплив на інтереси НАТО.
Медична (medical)	Інформація щодо медичних доповідей або пов'язані з цим матеріали, які стосуються персоналу та підрозділів НАТО.
Особиста (personal)	Інформація, яка належить фізичній особі або яка їй адресована й рішення щодо оприлюднення якої належить цій фізичній особі.
Щодо штату (staff)	Інформація, що містить посилання на визначеного або невизначеного співробітника(ів).

Наприклад: NATO UNCLASSIFIED-MEDICAL (некласифікована медична інформація НАТО)

Також можуть застосовуватися адміністративні грифи обмеження розповсюдження (передання інформації лише до визначеної групи).

NATO UNCLASSIFIED but sensitive Releasable to OSCE	НАТО НЕКЛАСИФІКОВАНА, але чутлива (лише для OSCE)
NATO UNCLASSIFIED but sensitive EF 2000 Project ONLY	НАТО НЕКЛАСИФІКОВАНА, але чутлива (лише для проекту EF 2000)

Згідно з документом C-M (2002) 60 до інформації "НАТО/Некласифікована" (NATO/Unclassified) належить інформація, яку можна оприлюднювати. Вона не повинна мати жодних грифів.

Подальший розвиток стандартизації в НАТО до недавнього часу не був проблемою. Однак, як свідчить аналіз публікацій, бажання відкрити доступ до НАТО новим членам із Центральної та Східної Європи, надання їм допомогти у трансформуванні їхніх суспільних та військово-політичних структур змушують НАТО повертатися до питань стандартизації.

Фахівці дослідницьких центрів НАТО зазначають, що останній раунд розширення Альянсу призвів до неузгодженості у стандартизації. Майже всі нові члени раніше були або частиною СРСР, або учасниками Варшавського договору. У цих країнах традиційно сильною була централізація та стандартизація. Причому не лише у військово-технічній, але й у промисловій, соціальній і політичних галузях. Альянс, як зазначають спеціалісти дослідницьких центрів, ніколи не сприймав стандарти таким чином: вони приймалися в умовах демократизму. НАТО визнає, що є чимало напрямів трансформації армії та системи безпеки, але для Альянсу краще не намагатися диктувати, а надавати можливість країнам обирати свій шлях, виходячи з економічних можливостей та політико-історичних традицій, які відбивають національні реалії.

Фахівці дослідницьких центрів НАТО зазначають, що для того, щоб бути об'єктивними, стандарти мають бути еквівалентними як для нових, так і для старих членів. На їхню думку, важливо визначити нові параметри стандартизації, що дозволить установлювати реалістичні, досяжні цілі й оцінювати досягнутий рівень безпеки, не порушуючи суверенітет учасників Альянсу.

Викладене вище свідчить, що дослідження та систематизація стандартів НАТО з питань захисту інформації є об'єктивною потребою своєчасності, базою для укладання ефективних угод про взаємний захист інформації з країнами Євросоюзу та НАТО.

8.4. МІЖНАРОДНІ СТАНДАРТИ ЗАХИСТУ ІНФОРМАЦІЇ

Перехід до системи демократичних цінностей, відкритого суспільства, європейська та євроатлантична спрямованість України змушують державу й суспільство звертатися до системи міжнародних стандартів у такій делікатній галузі, як безпека.

Інформація вийшла за межі сфери професійної діяльності мільйонів людей ще тому, що не вугілля, залізо та нафта, а саме вона перетворилась на основне загальнолюдське багатство.

Безумовно, жодне суспільство не може існувати без законодавства та нормативних документів, які регламентують правила, процеси, методи виготовлення й контролю якості товарів, робіт і послуг, а також гарантують безпеку життя, здоров'я й майна людей та навколишнього середовища. Стандартизація якраз і є тією діяльністю, яка виконує ці функції.

Стандартизація – діяльність, що полягає у встановлення положень для загального й багаторазового застосування наявних чи можливих завдань із метою досягнення оптимального ступеня впорядкування в певній сфері, результатом чого є підвищення ступеня відповідності продукції, процесів та послуг їхньому функціональному призначенню; усунення бар'єрів у торгівлі й сприяння міжнародному співробітництву.

Відносини, пов'язані з діяльністю у сфері стандартизації та застосування її результатів, регулюються Законом України "Про стандартизацію" від 17 травня 2001 р. Цей Закон установлює правові та організаційні засади стандартизації в Україні й спрямований на забезпечення єдиної політики в цій сфері.

Об'єктом стандартизації є продукція, процеси та послуги, зокрема матеріали, складники, обладнання, системи, їх сумісність, правила, процедури, форми, методи чи діяльність.

Мета стандартизації в Україні – забезпечення безпеки життя та здоров'я людини, тварин, рослин, а також майна й охорони довкілля, створення умов для раціонального використання всіх видів національних ресурсів та відповідності об'єктів стандартизації своєму призначенню, сприяння усуненню технічних бар'єрів у торгівлі.

Державна політика у сфері стандартизації базується на таких принципах:

- забезпечення участі фізичних і юридичних осіб у розробленні стандартів та вільному виборі видів стандартів при виробництві чи постачанні продукції;
- відкритості та прозорості процедур розроблення і прийняття стандартів з урахуванням інтересів усіх зацікавлених сторін, підвищення конкурентоспроможності продукції вітчизняних виробників;
- доступності стандартів та інформації щодо них для користувачів;
- відповідності стандартів законодавству;
- адаптації до сучасних досягнень науки й техніки з урахуванням стану національної економіки;
- пріоритетності прямого упровадження в Україні міжнародних та регіональних стандартів;
- дотриманні міжнародних та європейських правил і процедур стандартизації;
- участі в Міжнародній (регіональній) стандартизації.

Суб'єктами стандартизації є:

- центральний орган виконавчої влади у сфері стандартизації;
- рада стандартизації;
- інші суб'єкти, котрі займаються стандартизацією.

Залежно від рівня суб'єкта стандартизації, який приймає чи схвалює стандарти, розрізняють:

- національні стандарти, кодекси усталеної практики та класифікатори, прийняті чи схвалені центральним органом виконавчої влади у сфері стандартизації, видані ним каталоги та реєстри загальнодержавного застосування;
- стандарти, кодекси усталеної практики й технічні умови, прийняті чи схвалені іншими суб'єктами, що займаються стандартизацією.

Застосування стандартів чи їх окремих положень обов'язкове:

- для всіх суб'єктів господарювання, якщо це передбачено в технічних регламентах чи інших нормативно-правових актах;

- для учасників угоди (контракту) щодо розроблення, виготовлення чи постачання продукції, якщо в ній (ньому) є посилання на певні стандарти;
- для виробника чи постачальника продукції, якщо він склав декларацію про відповідність продукції певним стандартам чи застосував позначення цих стандартів у її маркуванні;
- для виробника чи постачальника, якщо його продукція сертифікована щодо дотримання вимог стандартів.

Міжнародні стандарти та стандарти інших країн, якщо їхні вимоги не суперечать законодавству України, можуть бути застосовані в Україні в установленому порядку шляхом посилання на них у національних та інших стандартах. Що ж таке ISO? Це міжнародна організація зі стандартизації, котра була заснована в 1947 році (штаб-квартира в Женеві). Першочерговою її метою було створення системи стандартів, яка б сприяла міжнародній торгівлі. Більшість країн світу мають національні представництва та національні комітети в ISO. ISO тісно співпрацює з іншими міжнародними організаціями із стандартизації. У галузі інформаційної безпеки такою організацією є для неї МЕК – Міжнародна електротехнічна комісія, котра була створена ще в 1906 р. для установлення міжнародних стандартів у всіх галузях, пов'язаних з електрикою, електронікою та радіотехнікою.

Саме з цієї причини правильною та повною назвою стандарту є *ISO/IEC 17799 2005 Information Security Management Standard,* тобто стандарт ІСО та МЕК з управління інформаційною безпекою.

ISO взаємодіє не лише з міжнародними спеціалізованими організаціями в галузі стандартизації, але й із найбільшими національними. Наш стандарт теж виник не на порожньому місці – він розроблений на основі британського стандарту BS 7799, що призначений для управління інформаційною безпекою організації незалежно від її сфери діяльності.

Цей стандарт припускає, що служба безпеки, IT-відділ (відділ інформаційних технологій), керівництво компанії повинні працювати відповідно до загального регламенту, незалежно від того, мова йде про захист паперового документообігу або електронних даних.

Останні кілька років ISO 17799 почав упевнено просуватися країнами СНД. У Республіці Білорусі з 1 листопада 2004 р. він став національним державним стандартом. У Молдові завдяки позиції Національного банку всі банки з

2003 року проходять регулярну перевірку на відповідність ISO 17799. У Росії прийняття Держстандарту 17799 відбулося у 2006 році.

Сьогодні стандарт ISO 17799 міцно увійшов у наше життя, ставши на практиці де-факто стандартом побудови систем управління інформаційною безпекою провідних компаній як у Європі та Азії, так і в країнах СНД. До 2005 року навчальний курс, розроблений підприємством Digital Security, був єдиним у СНД курсом із цього стандарту. Вартість навчання на цих курсах – одна − дві тисячі доларів США. До теперішнього часу в країнах СНД пройшло це навчання кілька тисяч фахівців різних компаній, при цьому курс неодноразово проводився в таких містах, як Київ, Дніпропетровськ, Одеса, Кишинів, Рига, Таллінн, Алмати, Ташкент, Москва.

Цікаво розглянути (хоча б оглядово) історію стандарту ISO 17799.

У середині 90-х років Британський інститут стандартів (BSI) за участі комерційних організацій Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica та ін. зайнявся розробленням стандарту управління інформаційною безпекою Так у 1995 р. був прийнятий національний британський стандарт BS 7799 з управління інформаційною безпекою та її організації незалежно від сфери діяльності. Перша частина стандарту мала рекомендаційний характер, друга – була призначена для сертифікації та містила частину обов’язкових вимог, що не входили в першу частину.

Як і будь-який національний стандарт, BS 7799 у період 1995−2000 рр. користувався помірною популярністю лише в рамках країн британської співдружності.

Наприкінці 1999 експерти міжнародної організації зі стандартизації ISO прийшли до висновку, що в рамках стандартів ISO відсутній спеціалізований стандарт управління інформаційною безпекою. Відповідно, ISO було ухвалене рішення не починати розроблення нового стандарту, а за узгодженням із Британським інститутом стандартів, узявши за основу BS 7799:1, прийняти стандарт ISO 17799.

Тому 2000 рік вдихнув нове життя в BS 7799:1, який, ставши ISO 17799, одержав статус міжнародного стандарту, що кардинально змінило розміщення сил і ставлення до стандарту (між локальним і міжнародним стандартом різниця очевидна).

Що ж стосується офіційної сертифікації за ISO 17799, то вона спочатку не була передбачена (повна аналогія із BS 7799). Була визначена тільки сертифікація за BS 7799:2, що становить низку обов'язкових вимог (не увійшли в першу частину BS 7799/ISO 17799). Процедура сертифікації за ISO повинна була з'явитися тільки після виходу в рамках ISO стандарту аналога BS 7799:2 (відзначимо, що це відбулося тільки наприкінці 2005 року з виходом сертифікаційного стандарту ISO 2700).

Лютий 2002 року можна сміливо називати відправною точкою розвитку стандарту ISO 17799 у країнах СНД. У середині 2001 року у світі виникла непроста ситуація в галузі стандартизації з інформаційної безпеки. Існували різні стандарти, застосування яких на практиці викликало питання та серйозні сумніви. Крім того, переважав винятково технологічний підхід фахівців до захищеності (тобто визнавалися лише технічні методи захисту). Питанням організаційно-правового управління безпекою приділялася мінімальна увага. Однак вузьке коло фахівців уважало, що винятково технологічний підхід до захисту інформації – це шлях у нікуди, це ще далеко не все. Тому з'явилося, нарешті, розуміння, що нам усім життєво необхідно виробити єдиний підхід до того, що тепер називається системою управління інформаційною безпекою. І тут у пригоді стає ISO 17799, який спеціалізується саме в питаннях управління інформаційною безпекою.

До кінця 2002 року кількість компаній у світі, що мали сертифікат BS 7799, становила близько 150.

Ставлення до стандарту бізнесових кіл і більшості фахівців-практиків у нашій державі й у всіх інших країнах СНД на той час, як і тепер, визначалося однією фразою: "Ми до цього ще не доросли".

Але незабаром ситуація повністю змінилася: у 2003 році почалося експонентне зростання інтересу до ISO 17799.

Цього ж року Національний банк Молдови почав першим у СНД на практиці застосовувати вимоги стандарту, поставивши за обов'язок усім місцевим банкам виконувати його вимоги, створюючи систему управління інформаційною безпекою на основі ISO 17799.

Через рік чисельність компаній у світі, що одержали офіційний сертифікат, зросла до 350.

Загальна лібералізація ринку інформаційної безпеки привела до того, що Білорусь першою в СНД у листопаді 2004 року прийняла Держстандарт 17799. Аналіз і управління інформаційними ризиками – основа стандарту ISO 17799 – стали активно застосовуватися на практиці.

Більше 1000 компаній у світі одержали офіційний сертифікат. 2004 рік показав тенденцію загального практичного інтересу до стандарту у світі й країнах СНД (Росія, Казахстан, Молдова, Узбекистан, Україна).

Вийшла нова, значно розширена в порівнянні з 2000 роком, редакція стандарту ISO 17799:2005; чисельність компаній у світі, що одержали офіційний сертифікат, зросла до 1800.

Отже, стандарт ISO 17799, заснований на аналізі й управлінні ризиками, зайняв лідируючі позиції в Європі й Азії, став стандартом де-факто в побудові систем управління інформаційною безпекою.

Слід зазначити, що цей напрям одержав подальший розвиток: уперше в рамках ISO з'явився сертифікаційний стандарт ISO 27001. Якщо ISO 17799 обумовлює цілі та методи упровадження в компаніях стандартів інформаційної безпеки, то відповідно до ISO 27001 здійснюється сертифікація.

Стандарт ISO/IEC 27001:2007 був розроблений підкомісією по безпеці (SC 27) Об'єднаного технічного комітету з інформаційної технології (ISO/IEC JTC 1). Новий ISO/IEC 27001:2007 замінив попередню версію стандарту ISO/IEC 17799:2007, що є тепер застарілою. Основний зміст стандарту зберігся, але багато що було повністю перероблене з урахуванням нових інформаційних загроз і викликів безпеки. Крім того, додано новий розділ "Управління інцидентами інформаційної безпеки".

Стандарт ISO/IEC 17799:2000 складається з 13 розділів:

1. Загальна частина.
2. Терміни та визначення.
3. Політика безпеки.
4. Організаційні методи забезпечення інформаційної безпеки.
5. Управління ресурсами.
6. Користувачі інформаційної системи.
7. Фізична безпека.
8. Управління комунікаціями та процесами.
9. Контроль доступу.

10. Придбання, розробка та супровід інформаційних систем.
11. Управління інцидентами інформаційної безпеки.
12. Управління безперервністю ведення бізнесу.
13. Відповідність вимогам.

Кожен із розділів має таку структуру:

1. Мета – вказує, яка мета повинна бути досягнута.
2. Управління – визначає цілі, які можуть бути досягнуті.
3. Керівництво – вказує, як управління може бути реалізовано.
4. Примітки – подаються корисні зауваження та пояснення.

ISO/IEC 17799:2000 призначений для використання будь-якою організацією (в тому числі українською), що допускає встановити систему ефективного інформаційного захисту або поліпшувати наявні методи інформаційного захисту.

Разом із тим, це означає, що всі рекомендації стандарту повинні бути безумовно прийняті в нашій державі. Все залежить від конкретних місцевих інформаційних ризиків та вимог.

Таким чином, міжнародний стандарт ISO 17799 містить рекомендації з управління інформаційною безпекою, призначені для співробітників, відповідальних за створення, впровадження й підтримку заходів, які забезпечують безпеку на державному підприємстві або в недержавній організації. Рекомендації, наведені в проаналізованому стандарті, слід виконувати з урахуванням чинних українських законів і нормативних вимог. Він повинен послужити основою для розроблення стандартів безпеки й ефективних методів управління безпекою в конкретній організації. Крім того, цей стандарт допоможе підтримати взаємну довіру при контактах між українськими організаціями.

Міжнародний стандарт ISO / IEC 27001:2005 Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Вимоги (Information technology. Security techniques. Information security management systems. Requirements) є одним із найбільш відомих стандартів у галузі захисту інформації.

Він установлює вимоги до розроблення, впровадження, функціонування, моніторингу, аналізу, підтримання та вдосконалення документованої Системи менеджменту інформаційною безпекою (далі – СМЗІ) в контексті бізнес-ризиків організації. Вимоги цього стандарту мають загальний характер і мо-

жуть бути застосовані до всіх організацій незалежно від їх типу, розміру, форми власності.

ISO / IEC 27001:2005 може використовуватися для захисту будь-яких видів інформації, включаючи фінансову, кадрову, будь-які інші дані компанії і, що важливо, інформацію, що належить партнерам / клієнтам – одним словом, все, що є значущим інформаційним активом будь-якої компанії, і все, що уразливе стосовно загроз безпеці. Таким чином, основну мету Стандарту можна сформулювати як створення загальної методології для розроблення, впровадження та оцінки ефективності СМЗІ, застосовну в умовах як комерційних компаній, так і державних і некомерційних структур.

ISO / IEC 27001:2005 має такі розділи:

1. Вступ.
2. Галузі застосування.
3. Нормативні посилання.
4. Терміни та визначення.
5. Системи менеджменту захисту інформації.
6. Відповідальність керівництва.
7. Внутрішні аудити СМЗІ.
8. Управлінський аналіз СМЗІ.
9. Вдосконалення СМЗІ.

Крім цього, ISO / IEC 27001:2005 “Інформаційні технології. Методи захисту. Системи менеджменту захисту інформації. Вимоги” містить три додатки.

Стандарт ISO / IEC 27001:2005 установлює процесний підхід для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримки в робочому стані й поліпшення СМЗІ організації.

Процесний підхід до менеджменту захисту інформації, представлений у цьому міжнародному стандарті, допомагає користувачам підкреслити важливість:

1) розуміння вимог захисту інформації та потреби встановити політику й цілі для захисту інформації організації;

2) засобів реалізації та управління ризиками для менеджменту організації, пов’язаних із захистом інформації, в контексті загальних ділових ризиків організації;

3) постійного контролю та аналізу якості виконання й результативності СМЗІ;

4) безперервного поліпшення, заснованого на об'єктивному вимірі.

Цей міжнародний стандарт приймає модель "Plan-Do-Check-Act" (PDCA), яка застосовується для структуризації всіх процесів СМЗІ.

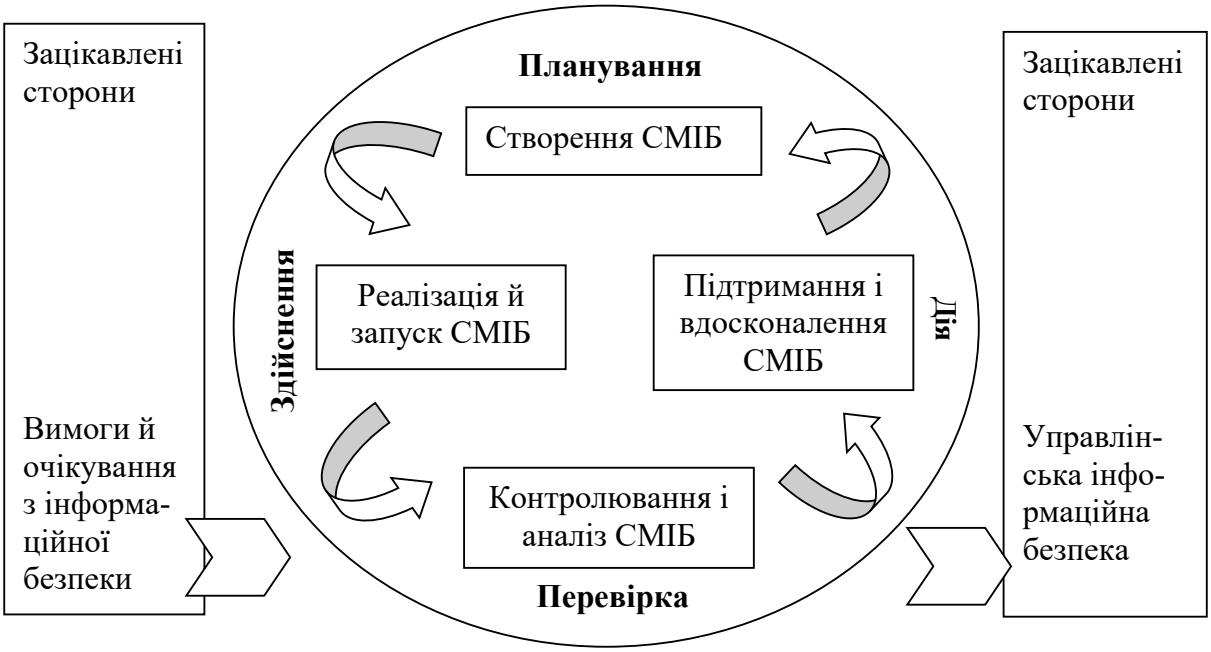

Рис 8.4. Модель PDCA, застосована до процесів СМЗІ

Прийняття СМЗІ має бути стратегічним рішенням для організації. Для розроблення СМЗІ організація повинна виконати такі кроки:

1. Визначити галузь застосування СМЗІ.
2. Розробити політику інформаційної безпеки.
3. Визначити (розробити) підхід до оцінювання ризиків.
4. Ідентифікувати ризики.
5. Проаналізувати та оцінити ризики.
6. Прийняти рішення з оброблення ризиків:

- застосувати до ризику відповідні засоби управління;
- прийняти ризик відповідно до розроблених критеріїв прийняття ризиків;
- піти від ризику (уникнути ризику);
- передати ризик іншій стороні (наприклад, страховій компанії, провайдеру).

7. Вибрати засоби управління, які можна застосувати для зменшення ризиків. При виборі засобів управління повинні враховуватися критерії прийняття ризиків, законодавчі, договірні вимоги.

8. Отримати згоду керівництва за залишковими ризиками.

9. Підготувати Положення про застосовність – один з обов'язкових документів СМЗІ.

Організація для постійної придатності, адекватності й результативності повинна проводити внутрішні аудити СМЗІ через заплановані інтервали з метою визначення:

1) чи відповідає вимогам цього міжнародного стандарту законодавство конкретної країни;

2) чи відповідають стандарти виявленим вимогам захисту інформації тощо.

Програма аудиту повинна бути спланована з урахуванням статусу та важливості процесів і галузей, які потрібно перевіряти, а також результатів попередніх аудитів.

Крім того, керівництво повинно аналізувати СМЗІ організації через заплановані інтервали та проводити коригувальні дії. Тобто організація має проводити дії з усунення причин невідповідності вимогам СМЗІ для того, щоб запобігати повторенню. Задокументована методика для коригуючих дій повинна визначати вимоги для:

1) виявлення невідповідностей;

2) визначення причин невідповідностей;

3) оцінювання потреби в діях, щоб гарантувати, що невідповідності не виникнуть знову;

4) визначення та реалізації потрібних коригувальних дій;

5) записування результатів виконаних дій;

6) аналізу проведеної коригуючої дії.

Основною перевагою, що досягається при впровадженні стандарту ISO / IEC 27001:2007, є сертифікація на відповідність стандарту, яка дозволяє наочно показати діловим партнерам, інвесторам і клієнтам, що в організації налагоджено ефективне управління захистом інформації.

Міжнародний стандарт ISO / IEC 27002:2005 Інформаційні технології. Методи забезпечення безпеки. Практичні правила для захисту інформації (Information technology. Security techniques. Code of practice for information

security management) є міжнародно визнаним стандартом практики для забезпечення захисту інформації. Сотні тисяч організацій у всьому світі користуються ISO / IEC 27002.

Нинішній стандарт є переглядом версії вперше опублікованого в ISO / IEC у 2000 р., який був дослівною копією британського стандарту (BS) 7799-1:1999.

ISO / IEC 27002:2005 нині також переглядається паралельно із ISO / IEC 27001, ISO / IEC JTC1/SC27. Численні зауваження і пропозицій щодо поліпшення ISO / IEC JTC1/SC27 обговорювалися на зустрічі в Пекіні в травні 2009 року, на засіданні Редмонд у листопаді 2009 року. На сьогодні ISO / IEC 27001:2005 має такі розділи:

- Вступ.
- Галузь застосування.
- Терміни та визначення.
- Структура цього стандарту.
- Оцінка ризику.
- Політика безпеки.
- Організовані методи забезпечення захисту інформації.
- Управління активами.
- Питання безпеки, пов’язані з персоналом.
- Фізичний захист і захист від загроз навколишнього середовища.
- Управління передачею даних і операційною діяльністю.
- Контроль доступу.
- Інформаційні системи придбання, розробки і супроводження.
- Захист інформацій управління інцидентами.
- Управління безперервністю бізнесу.
- Відповідність вимогам.

У стандарті уміщено досить добре структурований набір заходів контролю для усунення ризиків захисту інформації, що охоплюють конфіденційність, цілісність та доступність. Організації, які беруть участь у ISO / IEC 27002, повинні оцінювати свої ризики захисту інформації й уживати належних заходів щодо контролю, використовуючи стандартні вимоги для керівництва.

Також визначається політика безпеки. Опис політики захисту інформації повинен бути схвалений керівництвом, опублікований і за необхідності розповсюджений серед усіх співробітників. Цей документ має виражати підтримку

керівництва компанії й визначати підхід до управління захистом інформації, що буде застосовуватися в організації. Як мінімум цій документ повинен включати такі відомості:

1. Визначення захисту інформації, її загальних цілей і галузей дії, а також відомостей про важливість безпеки як механізму, що робить можливим спільне використання інформації.

2. Заяву про наміри керівництва, яка висвітлює цілі й принципи управління захистом інформації.

3. Короткий опис політики безпеки, принципів, стандартів і нормативних вимог, що мають певне значення для організації, наприклад:

- відповідність вимогам законодавства й умовам контрактів;
- вимоги до освітньої підготовки в галузі безпеки;
- захист від вірусів й інших зловмисних програм;
- підтримання безперервності бізнесу;
- наслідки порушення політики безпеки.

4. Визначення загальних і приватних обов'язків з управління захистом інформації, у тому числі надання відомостей про інциденти.

5. Посилання на документацію, що може доповнювати опис політики, наприклад, більш докладні описи політик й інструкцій для конкретних інформаційних систем або правила безпеки, яких повинні дотримуватися користувачі. Цей опис політики необхідно поширити серед користувачів у всій організації в прийнятному для них вигляді.

Слід призначити співробітника, відповідального за підтримання політики та її оновлення відповідно до прийнятої процедури.

Важливим аспектом, що регулює цей стандарт, є контроль доступу до інформації, а саме реєстрація користувачів. Необхідна формалізована процедура реєстрації та зняття з реєстрації користувачів щодо надання доступу до всіх багатокористувальних інформаційних систем і сервісів.

Доступ до багатокористувальних інформаційних сервісів має бути контрольованим за допомогою формалізованого процесу реєстрації користувачів, який повинен включати:

- використання унікальних ідентифікаторів або імен (ID) користувачів таким чином, щоб дії у системі можна було б зіставити з користувачами та

встановити відповідальних. Використовувати групові ID слід тільки якщо це необхідно, з урахуванням особливостей виконуваної роботи;

- перевірку того, що користувач має авторизацію від власника системи на користування інформаційною системою або сервісами. Крім того, може бути доцільний додатковий дозвіл на надання прав від керівництва;
- перевірку того, що рівень наданого доступу відповідає виробничій необхідності, а також ураховує вимоги політики безпеки організації, наприклад, не порушує принципу розподілу обов'язків;
- надання користувачам письмового документа, в якому вказані їх права доступу;
- вимогу того, щоб користувачі підписували документ про те, що вони розуміють умови надання доступу;
- забезпечення впевненості в тому, що постачальники послуг не надають доступу, доки процедури авторизації не завершені;
- ведення формалізованого обліку щодо всіх осіб, зареєстрованих для використання сервісів;
- негайне скасування прав доступу користувачів, у яких змінилися посадові обов'язки або які звільнилися з організації;
- періодичну перевірку й видалення надлишкових користувачевих ID і облікових записів;
- забезпечення того, щоб надлишкові для користувача ID не були передані іншим користувачам.

Міжнародний стандарт ISO / IEC 27004:2009 Інформаційні технології. Методи забезпечення безпеки. Системи управління захистом інформації. Вимірювання (Information technology. Security techniques. Information security management. Measurement) містить інформацію щодо вимірів безпеки, управління, як правило, відомих як метрики безпеки.

Цей стандарт був опублікований у грудні 2009 року, містить рекомендації щодо розроблення та вжиття заходів і вимірювань із метою оцінювання ефективності СМЗІ. У ньому також містяться рекомендації щодо заходів і показників для контролю або груп контролю. Всі поради й рекомендації в рамках ISO / IEC 27004:2009 призначені для використання в рамках ISO / IEC 27001.

Цей міжнародний стандарт передбачає, що відправною точкою при розробленні заходів і вимірюванні є чітке розуміння ризиків захисту інформації, з

якими організація стикається, і щоб діяльність із організації в оцінюванні ризиків була виконана правильно (тобто на основі стандарту ISO / IEC 27005).

ISO / IEC 27004:2009 має такі розділи:

- Вступ.
- Сфера застосування.
- Нормативні посилання.
- Терміни та визначення.
- Структура цього міжнародного стандарту.
- Вимірювальний огляд захисту інформації.
- Управлінські функції.
- Заходи і вимірювання розвитку.
- Вимірювання операції.
- Аналіз даних та результатів вимірювань звітності.
- Вимірювання захисту інформації. Програма оцінки і вдосконалення.

Крім згаданих вище розділів, містяться два додатки із шаблонами та прикладами вимірювання захисту інформації.

Цей стандарт досить докладно описує з точки зору механіки вимірювання процесів: як ретельно збирати “базу показників”, агрегацію використання та математичні розрахунки, щоб генерувати “похідні показники”, а потім застосовувати аналітичні методи й критерії рішення для створення “показників”, які використовуються для цілей СМЗІ.

ISO / IEC 27004:2009 Інформаційні технології. Методи забезпечення безпеки. Системи управління захистом інформації. Вимірювання дає рекомендації щодо таких основних видів діяльності для організації виконання вимірювань відповідно до вимог, зазначених у ISO / IEC 27001:

- розроблення заходів (тобто заходів бази, похідних показників і показників);
- упровадження та забезпечення функціонування інформаційної безпеки вимірювань програмою;
- збирання й аналіз даних;
- обговорення результатів вимірювань із відповідними зацікавленими сторонами;
- використання результатів вимірювань для визначення потреб у поліпшенні функціонування СУІБ, включаючи політику, цілі, засоби управління процесами і процедурами;

•сприяння постійному вдосконаленню вимірювання програм захисту інформації.

Використання цього стандарту створює можливості для виявлення сфер, що потребують поліпшення, скороченню витрат і збільшенню ефективності.

Хоч в Україні поки що немає офіційного перекладу цих стандартів українською мовою, але багато вітчизняних компаній і фірм на практиці впроваджують та застосовують вимоги цих стандартів. Із кожним днем таких компаній і фірм стає все більше. Як правило, в Україні компанії починають виділяти кошти на формування СМЗІ з таких причин:

• компанії досягли певного рівня розвитку, коли без СМЗІ неможливе їхнє стабільне функціонування;

• компанії зазнали відчутних втрат від неефективного управління захистом інформації;

• інвестори потребують усебічного захисту бізнесу. Приміром, у банківській сфері обсяг замовлень на послуги з установлення захисту інформації різко виріс більше року тому, коли власники фінансових установ стали готувати їх до продажу. Відчутний сплеск інтересу компаній до сфери управління безпекою очікується в найближчі півроку, оскільки багато вітчизняних компаній зараз активно готується до залучення інвестицій.

Більше 80 % закордонних підприємств проводять спеціалізовані аудити для визначення слабких місць своїх систем управління захисту інформації, що дозволяє їх оперативно оновлювати. У нас таких компаній дуже мало, хоча останнім часом спостерігається тенденція до збільшення їх кількості.

Надавати комплексні послуги із захисту інформації українські компанії почали у 2002 році. Однією з перших стала “БМС Консалтинг”, у якої уже був багатий досвід з упровадження інформаційних систем, але не було навичок роботи із системами безпеки. Оскільки тоді в Україні не було фахівців у сфері захисту інформації, компанія відправляла своїх співробітників на навчання до Європи, США та Росії. Сьогодні в Україні функціонує безліч організацій із навчання спеціалістів на основі ISO / IEC 27001:2005, ISO / IEC 27002:2005, ISO / IEC 27004:2009 та інших міжнародних стандартів у сфері захисту інформації (наприклад, навчальні семінари компанії InfoSafe).

Важливою подією стала спільна прес-конференція, що відбулася 3 жовтня 2006 р. в Навчальному центрі “AM-SOFT” із нагоди першого в історії українського бізнесу вручення сертифікату відповідності міжнародному стандарту

інформаційної безпеки ISO / IEC 27001:2005. Цей документ був наданий компанії "Арт-майстер" по закінченню сертифікаційного аудиту, проведеного Міжнародним технічним товариством БЮРО ВЕРІТАС. Після цього чисельність організацій, сертифікованих за стандартом ISO / IEC 27001:2005, збільшилося на третину, і ця тенденція за прогнозами збережеться мінімум до 2012 року.

Сертифікація на відповідність стандарту ISO 27001:2005 забезпечує компанії такі переваги:

- партнери й клієнти бачать, що вимоги до безпеки дотримані, а компанія демонструє прагнення зменшити ризики;
- компанія отримує можливість відслідковувати процес виконання політики безпеки (знаходити й усувати слабкі місця в системі захисту інформації);
- забезпечується ефективне управління системою в критичних ситуаціях;
- досягається зниження й оптимізація вартості підтримки системи безпеки;
- полегшуються інтеграція підсистеми безпеки в бізнес-процеси та приєднання до ISO9001: 2000;
- сертифікація дозволить переконатися в тому, що система управління інформаційною безпекою правильно розроблена, впроваджена і зумовлює реальні поліпшення в компанії.

Запитання і завдання для самоперевірки

1. Як тлумачать поняття "політика інформаційної безпеки" в НАТО і ЄС?
2. Назвіть основні принципи політики інформаційної безпеки в НАТО і ЄС.
3. Дайте визначення поняття "інформація з обмеженим доступом НАТО".
4. Охарактеризуйте основні мінімальні стандарти НАТО і ЄС.
5. Покажіть, як законодавчі акти країн НАТО та ЄС відповідають фундаментальним основам політики безпеки НАТО.
6. Розкрийте моделі, які втілені у двох типах законодавчих актів і двох формах організаційно-правового регулювання захисту інформації з обмеженим доступом, прийнятих у країнах НАТО і ЄС.
7. Назвіть закони й основні підзаконні нормативно-правові акти в галузі захисту інформації в країнах НАТО і ЄС.
8. Спробуйте зіставити Закон України "Про державну таємницю" із стандартами країн НАТО і ЄС у галузі захисту інформації.

9. Охарактеризуйте міжнародні стандарти у сфері захисту інформації з обмеженим доступом (на прикладі 27001).

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексеев С.С. Право на пороге третьего тысячелетия: некоторые тенденции мирового правового развития – надежда и драма современной эпохи / С.С.Алексеев. – М. : Изд-во “Юрист”, 2000. – 285 с.

2. Алексеев С.С. Право: азбука – теория – философия: опыт комплексного исследования / С.С.Алексеев. – М. : Изд-во “Юрист”, 1999. – 193 с.

3. Алексенцев А.И. Конфиденциальное делопроизводство / А.И.Алексенцев. – М. : ЗАО “Бизнес-школа Интел-Синтез”, 2001. – 156 с.

4. Анисимцев Н.В. Конституционные проблемы современной Японии / Н.В.Анисимцев // Право и политика. – 2001. – № 2. – С. 62−71.

5. Апаров Т.В. Суды и судебный процесс Великобритании: Англия, Уэльс, Шотландия / Т.В.Апаров. – М. : Изд-во “Триада”, 1996. – 143 с.

6. Артемов В.Ю. Особистісно-орієнтований підхід та модель світу інформаційного аналітика / В.Ю.Артемов // Педагогічний процес. – 2005. – № 2. – С. 15−22.

7. Артемов В.Ю. Реалізація головних засад захисту інформації з обмеженим доступом у внутрішньому праві країн – членів НАТО / В.Ю.Артемов // Наук. вісн. Ужгородського нац. ун-ту. – 2005. – Вип. № 4. – С. 149−153.

8. Артемов В.Ю. Захист інформації з обмеженим доступом в країнах НАТО (на прикладі Чехії і Словаччини) / В.Ю.Артемов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. – Вип. 11. – С. 60−63.

9. Артемов В.Ю. Організаційно-правові засади захисту інформації з обмеженим доступом НАТО / В.Ю.Артемов // Держава і право : зб. наук. праць. – К. : Ін-т держави і права ім. В.М.Корецького НАН України. – 2006. – Серія 32. – Вип. 18. − С. 174−179.

10. Артемов В.Ю. Загальна характеристика основних нормативних документів, що регламентують питання охорони державної таємниці в країнах – членах НАТО / В.Ю.Артемов // Господарство, підприємство і право. – 2006. – № 10. – С. 67−74.

11. Артемов В.Ю. Організаційно-правові засади захисту інформації з обмеженим доступом в інформаційно-комунікаційних мережах НАТО : тези доп. / В.Ю.Артемов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. − 1−3 березня. – С. 1−22.

12. Артемов В.Ю. Порівняння організаційно-правових норм захисту інформації з обмеженим доступом країн – членів НАТО : навч.-метод. посіб. / В.Ю.Артемов. – К. : Вид-во “КНТ”, 2007. – 171 с.

13. Балыбердин А.Л. Государственная тайна в Российской Федерации / А.Л.Балыбердин, М.А.Вус, В.Н.Рябчук // Вопросы защиты информации. – 2002. – № 1. – С. 14−23.

14. Балыбердин А.Л. Государственная тайна или государственные секреты? / А.Л.Балыбердин // Вопросы защиты информации. – 1994. – № 1. – С. 3−11.

15. Бартошок М. Римское право: понятие, термины, определения / М.Барташок ; пер. с чешского. – М. : Изд-во “Знание”, 1989. – 160 с.

16. Бачило И.Л., Информационное право : учебн. для ВУЗов / И.Л.Бачило, В.Н.Лопатин, М.А.Федотов ; под ред. Б.Н.Топорнина. – М. : Изд-во Юридический центр “Пресс”, 2001. – 789 с.

17. Бахин С.В. Интегральные конвенции как способ унификации национального законодательства / С.В.Бахин // Господарство, підприємство і право. – 2003. – № 7. – С. 73−79.

18. Белов Г.В. Концептуальные основы правового обеспечения информатизации России / Г.В.Белов, И.Л.Бачило, В.А.Копылов // Проблемы информатизации. – 1992. – Вып. 2. – С. 36−42.

19. Берман Г.Дж. Западная традиция права: эпоха формирования / Г.Дж.Берман. – М. : Изд-во “Юрист”, 1994. – 198 с.

20. Бернхем В. Вступ до права та правової системи США / В.Бернхем. – К. : Вид-во “Основи”, 1999. – 206 с.

21. Боботов С.В. Правосудие во Франции / С.В.Боботов. – М. : Изд-во “ЕАВ”, 1998. – 256 с.

22. Боботов С.В. Введение в правовую систему США / С.В.Боботов, И.Ю.Жигачев. – М. : Изд-во “ЕАВ”, 1997. – 189 с.

23. Богдановская И.Ю. Закон в английском праве / И.Ю.Богдановская. – М. : Изд-во “Знание”, 1987. – 56 с.

24. Богдановская И.Ю. Судебный прецедент как категория общего права / И.Ю.Богдановская // Право и политика. – 2002. – № 7 (31). – С. 18−23.

25. Бойцова Л.В. Будущее сравнительного права: возможности двадцать первого века / Л.В.Бойцова, В.В.Бойцова // Юридический мир. – № 4. – 2002. – С. 17−25.

26. Божков І.І. Державна таємниця та система її охорони / І.І.Божков // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : МОН України, НТУУ “КПІ”, ДСТСЗІ. – 2001. – № 4. – С. 7−10.

27. Большой юридический энциклопедический словарь / [под ред. А.Б.Барихина]. – М. : Изд-во “Книжный мир”, 2006. – 720 с.

28. Бондаренко І. Адаптація законодавства України до європейського законодавства – один з пріоритетних напрямів реформування правової системи України / І.Бондаренко // Право України. – № 7. – 2002. – С. 63−65.

29. Борко Ю.А. Европейское право ВУЗам / Ю.А.Борко. – М. : Изд-во “Юрист”, 1998. – 237 с.

30. Будаков М.О. Організаційно-правові засади діяльності спеціальних служб держав НАТО : моногр. / М.О.Будаков. – К. : Вид-во НА СБ України, 2004. – 188 с.

31. Введение в шведское право. – М. : Изд-во “Знание”, 1986. – 78 с.

32. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI сторіччя // Юридичний вісник. – 2000. – С. 23−35.

33. Вус М.А. К вопросу об информационной безопасности государства / М.А.Вус // Вопросы защиты информации. – 2000. – № 3. – С. 14−23.

34. Гавердовский А.С. Противоправность колониализма по современному международному праву : автореф. дисс. на соискание учен. степени канд. юрид. наук / А.С.Гавердовский. – К. : Ун-т им. Т.Г.Шевченко, 1969. – 26 с.

35. Герасименко В.А. Организация комплексной защиты информации на современных объектах / В.А.Герасименко // Вопросы защиты информации. – 1993. – № 1(24). – С. 12−16.

36. Гвирцман М.В. Правовое регулирование банковской тайны / М.В.Гвирцман // Деньги и кредит. – 1992. – № 6. – С. 24−27.

37. Ефимова Л.Г. Банковская тайна: сравнительный аспект / Л.Г.Ефимова // Бизнес и банки. – 1991. – № 46. – С. 27−31.

38. Гиленсен В.М. Федеральное бюро расследований США, 1908–1939 гг. / В.М.Гиленсен. – М. : Политиздат, 1979. – 135 с.

39. Голубєв В.О. Інформаційна безпека: проблеми боротьби зі злочинами в сфері використання комп'ютерних технологій : моногр. / В.О.Голубєв, В.Д.Гавловський, В.С.Цимбалюк ; за заг. ред. Р.А.Калюжного. – Запоріжжя : "Просвіта", 2001. – 252 с.

40. Гончаров Д. О банковской и коммерческой тайне / Д.Гончаров // Законность. – 2000. – № 1. – С. 52–57.

41. Горбулін В.П. Обраний внутрішньо- та зовнішньополітичний курс залишиться незмінним / В.П.Горбулін // Україна – НАТО : інформ.-аналіт. журн. Інформаційного центру з питань євроатлантичної інтеграції. – 2006. – № 5 (11). – С. 4−6.

42. Поступ України до інформаційного суспільства (організаційно-правовий аспект) / В.Гриценко, В.Гавловський, В.Цимбалюк, Р.Ковпак // Науковий вісник. – Ірпінь, 2001. – № 3 (13). – С. 184−187.

43. Інформаційне право України: концептуальні основи формування / В.В.Гриценко, Р.А.Калюжний, В.Д.Гавловський, В.С.Цимбалюк // Науковий вісник Дніпропетровського інституту МВС України : зб. наук. праць. – 2001. – № 3. – С. 234−244.

44. Щодо питань реформування законодавства України в сфері суспільних інформаційних відносин / В.М.Гуцалюк, Р.А.Калюжний, В.Д.Гавловський,

В.С.Цимбалюк // Проблеми боротьби з корупцією, організованою злочинністю та контрабандою. – К. : Ін-т “Проблеми людини”, 2001. – С. 378−384.

45. Інформаційному суспільству України інформаційне законодавство (щодо питань реформування законодавства в сфері суспільних інформаційних відносин) / М.Гуцалюк, Р.Калюжний, В.Гавловський, В.С.Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : НТУУ “КПІ”, 2001. – № 2. – С. 7−11.

46. Давид Р. Основные правовые системы современности / Р.Давид, К.Жоффре-Спинози. – М. : Изд-во “Юрист”, 1996. – 123 с.

47. Дайси А.В. Основы государства и права Англии / А.В.Дайси. − М. : Изд-во “Юрист”, 1997. – 135 с.

48. Дженкинс Э. Английское право / Э.Дженкинс // Аннерс Э. История европейского права. – М. : Изд-во “Юрист”, 1996. – 97 с.

49. Дундуков М.Ю. Разведка США: правовое регулирование организации и деятельности / М.Ю.Дундуков. – Калуга : Калужский ЦНТИ, 2002. – 274 с.

50. Дріжчаний І.П. Зовнішні фактори впливу на формування державної безпеки України в умовах геополітичної перебудови світу / І.П.Дріжчаний // Україна – НАТО : інформ.-аналіт. журн. – 2006. – № 5(11). – С. 11−14.

51. Закон України “Про захист інформації в автоматизованих системах” // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 287.

52. Закон України “Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави” // Відомості Верховної Ради України. – 2003. – № 46. – Ст. 366.

53. Закон України “Про державну таємницю” // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

54. Закон України “Про оперативно-розшукову діяльність” // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.

55. Закон України “Про контррозвідувальну діяльність” // Відомості Верховної Ради України. – 2003. – № 12. – Ст. 89.

56. Закон України “Про розвідувальні органи України” // Відомості Верховної Ради України. – 2001. – № 19. – Ст. 94.

57. Закон України “Про Службу зовнішньої розвідки України” // Відомості Верховної Ради України. – 2006. – № 8. – Ст. 94.

58. Закон України “Про Службу безпеки України” // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.

59. Інформатизація, право, управління (організаційно-правові питання) : моногр. / [Р.А.Калюжний, О.Д.Крупчан, В.Д.Гавловський та ін.] ; за ред. М.Я.Швеця, О.Д.Крупчана. – К. : НДЦ правової інформатики АПРНУ, 2002. – 191 с.

60. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики : моногр. / [Р.А.Калюжний, В.О.Шамрай, В.Д.Павловський та ін.] ; за ред. Р.А.Калюжного, В.О.Шамрая. – К. : АДПС України, 2002. – 296 с.

61. Иностранное конституционное право / [под ред. В.В.Маклакова]. – М. : Изд-во “Знание”, 1996. – 237 с.

62. Калюжний Р. Питання кодифікації законодавства України про інформацію з обмеженим доступом / Р.Калюжний, В.Гавловський, В.С.Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУУ “КПІ”. – 2001. – № 3. – С. 35−38.

63. Карташев Д.А. Система систем. Очерки общей теории и методологии / Д.А.Карташев. – М. : Изд-во “Прогресс – Академия”, 1995. – 221 с.

64. Керимов Д.А. Законодательная техника / Д.А.Керимов. – М. : Изд-во “Знание”, 1998. – 154 с.

65. Климчук С.О. Становлення нормативно-правової бази Фінляндії, яка регулює захист інформації з обмеженим доступом, у сфері міждержавної співпраці / С.О.Климчук, В.Ю.Артемов // Юридичний вісник. – К. : Вид-во “Юстиніан”, 2006. – № 4 (96). – С. 79−81.

66. Климчук С.О. Законодавчі проблеми захисту інформації з обмеженим доступом в комп’ютерних мережах / С.О.Климчук, В.Ю.Артемов // Економіка і право : науковий часопис НПУ ім. М.Драгоманова. – 2006. – № 4. – С. 45−49.

67. Климчук С.О. Організаційно-правові засади захисту інформації в автоматизованих системах Німеччини / С.О.Климчук, В.Ю.Артемов // Юридичний вісник. – К. : Вид-во “Юстиніан”, 2006. – № 5 (96). – С. 50−52.

68. Кнапп В. Крупные системы права в современном мире / В.Кнапп // Сравнительное правоведение. – М. : Изд-во “Знание”, 1978. – С. 230−237.

69. Комаров А.С. Источники права Швеции / А.С.Комаров // Советское государство и право. – 1986. – № 6. – С. 92−102.

70. Королев Е.Н. Некоторые пути обеспечения информационной безопасности в процессе подготовки и реализации международных договоров и соглашений по контролю за военной деятельностью / Е.Н.Королев, С.С.Лютиков, В.С.Никифоров // Вопросы защиты информации. – 1995. – № 2. – С. 12−14.

71. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

72. Конституции государств Европейского Союза / [под. ред. Л.А.Окунькова]. – М. : ИНФРА-М, НОРМА, 1997. – 816 с.

73. Конституции зарубежных государств: США, Великобритания, Франция, Германия, Италия, Япония, Канада / [под ред. В.В.Маклакова]. – М. : Изд-во “БЕК”, 1996. – 432 с.

74. Конституционное право развивающихся стран. Общество, власть и личность. – М. : Изд-во “Знание”, 1990. – 178 с.

75. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : моногр. / Б.А.Кормич. – Одеса : Вид-во “Юрид. література”, 2003. – 472 с.

76. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня д-ра юрид. наук : 12.00.07 / Б.А.Кормич. – Х. : Вид-во НХУ України, 2004. – 27 с.

77. Кормич Б.А. Інформаційна безпека: організаційно-правові основи : навч. посіб. / Б.А.Кормич. – К. : Кондор, 2004. – 384 с.

78. Кормич Б.А. Національна безпека як правова категорія аналізу митної діяльності держави / Б.А.Кормич // Актуальні проблеми політики : зб. наук. праць. – Одеса : Юридична література, 2001. – Вип. 10. – С. 56−61.

79. Кормич Б.А. Засади правового захисту національної безпеки в сфері зовнішньоекономічних відносин / Б.А.Кормич // Актуальні проблеми політики : зб. наук. праць. – Одеса : Вид-во “Юрид. літ-ра”, 2001. – Вип. 11. – С. 732−738.

80. Кормич Б.А. Співвідношення національної безпеки та національних інтересів / Б.А.Кормич // Вісник університету внутрішніх справ. – Х., 2001. – Вип. 13. – С. 71−76.

81. Кормич Б.А. Захист інтелектуальної власності в аспекті захисту інформаційної безпеки України / Б.А.Кормич // Актуальні проблеми політики : зб. наук. праць. – Одеса, 2001. – Вип. 12. – С. 177−181.

82. Кормич Б.А. Деякі проблеми інформаційної безпеки в Україні / Б.А.Кормич // Держава і право : зб. наук. праць. – К. : Ін-т держави і права ім. В.М.Корецького НАН України, 2001. – Вип. 14. – С. 180−185.

83. Кормич Б.А. Проблеми судового захисту інформаційної безпеки в Україні / Б.А.Кормич // Актуальні проблеми політики : зб. наук. праць. – Вип. 14. – Одеса : Вид-во "Юрид. література", 2001. – С. 430−435.

84. Кормич Б.А. Поняття національної безпеки та проблеми її нормативно-правового регулювання / Б.А.Кормич // Наукові праці Одеської національної юридичної академії. – Одеса : Вид-во "Юрид. література", 2002. – Т. 1. – С. 190−199.

85. Кормич Б.А. Класифікація видів інформаційної безпеки / Б.А.Кормич // Митна справа : наук.-аналіт. журн. – 2004. – № 5. – С. 30−36.

86. Крутов В.В. Національна безпека України у XXI столітті / В.В.Крутов // Україна – НАТО : інформ.-аналіт. журн. Інформаційного центру з питань євроатлантичної інтеграції. – 2006. – № 3 (13) – С. 5−11.

87. Кузнецов В. Религия в обществе и государстве / В.Кузнецов // Азия сегодня. – 2001. – № 6. – С. 13−20.

88. Курикалов Ю.Л. Классификация как вид семиотического моделирования / Ю.Л.Курикалов // Ред. журн. НТИ. – 1991. – № 11. – Сер. 2. – С. 1−5.

89. Курило А.П. Об ответственности за правонарушения при работе с информацией / А.П.Курило // Вопросы защиты информации. – 1994. – № 2. – С. 19−20.

90. Лафитекий В.И. Основы конституционного строя США / В.И.Лафитекий. – М. : Изд-во "Знание", 1998. – 87 с.

91. Лі С.І. Інтеграція у світовий інформаційний простір / С.І.Лі // Україна – НАТО : інформ.-аналіт. журн. Інформаційного центру з питань євроатлантичної інтеграції. – 2006. – № 3(13). – С. 60−72.

92. Лисенко О. Предмет порівняльного правознавства / О.Лисенко // Право України. – 2001. – № 3. – С. 54−57.

93. Лукащук И.И. Законодательство Украины и международное право (проблемы гармонии) / И.И.Лукащук // Государство и право. – 1999. – № 9. – С. 123−126.

94. Лукич Р. Методология права / Р.Лукич. – М. : Изд-во “Знание”, 1981. – 178 с.

95. Марченко М.Н. Сравнительное правоведение. Общая часть. / М.Н.Марченко. – М. : Изд-во “Знание”, 2001. – 237 с.

96. Марченко М.Н. Вторичные источники романо-германского права, прецедент, доктрина / М.Н.Марченко // Вестник МГУ.– 2000. – № 4. – С. 52−63. – (Серия 11. Право).

97. Марченко М.Н. Закон в системе источников романо-германского права / М.Н.Марченко // Вестник МГУ. – 2000. – № 3. – С. 33−43. – (Серия 11. Право).

98. Марченко М.Н. Источники романо-германского права: понятие, виды, классификация / М.Н.Марченко // Вестник МГУ. – 2000. – № 2. – С. 14−28. – (Серия 11. Право).

99. Марченко М.Н. Курс сравнительного права в системе юридического образования / М.Н.Марченко // Правоведение. – 1999. – № 1. – С. 24−28.

100. Марченко М.Н. Отличительные особенности романо-германского права / М.Н.Марченко // Вестник МГУ. – 2000. – № 1. – С. 26−42. – (Серия 11. Право).

101. Мидор Д.Д. Суди в США / Д.Д.Мидор ; пер. з англ. – К. : Вид-во “Либідь”, 1991. – 85 с.

102. Миколайчик В.М. Кризисы правовых основ полицейской борьбы с преступностью в США / В.М.Миколайчик. – М. : Изд-во “Наука”, 1982. – 75 с.

103. Международное право в документах : учеб. пособ. для студентов юрид. ВУЗов / Н.Т. Блатова, Г.М. Мелков. – [2 изд., перераб. и доп.]. – М. : Изд-во “Инфра М”, 1997. – 696 с.

104. Методология права / [под ред. Д.А.Керимова]. – М. : Изд-во “Прогресс”, 1981. – 304 с.

105. Національна безпека в контексті євроатлантичної інтеграції України: нормативно-правові аспекти : наук.-інформ. зб. / [за ред. В.П.Горбуліна]. – К. : Вид-во “Євроатлантікінформ”, 2005. – 287 с.

106. Національна безпека України: сучасний стан, проблеми та напрями їх вирішення : наук. доп. – К. : Вид-во НІСД, 1996. – С. 57.

107. Новицький Г.В. Щодо визначення об’єктів національної безпеки України / Г.В.Новицький // Україна – НАТО : інформ.-аналіт. журн. Інформаційного центру з питань євроатлантичної інтеграції. – 2006. – № 5 (11). – С. 67−72.

108. Оксамытный В.В. Курс сравнительного правоведения / В.В.Оксамытный, Ю.А.Тихомиров // Государство и право. – 1996. – № 8. – С. 116−119.

109. Олейник О.М. Основы банковского права : курс лекций / О.М.Олейник. – М. : Изд-во “Юрист”, 1999. – С. 218−219.

110. Олейник О. Правовые проблемы банковской тайны / О.М.Олейник // Хозяйство и право. – 1997. – № 6. – С. 135−138.

111. Організаційно-правові основи захисту інформації з обмеженим доступом / [за ред. В.С.Сідака]. – К. : Вид-во ЄУ, 2006. – 168 с.

112. Осакве К. Сравнительное правоведение в схемах : общая и особенная части : учеб.-прак. пособ. / К.Осакве. – М. : Изд-во “Знание”, 2000. – 237 с.

113. Перегудов Ф.И. Введение в системный анализ : учеб. пособ. для ВУЗов / Ф.И.Перегудов, Ф.П.Тарасенко. – М. : Изд-во “Высш. школа”, 1989 – С. 68.

114. Плэт В. Стратегическая разведка. Основные принципы / В.Плэт. – М. : Издательский Дом “Форум”, 1997. – 193 с.

115. Питання концепції реформи інформаційного законодавства України // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : НТУУ “КПІ”, 2000. – С. 17−21.

116. Політі А. Нові транснаціональні ризики і європейська безпека / А.Політі ; пер. з фр. – К. : Вид-во “Знання”, 1997. – 52 с.

117. Постанова Кабінету Міністрів України від 13.12.1999 р. № 2292 “Про затвердження Угоди про взаємне забезпечення міждержавних секретів у галузі правової охорони винаходів” // Правова база НАУ, версія 8.4.40.

118. Постанова Кабінету Міністрів України від 22.05.1996 р. № 558 “Про затвердження Інструкції про порядок охорони державної таємниці, а також іншої інформації з обмеженим доступом, що є власністю держави, під час прийому іноземних делегацій, груп та окремих іноземців і проведення роботи з ними” // Правова база НАУ, версія 8.4.40.

119. Постанова Кабінету Міністрів України від 29.11.2001 р. № 1601 “Про затвердження Положення про порядок надання, переоформлення, зупинення дії або скасування дозволу на провадження діяльності, пов’язаної з державною таємницею” // Правова база НАУ, версія 8.4.40.

120. Постанова Кабінету Міністрів України від 4.08.1995 р. № 609 “Про затвердження Положення, про режимно-секретні органи в міністерствах, відомствах, Уряді Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах, в установах і організаціях” // Правова база НАУ, версія 8.4.40.

121. Постанова Кабінету Міністрів України від 16.11.1994 р. № 779 “Про встановлення письмової форми договорів з працівниками, діяльність яких пов’язана з державною таємницею” // Правова база НАУ, версія 8.3.1.0.

122. Постанова Кабінету Міністрів України від 15.06.1994 р. № 414 “Про види, розміри і порядок надання компенсації громадянам у зв’язку з роботою, яка передбачає доступ до державної таємниці” // Правова база НАУ, версія 8.4.40.

123. Порівняльне правознавство / [за ред. В.А.Туманова]. – К. : Вид-во “Знання”, 1988. – 187 с.

124. Правова інформатика: система інформатизації законотворчої, правозастосовчої, правоохоронної, судочинної та правоосвітньої діяльності в Україні : моногр. / [В.М.Брижко, І.А.Вознюк, В.Д.Павловський та ін.] ; за ред. М.Я.Швеця, Р.А.Калюжного. – Ужгород : Вид-во “ІВА”, 2003. – 168 с.

125. Правовые системы стран мира : энциклопедический справочник / [отв. ред. А.Я.Сухарев]. – М. : Изд-во БЭ, 2001. – 375 с.

126. Пугинский Б.И. О норме права / Б.И.Пугинский // Вестник Московского университета.– 1999. – № 5. – С. 23. − (Серия 11. Право).

127. Радецький В.Г. Європейська та євроатлантична інтеграція як важливий фактор національної безпеки держави / В.Г.Радецький // Україна – НАТО : інформ.-аналіт. журн. Інформаційного центру з питань євроатлантичної інтеграції. – 2006. – № 5 (11). – С. 42−45.

128. Рене Д. Основные правовые системы современности / Д.Рене. – М. : Изд-во “Знание”, 1988. – 120 с.

129. Решетников Ф.М. Правовые системы стран мира / Ф.М.Решетников. – М. : Изд-во “Юрист”, 1993. – 208 с.

130. Робертс Асл. С. НАТО, секретность и право на информацию / Асл. С.Робертс // Информационная безопасность в НАТО : матер. второй междунар. конф. – М. : Изд-во “ВЭТ”, 2006. – С. 57−64.

131. Розова С.С. Классификационная проблема в современной науке / С.С.Розова. – Новосибирск : Изд-во “Наука”, 1986. – 224 с.

132. Розпорядження Президента України від 21 квітня 2005 року № 990 “Про Цільовий план Україна – НАТО на 2005 рік у рамках Плану дій Україна − НАТО” // Правова база НАУ, версія 8.4.40.

133. Рубанов В.А. “Секрет фирмы” и экономическая безопасность страны / В.А.Рубанов // Правительственный вестник. – 1990. – № 15. – С. 28.

134. Савин А.Н. О защите государственной тайны при проведении научно-исследовательских и опытно-конструкторских работ / А.Н.Савин // Вопросы защиты информации. – 1994. – Вып. 2 (27). – С. 25–31.

135. Саидов А.Х. Введение в основные правовые системы современности / А.Х.Саидов. – М. : Изд-во “Юрист”, 1988. – 124 с.

136. Саідов А.Х. Введення в порівняльне правознавство / А.Х.Саідов. – Х. : Вид-во “Міст”, 1988. – 170 с.

137. Саидов А.Х. Сравнительное правоведение (основные правовые системы современности) : учеб. / А.Х.Саидов ; под ред. В.А.Туманова. – М. : Изд-во “Юрист”, 2000. – 178 с.

138. Сарбаш С.В. Договор банковского счета: проблемы доктрины и судебной практики / С.В.Сарбаш. – М. : Изд-во “Статут”, 1999. – 143 с.

139. Семкин С.Н. Анализ международного опыта правового обеспечения информационной безопасности / С.Н.Семкин // Право, информация, безопасность. – 2001. – № 1. – С. 45−52.

140. Сідак В.С. Організація захисту інформації в Німеччині: еволюція і сучасний стан / В.С.Сідак // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – Вип. 2(13). – С. 79−83.

141. Сідак В.С. Організаційно-правові засади захисту інформації з обмеженим доступом в інфораційно-комунікаційних мережах НАТО / В.С.Сідак, В.Ю.Артемов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – Вип. 2 (13). – С. 79−83.

142. Сідак В.С. Проблеми забезпечення інформаційної безпеки у Сполучених Штатах Америки / В.С.Сідак, В.Ю.Артемов // Господарство, підприємство і право. – 2007. – Вип. 2(134). – С.73−75.

143. Синюков В.Н. Правовые системы и правовые семьи // Теория государства и права : курс лекций / В.Н.Синюков ; под ред. Н.И.Матузова, А.В.Малько. – М. : Изд-во “Знание”, 1999. – 234 с.

144. Синюков В.Н. Российская правовая система / В.Н.Синюков. – Саратов : Изд-во “Мера”, 1994. – 180 с.

145. Скобликов П. Коммерческая и банковская тайна: проблемы правового регулирования / П.Скобликов // Российская юстиция. – М., 1997. – № 11.

146. Сравнительное правоведение : сб. ст. / [отв. ред. В.А.Туманов]. – М. : Изд-во “Знание”, 1978. – 185 с.

147. Спасов Б. Закон и его толкование / Б.Спасов. – М. : Изд-во “Знание”, 1986. – 58 с.

148. Закон України “Про стандартизацію” від 17.05.2001 р. // Правова база НАУ, версія 8.4.40.

149. ISO / IEC 27001:2005 “Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Вимоги” (Information technology. Security techniques. Information security management systems. Requirements).

150. ISO / IEC 27002:2005 “Інформаційні технології. Методи забезпечення безпеки. Практичні правила для управління інформаційною безпекою” (Information technology. Security techniques. Code of practice for information security management).

151. ISO / IEC 27004:2009 “Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимірювання” (Information technology. Security techniques. Information security management. Measurement).

152. Василюк В. Інформаційна безпека / В.Василюк, С.Климчук. – К. : КНТ, 2008. – 190 с.

153. Куберт П. Международный стандарт ISO 17799. Информационные технологии – практические правила управления информационной безопасностью / П.Куберт, В.Безштанько, В.Цукран // Бизнес и безопасность. − 2006. − № 3 (53).

154. Куберт П. Обеспечение безопасности при эксплуатации по ISO 17799. / П.Куберт // Бизнес и безопасность. − 2007. − № 1 (57).

155. Анализ международного стандарта ISO 15408 Информационная технология, методы и средства // Бизнес и безопасность. − 2007. − № 5 (61).

156. Галатенко В.А. Стандарты информационной безопасности. Курс лекций : учеб. пособ. / В.А.Галатенко. – [2-е изд.] – М. : ИНТУИТ.РУ “Интернет-университет информационных технологий”, 2006. – 264 с.

157. Гарбузов Г. Стандартизация в области ИБ: зарубежный опыт / Г.Гарбузов // Информационная безопасность”. − 2009. − № 1.

158. Кудрявцева С.П. Міжнародна інформація : навч. посіб. для студентів вищих навч. закладів / С.П.Кудрявцева, В.В.Колос. – К. : Видавничий дім “Слово”, 2005. – 400 с.

159. Плешивцева Т. Червяк в паутине / Т.Плешивцева // Эксперт Украины. 2007. – № 12 (110).

160. Ступницький О. Міжнародні стандарти інформаційної безпеки в Україні: “неоконсервативний” анклав чи “транснаціональна” інтеграція / О.Ступницький // Економічний часопис. – 2004. – № 4.

161. Суханов А. Аналіз ризиків в управлінні інформаційною безпекою /А.Суханов // Інформзахист. − 2008. – № 11 (120).

РОЗДІЛ 9

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ ФАХІВЦЯ В ГАЛУЗІ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

9.1. ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ ЗМІСТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Наявність інформаційної культури обов'язкова для виконання будь-яких видів робіт, пов'язаних з обробленням інформації та інформаційними процесами. Основним завданням, на вирішення якого повинна бути спрямована інформаційна культура фахівця з охорони інформації, є підвищення ефективності його професійної діяльності. Тому доцільно проаналізувати зміст роботи з інформацією з позицій діяльнісного підходу, а саме зміст і сутність поняття інформаційної діяльності. Для цього спочатку коротко розглянемо поняття діяльності в когнітивному й пізнавальному аспектах.

За А.М.Лєонтьєвим, діяльність є молярною неадитивною одиницею життя тілесного, матеріального суб'єкта. Діяльність – це не реакція і не сукупність реакцій, а система, яка має свою будову, свої внутрішні переходи й перетворення, свій розвиток.

А.Л.Нікіфоров визначає діяльність як специфічно людську форму активності, змістом якої є доцільна зміна і перетворення оточуючого людину світу.

Г.А.Каплан розуміє під діяльністю різносторонній процес створення людиною умов свого існування й розвитку, процес перетворення соціальної реальності відповідно до суспільних потреб, мети і завдань. Діяльність – це специфічна форма активного ставлення людини до навколишнього світу, зміст якої становить доцільна зміна й перетворення.

За Т.М.Дрідзе, діяльність виступає як усвідомлена, мотивована, тобто психічно регульована предметна й цілеспрямована соціально регламентована активність суспільного суб'єкта, яка опосередковує всі його зв'язки з природним, техніко-економічним і соціокультурним відображенням.

Основою або базовою характеристикою діяльності виступає її предметність. У самому понятті діяльності вже міститься поняття її предмета. Предмет діяльності виступає двояко: первинно – у своєму незалежному існуванні, як такий, що підкоряє собі та перетворює діяльність суб'єкта; вторинно – як образ предмета, продукт психічного відображення його властивостей, яке здійснюється в результаті діяльності суб'єкта й інакше здійснюватися не може.

Діяльність має цілеспрямований характер, тобто це така активність, яка направлена на досягнення свідомо поставленої мети. Крім того, будь-якій діяльності властива попередня продуманість. Після того як мета поставлена, людина аналізує ситуацію, в якій їй доведеться діяти, й обирає способи і засоби досягнення мети. В.А.Козаков уважає, що діяльність – це активна взаємодія людини з середовищем, у якому вона (людина) досягає свідомо поставленої мети, що виникла в результаті появи в неї певної потреби.

Отже, можна стверджувати, що будь-яка діяльність детермінується активністю, предметністю, цілеспрямованістю, а також потребами. Крім того, будь-яка діяльність характеризується наявністю мети, мотиву, предмета, умови й результату.

Під метою діяльності розуміють очікуваний результат діяльності, спрямований на предмет, за допомогою якого суб'єкт має намір задовольнити ту чи іншу потребу.

Мотиви діяльності – це психічні явища, які стали збудниками виконання тієї чи іншої дії, вчинку.

Суб'єкт діяльності – це індивід, який цілеспрямовано діє для задоволення своїх потреб.

Процес діяльності визначається як сукупність цілеспрямованих дій із зміння стану предмета діяльності відповідно до поставленої мети.

Предмет діяльності – це те, що перетворюється в діяльності.

Умова діяльності – це середовище, засоби, в якому або за допомогою яких проводиться діяльність.

Результат діяльності – це досягнення мети через задоволення потреб.

Діяльність повинна бути результативною, тобто вона повинна досягати своєї мети.

Людська діяльність складна за будовою. Її структура становить діалектичний взаємозв'язок передусім двох підсистем – предметної (інтелектуальної) й комунікативної діяльності. Вона є розчленованою цілісністю двох зазначених видів діяльності.

Діяльність опосередковується матеріальною й духовною культурою, виробленою в суспільстві. Ця культура міститься нібито між суб'єктом і предметом діяльності. Тому суб'єкт, який не досяг певного культурного розвитку, не в змозі перетворювати навколишнє середовище, не здатний проводити предметну діяльність. При цьому сама культура виробляється в процесі предметної діяльності.

Однак діяльність генетично пов'язана не лише з культурним, але й із інформаційним аспектом. Зокрема духовна діяльність, входячи як підсистема нарівні з практичною діяльністю до системи діяльності, натомість має на три основні форми: пізнавальну, прогностичну й ціннісно-орієнтаційну. Кожна з цих форм безпосередньо пов'язана з інформацією і знаннями. Діяльність не може відбуватись в умовах інформаційного вакууму, без інформаційної підтримки. У зв'язку з цим доцільно навести визначення, яке дав Є.С.Маркарян: діяльність – це інформаційно спрямована активність живих систем, яка виникає на основі їх відношення до середовища з метою самопідтримки. Таким чином, діяльність, окрім іншого, детермінується ступенем інформаційної підтримки. Тому одним із підвидів предметної діяльності є інформаційна діяльність, яка і забезпечує підтримку інших видів діяльності.

Загалом під інформаційною діяльністю розуміють сукупність операцій із сприйняття, перероблення і видання інформації в межах системи комунікацій. За своєю сутністю інформаційна діяльність є відображувальною, оскільки проводиться через відображення інформації у свідомості людини.

Проаналізуємо структуру інформаційної діяльності інформаційно-аналітичних служб.

Метою інформаційної діяльності виступає задоволення інформаційних потреб основних споживачів, якими є керівники та співробітники установ і організацій; об'єктом – уся інформація, яка циркулює в зазначених установах та організаціях.

Суб'єктами інформаційної діяльності виступають фахівці з оброблення інформації.

Процес інформаційної діяльності становить сукупність цілеспрямованих дій із збирання, зберігання, пошуку, перетворення й обміну інформацією.

Результатом інформаційної діяльності є готовий інформаційний продукт (документ), який у подальшому може бути використаний зокрема для прийняття управлінських рішень.

Інформаційна діяльність безпосередньо пов'язана з інформаційними потребами. При цьому роль інформаційної культури в інформаційній діяльності зводиться до підвищення адекватності вияву, формулювання інформаційних потреб і якості їх задоволення.

Тому розглянемо зміст і сутність потреб загалом й інформаційних потреб зокрема, а також їхню роль у деяких видах діяльності.

Потреба – це властивість (здатність) живих систем активно реагувати на неузгодженість між наявними й оптимальними зовнішніми і внутрішніми умовами їх життєдіяльності.

Потреба в широкому розумінні – це нестаток суб'єкта в дечому, для задоволення якого необхідна та чи інша форма активності. Суб'єктом потреб виступають особи, у яких у процесі виконання якої-небудь роботи виникають потреби. Ці потреби можна розглядати як певне ставлення індивіда до умов його життя. Будь-яка конкретна потреба становить єдність двох сторін: суб'єктивної, яка виступає як необхідність у певних умовах нормального життя й розвитку суб'єкта, та об'єктивної, що становить предмет потреби.

З точки зору психологічної науки, потреба – це психічне явище відображення потреби організму особи в необхідних умовах, які забезпечують її життя або розвиток.

Участь потреб у детермінації людської діяльності виявляється різноманітно. Потреби – це внутрішні об'єктивні фактори, які виступають як причини виникнення і проведення діяльності, оскільки остання в кінцевому рахунку завжди проводиться для задоволення соціальних або індивідуальних, актуальних чи потенційних потреб.

Згідно з уявленнями сучасної психології та соціології людські потреби мають складну структуру, котру можна подати у вигляді так званої піраміди Маслоу, яка умовно складається з двох частин. Основу піраміди становлять фізіологічні потреби (у сні, їжі тощо), а вершину – інтелектуальні потреби (у спілкуванні, самовдосконаленні, самореалізації й т. ін.).

Невід'ємною складовою другого виду потреб є пізнавальні потреби, які формуються в процесі індивідуального розвитку людини під впливом виховання й навчання з первинної природної потреби в притоці сенсорної інформації. Пізнавальна потреба виступає певним внутрішнім динамічним фактором усвідомлення, який ініціює мотивацію і діяльність. Передумовою виникнення пізнавальної потреби в суб'єкта є наявна в нього неповна і невизначена інформація, яка не здатна задовольнити деякі потреби в досягненні поставленої мети.

Пізнавальна потреба може розвиватися лише за наявності певної апріорної інформації. Вона відкриває перед людиною нові "інформаційні горизонти", до яких ця людина прямує. Відсутність такої інформації обмежує пізнавальні потреби, виключає їх стимулювання.

Активний стан виникає в людини тоді, коли вона володіє відносно розвиненою структурою пізнавальних потреб. Пізнавальна потреба формується й задовольняється в процесі соціалізації особистості. Однак знань, отриманих на початковому етапі становлення особистості, недостатньо для нормальної життєдіяльності. Потрібні додаткові знання як для загального розвитку, так і для вирішення конкретних завдань. Таким чином, формується інформаційна потреба, яка сприяє процесу мотивованого споживання інформації в прагматичному аспекті. В цьому й полягає сутність інформаційної потреби, яка є другорядною по відношенню до потреби пізнавальної.

Необхідність в інформації суб'єктивно виражається в інформаційній потребі як у певному ставленні суб'єкта до соціального й природного середовища в процесі його діяльності.

За своєю природою інформаційна потреба має подвійний характер. Вона може розглядатися як одна з базисних потреб, що властива всім високоорганізованим істотам, і як потреба в інформації, що формується в процесі людської діяльності.

Сутність інформаційної потреби багато в чому залежить від інформації, під якою розуміють відображену різноманітність. Тоді сама інформаційна потреба визначається як:

- властивість суб'єкта, яка відображає необхідність отримання інформації;
- необхідне ставлення суб'єкта до інформації, відображене його (суб'єкта) психікою і свідомістю;
- визначена форма ставлення суб'єкта до предмета потреби – інформації;
- властивість, яка відображає необхідність одержання інформації;
- вираження неузгодження між метою, яка стоїть перед споживачем, і можливістю її досягнення без керуючого впливу;
- відношення людини, спрямоване на присвоєння або використання інформації;
- вираження необхідності раціонального використання наявних ресурсів для вирішення прикладних завдань;

- необхідність отримання впродовж обмеженого часового проміжку інформації визначеної тематики.

Як уважає Б.С.Єлєпов, загальним базисом, на якому ґрунтуються судження з проблематики інформаційних потреб, є визначення останніх як атрибута діяльності споживачів. Якщо в процесі діяльності будь-якого роду у свідомості суб'єкта повинна виникнути "ідеальна модель", яка відображає цілі, предмет, умови, взаємозв'язки, засоби і методи його конкретних дій, то інформаційні потреби є ніщо інше, як прагнення мати у своїй свідомості інформаційні компоненти, яких не вистачає для побудови "ідеальної моделі", тобто отримати знання про об'єкти, на які спрямована діяльність.

Іншими словами, інформаційна потреба виникає лише тоді, коли при прагненні до досягнення якої-небудь більш-менш усвідомлюваної, але безпосередньо недоступної мети у свідомості людини не проявляється необхідний для цього спосіб або засіб, а їх потрібно свідомо шукати. Знаходження способу або засобу досягнення мети й означає задоволення потреби.

Інформаційні потреби зумовлені функціонально – характером доцільної діяльності навколишньої системи. Інформаційні потреби задовольняються не стільки в результаті, скільки в процесі споживання інформації. Тому перетворення інформації є моментом її споживання.

Розмаїття інформаційних потреб за формою і змістом характеризується різноманітними мотивами звернення до інформації, які визначаються видами діяльності. Інформаційні потреби, будучи суспільним продуктом, відображають форми прояву пізнавальної активності й діяльності особистості. При цьому динаміка інформаційних потреб є результатом інформаційної активності особистості.

Важливим детермінантом інформаційних потреб виступають інформаційні мотиви. Будь-яка діяльність, у тому числі інформаційна, відбувається під впливом цілого комплексу таких мотивів (спонукань). Сила мотиву пов'язується із зовнішніми потребами через відношення із внутрішніми особистісними спонуканнями індивіда. При цьому мотив виконує роль спонукального моменту, певного суб'єктивного образу мети, яку необхідно досягнути. Мотив однозначно визначиться як спонукання поведінки і діяльності. Мотиви поведінки й діяльності виникають при відображенні потреб – їх усвідомленні, – отже, можуть належати до властивостей особистості. Оскільки інформаційна діяльність детермінується професійною діяльністю, то інформаційний мотив може бути визначений

як різновид мотиву професійної діяльності, спонукальна функція якого спрямовує процеси задоволення окремих інформаційних потреб або їх систем.

Окрім того, інформаційні потреби можуть розглядатися у співвіднесеності з інформаційними інтересами. Інформаційний інтерес виступає як відображення об'єктивної інформаційної потреби у свідомості. Інформаційні потреби, інтереси, мотиви прямо співвідносяться з цілями інформаційної й професійної діяльності. Звичайно мета визначається як відображення об'єктивної потреби.

Розрізняють три типи інформаційних потреб:

- суспільні (визначаються соціальними завданнями суспільства);
- колективні (потреби групи фахівців, які вирішують спільне завдання);
- індивідуальні.

Інформаційні потреби мають складну структуру, яка формується в результаті органічного синтезу двох компонентів – особистісного (суб'єктивного) й діяльнісного або предметного (об'єктивного). Перший є продуктом виховання та розвитку особистості, результатом внутрішніх психічних процесів. Суб'єктивний компонент багато в чому залежить від рівня соціалізації індивіда. Другий компонент виступає абсолютним інваріантом стосовно особистості й визначається зовнішніми факторами, тобто безпосередньо практичними завданнями, які підлягають вирішенню.

Розглянемо детально обидві ці складові, а також процес їх формування. Для цього уведемо поняття інформаційної моделі особистості, за допомогою якої спробуємо пояснити роль фахівця з оброблення інформації в інформаційній діяльності. Така модель допоможе краще зрозуміти механізм і особливості формування інформаційних потреб особистості, виділити їхню сутність і розкрити зміст, а також знайти шляхи їх оптимального задоволення.

Зміст інформаційної моделі може бути описаний через тезаурус і представлений у вигляді фільтра, через який "пропускається" будь-яка вхідна інформація, виражена в знаковій формі.

Тезаурус – це передусім упорядкована сукупність знань, якими володіє індивід. Різні вчені, зокрема О.М.Леонтьєв, В.В.Морковкін, Г.М.Ільїн, Б.В.Якушин, Є.Ю.Артем'єва, інтерпретують тезаурус як "модель світу", "образ світу", "суб'єктивну картину світу", "модель середовища". Тезаурус – це множина описів станів певної моделі зовнішнього середовища. При цьому інформація розглядається як певний оператор над тезаурусом. Кількістю семантичної інфо-

рмації відносно тезаурусу називається міра змінення тезаурусу в результаті аналізу тексту. Такий підхід є прийнятним для ситуацій, коли виникає необхідність в оцінці прагматичної цінності семантичної інформації та потреби в ній.

Як указує Т.М.Дрідзе, тезаурус – це відкрита й динамічна система значень, яка зберігається в пам'яті індивіда та організована за принципом: від загального до часткового в межах визначеної предметної сфери. Під час інформаційного обміну індивід безперервно здійснює над тезаурусом мотивовані й цілеспрямовані інтелектуально-мисленнєві та комунікативно-пізнавальні операції, в процесі яких постійно корегуються зв'язки між значеннями.

Як відомо, тезаурус носія мови і, відповідно, інформаційна модель особистості формуються його комунікативним оточенням. Люди, які володіють відносно спільним тезаурусом у межах заданої мовної підсистеми й певним комплексом семіотичних умінь і навичок, зокрема уміннями оперувати цим тезаурусом, можуть бути об'єднані в так звані семіотичні групи. Чим вище семіотичний рівень носія мови, тим менше розрив між умінням оперувати мисленнєвими й мовними категоріями. Рівень спільності особистісних тезаурусів визначає глибину потенційно можливого інформаційного обміну. Тезаурус детермінує розмірність семантичного та лексичного просторів, задаючи їх такими вимірами, як значення − значення, значення − знак, знак − значення, знак − знак. Кожний із цих вимірів визначає семантику словникового запасу з урахуванням синонімічних, антонімічних та інших відношень.

Однак сам по собі тезаурус особистості не є тотожним її інформаційній моделі, до складу якої, окрім тезаурусу, входить і так званий інформаційний інтерес. Останній формується в процесі становлення й соціалізації особистості опосередковано, через навчання, виховання, практичну діяльність. Інформаційний інтерес багато в чому відображає життєві пріоритети особистості, її схильності й симпатії. Тому він має певну інерційність і консервативність. Зміна або перебудова інтересу, які супроводжуються переміщенням осередку оптимального збудження в корі мозку або появою нових осередків, є досить тривалим процесом. Більше того, якщо задоволення інформаційної потреби ліквідує її, то задоволення інтересу частіш за все веде до його посилення і закріплення.

При цьому під інформаційною моделлю особистості будемо розуміти складну систему психічної взаємодії тезаурусу особистості та її інформаційного інтересу, яка визначає певний рівень сприйняття семантичної інформації, а та-

кож потребу в ній. У загальному випадку розвиненість інформаційної моделі особистості визначає таку її системну властивість, як алостерія, тобто здатність оцінювати вплив як символи і повідомлення. Сутність інформаційної моделі ґрунтується на так званому "подвійному відображенні", адже інформаційна модель відображає інформацію, яка натомість є відображенням об'єктивного світу. Інформаційна модель сама становить продукт "подвійного відображення". Вона тим розвиненіша, чим краще в ній реалізований ефект "подвійного відображення". Не кожне відображення відбувається на інформаційному рівні, й не кожна система здатна оцінювати взаємодію як символи і повідомлення. Тому алостерія є якісною характеристикою антиентропійних (самоорганізуючих) систем, до яких належить й інформаційна модель особистості.

Формування інформаційної моделі особистості в цілому і зокрема інформаційного інтересу відбувається у "формативний" період (12−20 років), коли здійснюється становлення ціннісної та аксіометричної картини світу.

Важливою властивістю інформаційної моделі особистості є її адаптивність, яка полягає у здатності змінювати свою структуру відповідно до діяльності й інформації, що надходить. Таким чином, адаптивність інформаційної моделі є важливим критерієм її розвиненості.

Виникнення інформаційної потреби відбувається у випадку відсутності деяких елементів інформаційної моделі, необхідних для цілісного сприйняття навколишньої дійсності та проведення практичної діяльності. Однак така "недобудованість" інформаційної моделі зовсім не є свідоцтвом її нерозвиненості. Навпаки, постійна потреба в інформації означає безперервність процесу розвитку інформаційної моделі. "Білі плями" в цій структурі виступають доказом прогресу і відкритості системи. А їхня відсутність підтверджує неможливість подальшого розвитку системи та її закритість.

Таким чином, інформаційна модель, що розвивається, ніколи не може досягти досконалості, але завжди прямує до неї. Саме таке прагнення зумовлює появу інформаційних потреб. Особливу роль у цьому відіграє метаінформація, під якою розуміють відомості про наявність інформації. В загальному випадку метаінформація – це передусім посилання на тематичні відомості за певною проблематикою. Метаінформація дає змогу індивіду орієнтуватися в інформаційному просторі.

Метаінформація зумовлює виникнення інформаційних потреб. Вона досить часто породжує і стимулює їхній розвиток. Володіючи метаінформацією, її спо-

живач швидше й точніше зможе сформулювати свою потребу в інформації. Об'єктивний компонент інформаційних потреб, який детермінується виключно функціональною необхідністю, може бути представлений за допомогою інформаційного кадастру. Під інформаційним кадастром розуміють повну і добре структуровану сукупність даних, необхідних та достатніх для ефективного функціонування установи чи організації й виконання поставлених перед ними завдань. Злагодженість структури кадастру визначається однорідністю переліку реалій об'єктивного світу, які входять до його складу, зокрема професійної діяльності. Тому її розроблення повинне здійснюватися в такій послідовності:

1) на основі аналізу завдань підрозділу складається по можливості повний перелік тих реалій, відомості про які необхідні для його інформаційного забезпечення;

2) складений перелік класифікується на групи таким чином, щоб у межах кожної з них були по можливості більш однорідні елементи;

3) для кожної групи реалій складається перелік характеристик і критеріїв, за якими повинні збиратися відомості про них;

4) для всіх груп реалій установлюються їхні взаємозв'язки, визначаються залежності.

Отриманий таким чином інформаційний кадастр є відображенням діяльності установи чи організації й безпосередньо залежить від виконуваних ними завдань.

Цілісна структура інформаційних потреб формується як результат органічного синтезу інформаційної моделі особистості та інформаційного кадастру установи чи організації. При цьому важливо, щоб в обох складових були спільні "точки дотику", які забезпечуватимуть однорідність і внутрішню несуперечливість сформованих інформаційних потреб. Тобто можна стверджувати, що остаточні інформаційні потреби є продуктом складної взаємодії зовнішніх і внутрішніх факторів. Необхідно, щоб інформаційна модель та інформаційний кадастр узгоджувалися між собою, мали однакову направленість. Тоді інформаційні потреби проявляються як колінеарність (однакова спрямованість) векторів інформаційної моделі особистості споживача інформації та інформаційного кадастру установи чи організації.

Як зазначає Д.І.Блюменау, остаточні інформаційні потреби можуть проявлятися як потреби в:

- поточній і ретроспективній інформації;

- вузькотематичній і широкотематичній інформації;
- галузевій і міжгалузевій інформації;
- фактографічній і концептуальній інформації.

Трансформуючись до рівня споживача інформації (фахівця з ОІ), інформаційні потреби можуть проявлятися як:

1) потреби в установчій об'єктовій інформації, наприклад у відомостях щодо найменування організації, категорії (підприємство із зазначенням форми власності, міністерство, навчальний або науковий заклад тощо), державної належності, коду в чинній системі класифікаторів тощо;

2) потреби у фактографічній об'єктовій інформації, які передбачають отримання відомостей про факти діяльності окремих об'єктів або про події, учасниками яких були ці об'єкти;

3) потреби в галузевій і вузькотематичній інформації, яка містить оглядові або аналітичні відомості про певну сукупність об'єктів, фактів, подій;

4) потреби в міжгалузевій і широкотематичній інформації, яка висвітлює результати діяльності установи чи організації за окремими напрямами.

Із наведеного вище можна зробити висновок, що зміни в структурі інформаційних потреб здійснюються насамперед за рахунок змін в інформаційній моделі особистості, які пов'язані з надходженням нової інформації. Вони також можуть проявлятися як реакція на зворотний зв'язок у вигляді інформації, що надійшла раніше. Реструктуризація інформаційних потреб може відбуватися і під впливом так званої фонової інформації, яка надходить до особистості незалежно від уже сформованих інформаційних потреб. Прикладом фонової інформації можуть бути енциклопедичні масиви (відомості з енциклопедій, словників, довідників, їхніх електронних аналогів тощо).

Остаточна структура інформаційних потреб має складну організацію. Вона може існувати лише на рівні свідомості людини як сукупність реакцій на вхідну інформацію. При цьому досить складно відбувається процес трансляції інформаційних потреб із мисленнєвого до мовленнєвого рівня. Цей процес детермінується розумовим і психіко-емоційним розвитком особистості.

При такій трансляції особливо важливий правильний вияв у словесній формі тих інформаційних потреб і очікувань, які формуються інформаційною моделлю особистості. Досить часто нездатність людини до висловлювання своїх думок, погане володіння мовним апаратом, недостатній словниковий запас веде

до зниження ефективності інформаційної діяльності в цілому. Інформаційна культура при цьому повинна бути спрямована на розвиток мовних умінь і навичок, спроможності вираження своїх думок, підвищення комунікативності. Таким чином, кожен спеціаліст повинен прагнути до найбільш повного й адекватного вираження своїх потреб та інтересів. Така адекватність дуже важлива при трансформації інформаційних потреб в інформаційний запит.

Якщо споживачу важко сформулювати запит і вкласти в нього своє розуміння потрібної інформації, йому необхідно допомогти. Для цього можна використати наявні масиви інформації. Аналізуючи, а іноді навіть просто копіюючи у свідомості ті чи інші інформаційні фрагменти, споживач може синтезувати свій інформаційний запит. Отже, одночасно відбувається розширення словниково-лексичного простору особистості. Однак у такому випадку необхідно володіти певною апріорною інформацією про спрямованість інформаційних потреб, щоб підібрати максимально наближені до них фрагменти інформації.

Іншим варіантом вирішення цієї проблеми може бути використання метаінформації. Володіння останньою набагато полегшує процес формування інформаційного запиту і його співвідношення з інформаційними потребами. Таким чином, інформаційна потреба може існувати лише в тісному зв'язку з так званою метаінформаційною потребою. Обидві ці сутності існують паралельно, вони взаємозалежні. При цьому метаінформаційна потреба стимулює інформаційну. Тоді можна стверджувати, що інформаційний запит є результатом як інформаційних, так і метаінформаційних потреб, де другі виступають засобом по відношенню до перших.

Для якісного задоволення сформованих інформаційних потреб необхідно якомога краще їх вивчити і зрозуміти. Р.Н.Іванов виділяв такі методи аналізу інформаційних потреб:

- анкетування;
- спостереження за роботою споживачів (спеціалістів установи чи організації);
- аналіз на основі переліку (рубрикатора);
- аналіз інформаційних запитів;
- отримання коментарів у споживачів;
- вивчення нормативних документів.

Анкетування дає змогу отримати суб'єктивні дані про потреби споживачів в інформації за різноманітними тематиками. При цьому надається можливість

окреслити коло питань, які становлять інтерес, але ніяк не виявити їх глибинний смисл і внутрішній зміст. Натомість проведення анкетування – процес трудомісткий та тривалий. Тому цей метод не завжди доцільно застосовувати на практиці.

Спостереження за роботою споживачів у режимі реального часу може дати точне й реальне уявлення про структуру інформаційних потреб, дозволить відділити об'єктивні потреби від суб'єктивних. При цьому можуть бути виявлені додаткові потреби в інформації, які навіть ще не усвідомлюються. Таким чином, виникають передумови для задоволення потреб, які ще не були відтрансльовані у вигляді інформаційного запиту. Такий підхід може підвищити якість задоволення інформаційних потреб зокрема і якість інформаційної діяльності в цілому. Однак такого роду спостереження також вимагає докладання певних зусиль. До того ж у процесі спостереження можна отримати уявлення про інформаційні потреби обмеженої групи споживачів.

Аналіз інформаційних потреб на основі їхнього переліку в загальних рисах ідентичний анкетуванню. Хоча, на відміну від анкети, перелік тематик, які становлять інтерес, складають самі споживачі. Він є відображенням наявних інформаційних потреб і найкращим чином відповідає трансформації інформаційних потреб в інформаційний запит. Позитивне в методі аналізу інформаційних потреб те, що він не вимагає яких-небудь суттєвих витрат і дає можливість отримати узагальнену оцінку інформаційних потреб.

На відміну від попереднього методу, аналіз інформаційних запитів дає уявлення про поодинокі інформаційні потреби, які виникають при вирішенні окремих завдань.

Коментуючи свій інформаційний запит, споживач більш глибоко розкриває свої інформаційні потреби. При цьому він також посилається на мотиви виникнення таких потреб. З'являється можливість зрозуміти структуру інформаційної моделі його особистості, а також те місце, яке відводиться або буде відведено очікуваній інформації в цій структурі. Нерідко в процесі таких коментарів споживач починає сам чіткіше усвідомлювати свої потреби в інформації й більш коректно формулювати запит, який ґрунтується на цих потребах. Досить часто під час таких коментарів і пояснень до них із боку фахівця з оброблення інформації простежуються зміни у змісті та сутності інформаційних потреб споживача. При цьому можуть відбуватися певні трансформації інформаційної моделі останнього, яка піддається зміні й корекції. Завдяки цьому споживач

може більш критично оцінювати свої потреби в інформації та можливості їх задоволення. Останнє свідчить про підвищення рівня його інформаційної культури. Таким чином, можна уважати, що розглянутий метод досить ефективний як у плані вивчення інформаційних потреб, так і щодо здійснення впливу на них із метою корекції й підвищення адекватності їхнього вираження.

Вивчення нормативних документів надає перелік об'єктивних реалій, інформація про які може накопичуватися і використовуватися для задоволення інформаційних потреб споживачів. При цьому увага приділяється скоріше формі вираження й задоволення інформаційних потреб, а не змісту. Крім того, цей метод не дає змоги отримати повне уявлення про перелік тематик, які становлять інтерес, і про реальну структуру інформаційних потреб.

Кожний із наведених методів дозволяє тією чи іншою мірою оцінити інформаційні потреби як окремих споживачів, так і організації в цілому. При цьому підвищується якість їх інформаційного забезпечення, а також ефективність інформаційної діяльності загалом. У подальшому не виключена можливість появи нових, більш досконалих методів аналізу інформаційних потреб.

Інформаційну потребу споживача, що знайшла своє відображення в інформаційному запиті, задовольняє фахівець із оброблення інформації. Для її якісного задоволення необхідно, щоб під впливом інформаційного запиту в інформаційній моделі останнього була сформована інформаційна потреба, ідентична тій, яка виникла у споживача. Для формування такої потреби і здійснення відповідного впливу на інформаційну модель фахівця з оброблення інформації, окрім інформаційного запиту, можуть використовуватися всі наведені вище методи аналізу інформаційних потреб. При цьому за мету ставиться "переналаштування" інформаційної моделі суб'єкта інформаційної діяльності, яким виступає фахівець з оброблення інформації, та максимальна адаптація її до інформаційних потреб споживача. Таким чином, потреба в інформації повинна передатися суб'єкту й виходити вже нібито від нього. Тільки тоді фахівець з ОІ буде в змозі правильно її оцінити та знайти адекватні засоби задоволення.

При цьому, на нашу думку, слід розрізняти два види інформаційних потреб за ступенем їх задоволення – статичні й динамічні. Статичними будемо називати потреби, які можуть бути задоволені в процесі одноразового отримання споживачем інформації. Характерною властивістю таких потреб є їхня часова, тематична й об'єктова обмеженість. До статичних потреб слід віднести потреби в

інформації, повний обсяг якої не підлягає доповненню, скажімо, реєстраційні дані установ чи організацій.

Під динамічними потребами розумітимемо потреби, які не можуть бути задоволені обмеженою кількістю інформації. Тому їхньою характерною особливістю є необмеженість. До динамічних потреб слід відносити потреби в інформації, повний обсяг якої визначити неможливо. Така інформація завжди може бути доповнена новими відомостями.

На початковому етапі пошуку необхідної інформації суб'єкт повинен абстрагуватися, здійснити перехід від конкретної інформаційної потреби до її узагальненої моделі. Це передусім дозволяє визначити сферу подальшого пошуку, а також зробити припущення щодо очікуваних результатів. Особливого значення таке абстрагування набуває в умовах автоматизованого машинного пошуку, коли необхідно задати узагальнений алгоритм первинного відбору інформації. Будь-які зміни параметрів у такому алгоритмі можуть призвести до того, що будуть відібрані великі обсяги апріорно непотрібної інформації або, навпаки, пропущені значні обсяги потенційно змістовних інформаційних масивів.

Надалі відібрана інформація піддається селективному обробленню. При цьому стають більш жорсткими критерії відбору потрібних відомостей і звужується коло інформації, яка потенційно їх задовольняє. Особливістю цього етапу задоволення інформаційних потреб є те, що тут не лише відбираються відомості, які явно відповідають критеріям пошуку, але й виділяється та інформація, яка формально не відповідає цим критеріям і в якій нібито не виникало потреби. Однак при більш глибокому аналізі такої інформації й зіставленні з вираженими інформаційними потребами може виявитися, що вона також може стати в нагоді споживачу. Але через деякі причини потреба в зазначеній інформації не знайшла свого відображення в інформаційному запиті. Однією з цих причин може бути неусвідомлення такої потреби (існування на рівні підсвідомості) або нездатність до її вираження у словесній формі. Таким чином, інформація, що обробляється, може сприяти уточненню інформаційних потреб і виконувати по відношенню до них корегуючу функцію.

На наступному етапі задоволення інформаційних потреб відбувається сприйняття й усвідомлення відібраної інформації. При цьому здійснюється її зіставлення з інформаційною моделлю фахівця з оброблення інформації та остаточне визначення, наскільки ця інформація задовольняє статичні або відповідає динамічним інформаційним потребам.

Для цього використовують два важливих поняття – релевантність і пертинентність. Під релевантністю розуміють смислову відповідність між змістом відібраної інформації й текстом інформаційного запиту. Розрізняють змістову та формальну релевантність. Змістова релевантність розглядається як оцінка відповідності смислу відібраної інформації інформаційному запиту, формальна – як оцінка за допомогою формальних методів відповідності відібраної інформації інформаційному запиту. Під пертинентністю розуміють смислову відповідність змісту відібраної інформації фактичній інформаційній потребі споживача, яка була сформульована його інформаційною моделлю.

Таким чином, за допомогою релевантності оцінюється відповідність змісту відібраної інформації тексту інформаційного запиту; пертинентності − відповідність відібраної інформації наявній інформаційній потребі, а також співвіднесення цієї інформації з інформаційною моделлю особистості й визначення її місця в цій моделі. При цьому слід зазначити, що пертинентність є суб'єктивною оцінкою, яку може дати лише сам ініціатор запиту.

Інформація, яка пройшла через усі встановлені фільтри відбору та була оцінена як релевантна інформаційному запиту, залежно від останнього може бути передана споживачу у вигляді:

1) максимально можливого текстового масиву, який може бути підданий обробленню самим споживачем;

2) одного тексту, який містить контекстні посилання на інші джерела (метаінформація);

3) одного самостійного тексту;

4) фрагменту тексту.

Слід зазначити, що для задоволення статичної потреби використовуються переважно дві останні форми подання інформації та в окремих випадках – текст із контекстними посиланнями. Перші дві форми застосовуються, як правило, для задоволення динамічних потреб.

Інформація, яка отримується споживачем у процесі задоволення його потреб, використовується ним для напрацювання алгоритму прийняття рішення і його реалізації, а також для цілепокладання й цілевизначення. Крім того, як зазначалося вище, ця інформація застосовується для корекції й розширення обсягу динамічних інформаційних потреб та певної трансформації інформаційної моделі споживача й відіграє при цьому роль зворотного зв'язку.

Таким чином, увесь процес формування й задоволення інформаційних потреб, який у загальному випадку є основним елементом інформаційної діяльності, може бути представлений у вигляді схеми (рис. 9.1).

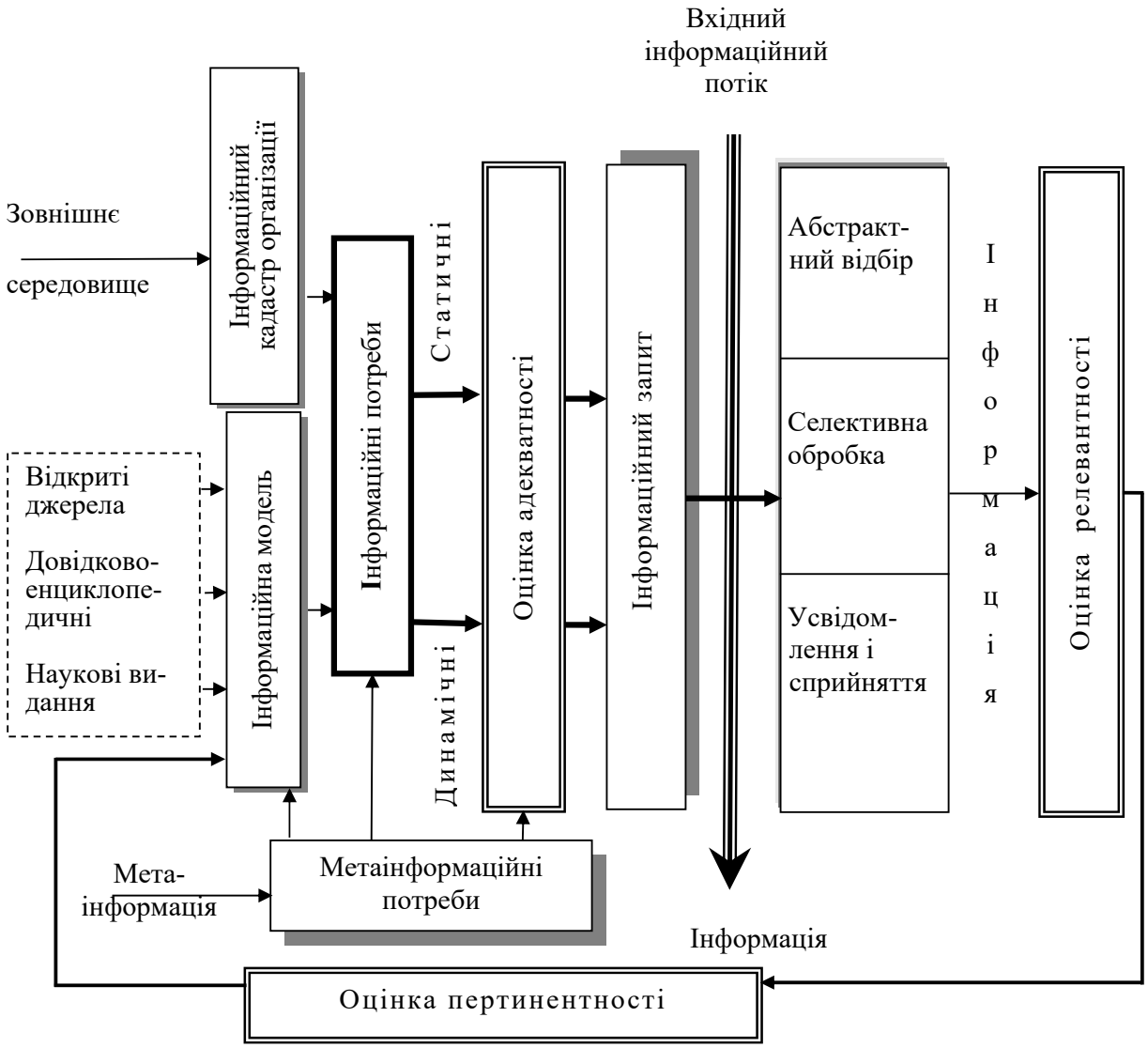

Рис. 9.1. Послідовність формування й задоволення інформаційних потреб у межах інформаційної діяльності

У наведеній схемі не розглядається окремо взаємодія інформаційних моделей споживача та фахівця з оброблення інформації. Будемо уважати, що вказана структура прийнятна як для першого, так і для другого випадків. При розг-

ляді цієї структури стосовно споживача інформаційна модель фахівця випущена як проміжна.

Окремо слід зупинитися на формуванні інформаційних потреб під впливом так званих сторонніх джерел інформації. Останніми будемо вважати джерела інформації, які існують поза або не залежно від самої установи чи організації. Всі сторонні джерела інформації можна умовно поділити на три групи:

1) відкриті джерела, у тому числі засоби масової інформації, науково-популярна й художня література (сюди відносять усі газетні та журнальні публікації, повідомлення радіо і телебачення тощо);

2) довідково-енциклопедичні видання і їхні електронні копії (до них належить вся інформація, яку можна отримати за допомогою різноманітних широкотематичних і вузькопрофільних довідкових та енциклопедичних видань;

3) наукові видання і навчальна література (спеціальні вузькотематичні видання, які висвітлюють окремі наукові напрями і розробки).

Перша група сторонніх джерел інформації є найоб'ємнішою. Як уже зазначалося, саме вона використовується для формування інформаційної моделі особистості й цілісної картини світу. Відкриті джерела надають максимум інформації про навколишню дійсність, політичну, економічну та соціальну ситуацію в країні, світі.

На відміну від розглянутих вище джерел інформації, довідково-енциклопедичні видання застосовуються набагато рідше. Їх основне призначення – надання споживачу узагальненої інформації з усіх можливих питань, які стосуються життя й діяльності людини та навколишнього світу. Основною властивістю таких масивів повинна бути універсальність. Довідково-енциклопедичні матеріали можуть бути структуровані приблизно таким чином:

1. Відомості, що стосуються особливостей використання мовних засобів, які висвітлюють окремі питання правопису, лексики, семантики, орфографії, фразеології, синтаксису тощо. Тут маються на увазі передусім різноманітні довідники і словники, у тому числі тлумачні, фразеологічні, слововживання, іноземних і рідковживаних слів. Використання цих інформаційних масивів дозволить підвищити рівень мовної культури спеціалістів.

2. Відомості з географії, зокрема фізичні та політичні карти й атласи від окремого населеного пункту до земної поверхні в цілому, довідники адміністративно-територіального розподілу, покажчики географічних назв.

3. Відомості, які стосуються суспільно-політичних і соціально-економічних аспектів розвитку людини, соціальних груп, суспільства й держави. Тут маються на увазі універсальні енциклопедії й довідники, а також аналітичні видання з історії, політики, економіки, правознавства, соціології, екології й т. ін.

4. Відомості про історію та сучасний стан і розвиток науки й техніки (засобів виробництва).

5. Відомості про основні напрями фундаментальної науки (фізики, хімії, біології, медицини тощо).

Становленню й розвитку довідково-енциклопедичних масивів необхідно приділяти постійну увагу. Із метою економії засобів і ресурсів їх доцільно зберігати в електронному вигляді на магнітних носіях. Однак при цьому слід забезпечити безперервний доступ до цих відомостей, а також навчити їхніх користувачів ефективному пошуку.

Розглядаючи третю групу сторонніх джерел інформації (наукові й навчальні матеріали), слід зазначити, що до неї входять відомості, які рідко використовуються. Звернення до них може здійснюватися лише у виняткових випадках, коли з'являється необхідність глибокого вивчення досить специфічного питання.

Розглянута сукупність сторонніх джерел інформації, особливо їхня друга група, відіграє важливу роль як у підвищенні ефективності інформаційної діяльності в цілому, так і в стимулюванні й корегуванні інформаційних потреб споживачів.

На жаль, не всі спеціалісти ефективно застосовують наявну інформацію у своїй діяльності. У зв'язку з цим необхідно розглянути цілий клас суб'єктів інформаційної діяльності, який об'єднує так званих інфонеспоживачів.

Природа інфонеспоживання полягає насамперед у неготовності інформаційної моделі особистості до сприйняття інформації. Адже бажання отримувати інформацію виникає у споживача лише тоді, коли він відчуває, що його власних знань недостатньо для побудови інформаційної моделі. При цьому людина повинна усвідомлювати свою потребу в інформації. Тобто, потреба в інформації тісно пов'язана зі свідомістю особистості. А відсутність такої потреби може розглядатися як її неусвідомлення або невираженість. Однак у деяких випадках інфонеспоживання є результатом дії інших факторів.

Першу спробу класифікації інфонеспоживачів здійснив В.З.Коган. За аналогією, наведемо класифікацію інфонеспоживачів інформаційної продукції:

- проінформовані;
- всезнаючі;
- скептики;
- завантажені;
- байдужі;
- самостійні;
- залежні;
- заперечувальники.

Проінформовані становлять єдиний клас інфонеспоживачів, щодо яких не потрібне стимулювання інформаційних потреб. До цієї категорії належать потенційні споживачі, які вже володіють інформацією, що їм пропонується. Зрозуміло, що надавати їм ту саму інформацію не тільки не доцільно, але й не припустимо. Це призведе до небажаних наслідків у вигляді інформаційного перенасичення і збитковості. Утім, від інформації, що пропонується, можуть відмовлятися й потенційні споживачі, яким ці відомості непотрібні, оскільки не відповідають їхнім прямим функціональним завданням.

Всезнаючі відмовляються від інформації, яка їм пропонується, з тієї причини, що вони нібито і так все знають. Однак насправді може з'ясуватися, що потенційний споживач не знає окремих фактів, узагальнених відомостей тощо. Таким чином, уявлення, які склалися в цього споживача, є неповними, в них може бути відсутня цілісність.

Скептики відмовляються від пропонованої інформації через побоювання заплутатися в сукупності всіх відомостей і невпевненість у здатності їх якісно обробити. Деякі з них остерігаються, що надана інформація просто не стане їм у нагоді.

Завантажені не бажають отримувати інформацію нібито через дефіцит часу. При цьому недоотримання інформації часто призводить до ще більших часових витрат на пошуки цих самих відомостей іншими шляхами.

До байдужих належать потенційні споживачі, які не виявляють жодного інтересу до появи нової інформації та поповнення своїх знань. Їхня інформаційна модель характеризується загальною пасивністю.

Самостійні відмовляються від інформації, оскільки уважають, що можуть добути її самі або взагалі обійтися без неї.

До залежних належать ті споживачі, чиї інформаційні потреби залежать від указівок і розпоряджень керівництва. Вони формально керуються наявними наказами й інструкціями, пропускаючи при цьому потрібну їм інформацію.

Заперечувальники відмовляються від споживання будь-якої інформації, оскільки думають, що вона ні за яких обставин не стане їм у пригоді.

Іншим аспектом проблеми інформаційного споживання є надмірне споживання інформації. При цьому споживач не лише збирає всю потрібну й непотрібну йому інформацію, але, не встигаючи її обробити, "тоне" в інформаційному потоці.

Останній випадок, на нашу думку, є досить рідкісним. Значно частіше трапляється недоспоживання інформації. У зв'язку з цим розглянемо деякі заходи, у тому числі педагогічного, просвітницького характеру, які б стимулювали розвиток інформаційних потреб споживачів.

Передусім необхідно запропонувати заходи із стимулювання інформаційного інтересу й підвищення адаптивності інформаційної моделі спеціаліста до сприйняття широкого діапазону інформації. З цією метою можуть бути використані різні форми спілкування: бесіди, лекції, обмін досвідом тощо. При цьому повинен передаватися максимум метаінформації про об'єкти й події, які потенційно можуть зацікавити спеціаліста.

Стимулюванню інформаційних потреб, а також їх структуризації та адекватності вираження в інформаційному запиті можуть сприяти заходи, спрямовані на "прозорість" інформаційного супроводження. Така "прозорість" полягає в пропаганді й роз'ясненні основних принципів інформаційного супроводження як одного з елементів інформаційної діяльності, спрямованого на задоволення інформаційних потреб.

Таким чином, можна стверджувати, що важливим аспектом інформаційної діяльності спеціаліста, що вказує на рівень інформаційної культури, виступає формування його інформаційних потреб. Тоді роль інформаційної культури буде полягати в розвитку інформаційної моделі спеціаліста й удосконаленні його інформаційних потреб. Крім того, інформаційна культура повинна відігравати провідну роль при підготовці інформації з метою задоволення зазначених потреб. Ця проблема, а також питання залежності ступеня розуміння та сприйняття спеціалістом інформації від рівня його інформаційної культури будуть розглянуті в наступній главі.

9.2. ІНФОРМАЦІЙНИЙ ВПЛИВ СУСПІЛЬСТВА НА ФОРМУВАННЯ ОСОБИСТОСТІ ФАХІВЦЯ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ

Робота з інформацією, її сутність і зміст, а також проблема відповідної підготовки кадрів не можуть розглядатися у відриві від процесів, пов'язаних із сприйняттям і переробленням інформації особистістю.

Практично будь-яка система освіти, орієнтована на передання особі певних знань, формування відповідних умінь і навичок, фактично ставить за мету відтранслювати індивіду деякі масиви інформації й забезпечити їхнє сприйняття.

Виходячи з цього, можна стверджувати, що будь-яка діяльність, пов'язана із сприйняттям і переробленням інформації, крім практично-перетворювальної функції, частково реалізує освітню функцію.

Тож робота з інформацією містить елементи освітньо-виховного процесу, а останній тісно пов'язаний з інформаційним сприйняттям. При цьому виховання й освіта, а також інформаційне сприйняття мають єдину пізнавальну природу. Тому в подальшому при розгляді питань підготовки кадрів до інформаційно-аналітичної роботи аналізуватимемо процес професійного становлення особистості передусім із позицій її інформаційного розвитку.

Від народження індивіда його розвиток, виховання і становлення як особистості здійснюється під впливом інформації, отримуваної в процесі комунікативної взаємодії з навколишнім світом. До того ж, якщо для побутової чи суспільної комунікації інформаційний вплив має, як правило, випадковий характер, то освітньо-виховний процес передбачає здійснення на особистість виключно цілеспрямованого інформаційного впливу.

Кожна особистість є продуктом (результатом) інформаційного впливу як випадкового, так і цілеспрямованого характеру. Кожний фахівець із захисту інформації з обмеженим доступом, який приступає до роботи з інформацією, апріорно має певний досвід її сприйняття й оброблення. Тому вказаний вид діяльності не є для нього принципово новим і, здавалося б, не вимагає вивчення нових форм і методів оброблення. Разом із тим, робота з інформацією неможлива без розуміння поставлених цілей, вивчення нових алгоритмів її оброблення. Слід ураховувати, що особливості процесу оброблення інформації багато в

чому залежать від змісту останньої. При цьому кожна нова порція інформації здійснює певний вплив на особистість – збільшує обсяг її знань.

Виходячи з цього, можна стверджувати, що для фахівця з організації захисту інформації характерна наявність певних початкових умінь і навичок роботи з інформацією, а також їхній подальший розвиток і вдосконалення. Таким чином, неперервний вплив інформації на індивіда протягом усього його життя зумовлює постійний розвиток умінь і навичок оброблення цієї інформації. Тому характерною особливістю підготовки фахівців з організації захисту інформації є її неперервність.

Неперервність освіти – один із найважливіших принципів, який надає особистості можливість постійно поглиблювати свій загальноосвітній рівень і рівень професійної підготовки. Неперервна професійна освіта сприяє досягненню цілісності й послідовності в навчанні та вихованні, перетворенню навчання і подальшого вдосконалення отриманих умінь та навичок на процес, який триває протягом усієї професійної діяльності індивіда.

Таким чином, фахівець з організації захисту інформації зазнає неперервного впливу двох взаємопов'язаних процесів – освітнього та інформаційного. При цьому інформація одночасно виступає і як засіб навчання (виховання), і як об'єкт оброблення. При розгляді проблеми підготовки кадрів до роботи з інформацією особливо важливо взяти до уваги вплив двох зазначених вище факторів.

Перш ніж заглиблюватися в пошуки ефективних шляхів підвищення професійного рівня фахівців з організації захисту інформації, слід виявити соціальні й педагогічні умови формування особистості під дією інформації, що надходить до неї з навколишнього середовища. Також доцільно розглянути процес професійної соціалізації як результат дії інформації, проаналізувати особливості взаємодії в системі "людина – інформація", які виступають передумовою до подальшого формування особистісних якостей і професійних умінь та навичок, необхідних для якісного оброблення інформації. Розкриття механізму такої взаємодії зумовлює розгляд функцій інформаційного суспільства, через які формується свідомість особистості.

Методологічну основу подальшого дослідження, на нашу думку, становить поняття інформації. Саме з'ясування його сутності й змісту надасть можливість якісно розглянути проблеми становлення інформаційного суспільства і в цьому контексті проаналізувати рівень загальної та спеціальної підготовки фахівців з

оброблення інформації, а також напрацювати на цій основі рекомендації щодо їхнього вдосконалення.

У цьому зв'язку актуальний весь комплекс питань, пов'язаних з інформацією, включаючи її властивості, особливості, види, а також похідні поняття, наприклад знання. Заслуговує на увагу і середовище, в якому відбувається взаємодія в межах системи "людина – інформація". Саме таким середовищем є інформаційне суспільство.

Лише застосування такого комплексного підходу дасть змогу охопити й адекватно інтерпретувати всю множину різноманітних факторів, що впливають на становлення особистості в інформаційному аспекті, а також пояснити їхню роль у професійній підготовці фахівців з організації захисту інформації та підготувати рекомендації, спрямовані на підвищення професійного й загальноосвітнього рівня.

Поняття інформації (від латинського informatio – роз'яснення, викладення, поінформованість) застосовувалося здавна. У найбільш загальному випадку під ним розуміють повідомлення про що-небудь; відомості, які є об'єктом зберігання, перероблення та передавання; відомості про навколишній світ і процеси, що в ньому відбуваються та сприймаються людиною; відомості про стан справ у якійсь галузі; відомості про що-небудь; деякі відомості, сукупність яких-небудь даних, знань тощо.

Першим поняття інформації в науці вжив К.Шеннон, який розробив математичну теорію інформації. Останню іноді називають теорією зв'язку або теорією каналів зв'язку. Ця теорія розглядала інформацію з точки зору керуючих сигналів у кібернетичних системах. Але при цьому не враховувалися різноманітні аспекти інформації, в тому числі якісний, смисловий, ціннісний. Через однобокість такого підходу теорія К.Шеннона неодноразово критикувалася. Однак саме вона відіграла роль поштовху в подальшому дослідженні категорії інформації, її сутності, форм та змісту, що знайшло своє відображення в літературі методологічного й філософського спрямування.

Першою логіко-семантичною теорією інформації була теорія Карнапа та Бар-Хіллела, яка заклала основи широкого застосування семантичної логіки, логічної семантики, аналізу інформаційного змісту. Пізніше багато вчених робили спроби дослідити гуманітарні аспекти інформації, розробити підходи до

оцінювання її смислу, цінності тощо. Підтвердженням цього можуть бути тлумачення інформації, які найбільш широко застосовуються науковцями:

- позначення змісту, що був отриманий із зовнішнього світу в процесі пристосування до нього (Н.Вінер);
- заперечення ентропії (К.Бріллюен);
- передання різноманітності (У.Ешбі);
- оригінальність, новизна; ступінь складності структур (А.Моль);
- імовірність вибору (Яглом);
- упорядковане відображення різноманітності (А.Урсул).

Усі визначення інформації відображають різноманітні підходи до її дослідження. При цьому у вітчизняній літературі перевага надається останньому визначенню, уведеному А.Д.Урсулом у 1971 році. Це визначення, зважаючи на його всепоглинаючий характер і філософську природу, прийняте як основне, базове, таке, що найкращим чином уособлює всі різноманітні аспекти феномену інформації. Тому слід стисло розтлумачити зміст "відображеної різноманітності". Відображення – це загальна властивість рухомої матерії. У найбільш широкому розумінні під властивістю відображення розуміють здатність будь-якого об'єкта реагувати певними змінами своєї структури на вплив іззовні, а також зовнішньою відповідною дією, в результаті якої у відображувальній системі відтворюються в тій чи іншій формі особливості, властивості відображуваного об'єкта. Інакше кажучи, відображення – це відтворення об'єкта в іншому класі взаємодії. (Як приклад можна навести вольтметр, який відображає характеристику електричного кола). Поняття взаємодії, що лежить в основі відображення, більш широке, ніж поняття інформації. Лише взаємодію, що приводить до впорядкованого відображення, можна пов'язувати з поняттям інформації. Насправді, наявність інформації, що сприймається, залежить від відображувальної системи та її готовності до використання отриманої інформації. Найвищим видом відображувальних систем є людська свідомість.

За В.З.Коганом, процес відображення, тобто формування інформації, можна представити як послідовність, у результаті якої виділяються властивості об'єкта, формуються відомості про них і повідомлення, які містять ці відомості. Інформацією є кількість сприйнятих із повідомлення відомостей. Уважається, що інформація є всюди, де є різноманітність, неоднорідність.

Таким чином, відображення і його результат – інформація – виникають унаслідок взаємодії двох довільних матеріальних систем. При цьому важливою спі-

льною рисою відображення й інформації визнається ізоморфізм, який проявляється у взаємооднозначній відповідності відображуваного й відображення, джерела інформації й самої інформації. Завдяки ізоморфізму відображення, уведення між системою, що відображається, і системою, що відображає, будь-якої кількості опосередковуючих систем дозволяє змінювати лише її форму при збереженні змісту. Цим і зумовлена необхідність розрізняти зміст і форму відображення в інформаційних процесах. Оскільки немає абсолютно невпорядкованих систем, то запропоноване А.Д.Урсулом розуміння інформації як впорядковане відображення різноманітності може бути застосовано до будь-якої відображувальної системи незалежно від рівня організації цієї системи, від якого можуть залежати лише якісно різні види інформації.

Саме відображення породжує складність, неоднозначність, суперечливість взаємовідносин змісту й форми в інформаційних феноменах. Найчастіше змістова сутність інформації проявляється дуже опосередковано, неявно, через оболонку її форми. Аналіз змісту інформаційних процесів передбачає розкриття його структури, дослідження його елементів, зіставлення із структурою процесу відображення, з'ясування природи інформації, виявлення й дослідження інших аспектів інформаційних процесів.

Окрім розуміння змісту поняття інформації, досить важливе розуміння її природи, трактування її сутності. До цієї проблеми є два підходи – функціонально-кібернетичний та атрибутивний. Прихильники функціонально-кібернетичної концепції (М.І.Жуков, О.М.Коршунов, Б.С.Українцев та ін.) тлумачать інформацію як властивість лише самокерованих, самоорганізуючих систем, живих організмів, суспільства. На їхню думку, виникнення інформації залежить від рівня розвитку і складності організації системи.

Прихильники іншої концепції (В.М.Глушков, А.Д.Урсул, І.Земан та ін.) уважають інформацію атрибутом будь-якої системи, в тому числі неживої. При цьому В.М.Глушков зазначав, що не обов'язково пов'язувати з поняттям інформації вимоги її осмисленості. Інформацію несуть не лише конкретні повідомлення, але й, наприклад, шум дощу, шелестіння листя. Характерно, що різниця між цими двома підходами полягає переважно у визнанні тих чи інших меж екстраполяції інформації. Чим ці межі ширші, тим глибше буде розуміння проблеми.

Сама природа інформації зумовлює різноманітність аспектів, із точки зору яких інформація може виступати об'єктом дослідження. Оскільки в нашій роботі увага буде приділятися впливу змісту інформації на свідомість особистості, то

насамперед нас цікавитимуть синтаксичний, семантичний, гносеологічний, аксіологічний, праксеологічний, системний аспекти, які стисло й розглянемо.

Синтаксичний аспект передбачає оцінку якості кодування інформації за допомогою різноманітних знакових систем, оцінку форми подання інформації.

Семантичний аспект інформації ставить питання про знаходження оптимальних для фіксації значень видів знакових виразів і оптимальних для формування змісту структур повідомлень, їх змістовності.

Гносеологічний аспект передбачає розгляд загальних принципів, засобів, методів теоретичного пізнання, а також логіко-семантичний аналіз когнітивної інформації.

Аксіологічний аспект пов'язується з проблемами визначення цінності інформації. Академік А.А.Харкевич визначав цінність інформації як те, наскільки вона сприяє досягненню поставленої мети. Одна й та сама інформація може мати різну цінність, якщо її розглядати з точки зору використання з різною метою. Також не можна не враховувати багатоаспектний характер цінності. У найбільш загальному випадку, окрім цільової залежності, можна виділити залежність цінності від споживача інформації. Це передбачає, що інформація містить об'єктивну істину про навколишню дійсність незалежно від того, як ця інформація сприймається окремими суб'єктами. При цьому А.Моль пов'язує цінність інформації з її неочікуваністю, непередбаченістю, оригінальністю.

Праксеологічний (прагматичний) аспект торкається питань використання інформації в практичній діяльності, а також ефективності впливу інформації на поведінку її споживача і рішення, які він приймає. Саме цей аспект визначає освітній і виховний вплив інформації.

Системний аспект ґрунтується на таких системно-інформаційних принципах:

- принцип інформаційної цілісності (інформація, яка диференційована за вузькими галузями, повинна в подальшому об'єднувати ці галузі);
- принцип максимально можливої повноти (діяльність має насичуватися інформацією з максимально можливою повнотою);
- принцип "проконтровості" (в діяльності необхідно враховувати позитивні ("pro") і негативні ("contra") аспекти).

Однак системний аспект не обмежується тільки цими принципами. Адже інформація не лише задовольняє системні вимоги, а й відіграє важливу роль у функціонуванні різного роду систем. Тоді призначення інформації в найбільш

загальному вигляді може бути зведене до створення умов для досягнення двох цілей – забезпечення стійкості й розвитку відповідної системи.

В цьому випадку інформацію можна визначити як специфічний атрибут об'єктивного світу, що створює умови, необхідні для стійкості й розвитку систем різної природи.

Чим складніша система об'єктивного світу, тим складніші, різноманітніші ті види інформації, які необхідні для досягнення в цій системі вказаних вище цілей. Стійкість і розвиток системи досягається в результаті раціонального управління. Останнє не можливе без оброблення циркулюючих інформаційних потоків. Більш того, сутність управління й полягає в прийнятті раціональних рішень на основі наявної інформації. Таким чином, управління в системах будь-якої природи має інформаційний характер. Діалектичний зв'язок інформації й управління проявляється не лише в безпосередньому використанні інформації з метою управління системою, а й у появі інформації в результаті відхилення деяких параметрів від допустимих.

З іншого боку, інформація виступає не лише як фактор, необхідний для функціонування систем, а і як критерій оцінювання рівня їх організованості. Тобто інформація визначає ступінь організованості системи, а її протилежність, ентропія, – ступінь дезорганізованості. Як уважає Ю.А.Шрейдер, складні системи відрізняються від простих саме семіотичною (тобто повноцінно мовною) природою інформаційних зв'язків між підсистемами. У складних системах обмін інформацією відбувається на семантичному рівні на противагу простим системам, де всі інформаційні зв'язки здійснюються на синтаксичному рівні. У складних системах деяка частина інформації використовується проти зростання ентропії системи (так званий "антиентропійний ефект"). Складна система є високоорганізованою і неентропійною, якщо управління й здатність до адаптації розподілені в ній на всіх рівнях ієрархії з можливістю самоорганізації в найнижчих ланках.

Кожна особистість за рівнем обміну інформацією може розглядатися саме як високоорганізована система, формування якої є результатом цілеспрямованого виховного впливу шляхом передавання їй певних обсягів інформації. До того ж отримана інформація підвищує "антиентропійний ефект", а зменшення ентропії в термінах системного підходу адекватне підвищенню рівня вихованості, загальноосвітньої та професійної підготовки.

Остаточне розуміння інформації як системи й ролі інформації у функціонуванні різноманітних, зокрема високоорганізованих, систем не можливе без методологічного обґрунтування, яке намагався розробити Брукс у межах теорії "трьох світів" К.Поппера. Ця теорія передбачає наявність таких структур:

1. Світ усіх фізичних тіл, сил і полів цих тіл, а також організмів, мозку (світ матерії).
2. Світ людського мислення, свідомого відчуття, думок, почуттів, цілей, планів, дій (світ суб'єктивного знання).
3. Світ продуктів людського духу, мови, міфів, наукових теорій, творчості, мистецтва (світ об'єктивного знання, світ культури).

Теорія "трьох світів" дозволяє об'єднати матеріальний та ідеальний підходи до вирішення основного питання філософії; пов'язати прогресивний розвиток матерії з процесами відображення і накопичення інформації. Більш того, як указує Е.А.Сєдов, у цьому випадку підтверджується істинність атрибутивного підходу до інформації. Адже в неживій природі також існують найпростіші види інформаційної взаємодії, які переходять у живу природу і відповідають формам руху (їхнім матеріальним носіям):

- механічна (маси);
- фізична (молекули);
- хімічна (атоми);
- біологічна (білки);
- соціальна (індивідууми).

Таким чином, об'єкти неживої природи містять інформацію у своїй структурі. Як атрибут матерії, інформація брала участь у процесах її самоорганізації, сприяла виникненню живого. А з появою життя вона стала використовуватися цілеспрямовано для збереження цілісності в умовах впливу навколишнього середовища і виступати як ступінь упорядкованості структур та їхньої взаємодії; об'єктивна характеристика на всіх стадіях організації матерії.

Інформація, як і матерія, рух, була й буде завжди. Це невід'ємний атрибут матерії й руху. Як уважають сучасні вчені, інформація є філософською категорією, вона задовольняє всі вимоги, які висуваються до філософської категорії. Інформація така ж основна категорія, як простір, час, матерія, енергія.

Інформаційний підхід до розвитку світу дає змогу сформувати інформаційну картину світу, яка підтверджує послідовний розвиток усієї матерії як спадкове

накопичення інформації, різноманітність. Інформаційна картина світу підтверджує також діалектику як процес розвитку видів інформації, з одного боку, і як накопичення різноманітності (зародження і вдосконалення інформаційних структур) – з іншого. Інформаційна картина світу наочно й цілісно представляє загальні зв'язки та взаємозумовленість явищ розвитку. Крім того, вона містить максимальний інформаційний масив, який може бути використаний у процесі навчання і виховання особистості, а також сприяти її професійній соціалізації.

Зрозуміло, що жодна людина не зможе засвоїти інформаційну картину світу в повному обсязі, але остання становить, так би мовити, ідеальну модель, до якої слід прямувати. Спроби розглядати проблеми навчання й виховання з позицій інформаційного підходу робив відомий німецький філософ і педагог О.Ф.Больнов. При цьому він намагався пояснити феномен інформації, відштовхуючись від філософських проблем комунікації та спілкування, в основі яких лежить педагогічна теорія й екзистенціальна філософія.

Розглянувши різні аспекти феномену інформації та установивши зв'язок між інформацією і проблемами її сприйняття, слід зазначити, що на формування особистості впливає не вся наявна інформація, а лише її найвища форма – соціальна інформація. Адже це єдина форма інформації, що циркулює в суспільстві та інших соціальних системах. Саме через цю інформацію відбувається формування знань особистості, набуття нею необхідних умінь і навичок. М.С.Коган під соціальною інформацією розуміє сприйнятий зміст повідомлення щодо того чи іншого факту, що передається індивідом або їхньою групою. На думку І.Б.Новіка, соціальна інформація є когнітивною інформацією в соціальній формі або суспільною формою індивідуальної свідомості.

Соціальна інформація може бути по-різному класифікована. Зокрема А.Д.Урсул виділяв ідеальну й матеріальну соціальну інформацію. Матеріальна інформація є довільною відображеною різноманітністю у сфері взаємодії природи та суспільства, що не обов'язково відображається у свідомості індивіда, а характеризує лише процеси відображення в соціальних об'єктах, які є предметами, що існують поза свідомістю індивіда (тобто мають специфічно соціальну природу). Ідеальна інформація виступає як відображення різноманітності об'єктивної реальності у свідомості й формах діяльності суб'єкта (суспільства).

Також визначають два рівні соціальної інформації. До першого належить інформація, що використовується індивідом у його діяльності. Це суспільно-історична інформація, об'єктивована в матеріальних носіях духовна культура.

До другого рівня відносять інформацію, яку суб'єкт отримує в процесі пізнання об'єктів (вільна інформація). Ці два рівні поєднуються в інфосферу.

Однак найбільш обґрунтованою класифікацією соціальної інформації слід уважати засновану на концепції В.З.Когана, згідно з якою всю різноманітність соціальної інформації можна звести до двох видів – семантичної та естетичної. При цьому семантичною є інформація, яка піддається універсальній логіці, має закінчену структуру, передбачає точне уявлення, перекладається на інші мови. Естетична інформація не може бути адекватно виражена в певній знаковій системі. Вона, як правило, є унікальною як за своєю формою, так і за змістом; теоретично не "перекладається" на іншу мову, оскільки іншої мови для передавання цієї інформації не існує.

Окремим підкласом соціальної інформації є інформація спеціальна (професійна), яка має значення в межах певних формальних соціальних груп. Вона має професійний характер, потреба в ній індивіда детермінується належністю до тієї чи іншої формальної структури. Намагання отримати таку інформацію усвідомлюється як необхідність оволодіння апріорним інформаційним масивом для вироблення алгоритму прийняття рішення в професійній діяльності.

Найбільший вплив на особистість із боку соціальної інформації здійснюється тоді, коли для цього створені відповідні умови. Основною такою умовою є перехід до так званого інформаційного суспільства, в якому інформації й інформаційним потокам відводиться пріоритетна роль. Підвищення ефективності формуючого впливу на особистість соціальної інформації в умовах інформаційного суспільства можна пояснити, розглянувши сутність цього соціального утворення.

Концепція "інформаційного суспільства" вийшла із західної концепції "постіндустріального суспільства". Програма інформатизації суспільства розроблялася в Японії, там була апробована перша у світі модель інформаційного суспільства. У Німеччині кібернетик Г.Браун розробляв концепцію "комп'ютерної демократії". На Гаваях американський соціолог Г.Беккер проводив практичний експеримент із "теледемократії". Вже під час указаних заходів були виявлені окремі фактори, що впливають на процес формування особистості та її інформаційну безпеку.

Наведемо деякі з визначень інформаційного суспільства.

Інформаційне суспільство – це децентралізована, така, що динамічно розвивається, система рівнозначних взаємопов'язаних підсистем: економіки, політики, культури (науки, технології, системи цінностей).

Інформаційне суспільство – соціальна система, в якій наукова інформація стає фактором соціально-економічних якісних змін; знання стає основною виробничою силою суспільства. Інформаційне суспільство відрізняється від суспільства, в якому домінують традиційна промисловість і сфера послуг, тим, що інформація, знання, інформаційні послуги і всі галузі, пов'язані з їх виробництвом, зростають більш швидкими темпами, стають домінуючими в економічному розвитку.

А.І.Ракітов наводить критерії, за якими можна отримати уявлення про ступінь наближеності суспільства до інформаційного:

1) будь-який індивід, група осіб, організація тощо можуть отримати будь-яку інформацію і знання, необхідні для їх життєдіяльності й нормального функціонування;

2) у суспільстві має функціонувати технологія, яка забезпечує виконання пункту 1;

3) повинні існувати розвинені інфраструктури, що забезпечують створення національних інформаційних ресурсів;

4) суспільство у змозі виробляти всю необхідну для своєї життєдіяльності інформацію;

5) відбуваються радикальні зміни соціальних структур, наслідком яких є розширення сфери інформаційної діяльності й послуг.

Для філософії інформаційне суспільство – це майбутня модель руху матерії від стратегії природи до стратегії розуму. Інформаційне буття зумовить новий рівень свідомості, мислення, сформує інноваційні якості самої людини.

Із позиції соціальної педагогіки, інформаційне суспільство – це суспільство, в якому максимально реалізовуватимуться можливості з виховання і навчання людини, а також всебічного розвитку особистості на основі інформації, що отримується і переробляється. Перехід до інформаційного суспільства повинен супроводжуватися створенням потужної, глибоко ешелонованої системи освіти та розвитку в індивіда творчих здібностей, напрацювання високого інтелектуального потенціалу й потенціалу самодостатності.

Найкраще сутність механізмів впливу суспільства на формування особистості розкривається при розгляді інформаційної ієрархії суспільства. На думку

деяких учених, зокрема В.З.Когана, указана ієрархія містить два компоненти: інфопотік та інфофонд. Під інфопотоком розуміють ту інформацію, яка в цей час циркулює в суспільстві, використовується як соціальна в будь-якому вигляді діяльності. Інфофонд – вся інформація, якою володіє суспільство на поточному етапі його розвитку. Інфофонд – стійке утворення, його структура визначається обсягом і змістом інформації, яка постійно в ньому перебуває або знову надходить до нього. Уявлення про інфофонд пов'язані з селекцією інформації, її верифікацією, накопиченням тощо. Таким чином, інфофонд становить стале консервативне утворення, яке важко піддається будь-яким змінам. Крім того, інфофонд можна умовно розділити на дві частини – використовувану й невикористовувану (динамічну і статичну). Невикористовувана частина, як правило, врешті-решт відмирає і залишає інфофонд. Тобто вона не може використовуватися для формування особистості. Більш практична динамічна частина інфофонду. Це відносно стабілізовані інформаційні масиви, які піддаються постійній корекції з боку зовнішнього середовища. Іншими словами, цю частину інфофонду становлять знання.

Знання є унікальним феноменом в інформаційних процесах, головним багатством інформаційного суспільства. Вони, з одного боку, виступають ніби складовою інформації, а з іншого – цілком незалежні від неї. Слід одразу зазначити, що ототожнення знань з інформацією неприпустиме. Ці поняття характеризують процес людського пізнання з різних підходів: знання – лише з гносеологічного, інформацію − здебільшого з комунікативного.

Можна сказати, що знання є особливим видом інформації, що володіє низкою властивостей, яких вся інша інформація не має. До таких властивостей передусім слід віднести системність. Насправді, будь-які знання повинні бути систематизовані. Інакше їх не можна назвати знаннями.

По-друге, знання завжди є істинним, об'єктивним відображенням реальності на противагу інформації (інформація – відображена різноманітність). При цьому знання досить часто мають вигляд сформованих законів або теорій.

Із цього випливає наступна властивість знань, яка може бути охарактеризована як статичність. Знання, як правило, є консервативними за своєю сутністю й інваріантними по відношенню до часового фактору. Тобто, після своєї появи знання, як правило, не піддаються суттєвим деформаціям. Вони можуть лише доповнюватися чи уточнюватися.

Таким чином, знання характеризують об'єкт із точки зору статики інформаційного процесу, а інформація – його динаміки. При цьому знання формуються шляхом перероблення (систематизації, аналізу тощо) деяких суттєвих інформаційних фрагментів.

Інструментом формування інфофонду є інфопотік. Характер інформації, яку приносить інфопотік, та інтенсивність останнього визначають динаміку інфофонду, характеризують темпи його застарівання й розвитку. В інфопотоці відображається все розмаїття навколишнього середовища. За своєю потужністю інфопотік адекватний інфофонду. Адже елемент інфопотоку підтверджує, доповнює або спростовує кожний елемент інфофонду. Таким чином, інфопотік становить багаточленне полісемантичне утворення.

Інформацію, що циркулює в інфопотоці, умовно можна розділити на три класи: особиста, спеціальна, масова.

Інформація першого класу відображає ті чи інші події у сфері особистого життя індивіда. Час і розмах її циркуляції дуже обмежені і в більшості випадків прямують до нуля. Досить рідко, коли інформація цього класу стосується особи високого соціального статусу (особисте життя, здоров'я тощо), вона може мати своє відображення в інформації третього класу. Вплив такої інформації на становлення особистості обмежується родинним колом або особистими контактами індивіда.

До другого класу належить інформація, що використовується в межах певних формальних соціальних груп. Вона має професійний або вузько спрямований характер, потреба індивіда в ній детермінується належністю до тієї чи іншої формальної структури. До цього класу відносять усю інформацію (знання), що отримуються особистістю в процесі різноманітних видів діяльності. Однією з властивостей спеціальної інформації є те, що вона може отримуватися шляхом перетворення інформації першого класу, а також сама перетворюватися на інформацію третього класу. Її вплив на формування особистості виражається передусім через передання їй знання.

Масова інформація – найбільш поширений і найбільш використовуваний клас інформації. Сюди слід віднести всі види соціальної інформації, яка не входить у перші два класи. При цьому слід зазначити, що такий клас інформації здійснює найбільший вплив на становлення й формування особистості. Рівень і якість інформації третього класу, що надходить до індивіда, повністю визначають його життєву, світоглядну, соціальну, ідеологічну та інші позиції.

Суспільство загалом і окремі соціальні групи впливають на формування особистості шляхом доведення до її свідомості тієї чи іншої інформації третього класу. Однак однією з головних умов цілісності й неперервності педагогічного впливу з боку соціальної інформації є несуперечливість інфопотоку масивам інфофонду. Насправді, досить проблематично довести за допомогою інфопотоку інформацію, яка суперечить знанням, що містяться в інфофонді. На підтвердження справедливості цієї тези можна зауважити, що, скажімо, в 70-ті роки XX століття з різних причин не була можлива сучасна інтерпретація історії України. Лише після змін, які систематично вносилися до інфофонду через інфопотік, відбулися суттєві трансформації його певної частини. Вони дозволили використовувати той самий інфопотік для доставляння нових знань.

Однак слід зазначити, що можливості інфопотоку з поширення інформації досить обмежені внаслідок так званих інформаційних бар'єрів. Вони є тим фактором, який обмежує ступінь інформаційного впливу суспільства на формування особистості. На думку деяких учених, найбільш повну класифікацію інформаційних бар'єрів пропонує О.В.Єлчанінова:

- географічні – визначаються відстанню між джерелом та споживачем інформації;
- історичні (часові) – пов'язані з часовим проміжком між моментом появи і моментом споживання інформації;
- державні – визначаються як наявністю державних кордонів, так і відмінностями державно-адміністративного устрою;
- відомчі – зумовлені передусім функціональною структурою й функціями тих чи інших установ і організацій;
- режимні – є найбільш характерними для спецслужб і спрямовані на запобігання витоку конфіденційної інформації з метою охорони державної й військової таємниці;
- економічні – виникають як результат нестачі економічних ресурсів, необхідних для нормального обміну інформацією;
- технічні – зумовлені недостатньою розвиненістю технічних засобів, що перешкоджає руху інформаційних ресурсів;
- мовні – є результатом семантичної невідповідності різноманітних систем;
- термінологічні – виникають у результаті взаємодії різноманітних предметних областей;

- психологічні – є наслідком відсутності психологічної готовності індивіда до сприйняття інформації;
- резонансні – виникають у результаті прагматичної невідповідності інформаційних масивів потребам конкретного споживача.

Наведені інформаційні бар'єри відіграють подвійну роль у передаванні інформації від суспільства до людини. З одного боку, вони здійснюють регулюючу (позитивну) функцію, запобігають міграції надлишкових інформаційних потоків, недоцільному витоку інформаційних ресурсів. При цьому бар'єри виконують також захисну функцію, захищаючи індивіда від непотрібної для нього або навіть шкідливої інформації. Оптимізація системи розстановки інформаційних бар'єрів у подальшому може розглядатися як один із засобів вирішення проблем забезпечення інформаційної безпеки особистості. Водночас інформаційні бар'єри регулюють інтенсивність інфопотоку, його насиченість.

З іншого боку, бар'єри виконують обмежувальну (негативну) функцію, позбавляючи в деяких випадках індивіда доступу до інформації.

Отже, визначальною структурою в ієрархії інформаційного суспільства, під впливом якої відбувається формування особистості, є інфофонд. Безпосередньо механізм впливу суспільства на особистість реалізується через інфопотік. Саме останній виступає сполучною ланкою між суспільством, його інфофондом та кожною окремо взятою особистістю.

Як уважає Ф.Н.Цирдя, саме інформація третього класу орієнтує індивіда в соціальній дійсності, впливає на формування й виховання особистості, визначає її поведінку, сприяє побудові внутрішньої моделі зовнішнього світу. Безпосереднє доведення такої інформації до кожної особистості здійснює суспільна система, яку умовно можна уявити у вигляді трьох елементів:

- культура;
- освіта;
- засоби масової інформації (ЗМІ).

Визначальною в цій тріаді, безумовно, є культура. Адже саме вона містить духовні основи розвитку людини, визначає морально-етичні риси майбутньої особистості. При цьому спостерігається міцний зв'язок між культурою та інфофондом. Останній становить своєрідний інформаційний прототип культури. Він містить усі знання, які входять до її складу. Кожне суспільство формує

найбільш прийнятний для нього симбіоз культурних, релігійних, ціннісних, ідеологічних, світоглядних та інших настанов. Культура може впливати на особистість як безпосередньо (шляхом установлення правил, схем, моделей поведінки), так і опосередковано (через систему освіти, ЗМІ).

Освіта є гносеологічним продовженням культури. Освіта реалізує культуру в практиці й водночас підпорядковується цій культурі. Транслюючи культуру особистості, освіта відіграє провідну роль у її духовному становленні. Саме система освіти закладає життєві й ціннісні орієнтири, формує багаж знань, виводить індивіда на той чи інший рівень культури (як загальної, так і спеціальної). З іншого боку, система освіти за своєю природою є адаптивною відображувальною системою, яка, по суті, лише виконує суспільне замовлення на виховання і професійну підготовку особистості. Тип суспільства повністю детермінує тип системи освіти, тобто апріорно визначає ті чи інші масиви інформації, що мають закладатися до свідомості індивіда. В цьому випадку роль освіти зводиться до ретрансляції суспільних установок в особистісні.

Зв'язок культури зі ЗМІ значно слабший, ніж із освітою. Однак це не заважає ЗМІ здійснювати великий інформаційний вплив на особистість. Те, що ЗМІ відіграють досить важливу роль у процесах формування особистості, пояснюється насамперед двома факторами – динамічністю і неперервністю. Перше означає, що ЗМІ, як правило, повністю відображають динаміку життя суспільства в цілому і його окремих індивідів. Друге свідчить про сталість процесу, що розглядається. ЗМІ забезпечують передання індивіду інформації з інфопотоку, тоді як система освіти орієнтована на передання особистості знань з інфофонду.

Інформація, що передається ЗМІ, не завжди сприймається окремими індивідами. Досить часто вона або ігнорується споживачем, або в силу різноманітних причин узагалі до нього не доходить. Таким чином, освіта відіграє першорядну, а ЗМІ – другорядну роль у формуванні й вихованні особистості. При цьому процес освіти за своєю природою є інформаційним, оскільки полягає в обміні інформацією.

У загальному випадку суттєві властивості інформації та механізми її впливу на формування особистості через суспільство можна подати у вигляді схеми, зображеної на рис. 9.2.

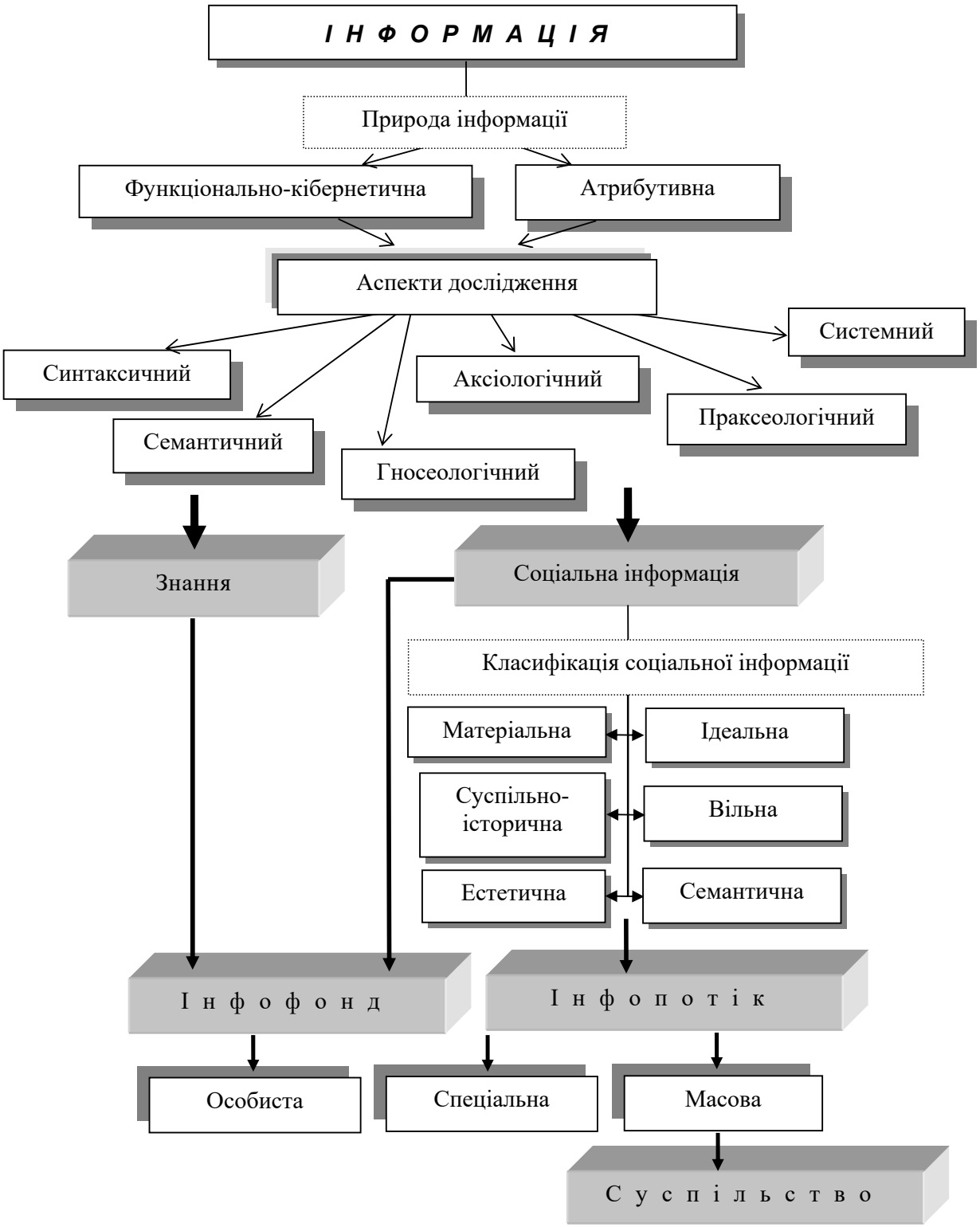

Рис 9.2. Вплив інформації на формування особистості.

Результатом формування особистості, здійснюваного через суспільні механізми, в термінах соціальної педагогіки є соціалізація особистості – складний двосторонній процес становлення особистості, що передбачає включення її в систему суспільних відносин і самостійне, активне відтворення цих відносин. На соціалізацію безпосередньо впливає найближче оточення індивіда, а також його вроджені, спадкові особливості. Вона відбувається одночасно в різних вимірах – особистісному, суспільному, професійному. Кожному виду соціалізації відповідає свій клас соціальної інформації, який, по суті, і здійснює той чи інший вид соціалізації.

Особистісна соціалізація полягає в набутті індивідом цінностей, норм, настанов, властивих його найближчому оточенню, передусім родині. Тут вирішальну роль відіграє інформація першого класу. Саме вона доносить до індивіда особистісні норми та цінності, сприяє їхньому закріпленню й подальшому розвитку.

При цьому особистісна соціалізація тісно пов’язана із суспільною. Здавна відомо, що повноцінне формування особистості можливе лише за умови її розвитку в певному суспільстві, колективі, соціальній групі. Особистість є продуктом колективу, вона детермінується наявними суспільними відносинами. Суспільна соціалізація відбувається через інформацію другого класу. Якщо інформація першого класу націлена, в основному, на формування особистісної інформаційної моделі індивіда, то інформація третього класу орієнтована на корекцію й подальший розвиток цієї моделі в межах інформаційної структури певного суспільства. Під час суспільної соціалізації виробляється ставлення особистості як до суспільства зокрема, так і до навколишнього світу в цілому. При цьому слід ураховувати тісний взаємозв’язок обох видів соціалізації індивіда. Так, особистісна соціалізація ні в якому разі не може бути завершальним етапом соціалізації індивіда. Після неї обов’язково повинна відбуватися суспільна соціалізація. З іншого боку, суспільна соціалізація принципово неможлива без її попереднього етапу – особистісної соціалізації. Відсутність соціалізації на початковому етапі свідчить про несформованість інформаційної моделі особистості, без якої неможливе свідоме сприйняття й пізнання реального світу. Отже, між двома указаними видами соціалізації існує ізоморфний зв’язок. Природно, що такого ж роду зв’язок діє між двома класами соціальної інформації (перший і третій).

Для розуміння глибинної сутності особистісної та суспільної соціалізації необхідно також розглянути роль у цьому процесі й співвідношення між хаотичністю та цілеспрямованістю (випадковістю і закономірністю) в інформації. Слід зазначити, що інфопотік, який відіграє вирішальну роль у забезпеченні індивіда поточною інформацією, є випадковим настільки, наскільки елементи випадковості й хаотичності присутні в дійсності, яка відображається інфопотоком. Таким чином, інфопотік несе в собі позитивну, негативну і нейтральну інформацію по відношенню до соціалізації особистості. При цьому важко спрогнозувати, яка саме інформація здійснить більший або вирішальний вплив на індивіда. І вже від особливостей його характеру, темпераменту, інших особистісних якостей, а також апріорно наявної інформації буде залежати специфіка формування особистості, у тому числі під впливом випадкових факторів.

Разом із тим, схоластичність інфопотоку є досить умовною. Як уже зазначалося, інфопотік не лише формує, але й залежить від змісту інфофонду. Тобто, повинна існувати певна кореляція між цими двома утвореннями, передусім щодо несуперечливості. Зміст інфопотоку не може антагонізувати зі змістом інфофонду. Саме в цьому плані можна стверджувати, що інфопотік є цілеспрямованим і, враховуючи зворотний зв’язок з інфофондом, він (інфопотік) певною мірою детермінується останнім. Отже, незважаючи на хаотичність інформації, яка утворює інфопотік, у ньому не лише присутні, а й переважають відомості, які декларуються інфофондом.

Тому можна зробити висновок, що соціальне, а пізніше й професійне становлення особистості залежить від діалектичної єдності хаотичного та цілеспрямованого в інформаційних процесах.

Професійна соціалізація є завершальним етапом складного процесу соціалізації особистості. Для її успішного здійснення необхідна завершеність двох попередніх видів соціалізації. Професійна соціалізація особистості полягає в повноцінному входженні індивіда у сферу професійних відносин, засвоєнні необхідних знань, умінь і навичок, а також здатності адаптуватися в умовах професійної діяльності й пристосовувати предметну сферу для вирішення актуальних завдань, що стоять перед суспільством. Якщо процес особистісної соціалізації здійснюється за допомогою соціальної інформації першого класу, а суспільної соціалізації – через інформацію як першого, так і третього класів, то професійна соціалізація можлива лише у взаємодії всіх трьох класів соціальної ін-

формації. Якщо індивід повною мірою засвоїв спеціальну інформацію, призначену для нього, набув необхідних професійних умінь і навичок, але через нестачу комунікативних контактів у процесі перших двох видів соціалізації недоотримав необхідний обсяг інформації першого й третього класів, то не можна говорити про його сформованість як особистості, про завершеність процесу соціалізації. І навпаки, професійна соціалізація, що відбувається після або одночасно з процесами особистісної й суспільної соціалізації, є показником завершеності соціалізації загалом і соціальної сформованості особистості.

Таким чином, шляхом інформаційного впливу суспільства на особистість реалізуються через такі функції:

1. Соціалізація особистості на мікрорівні через особистісну інформацію. Передбачає становлення індивіда, пробудження його свідомості й самоідентифікацію стосовно оточуючих його соціальних груп. Ця функція формує особисті ціннісні норми та настанови індивіда.

2. Соціалізація особистості на макрорівні через симбіоз особистісної, суспільної та, можливо, навіть спеціальної інформації. Ця функція завершує формування особистісних орієнтацій, а також закріплює переконання, забезпечує цілісність світогляду й самоідентифікацію в масштабах суспільства і всесвіту.

Соціалізація особистості на спеціалізованому (професійному) рівні відбувається за допомогою передусім спеціальної інформації. Передбачає накопичення в індивіда масивів спеціальних знань, сформованість певних умінь і навичок, накопичення досвіду, становлення індивіда як спеціаліста. Окрім того, ця функція забезпечує зворотність інформаційних процесів, коли не масиви інформації здійснюють формуючий вплив на особистість, а навпаки, особистість чинить домінуючий вплив на формування масивів інформації, їхню структуру та зміст.

У результаті можна стверджувати, що соціалізація особистості (будь-яка її форма) в інформаційному аспекті полягає у формуванні під впливом соціальної інформації певної внутрішньої інформаційної моделі індивіда, яка має у своїй структурі масив як моральних, етичних, ціннісних, світоглядних, загальнолюдських настанов, так і інформаційних, які містять відомості про навколишній світ, суспільство, предметну сферу діяльності. Таким чином, на особистісному рівні утворюється симбіоз уже розглянутих класів соціальної інформації –

особистісної, суспільної, спеціальної. А структура сформованої інформаційної моделі детермінує тип і структуру особистості.

Основним компонентом професійної соціалізації є професійна ідентифікація, яка виражається в самоототожненні індивіда з професійною групою або колективом, у відчутті особистої причетності до вирішення спільних завдань. При цьому професійна ідентифікація повинна містити не лише самоідентифікацію, але й визнання індивіда членами колективу. Саме тут велику роль відіграє як набуття особистістю в процесі перших двох видів соціалізації цінностей, настанов, переконань, так і її комунікативні можливості.

Процес соціалізації, насамперед професійної, має динамічну, а не статичну природу. Це пов'язано передусім із постійними змінами, які відбуваються як у навколишньому світі, так і в практичній діяльності. Тому соціалізація особистості може досягти своєї найвищої стадії – професійної соціалізації, але вона ніколи не буде завершеною. І тут провідна роль належить адаптації як процесу пристосування індивіда до змін навколишнього світу. Соціальна адаптація виражається у здатності особистості існувати й розвиватися в конкретних життєвих умовах. Соціальна адаптація тісно пов'язана із соціальною ідентифікацією. Адже соціальна адаптація починається одночасно з процесом ідентифікації. Вона полягає в пристосуванні індивіда до соціальних, політичних й економічних умов, а також до змін, що відбуваються. Останнє особливо актуальне в умовах нестабільності сучасного суспільства, оскільки соціальна адаптація може ототожнюватися зі здатністю особистості до виживання в складній економічній ситуації.

Всі зроблені вище висновки стосовно особливостей формування особистості під впливом інформації є справедливими незалежно від того, яким видом діяльності буде займатися ця особа в майбутньому. Тому розглянуті положення про властивості інформації, її роль в інформаційному суспільстві та впливі на різноманітні види соціалізації будуть використані в подальшому як методологічна основа при дослідженні проблем професійної підготовки фахівців з ОІ та формування їхньої інформаційної культури.

Стосовно інформації, яка найчастіше піддається аналітико-синтетичному обробленню, слід зазначити, що вона належить до спеціальної соціальної інформації. Проводячи межу між інформацією і знаннями, можна зазначити, що до знань, якими, як правило, оперує фахівець з ОІ, належать відомості про окремі

стійкі структури у сфері економіки, політики, оборони тощо, а до інформації слід відносити відомості про стан цих структур.

Однак при проектуванні розглянутих вище питань на діяльність інформаційно-аналітичних структур найбільший інтерес становлять проблеми професійної адаптації фахівців з ОІ. Необхідність такої адаптації пов'язана як безпосередньо з умовами здійснення професійної діяльності, так із впливом на цю діяльність соціального середовища. Це потребує постійного й безперервного вдосконалення професійних умінь та навичок фахівців з ОІ, підвищення рівня знань. Тому їхня професійна адаптація, особливо на післяідентифікаційному етапі (тобто після набуття необхідних умінь і навичок, засвоєння функціональних обов'язків), повинна бути спрямована на пристосування до роботи в умовах суттєвого збільшення потоків інформації й появи нових інформаційних технологій. Таким чином, вона полягає в постійному насиченні фахівців з ОІ переважно другого і третього класів. Тобто, розміри та структура апріорної інформації детермінують відповідні параметри апостеріорної інформації. А в термінах теорії управління будь-який фахівець з ОІ становить відкриту динамічну систему, вихідний потік інформації якої визначається не лише і не стільки вхідним потоком службової інформації, скільки соціальною і, головне, внутрішньою інформаційною моделлю індивіда, яка піддана впливу соціальної інформації.

9.3. МЕТОДИКИ ФОРМУВАННЯ УМІНЬ І НАВИЧОК РОБОТИ З ІНФОРМАЦІЄЮ

Наведені в цьому підрозділі методики формування умінь роботи з інформацією спрямовані, з одного боку, на підвищення професійного рівня у сфері оброблення інформації, а з іншого – на розвиток інформаційної культури фахівця з ОІ.

Оскільки проблема навчання роботі з інформацією практично не досліджувалась, до цього питання ми спробували підійти двома шляхами. В першому випадку були проаналізовані методики навчання роботі з текстами, які використовуються в освітніх закладах при викладанні курсів мови і літератури. Зазначені методики зорієнтовані на роботу з *конкретними* художніми текстами. Розвиваючи текстову логіку й образність сприйняття, формуючи уявлення про зв'язність і цілісність того чи іншого літературного твору, ці методики

найменше спрямовані на аналіз змісту з позицій оцінювання інформативності, цінності, практичного застосування відомостей, що містяться в тому чи іншому тексті. Тим більше зазначені методики не пропонують і не можуть пропонувати якого-небудь алгоритму оброблення інформації, зокрема щодо її сприйняття і засвоєння.

З іншого боку, при розробленні методик формування умінь роботи з інформацією була зроблена спроба скористатися наявними напрацюваннями в галузі бібліотекознавства. Огляд літератури в цій сфері свідчить про орієнтацію на роботу з книгою як носієм інформації, а не з інформацією конкретно. Напрацьовано безліч рекомендацій, у тому числі методичного характеру, що стосуються технічних аспектів пошуку й структурування літератури. Викладаються способи роботи з книгою, принципи організації бібліотечних каталогів тощо. Але питання методики оброблення інформації (зокрема проблема смислового аналізу змісту того чи іншого твору з метою віднесення до певного розділу каталогу) залишаються нерозкритими. Кожна людина сприймає, оцінює й аналізує інформацію виключно з позицій особистого суб'єктивізму (в нашій термінології – інформаційної моделі особистості). Водночас будь-яке коригування інформаційної моделі з позицій педагогіки не передбачається.

Викладене ще раз підтверджує необхідність розроблення методик формування умінь роботи з інформацією, а також указує на новизну й актуальність зазначеної розробки.

Надалі сформулюємо основні вміння роботи з інформацією, а також запропонуємо методики їх формування. При цьому зауважимо, що останні виходять насамперед з алгоритму (тобто послідовності дій), якого слід дотримуватися при роботі з інформацією.

До основних умінь роботи з інформацією відносять:

- уміння оцінювання інформації;
- уміння селекції інформації;
- уміння аналізу інформації;
- уміння інформаційного моніторингу;
- уміння критичного сприйняття інформації;
- уміння орієнтування в спеціальній інформації;
- уміння роботи з джерелами інформації;
- уміння інформаційної гігієни.

Перераховані уміння доцільно розподілити на дві групи: ті, які безпосередньо використовуються в інформаційній діяльності, й ті, що використовуються опосередковано. До першої групи належать уміння оцінювання, селекції, аналізу інформації, а також інформаційного моніторингу, які надалі будемо називати *безпосередніми.* До другої групи віднесемо уміння критичного сприйняття інформації, орієнтування в спеціальній інформації, роботи з джерелами інформації, інформаційної гігієни, які називатимемо *опосередкованими*. Такий розподіл зумовлений ступенем практичного використання тих чи інших умінь безпосередньо в процесі оброблення інформації. Тобто безпосередні уміння застосовуються в інформаційній діяльності, а опосередковані виступають скоріше як фонові, тобто такі, що обов'язково повинні бути присутні, але не завжди можуть застосовуватися.

Розкриємо зміст і наведемо методики формування кожної групи умінь.

В основу безпосередніх умінь покладені передусім ефекти сприйняття, а також згортання й розгортання інформації. Розкриваючи сутність зазначених умінь, зауважимо, що оцінювання, селекція, аналіз, моніторинг інформації як елементи інформаційної діяльності проводяться виключно в аспекті подальшого практичного застосування цих відомостей. Результати перероблення інформації використовуються як гносеологічна основа прийняття рішень. Саме тому оцінювання, селекція, аналіз і моніторинг інформації здійснюються, виходячи з конкретного завдання, для виконання якого й обробляється інформація. Залежно від змісту і спрямованості цього завдання можуть бути отримані різні результати, тобто одна й та сама інформація в різних умовах із точки зору її важливості, інформативності тощо може бути кваліфікована *по-різному* й ініціювати прийняття *різних* рішень.

При оцінюванні, селекції, моніторингу інформації завдання трансформуються в цілі, згідно з якими й відбувається оброблення інформації. Тому далі розглянемо деякі особливості постановки цілей.

Будь-яка мета може бути сформульована в трьох вимірах:

- від суб'єкта (хто, що);
- від об'єкта (з ким, чим);
- від процесу (що саме зробив).

У меті "від суб'єкта" вказуються характерні властивості суб'єкта, тобто учасника певного процесу. В меті "від об'єкта" називаються характерні властивості

об'єкта, над яким суб'єкт здійснює певну дію. Об'єктами можуть виступати певні засоби або продукти виробництва, сфери діяльності. У меті "від процесу" вказуються характеристичні властивості процесу, тобто зміст дії, яку суб'єкт чинить над об'єктом. Залежно від характеру завдання мета може бути сформульована як в одному, так і в кількох вимірах. Кількість вимірів, що використовуються при визначенні мети, детермінує обсяг і властивості інформації, яка переробляється.

Зважаючи на викладене, розглянемо процес формування безпосередніх умінь.

Формування *умінь оцінювання інформації* можна здійснювати двома способами.

У першому, більш простому випадку інформація оцінюється шляхом зіставлення так званих ключових слів, що зустрічаються в тексті. Для цього в того, хто навчається, формується чітко виражена структура ключових слів, яка дозволяє однозначно оцінювати інформацію. При цьому тексти, що несуть різноманітну інформацію, обов'язково будуть містити певний інваріантний набір повторюваних слів, які і є ключовими. Завдання об'єкта навчання полягає у виділенні цього інваріантного набору, його фіксуванні, запам'ятовуванні, а також у впізнанні контекстних ситуацій, у яких можуть зустрічатися ключові слова. Тоді при поверховому перегляді тексту достатньо знайти знайомі ключові слова й зафіксувати контекстну ситуацію, у якій вони зустрічаються. Якщо контекстна ситуація буде знайомою, одразу можна оцінити всю інформацію. Сама ж структура ключових слів буде утворюватися поступово в процесі детального (можливо неодноразового) прочитання оцінюваної інформації, а якість зазначеного утворення буде підвищуватися із набуттям досвіду.

Оцінювання текстів за ключовими словами доцільно здійснювати у випадках їх вузької тематичної спрямованості. Залежно від наявності в тексті ключових слів можна однозначно відповісти на питання щодо тематики зазначених відомостей, а отже, оцінити їх із позицій перспективності використання для вирішення поставленого завдання.

Окремим випадком оцінювання інформації з використанням ключових слів є оцінювання шляхом визначення наявності чи відсутності в тексті певної особистої назви, насамперед назви організації (наприклад, "Фієста", "Авіант").

Якщо ж тематична спрямованість тексту досить широка, спиратися на ключові слова недоцільно, оскільки це може призвести до некоректної оцінки. В цій ситуації тому, хто навчається, не вдасться сформувати набір ключових слів або ж відомі ключові слова будуть зустрічатися в нестандартних контекстних ситуаціях. Тоді застосовується так зване "смислове читання", коли фіксується смисл тексту, а не його формальні характеристики, якими є ключові слова. Для цього необхідно, передусім з'ясувати сутність дії, про яку йде мова: відшукується дієслово (воно в більшості випадків присутнє) і встановлюється смисловий зв'язок між об'єктом і суб'єктом дії. Зрозумівши сутність тексту, об'єкт навчання буде в змозі здійснити його оцінку.

Слід зазначити, що в обох випадках уміння оцінювання інформації формуються і проявляються швидше при роботі з інформацією, тематична спрямованість якої відома і звична для того, кого навчають, а текст, який її містить, має адекватну структурованість, зв'язність, абстрактність, насиченість, понятійний апарат. Інакше необхідна переорієнтація інформаційної моделі об'єкта навчання, яка здійснюється в процесі неодноразового прочитання ним текстів із відповідними характеристиками. Наприклад, якщо людина має досвід роботи з науковими текстами, які характеризуються високим рівнем структурованості, практичною відсутністю емоційної забарвленості й наявністю спеціального понятійного апарату, то вона (людина) буде не здатна без попередньої підготовки оцінювати публіцистичний текст, який є менш структурованим і абстрактним, більш емоційним, із використанням узагальненого понятійного апарату в порівнянні з науковим текстом.

Щодо сутності оцінювання інформації необхідно зазначити, що це оцінювання може здійснюватися у двох аспектах:

- оцінювання тематичної спрямованості інформації;
- оцінювання практичної важливості (можливості застосування) інформації.

Зрозуміло, що в першому випадку інформація оцінюється лише з метою визначення її тематики; у другому − відбувається зіставлення змісту інформації з певною існуючою незалежно від цієї інформації метою, що може об'єднати в собі кілька різноманітних тематик, а також прикладний аспект використання оцінюваної інформації. Простіше кажучи, оцінювання практичної важливості інформації зводиться до бінарної відповіді (типу "так-ні") на одне з питань:

- чи відповідає оцінювана інформація поставленій у вигляді набору тематик меті оцінки;
- чи може оцінювана інформація використовуватися в подальшому.

Запропонована методика формування умінь оцінювання інформації найбільш прийнятна для роботи з порівняно невеликими текстами (обсягом 5−10 тисяч друкованих знаків). За умови відповідної адаптації інформаційної моделі того, хто навчається, такі тексти можуть оцінюватися досить ефективно. При виникненні необхідності оцінити інформацію, яка міститься в тексті обсягом більше десяти тисяч друкованих знаків, його слід умовно поділити на менші фрагменти.

Таким чином, наведена методика, на нашу думку, може використовуватися для набуття умінь оцінювання інформації на віднесеність до певної тематики, а також щодо можливості її подальшого використання.

Уміння селекції інформації необхідні для відбору інформації з наявного інформаційного масиву з деякою наперед заданою апріорною метою. Формування зазначених умінь повинно відбуватися послідовно, в три етапи. При цьому на першому етапі той, хто навчається, формулює мету відбору інформації, яка є зовнішньою стосовно самої інформації. На другому етапі відповідно до сформульованої мети виділяються критерії відбору інформації, згідно з якими на завершальному (третьому) етапі буде безпосередньо відбиратися інформація. Для формулювання мети селекції об’єкт навчання чітко з’ясовує поставлене перед ним завдання. При цьому мета може бути сформульована вузько або розширено, залежно від чого вона може бути віднесена до однієї з трьох груп:

1. Група, яка містить найбільш узагальнені цілі, що стосуються тієї чи іншої тематики в цілому.

2. Група з помірними за обсягом цілями, що стосуються окремих проблем з тієї чи іншої тематики.

3. Група, до складу якої входять найбільш вузькі цілі, які стосуються окремих суб’єктів, що проходять за визначеною тематикою.

На другому етапі розширені цілі передбачають формування множини різноманітних критеріїв, окремі з яких можуть бути використані при відборі інформації з більш вузькими цілями.

Слід зазначити, що на практиці розширені цілі використовуються значно рідше, ніж вузькі. Це пояснюється можливістю практичного застосування відібраної інформації. Разом із тим, критерії відбору інформації для розшире-

них цілей сформувати значно важче, ніж критерії для вузьких, оскільки для розширених цілей виявляється досить трудомістким побудувати систему критеріїв, передбачивши всі можливі випадки при відборі інформації. У зв'язку з цим інколи при селекції інформації з розширеною метою доцільно не будувати критерії, що описують цю мету, а здійснювати смислове співвіднесення інформації, що відбирається, із самою метою. Утім, у цьому процесі, безумовно, буде присутня певна частка суб'єктивізму.

Зрозуміло, що елементи суб'єктивізму залишаться й на третьому етапі, коли той, хто навчається, буде порівнювати відібрану інформацію із сформульованими критеріями й приймати остаточне рішення. Адекватність остаточного рішення буде залежати від рівня сформованості інформаційної моделі об'єкта навчання, тобто чим досконаліша інформаційна модель, тим коректніше буде здійснюватися селекція інформації.

Формування умінь аналізу інформації частково полягає у відстеженні змін у стані об'єкта дослідження, для чого необхідно відповісти на такі питання:

1. У чому полягає сутність процесу зміни? У цьому випадку пропонується встановити, який об'єкт змінюється, що відбувається з ним в процесі зміни, чи переходить він з одного стану в інший або перетворюється на інший об'єкт.

2. У чому полягають причини й умови, що сприяли виникненню процесу зміни?

3. Який механізм процесу зміни?

Уміння аналізу інформації ґрунтуються на інформаційній моделі особистості. Безпосередньо процес аналізу інформації буде здійснюватися шляхом її порівняння з інформаційною моделлю. У цьому випадку пропонується дотримуватися такого алгоритму:

1. З'ясувати, про який об'єкт іде мова. Для цього встановлюється учасник дії, якого стосуються викладені відомості. Таким об'єктом може бути фізична особа, група осіб, підприємство, організація, установа тощо.

2. З'ясувати, в якому процесі зазначений об'єкт задіяний. Для цього установлюється сутність дії, розкривається її характер, прогнозуються можливі наслідки.

3. Оцінити, чи становлять зазначені об'єкт і процес інтерес для дослідника. Така оцінка здійснюється, виходячи із поставлених завдань та мети аналізу.

4. У випадку, якщо описувані об'єкт чи процес становлять інтерес для дослідника, бажано відшукати в інформаційній моделі ідентичні інформаційні масиви, які можуть бути використані як критерій при аналізі інформації. Ознакою ідентичності інформаційних масивів є наявність у них відомостей стосовно об'єкта чи процесу, інформація про які аналізується.

5. Установити логічні зв'язки між власною інформаційною моделлю й аналізованою інформацією. Для цього з'ясовується, що є спільного та відмінного в цій інформації й інформаційній моделі.

6. Шляхом зіставлення відповідних інформаційних масивів інформаційної моделі й інформації, що аналізується, визначити такі характеристики останньої:

- важливість;
- достовірність;
- повнота;
- можливість практичного застосування.

При цьому важливість може бути оцінена як ступінь впливу такої інформації на подальше прийняття рішень.

Достовірність визначається як загальна несуперечливість аналізованої інформації, що міститься в інформаційній моделі. В деяких випадках, якщо інформація суперечить інформаційній моделі, але, на думку дослідника, все-таки є достовірною, необхідно провести додаткові заходи для її перевірки. Водночас приймається рішення про можливу корекцію інформаційної моделі на основі інформації, що аналізується.

Повнота оцінюваної інформації визначається через кількість питань і незрозумілостей, що залишаються після прочитання інформації.

Загалом є два підходи до визначення повноти оцінюваної інформації. В одному випадку повнота тієї чи іншої інформації може визначатися як те, наскільки закінчено викладені в зазначеній інформації відомості. Тобто, для того, щоб така інформація була визнана повною, необхідно, щоб вона містила повний опис об'єктів і процесів, про які йде мова.

В іншому випадку повнота оцінюваної інформації визначається з позицій раніше відомої інформації з цього питання або проблеми. Отже, визначається не повнота інформації безпосередньо, а те, наскільки ця інформація доповнює вже наявні відомості, або ж те, чи достатньо зазначеної інформації для прийняття рішення з того чи іншого питання професійної діяльності. Таким чином, у

другому випадку повнота є суб'єктивною характеристикою, оскільки загальне розуміння того, про що йде мова в тексті, залежить не стільки від самого тексту, скільки від інформаційної моделі особистості. Адже нерідко уривчаста інформація доповнює відомості, що містяться в інформаційній моделі, й робить їх закінченими у смисловому відношенні.

Можливість практичного застосування оцінюється як потенціал використання цієї інформації при прийнятті рішень, оцінюванні або аналізі іншої значущої інформації. Так, якщо інформація містить нові відомості, які раніш були невідомі, то вона може суттєво вплинути на хід управлінської діяльності й процес прийняття рішення.

Уміння інформаційного моніторингу полягають у здатності виділяти з досліджуваного інформаційного потоку важливі інформаційні фрагменти. Інформаційний моніторинг може здійснюватися для вирішення двох завдань. Це, по-перше, відбір або оцінка вхідного інформаційного потоку на предмет наявності в ньому відомостей, що можуть бути використані для вирішення поставлених завдань; по-друге, загальна оцінка змісту повідомлень, із яких складається інформаційний потік, із метою визначення інформативності, повноти та інших характеристик цього потоку. Для вирішення першого завдання доцільно використовувати частковий інформаційний моніторинг, а для вирішення другого – повний.

Спершу розглянемо методику формування умінь часткового інформаційного моніторингу. На початку об'єкт навчання з'ясовує мету моніторингу, яка визначає критерії "значущості" окремих інформаційних повідомлень. Зазначені критерії трансформуються в перелік тематик, за якими відбирається й оцінюється інформація.

При цьому основне завдання того, хто навчається, полягатиме в оптимальному доборі елементів зазначеного списку, щоб останній не був перевантаженим або занадто деталізованим і водночас максимально відображав тематичну спрямованість інформаційного потоку. Слід зазначити, що моніторинг може здійснюватися не за одним, а за кількома завданнями, тобто відбирається інформація з кількох проблем. Тоді формуються окремі списки тематик із кожної проблеми, які на завершальному етапі інтегруються в загальний список.

Характерною особливістю часткового інформаційного моніторингу з однією або множиною цілей є те, що частина інформаційного потоку, що не відповідає

поставленим завданням, ігнорується і не знаходить свого відображення в списку тематик.

Для того, щоб отримати повний список тематик, відомості за якими наявні в інформаційному потоці, застосовується повний інформаційний моніторинг, коли замість однієї або кількох конкретних цілей використовується одна загальна мета, яка може бути сформульована як повне відображення усіх без винятку наявних в інформаційному потоці тематик. Слід зазначити, що практично здійснити такий моніторинг у повному обсязі досить важко. Адже кількість елементів списку тематик може бути великою, що значно ускладнить роботу з ним. Якщо припустити, що теоретично в інформаційному потоці містяться повністю різнорідні за своєю тематикою повідомлення, тоді в списку тематик повинно бути відображене кожне з цих повідомлень. Іншими словами, кількість елементів списку тематик буде дорівнювати кількості повідомлень в інформаційному потоці.

Як проміжний між частковим і повним інформаційним моніторингом можна запропонувати моніторинг з “антиметою”, коли визначаються одна або множина “антицілей”, згідно з якими інформація не повинна вноситися до списку тематик.

Як правило, список “антицілей” детермінує сам інформаційний потік. Остаточний вибір типу інформаційного моніторингу визначається завданням, що стоїть перед тим, хто навчається, і характеристиками інформаційного потоку.

Таким чином, сформовані повною мірою безпосередні уміння роботи з інформацією дозволяють забезпечити її якісний відбір, оцінювання й аналіз.

Опосередковані уміння є інваріантними стосовно характеру поставлених завдань, мети оброблення інформації й особливостей інформаційного потоку.

Формування умінь критичного сприйняття інформації відбувається як розвиток здібності виявляти інформаційні фрагменти, які негативно впливають на суспільну й особистісну свідомість. Під такими фрагментами будемо розуміти інформацію, під впливом якої людина або соціальна група приймають не вигідні для себе рішення або ж відбуваються деструктивні зміни в психіці та свідомості осіб. Зазначена інформація, як правило, подається у вигляді патогенних текстів, які пропагують хибні цінності, насаджують викривлене світосприйняття, закликають до змін суспільного та державного устрою. Крім того, критичне сприйняття інформації спрямовується на виявлення різного роду викривлень, фальсифікацій, помилкових суджень, які можуть зустрітися в повідомленні.

Як правило, такі викривлення виявляються в кожному випадку по-різному, на основі різноманітних критеріїв. При цьому провідну роль відіграє рівень розвитку інформаційної моделі, особистий досвід людини. Критичне сприйняття ґрунтується передусім на логічному підході до кожного повідомлення, коли об'єкт навчання повинен оцінити з позицій логіки, наскільки правдивою є ця інформація, які викривлення вона містить або може містити тощо.

Одним із способів фальсифікації інформації є розбиття (декомпозиція) описуваних подій на окремі факти. При цьому дійсна інтерпретація зазначених фактів і зв'язків між ними замінюється іншою, яка не має нічого спільного з попередньою. Таким чином, реальні факти слугують формуванню хибної концепції, яка використовується для їх пояснення і встановлення зв'язків. Така концепція і є фальсифікацією.

У цьому зв'язку для формування умінь критичного сприйняття інформації доцільно запропонувати алгоритм у вигляді запитань, відповівши на які об'єкт навчання зможе зробити остаточний висновок про ступінь своєї довіри до тієї чи іншої інформації:

1. Чи є факти, викладені в повідомленні, логічно пов'язаними між собою? (*Так.*)

2. Чи відповідають висновки фактичному матеріалу, на основі якого вони зроблені? (*Так, в основному відповідають.*)

3. Чи є така інтерпретація повідомлення однозначною? (*Так, скоріше так.*)

4. Чи може бути інша інтерпретація повідомлення? (*Ні, навряд чи, наведена інтерпретація є більш імовірною.*)

5. Чи володіє об'єкт навчання фактичною інформацією, яка суперечить викладеній? (*Ні.*)

6. Чи є зв'язки, встановлені між різними фактами і посиланнями, штучними? (*Ні.*)

7. Чи робиться в повідомленні спроба підмінити одні поняття іншими? (*Ні.*)

8. На якому аспекті – раціональному чи емоціональному – робиться акцент у повідомленні? (*Раціональному.*)

Якщо більшість відповідей збіглася з наведеними в дужках, то можна зробити висновок, що інформація не містить блоків, спрямованих на маніпулювання свідомістю особистості, нав'язування їй хибної точки зору тощо. В іншому ж випадку можна стверджувати протилежне.

Надалі розглянемо процес формування *умінь орієнтування в спеціальній інформації*. Під спеціальною інформацією в цьому випадку будемо розуміти інформацію з певної предметної сфери, наприклад наукову, технічну, пов'язану з виробництвом, підприємництвом, банківською системою тощо. Уміння орієнтування в такій інформації формуються в процесі роботи з нею, оволодіння понятійним апаратом відповідної предметної сфери. На ступінь оволодіння відповідними уміннями найбільший вплив здійснює рівень розвитку інформаційної моделі особистості. Адже чим більш розвинутою є зазначена модель, чим ширший світогляд особистості, тим легше їй сприймати нові відомості, з'ясовувати їхню сутність, оволодівати новітніми поняттями, у тому числі спеціальними знаннями з певної галузі. Водночас, якщо процес засвоєння нового відбувається швидше, то менше зусиль витрачається на вивчення інформації, яка це нове містить.

Для формування умінь орієнтування в спеціальній інформації можна запропонувати такий алгоритм:

1. Виділити основні (ті, що зустрічаються найчастіше) поняття.
2. Виділити допоміжні (інші) поняття.
3. Виділити об'єкти та суб'єкти (якщо такі є).
4. Установити зв'язки між різними поняттями, а також між об'єктами і суб'єктами.
5. З'ясувати мету тексту, розкрити сутність процесів, що відбуваються.

Викладений алгоритм зорієнтований на формування умінь, які дозволять спеціалісту зрозуміти текст, що містить спеціальну інформацію й стосується окремої галузі знань, а також установити потребу його подальшого використання в процесі оброблення іншої інформації або при прийнятті рішень.

Уміння роботи з джерелами інформації (далі − ДІ) використовуються для пошуку необхідної інформації. Вони формуються як здатність:

1. Знаходити ДІ.
2. Визначати можливість використання наявних (знайдених) ДІ.
3. Відшукувати у відібраних ДІ потрібні відомості.

Зважаючи на те, що ДІ можуть бути подані як у друкованому, так і в електронному вигляді, зазначимо, що їхній пошук може відбуватися по-різному.

Наприклад, для пошуку потрібної літератури в бібліотеках і документів в архівах необхідно знати основні принципи організації каталогів, рубрикаторів тощо. Для пошуку інформації в автоматизованих системах, а також у комп'ютерних мережах, у тому числі глобальних, слід мати уявлення про принципи побудови таких систем, а також навички роботи з ними. В обох випадках об'єкт навчання повинен володіти додатковими знаннями про особливості систематизації інформації при її зберіганні в тому чи іншому вигляді. Уміння пошуку інформації в зазначених системах формуються лише в процесі практичної роботи.

Разом із тим, в окремих випадках для пошуку потрібних ДІ не обов'язково володіти відповідними уміннями й навичками. Якщо систему, в якій зберігається інформація, обслуговують кваліфіковані фахівці, тому, хто навчається, достатньо коректно сформулювати запит на потрібні ДІ, адекватно висловивши свою інформаційну потребу.

Зауважимо, що питання формування інформаційних потреб особистості були детально розглянуті раніше. Тому лише підкреслимо, що важливу роль при пошуку потрібних ДІ для задоволення інформаційних потреб у всіх випадках відіграє метаінформація, яка є своєрідним орієнтиром у сукупності джерел, покажчиком найперспективніших у смислі виявлення потрібних ДІ каталогів, розділів тощо.

Можливість використання наявних (знайдених) ДІ визначається шляхом оцінювання назви джерела, його змісту, анотації й т. ін. Для джерел, що містять невеликі за обсягом документи, наприклад довідки, службові записки, рапорти тощо, достатньо ознайомитися з їхнім змістом, щоб визначити можливість використання.

Про пошук у відібраних ДІ потрібних відомостей доцільно говорити лише для ДІ великого обсягу. Тоді пошук у них необхідної інформації також здійснюється з використанням короткого змісту й анотації.

Отже, уміння роботи з ДІ є одними із найважливіших у плані пошуку потрібної інформації й задоволення власних інформаційних потреб.

Уміння інформаційної гігієни необхідні для запобігання негативному впливу інформації на особистість об'єкта навчання. Зазначені уміння формуються як здатність особистості уникати інформаційних потоків, що руйнують сві-

домість, психіку, викривляють світосприйняття, нівелюють духовні цінності. У зв'язку з цим наведемо основні ознаки інформації, споживання якої бажано обмежити. Ця інформація:

1. Принижує честь і гідність особистості.
2. Викликає роздратування або інші негативні емоції.
3. Пропагує ворожі особистості цінності або намагається здійснити їх підміну.
4. Нав'язує іншу позицію, що суперечить поглядам і переконанням особистості.
5. Намагається впливати на вчинки й поведінку особистості, маніпулювати нею.

Уміння інформаційної гігієни якраз і полягають у розумінні й здатності розрізняти на практиці інформацію із указаними ознаками.

Для усвідомлення наявності зазначених ознак в тих чи інших повідомленнях має здійснюватися психологічна підготовка особистості, що сприяє активізації внутрішнього самоконтролю, постійної оцінки свого психічного й емоційного стану. Людина, у якої ці якості відсутні або розвинені недостатньо, практично не зможе контролювати свій внутрішній стан, а також розрізняти інформацію з наведеними вище ознаками.

Таким чином, уміння інформаційної гігієни є досить специфічними. Вони виявляються не як здатність якісно обробляти інформацію, а як спроможність обмежувати вплив інформації на власну свідомість, контролювати емоції й почуття, які вона викликає, об'єктивно оцінювати вчинки, до яких "підштовхує" ця інформація, та передбачати можливі негативні наслідки.

Завершуючи розгляд методик формування умінь роботи з інформацією, зауважимо, що процеси формування безпосередніх умінь протікають більш інтенсивно, ніж процеси формування опосередкованих умінь. Адже в першому випадку набуттю умінь сприяє сама інформаційна діяльність, яка виступає необхідною й достатньою умовою їхнього активного засвоєння і подальшого успішного розвитку. Опосередковані уміння формуються під час не лише оброблення інформації, а й інших дій, пов'язаних із пошуком необхідних відомостей, прийняттям рішення тощо. Тому, на нашу думку, у того, хто займається

безпосереднім обробленням інформації, безпосередні уміння можуть бути сформовані значно швидше і з меншими зусиллями, ніж опосередковані уміння. Останні ж вимагають створення дещо специфічної обстановки, яка б сприяла формуванню окремих умінь. Наприклад, для набуття умінь орієнтування в спеціальній інформації бажано максимально заглибитися в літературу з певної галузі знань. До того ж було б не погано, щоб викладені там відомості були подані в систематизованому вигляді, що значно полегшило б їх засвоєння. Для набуття умінь роботи з джерелами інформації бажано опрацьовувати різні за змістом і формою подання джерела. Якщо, наприклад, мова йде про друковані видання, то доцільно з'ясувати особливості викладення інформації в різноманітних підручниках, монографіях, довідниках, статтях, рефератах тощо.

Отже, за умови постійного оброблення інформації безпосередні уміння, на відміну від опосередкованих, можна набути за досить короткий проміжок часу. При подальшій роботі вони постійно вдосконалюватимуться і на певній стадії реалізовуватимуться майже автоматично, не вимагаючи концентрації уваги й свідомості того, хто навчається. Останнє свідчить про трансформацію безпосередніх умінь у відповідні навички.

Щодо опосередкованих умінь можна зазначити, що їхня трансформація в навички відбувається дуже повільно, а в більшості випадків може не відбуватися взагалі.

З викладеного можна зробити висновок, що безпосередні уміння оброблення інформації в умовах активної інформаційної діяльності переростають у відповідні навички, а з опосередкованими уміннями таких змін, як правило, не відбувається. Тому зв'язок між уміннями і навичками роботи з інформацією, що формуються й розвиваються в процесі інформаційної діяльності, можна подати у вигляді схеми, зображеної на рис. 9.3.

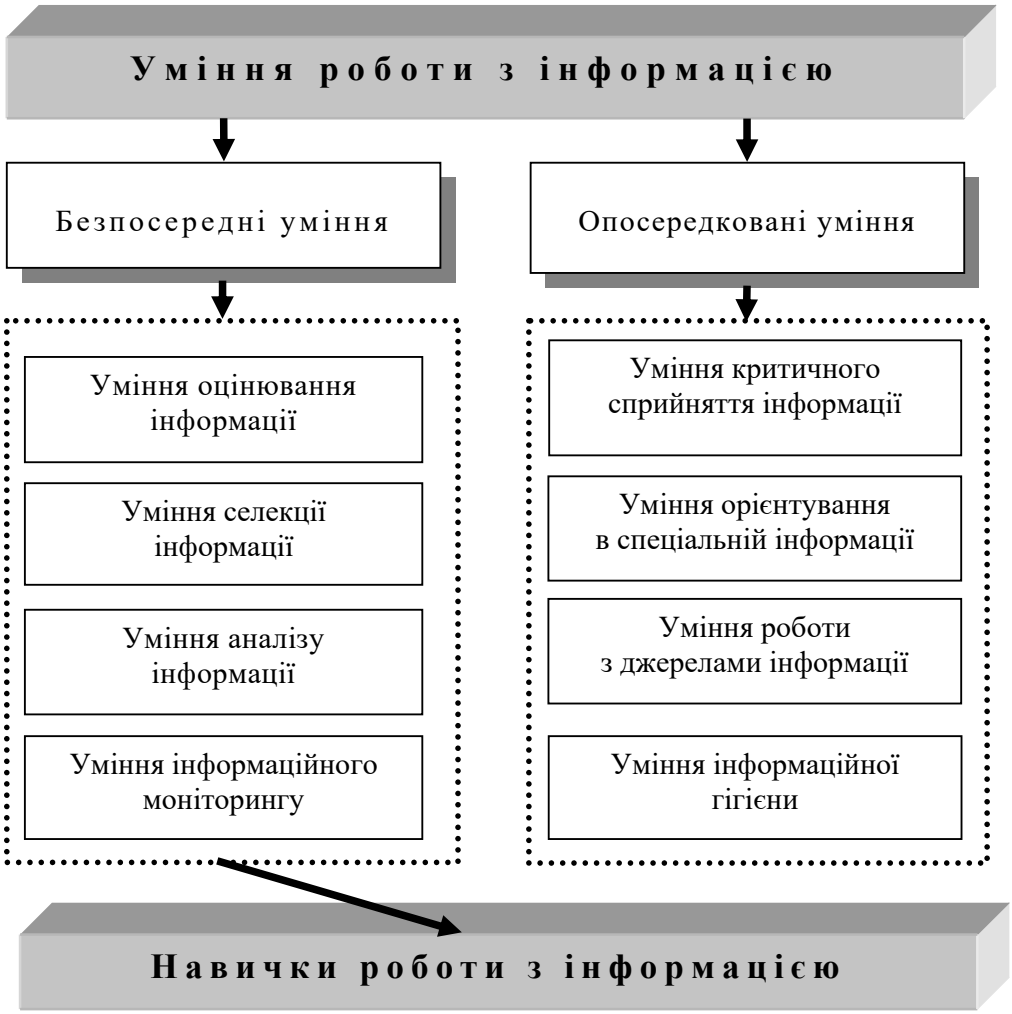

Рис. 9.3. Уміння й навички роботи з інформацією.

На нашу думку, набуття розглянутого вище комплексу умінь роботи з інформацією з подальшим перетворенням окремих із них на навички значно підвищить рівень інформаційної культури спеціалістів, що натомість сприятиме підвищенню ефективності інформаційної діяльності та якості прийняття управлінських рішень. Найкраще розвиток зазначених умінь і навичок відбувається виключно в процесі вирішення практичних завдань, пов’язаних із сприйняттям і обробленням інформації людиною. З огляду на тісний зв’язок умінь і навичок із практичною діяльністю, можна припустити, що надалі ця діяльність потребуватиме і сприятиме розвитку нових умінь. Наприклад, актуалізація завдань, що вимагають побудови інформаційних моделей із подальшим прогнозуванням, спричинить появу відповідних умінь, а пізніше – методики їх формування.

ЗАПИТАННЯ І ЗАВДАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Охарактеризуйте основні уміння роботи з інформацією.
2. У чому полягає відмінність між безпосереднім та опосередкованими уміннями роботи з інформацією?
3. Охарактеризуйте еволюцію семантичної теорії інформації.
4. Розкрийте соціальну природу інформації.
5. Визначте роль семантичної інформації в соціальному управлінні.
6. Перерахуйте основні ознаки інформаційного суспільства.
7. Охарактеризуйте діалектику взаємодії інфопотоку й інфофонду.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абдеев Р.Ф. Философия информационной цивилизации / Р.Ф.Абдеев. – М. : Владос, 1994. – 336 с.
2. Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста / [за ред. В.Д.Базилевича]. – К., 1994. − Ч. 1. – 279 с., Ч. 2. – 171 с.
3. Алексюк А.М. Педагогіка вищої освіти України: історія, теорія : підруч. / А.М.Алексюк. – К. : Либідь, 1998. – 558 с.
4. Алексюк А.М. Педагогіка вищої школи. Курс лекцій : Модульне навчання / А.М.Алексюк. – К. : Знання, 1999. – 220 с.
5. Аллаярова В.С. Личностный потенциал работника: проблемы формирования и развития / [В.С.Аллаярова и др.]. – М. : Наука, 1987. – 228 с.
6. Анализ нечисловой информации в социологических исследованиях / [под ред. В.Г.Андреенкова, А.И.Орлова, Ю.Н.Толстовой]. – М. : Наука, 1985. – 221 с.
7. Аналитико-семантическая обработка информации и подготовка обзоров / [сост. Х.Х.Миропольский и др.]. – М., 1972. – 46 с.
8. Андрющук А.А. Профессионально-ориентированные системы тестирования / А.А.Андрющук. – Луганск, 1997. – 66 с.

9. Аносов А.Д. Проблемы обеспечения информационно-психологической безопасности / А.Д.Аносов, В.Е.Ленский, А.А.Стрельцов // Информационное общество. – 1997. – № 4−6. – С. 43−47.

10. Антонов А.В. Информация: восприятие и понимание / А.В.Антонов. – К., 1988. – 182 с.

11. Антонов А.В. Сприймання та розуміння тексту / А.В.Антонов. – К., 1977. – 48 с.

12. Анурин В.Ф. Эмпирическая социология : учеб. пособ. / В.Ф.Анурин. – М. : Академ. проект, 2003. – 287 с.

13. Апресян Ю.Д. Новый толковый словарь русского языка / Ю.Д.Апресян. – М. : Школа “Языки русской культуры”, 1997. – Вып. 1. – 511 с.

14. Арнольдов А.И. Человек и мир культуры: введение в культурологию / А.И.Арнольдов. – М. : МГИК, 1992. – 240 с.

15. Арсентьев М.В. К вопросу о понятии “Информационная безопасность” / М.В.Арсентьев // Информационное общество. – 1997. – № 4−6. – С. 48−50.

16. Афонін Е.А. Управління соціальною поведінкою військовослужбовців (соціо-психологічний та аксіологічний аспекти) / Е.А.Афонін, В.В.Очеретяний. – Херсон : Взаємодія, 1995. – 20 с.

17. Бабанский Ю.К. Проблемы повышения эффективности педагогических исследований / Ю.К.Бабанский. – М., 1982. – 192 с.

18. Бакатанова В.Б. Психолого-педагогічні умови професійного відбору майбутніх інженерів-педагогів : дис. ... канд. пед. наук / В.Б.Бакатанова. – К., 1996. – 189 с.

19. Барановська О.В. Інформаційні методи навчання учнів / О.В.Барановська ; за ред. В.Ф.Паламарчука. – К. : Знання, 1999. – 34 с.

20. Бар-Хилел И. Основы теории множеств / И.Бар-Хилел, А.Френкель. – М. : Мир, 1966. – 537 с.

21. Баскаков О.Я. Методологічні проблеми формування культури економічних кадрів в сучасних умовах / О.Я.Баскаков ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 1. – С. 14−16.

22. Бережной Н.М. Человек и его потребности / Н.М.Бережной. – М. : Форум, 2001. – 160 с.

23. Береза А.М. Основи створення інформаційних систем / А.М.Береза. – К. : КНЕУ, 1998. – 140 с.

24. Блюменау Д.И. Информация и информационный сервис / Д.И.Блюменау. – Ленинград : Наука, 1989. – 192 с.

25. Блюменау Д.И. Проблемы свертывания научной информации / Д.И.Блюменау. – Ленинград : Наука, 1982. – 166 с.

26. Богданова І.М. Технології в освіті: теоретико-методологічний аспект / І.М.Богданова. – Одеса, 1999. – 146 с.

27. Богуславський И.М. Исследования по синтаксической семантике / И.М.Богуславський. – М. : Наука, 1985. – 175 с.

28. Бородыня В.И. Информационные потребности, их виды и свойства / В.И.Бородыня. – К., 1970. – 123 с.

29. Братко А.А. Информация и психика / А.А.Братко, А.Н.Кочергин. – Новосибирск : Наука, 1977. – 198 с.

30. Брунер Дж. Психология познания за пределами непосредственной информации / Дж.Брунер. – М. : Прогресс, 1977. – 412 с.

31. Бусигін Б.С. Прикладна інформатика / Б.С.Бусигін, Г.М.Коротенко, Л.М.Коротенко. – Д. : НГУ, 2004. – 560 с.

32. Бутенко Н.Ю. Воспроизводство специалистов с высшим образованием / Н.Ю.Бутенко. – К. : КГУ, 1990. – 136 с.

33. Бухштаб Ю.А. Анализ рефератов, документов для целей информационного поиска / Ю.А.Бухштаб, И.М.Губин. – М. : ИПМ, 1985. – 25 с.

34. Бююль А. SPSS: искусство обработки информации. Анализ статистических данных и восстановление скрытых закономерностей / А.Бююль, П.Цефель. – СПб. : ДисСофт, 2005. – 594 с.

35. Вайнер А.Я. Информатика в военном деле / А.Я.Вайнер. – М., 1989. – 126 с.

36. Васильєв В.В. Система адаптації робітників до професійної діяльності / В.В.Васильєв. – Дніпропетровськ : Вид-во Дніпропетровського ун-ту, 1999. – 298 с.

37. Ващекин Н.П. Информационная деятельность и мировоззрение / Н.П.Ващекин, Ю.Ф.Абрамов. – Иркутск, 1990. – 78 с.

38. Вейзе А.А. Реферирование текста / А.А.Вейзе. – Минск, 1978. – 126 с.

39. Верещагина Л.А. Психология потребностей и мотивация персонала / Л.А.Верещагина, И.М.Карелина. – Х. : Гуманитарный центр, 2002. – 153 с.

40. Винарник Л.С. Информационная культура: эволюция, проблемы / Л.С.Винарник, А.Н.Щедрин. – Донецк, 1999. – 144 с.

41. Виноградов В.А. Проблемы информационной деятельности в области социального и гуманитарного знания: статьи и доклады / В.А.Виноградов. – М., 2001. – 318 с.

42. Вишневский Ю.Р. Социологические проблемы образования и духовной культуры / Ю.Р.Вишневский. – Свердловск, 1976. – 95 с.

43. Вишняк А.И. Личность: соотношение трудового потенциала и системы потребностей / А.И.Вишняк. – К. : Наукова думка, 1986. – 108 с.

44. Вінарик Л.С. Ділова оцінка персоналу в умовах комп'ютеризації праці / [Л.С.Вінарик та ін.]. – Донецьк : ІЕП НАН України, 2001. – 48 с.

45. Вітгенштайн Л. Tractatus logicophilosophicus = Філософські дослідження / Л.Вітгенштайн ; пер. з нім. – К. : Основи, 1995. – 311 с.

46. Воробець З.Д. Педагогічний контроль і форми тестових завдань / З.Д.Воробець. – Львів, 1993. – 40 с.

47. Воробьев Г.Г. Документ: информационный анализ / Г.Г.Воробьев. – М. : Наука, 1973. – 255 с.

48. Воробьев Г.Г. Молодежь в информационном обществе / Г.Г.Воробьев. – М., 1990. – 255 с.

49. Воробьев Г.Г. Твоя информационная культура / Г.Г.Воробьев. – М., 1988. – 303 с.

50. Ворожцов А.В. Путь в современную информатику / А.В.Ворожцов. – М. : УРСС, 2003. – 142 с.

51. Воронкова В.Г. Проблеми формування політичної культури майбутнього спеціаліста / В.Г.Воронкова ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 1. – С. 82−84.

52. Гаджиев К.С. Тоталитаризм как феномен XX века / К.С.Гаджиев // Вопросы философии. – 1992. – № 2. – С. 3−25.

53. Гамаонов В.Г. Информация, информатизация, управление: системный подход (Теоретические и прикладные аспекты) / В.Г.Гамаонов. – Владикавказ, 2000. – 192 с.

54. Гамезо М.В. Познавательная функция знаков и психосемиотические факторы ее реализации / М.В.Гамезо // Межвузовский сборник научных трудов. – М., 1988. – С. 5−18.

55. Герасименко В.А. Гуманитарные аспекты современной информатики / В.А.Герасименко // Информатика и вычислительная техника. – 1996. – № 1−2. – С. 8−14.

56. Герасименко В.А. Информатика, информация, информационная грамота / В.А.Герасименко, М.А.Вус // Информатика и вычислительная техника. – 1996. – № 1−2. – С. 12−21.

57. Герасименко В.А. Основы информационной грамоты / В.А.Герасименко. – М., 1996. – 320 с.

58. Герасимов Б.М. Нечеткие множества в задачах проектирования, управления и обработки информации / Б.М.Герасимов, Г.Г.Грабовский, Н.А.Рюмшин. – К. : Техніка, 2002. – 140 с.

59. Гершунский Б.С. Информационное обеспечение прогнозирования развития системы непрерывного образования / Б.С.Гершунский. – М., 1990. – 224 с.

60. Гершунский Б.С. Менталитет и образование / Б.С.Гершунский. – М., 1996. – 156 с.

61. Гершунский Б.С. Методологическое знание в педагогике / Б.С.Гершунский, Н.Д.Никаноров // Политехнический музей. – М. : Знание, 1986. – 109 с.

62. Гершунский Б.С. Перспективы развития системы непрерывного образования / Б.С.Гершунский. – М. : Педагогика, 1990. – 224 с.

63. Гецов Г.Г. Работа с книгой: рациональные приемы / Г.Г.Гецов. – М. : Книга, 1984. – 120 с.

64. Гиляревский Р.С. Научные коммуникации и проблема информационной потребности / Р.С.Гиляревский, В.А.Маркусова, А.И.Черный // НТИ. – 1993. – Серия 1. – № 9. – С. 1−7.

65. Глотова Г.А. Человек и знак: семиотико-психологические аспекты онтогенеза человека / Г.А.Глотова. – Свердловск, 1990. – 253 с.

66. Глушков В.М. Моделирование развивающихся систем / В.М.Глушков, В.В.Иванов, В.М.Яненко. – М. : Наука, 1983. – 350 с.

67. Голицын Г.А. Информация – поведение – творчество / Г.А.Голицын, В.М.Петров. – М. : Наука, 1991. – 224 с.

68. Гольдгамер Г.И. Научно-информационная деятельность / Г.И.Гольдгамер. – М. : Радио и связь, 1987. – 280 с.

69. ГОСТ 16487-83 Делопроизводство и архивное дело: термины и определения. – М. : Изд-во стандартов, 1984. – С. 2.

70. Гречихин А.А. Жанры информационной литературы / А.А.Гречихин, И.Г.Здоров. – М., 1983. – 187 с.

71. Громов Г.Р. Очерки информационной технологии / Г.Р.Громов. – М. : ИнфоАрт, 1992. – 336 с.

72. Гуревич П.С. Культурология / П.С.Гуревич. – М. : Знание, 1996. – 288 с.

73. Дабагян А.В. Совершенствование профессиональной подготовки и переподготовки специалистов в современных условиях / А.В.Дабагян, А.М.Михайличенко. – Х., 1996. – 296 с.

74. Давыдов В.В. Теория развивающего обучения / В.В.Давыдов. – М. : Интор, 1996. – 544 с.

75. Даллес А. Искусство разведки / А.Даллес. – М. : Международные отношения, 1992. – 288 с.

76. Даль В.И. Толковый словарь русского языка / В.И.Даль. – М. : Русский язык, 1979. – Т. 2. – 779 с.

77. Демкова М.С. Доступ до інформації та електронне урядування / М.С.Демкова, М.В.Фігель. – К. : Факт, 2004. – 336 с.

78. Дерваль Л.И. Философия кибернетики (материализация и дематериализация: теория, методика, практика) / Л.И.Дерваль, Л.И.Дерваль-Малеш. – Мукачево : Блакитний кит, 1998. – 307 с.

79. Дмитриев Е.В. Диалектика содержания и формы в информационных процессах : автореф. дисс. на соискание учен. степени канд. философ. наук / Е.В.Дмитриев. – Минск, 1971. – 25 с.

80. Доблаев Л.П. Смысловая структура учебного текста и проблемы его понимания / Л.П.Доблаев. – М. : Педагогика, 1982. – 176 с.

81. Додонов Б.И. В мире эмоций / Б.И.Додонов. – К. : Политиздат Украины, 1987. – 141 с.

82. Доровской В.А. Формализация деятельности человека в эргатических системах / В.А.Доровской. – Кривой Рог : Наука і освіта, 1998. – 263 с.

83. Дослідження психолого-педагогічних особливостей професійної діяльності : методичні рекомендації до самостійної роботи з дисципліни “Основи психології та педагогіки” / [укл. В.А.Козаков]. – К. : КДЕУ, 1995. – 70 с.

84. Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита / Е.Л.Доценко. – М. : Черо, 1997. – 344 с.

85. Дридзе Т.М. Смысловое восприятие речевого сообщения / Т.М.Дридзе, А.А.Леонтьев. – М. : Наука, 1976. – 263 с.

86. Дридзе Т.М. Текстовая деятельность в структуре массовой коммуникации / Т.М.Дридзе. – М. : Наука, 1984. – 268 с.

87. Дридзе Т.М. Язык и социальная психология / Т.М.Дридзе. – М. : Высшая школа, 1980. – 221 с.

88. Дружинин Г.В. Качество информации / Г.В.Дружинин, И.В.Сергеева. – М. : Радио и связь, 1990. – 170 с.

89. Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті / О.П.Дубас. – К. : Генеза, 2004. – 208 с.

90. Дулин С.К. Тематический мониторинг информационных сообщений / С.К.Дулин, И.А.Кисилев, Н.Г.Дулина. – М. : Вычислительный центр РАН, 2000. – 83 с.

91. Елепов Б.С. Управление процессами использования информационных ресурсов / Б.С.Елепов, В.М.Чистяков. – Новосибирск, 1989. – 237 с.

92. Ерасов Б.С. Социальная культурология / Б.С.Ерасов. – М., 1997. – 591 с.

93. Еріксен Томас Гілланд. Тиранія моменту: швидкий і повільний час в інформаційну добу / Еріксен Томас Гілланд. – Л. : Кальварія, 2004. – 195 с.

94. Ефимов Н.А. Информационные потребности / Н.А.Ефимов. – Л., 1982. – 288 с.

95. Єжова Л.Ф. Інформаційний маркетинг : навч. посіб. / Л.Ф.Єжова. – К. : КНЕУ, 2002. – 560 с.

96. Жуков Н.И. Информация (философский анализ) / Н.И.Жуков. – Минск, 1966. – 346 с.

97. Заде Л.А. Понятие лингвистической переменной и ее применение к принятию приближенных решений / Л.А.Заде. – М. : Мир, 1976. – 165 с.

98. Закон України “Про інформацію” від 2.10.1992 р. № 2657-XII.

99. Закон України “Про освіту”.

100. Закон України “Про професійно-технічну освіту”.

101. Зарецкий Д.В. Информационная культура. Модуль : метод. пособ. / Д.В.Зарецкий. – М. : Дрофа, 1995. – 256 с.

102. Захарченко А.Н. Обработка информации в комплексных системах мониторинга / А.Н.Захарченко. – М., 2001. – 147 с.

103. Звєрєва І.Д. Діагностика моральної вихованості школярів / І.Д.Звєрєва, Л.Г.Коваль. – К., 1995. – 156 с.

104. Згуровский М.З. Исследование социальных процессов на основе методологии системного анализа / М.З.Згуровский, А.В.Доброногов, Т.Н.Померанцева. – К. : Наукова думка, 1997. – 222 с.

105. Зигмуратов А.Т. Вступ до філософської логіки / А.Т.Зигмуратов. – К. : Абрис, 1997. – 349 с.

106. Зимняя И.А. Педагогическая психология / И.А.Зимняя. – Ростов-на-Дону : Феникс, 1997. – 480 с.

107. Зимняя И.А. Психолого-педагогические механизмы порождения и восприятия текста / И.А.Зимняя // Сборник научных трудов. – М., 1985. – 188 с.

108. Зиятдинова Ф.Г. Социальные проблемы образования / Ф.Г.Зиятдинова. – М., 1999. – 283 с.

109. Злобіна О.Г. Особистість як суб’єкт соціальних змін / О.Г.Злобіна. – К., 2004. – 400 с.

110. Знаков В.В. Понимание в познании и общении / В.В.Знаков. – М., 1994. – 237 с.

111. Зязюн І.А. Краса педагогічної дії : навч. посіб. / І.А.Зязюн, Г.М.Сагач. – К., 1997. – 302 с.

112. Иванов Р.Н. Организация и методика информационной работы / Р.Н.Иванов. – М. : Радио и связь, 1982. – 191 с.

113. Интеллектуальная культура специалиста / [под ред. И.С.Ладенко]. – Новосибирск, 1988. – 272 с.

114. Информация, анализ, прогноз – стратегические рычаги эффективного государственного управления : матер. III Междунар. науч.-практ. конф. – К. : УкрИНТЭИ, 2002. – 216 с. – (Цель. Информация. Решения).

115. Іванов В.Ф. Інформаційне законодавство: український та зарубіжний досвід / В.Ф.Іванов. – К., 1999. – 208 с.

116. Іванченко Р.Г. Адекватність розуміння і ясність тексту / Р.Г.Іванченко. – К., 1991. – 48 с.

117. Інформаційне забезпечення державного та регіонального соціального управління / [О.Г.Осауленко, О.Ф.Новікова, Н.С.Власенко та ін.]. – Донецьк, 2004. – 655 с.

118. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики / [Р.А.Калюжний, В.О.Шамрай, М.Я.Швець та ін.]; Академія Державної податкової служби України. – К., 2002. – 296 с.

119. Інформація, аналіз, прогноз – стратегічні важелі ефективного державного управління : матер. Всеукр. наук.-практ. конф. – К. : УкрІНТЕІ, 2000. – 138 с.

120. Інформація, аналіз, прогноз – стратегічні важелі ефективного державного управління : матер. II Міжнар. наук.-практ. конф. – К. : УкрІНТЕІ, 2001. – 244 с.

121. Каган М.С. Философия культуры. Становление и развитие / М.С.Каган, К.А.Сергеев, Р.В.Светлов. – СПб., 1995. – 309 с.

122. Казмиренко В.П. Социальная психология организаций / В.П.Казмиренко. – К., 1993. – 384 с.

123. Каныгин Ю.М. Основы когнитивного обществознания: информационная теория социальных систем / Ю.М.Каныгин. – К., 1993. – 236 с.

124. Каплан Г.А. Соціальна діяльність: сутність, види, форми / Г.А.Каплан. – Х. : Прапор, 1998. – 59 с.

125. Караулов Ю.Н. Лингвистическое конструирование и тезаурус литературного языка / Ю.Н.Караулов. – М. : Наука, 1981. – 366 с.

126. Карнап Р. Значение и необходимость. Исследования по семантике и модальной логике / Р.Карнап. – М., 1959. – 360 с.

127. Карпичев В.С. Организация и самоорганизация социальных систем : словарь / В.С.Карпичев. – М. : Изд-во РАГС, 2001. – 125 с.

128. Катаева Л.А. Личность и культура: проблема целостности и взаимодействия / Л.А.Катаева. – Одесса, 1994. – 147 с.

129. Качанов П.А. Основы теории информации и управления / П.А.Качанов, В.В.Горбачев. – Х. : НТУ “ХПИ”, 2005. – 368 с.

130. Качуровський М.О. Щодо зміни методологічних підстав у формуванні культури сучасного спеціаліста / М.О.Качуровський ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 1. – С. 19−20.

131. Клепко Є.Ф. Інтегративна освіта і поліморфізм знання / Є.Ф.Клепко. – К. : Полтава, 1998. – 358 с.

132. Клімова Г.П. Освіта і цивілізація / Г.П.Клімова. – Х. : Право, 1996. – 127 с.

133. Коваль Л.Г. Соціальна педагогіка / Л.Г.Коваль. – К., 1997. – 392 с.

134. Ковтанюк М.Р. Роль і значення вивчення мов у формуванні професійної і гуманітарної культури спеціаліста / М.Р.Ковтанюк ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 2. – С. 80−82.

135. Коган В.З. Информационная работа / В.З.Коган. – Новосибирск, 1984. – 137 с.

136. Коган В.З. Информационное взаимодействие (опыт анализа субъектно-объектных отношений) / В.З.Коган. – Томск, 1980. – 184 с.

137. Коган В.З. К методологии информационного подхода / В.З.Коган ; под ред. И.С.Ладенко // Информатика и культура. – Новосибирск, 1990. – 232 с.

138. Коган В.З. Теория информационного взаимодействия / В.З.Коган. – Новосибирск, 1991. – 319 с.

139. Коган В.З. Человек в потоке информации (информационные потребности) / В.З.Коган. – Новосибирск, 1981. – 177 с.

140. Коган И.М. Прикладная теория информации / И.М.Коган. – М., 1981. – 216 с.

141. Коган М.С. Философия культуры / М.С.Коган. – СПб., 1996. – 416 с.

142. Кожевников В.Л. Основи збирання, обробки і передачі інформації. Теоретичні основи / В.Л.Кожевников, Л.В.Кожевников. – Д. : НГУ, 2005. – 108 с.

143. Козаков В.А. Дослідження особистості студента як суб’єкта майбутньої професійної діяльності : методичні вказівки до виконання самостійної роботи з дисципліни “Психологія діяльності і освітній менеджмент” / В.А.Козаков, В.С.Лозиця. – К., 1998. – 68 с.

144. Козаков В.А. Самостоятельная работа студентов и ее информационно-методическое обеспечение / В.А.Козаков. – К., 1990. – 247 с.

145. Козачук З.Я. Культура мовлення як важливий чинник формування гуманітарної культури спеціаліста / З.Я.Козачук ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч .2. – С. 89−91.

146. Козиев В.Н. Характеристика логической структуры текста / В.Н.Козиев ; под ред. Г.С.Сухобского // Особенности восприятия информации взрослыми людьми. – Ленинград, 1973. – С. 83−86.

147. Колин К.К. Информационное общество и проблема образования / К.К.Колин // Информационное общество. – 1997. – № 2−3. – С. 18−19.

148. Колин К.К. Информационные ресурсы в системе опережающего образования / К.К.Колин // Информационные ресурсы России. – 1997. – № 5. – С. 6−12.

149. Колин К.К. Информация в системе опережающего образования / К.К.Колин // Вестник Российского общества информатики и вычислительной техники. – 1996. – № 3. – С. 19−40.

150. Коренной А.А. Информация и коммуникация / А.А.Коренной. – К., 1986. – 135 с.

151. Корніяка О.М. Лабіринти розуміння: текст як об’єкт розуміння / О.М.Корніяка. – К., 1990. – 48 с.

152. Костенко Н.В. Досвід контент-аналізу: моделі та практики / Н.В.Костенко, В.Ф.Іванов. – К. : Центр вільної преси, 2003. – 200 с.

153. Кремянский В.И. Методологические проблемы системного подхода к информации / В.И.Кремянский. – М., Наука, 1977. – 228 с.

154. Кривега Л.Д. Мировоззренческие ориентации личности в условиях трансформации общества / Л.Д.Кривега. – Запорожье : ЗГУ, 1998. – 189 с.

155. Крулькевич М.И. Информационная деятельность в организациях / М.И.Крулькевич, Е.М.Сынкова. – Донецк : ДНУ, 2001. – 176 с.

156. Крылова Н.Б. Социальное управление и формирование культуры личности / Н.Б.Крылова. – М., 1978. – 86 с.

157. Крылова Н.Б. Формирование культуры будущего специалиста / Н.Б.Крылова. – М. : Высшая школа, 1990. – 142 с.

158. Крымский С.Б. Верификация социальных прогнозов: методологический аспект / С.Б.Крымский, В.Е.Пилипенко, Ю.В.Салюк. – К. : Наукова думка, 1992. – 116 с.

159. Кудін В.О. Освіта в інформаційному суспільстві / В.О.Кудін. – К. : Республіка, 1998. – 151 с.

160. Кузина С. Душа в компьютерных сетях / С.Кузина // Комсомольская правда . − 1995. − 6 окт.

161. Кузнецов И.П. Механизмы обработки семантической информации / И.П.Кузнецов. – М., 1978. – 175 с.

162. Кулешов С.Г. Документальні джерела наукової інформації: поняття, типологія, історія / С.Г.Кулешов. – К. : УкрІНТЕІ, 1995. – 192 с.

163. Кулешов С.Г. Управлінське документознавство : навч. посіб. / С.Г.Кулешов. – К. : ДАККіМ, 2003. – 58 с.

164. Кулєшов О.В. Філософські проблеми інформатики / О.В.Кулєшов. – Черкаси : Брама, 2004. – 100 с.

165. Кулюткин Ю.Н. Параметры сообщения, определяющие его актуальность / Ю.Н.Кулюткин ; под ред. Г.С.Сухобского // Особенности восприятия информации взрослыми людьми. – Ленинград, 1973. – С. 28−31.

166. Кульбаба В.В. Об информационном управлении / В.В.Кульбаба // Информатика и вычислительная техника. – 1996. – № 1−2. – С. 21−25.

167. Лазаревич А.А. Научное знание в информационном обществе / А.А.Лазаревич. – Минск, 1993. – 101 с.

168. Лазарєва С.Ф. Економіка та організація інформаційного бізнесу / С.Ф.Лазарєва. – К. : КНЕУ, 2002. – 667 с.

169. Лазутина Г.В. Технология и методика журналистского творчества : метод. указания к курсу “Теория и практика советской журналистики” / Г.В.Лазутина. – М., 1988. – С. 44.

170. Лактионова О.Е. Формирование логистических систем: методология и практика / О.Е.Лактионова. – Донецк, 2002. – 318 с.

171. Леонтьев А.А. Основы психолингвистики / А.А.Леонтьев. – М. : Смысл, 1997. – 287 с.

172. Леонтьев А.Н. Деятельность. Сознание. Личность / А.Н.Леонтьев. – М. : Политиздат, 1977. – 346 с.

173. Лиив Э.Х. Инфодинамика. Обобщенная энтропия и негэнтропия / Э.Х.Лиив. – Таллинн, 1998. – 199 с.

174. Линдсей П. Переработка информации у человека / П.Линдсей, Д.Норман. – М. : Мир, 1974. – 550 с.

175. Липовская Н.А. Интеллектуальный потенциал общества: сущность и динамика / Н.А.Липовская. – Днепропетровск, 1996. – 226 с.

176. Литвак Б.Г. Экспертная информация: методы получения и анализа / Б.Г.Литвак. – М. : Радио и связь, 1982. – 184 с.

177. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах : автореф. дис. на здобуття наук. ступеня канд. політ. наук / О.В.Литвиненко. – К., 1997. – 18 с.

178. Лігоцький А.О. Стратегія розвитку професійної освіти в Україні / А.О.Лігоцький. – К., 1997. – 49 с.

179. Лоза О.В. Діловодство та документування управлінської діяльності : навч. посіб. / О.В.Лоза. – К., 1997. – 67 с.

180. Лотман Ю.М. Несколько мыслей относительно типологии культуры / Ю.М.Лотман // Языки культуры и проблемы переводимости. – М. : Искусство, 1987. – 230 с.

181. Луговий В.І. Освіта і культура сучасного спеціаліста / В.І.Луговий ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 1. – С. 5−7.

182. Лузик Э.В. Концепция естественного роста знаний при многоступенчатой подготовке специалистов / Э.В.Лузик. – К. : КМУГА, 1996. – 132 с.

183. Лутай В.С. Філософія сучасної освіти / В.С.Лутай. – К. : Центр “Майстр-S”, 1996. – 226 с.

184. Макаров Н.Д. Контент-анализ (метод количественного изучения содержания социальной информации) / Н.Д.Макаров. – М. : НМЦ СПО, 2001. – 60 с.

185. Макеев Б.А. Информационная разведка в сумме технологий или основы компьютерной наукометрии / Б.А.Макеев. – М. : ЦНИИатоминформ, 2000. – 128 с.

186. Маковецький А.М. Формування морального світу особи та її ціннісних орієнтацій в кризовий період життя суспільства / А.М.Маковецький. – Чернівці, 1994. – 300 с.

187. Малюк А.А. Угрозы информации и информационные угрозы. Подготовка кадров в области информационной безопасности / А.А.Малюк // Вестник Российского общества информатики и вычислительной техники. – 1996. – № 4. – С. 65−70.

188. Мальчуков В.А. Теория знаков и познание психических явлений / В.А.Мальчуков, К.С.Жуков, И.А.Конопак. – Иркутск, 1993. – 145 с.

189. Маркарян Э.С. О генезисе человеческой деятельности и культуры / Э.С.Маркарян. – Ереван, 1973. – 146 с.

190. Маркевич А.А. Теория информации и ее приложения / А.А.Маркевич. – М. : Физматгиз, 1959. – 328 с.

191. Мартинюк С.Є. Генезис інформаційної цивілізації / С.Є.Мартинюк. – Запоріжжя : Просвіта, 2002. – 192 с.

192. Машлыник В.Г. Европейское информационное пространство / В.Г.Машлыник. – М. : Наука, 1999. – 95 с.

193. Мелюхин И.С. Информационно-аналитическая деятельность как она есть / И.С.Мелюхин // Информационные ресурсы России. – 1999. – № 1. – С. 11−14.

194. Мелюхин И.С. Концепции информационного общества и роль государства / И.С.Мелюхин // Информационные ресурсы России. – 1997. – № 2. – С. 13−18.

195. Мельник М.И. Политическая активность личности в системе национальной безопасности Украины / М.И.Мельник. – К., 1992. – 299 с.

196. Мельчук И.А. Опыт теории лингвистических моделей “Смысл-текст”. Семантика, синтаксис / И.А.Мельчук. – М. : Школа “Языки русской культуры”, 1999. – 346 с.

197. Методологія, теорія та практика соціологічного аналізу сучасного суспільства : зб. наук. праць / [за ред. О.О.Якуба та ін.]. – Х. : Видавничий центр Харківського нац. ун-ту ім. В.Н.Каразіна, 2001. – 565 с.

198. Милитарев В.Ю. Информационная культура эпохи НТР / В.Ю.Милитарев, И.М.Яглом ; под ред. И.С.Ладенко // Информатика и культура. – Новосибирск, 1990. – 232 с.

199. Мировоззренческая культура личности / [В.П.Иванов и др.]. – К. : Наукова думка, 1986. – 293 с.

200. Молчанов В.И. Системный анализ социологической информации / В.И.Молчанов. – М. : Наука, 1981. – 143 с.

201. Моль А. Теория информации и эстетическое восприятие / А.Моль. – М., 1966. – 386 с.

202. Москаленко А.З. Сучасна інформаційна політика / А.З.Москаленко. – К., 1999. – 190 с.

203. Моторин С.И. О моделировании интеллектуального понимания языка делового общения / С.И.Моторин // НТИ. – 1997. – Серия 3. – № 4. – С. 9−18.

204. Мудрик А.В. Общение и развитие личности школьника / А.В.Мудрик ; под ред. В.Д.Семенова // Социально-педагогические проблемы формирования личности. – Свердловск, 1982. – 136 с.

205. Муравьева А.А. Импликация как средство создания контекста / А.А.Муравьева ; под ред. К.М.Ириханова // Информативность текста и его компонентов. – М., 1986. – 163 с.

206. Навроцька Л.Г. Проблеми формування правової культури сучасного фахівця / Л.Г.Навроцька, В.Д.Сусоров ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 2. – С. 140−142.

207. Народные русские сказки / [под ред. А.Н.Афанасьева]. – М. : Правда, 1982. – 576 с.

208. Національна безпека України 1994 – 1996 рр. : наук. доповідь НІСД / [за ред. О.Ф.Бєлова]. – К., 1997. – 197 с.

209. Немец К.А. Информационное взаимодействие природных и социальных систем / К.А.Немец. – Х., 2005. – 428 с.

210. Неперервна професійна освіта: проблеми, пошуки, перспективи / [за ред. І.А.Зязюна]. – К. : Віпол, 2000. – 240 с.

211. Нестеров А.В. Компьютерные методы и средства глубокой обработки, анализа и синтеза общедоступных документов / А.В.Нестеров. – Новосибирск, 1991. – 214 с.

212. Нечитайло В.М. Інформаційне суспільство: критичний аналіз космополітичних концепцій майбутнього людства : автореф. дис. на здобуття наук. ступеня канд. філософ. наук / В.М.Нечитайло. – К., 1996. – 46 с.

213. Нижник Н.Р. Правова культура – елемент формування сучасного спеціаліста / Н.Р.Нижник ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 2. – С. 142−145.

214. Никанорова Л.В. Мировоззрение личности и возрастные особенности его формирования / Л.В.Никанорова. – К. : Наукова думка, 1989. – 116 с.

215. Никифоров А.А. Деятельность, поведение, творчество / А.А.Никифоров ; сост. И.Т.Касавин // Деятельность: Теория, методология, проблемы. – М. : Политиздат, 1987. – С. 52−69.

216. Ничкало Н.Г. Профессионально-техническое образование в Украине: проблемы исследований / Н.Г.Ничкало. – К. : Науковий світ, 1999. – 28 с.

217. Ніколас Девід. Оцінка інформаційних потреб: методи і технології / Ніколас Девід. – London : Асліб, 1996. – 76 с.

218. Новик И.Б. Введение в информационный мир / И.Б.Новик, А.Ш.Абдуллаев // ВИНИТИ. – М. : Наука, 1991. – 225 с.

219. Овчинников В.Г. Методологическое введение в информатику / В.Г.Овчинников. – М. : Компания Спутник+, 2004. – 217 с.

220. Овчинский С.С. Оперативно-розыскная информация / С.С.Овчинский. – М. : Инфра-М, 2000. – 367 с.

221. Ожегов С.И. Словарь русского языка / С.И.Ожегов. – М. : Советская энциклопедия, 1973. – 846 с.

222. Оноприенко Ю.И. Основы теории информации с элементами системного анализа информационных процессов в природе и в обществе : курс лекцій / Ю.И.Оноприенко. – Владивосток : Изд-во Дальневосточного ун-та, 2001. – 108 с.

223. Орбан Л.Е. Соціалізація особистості школяра / Л.Е.Орбан. – Івано-Франківськ, 1996. – 66 с.

224. Орієнтовний зміст освіти в національній школі / [за ред. Н.І.Бєлкіна]. – К., 1996. – 136 с.

225. Осауленко О.Г. Інформаційне забезпечення державного управління сталим розвитком / О.Г.Осауленко. – К., 2001. – 72 с.

226. Особенности восприятия информации взрослыми людьми / [под ред. Г.С.Сухобского] // Сборник научных трудов. – Ленинград, 1975. – Вып. 2. – 79 с.

227. Остин Дж. Как производить действия при помощи слов. Смысл и сенсибилии / Дж.Остин. – М. : Идея-Пресс, Дом интеллектуальной книги, 1999. – 329 с.

228. Падучева Е.В. Высказывание и его соотнесенность с действительностью / Е.В.Падучева. – М., 1985. – 271 с.

229. Партико З.В. Образна концепція теорії інформації / З.В.Партико. – Львів : Видавничий центр ЛНУ ім. І.Франка, 2001. – 133 с.

230. Педько С.С. Психологические особенности формирования смыслового содержания графических знаков / С.С.Педько. – Тбилиси, 1984. – 24 с.

231. Петлін В.М. Методи і критерії пізнання в енергоінформаційних науках / В.М.Петлін. – Львів : Каменяр, 2004. – 120 с.

232. Пехлецкий И.Д. Общая теория систем и анализ процесса обучения / И.Д.Пехлецкий. – Пермь, 1976. – 120 с.

233. Пирс Дж. Символы, сигналы, шумы: закономерности и процессы передачи информации / Дж.Пирс. – М. : Мир, 1967. – 332 с.

234. Пищулина О.Н. Изменения поведенческой ориентации личности в условиях трансформации культуры / О.Н.Пищулина. – Х., 1996. – 154 с.

235. Платонов К.К. Краткий словарь системы психологических понятий / К.К.Платонов. – М. : Высшая школа, 1984. – 46 с.

236. Поваляев С.А. Научная информация: деятельность, потребности, мотивы / С.А.Поваляев. – Минск, 1985. – 96 с.

237. Попов В.И. Концепция подготовки специалистов по применению информационных технологий в борьбе с организованной преступностью / В.И.Попов, А.С.Овчинский // Вестник Российского общества информатики и вычислительной техники. – 1996. – № 4. – С. 60–64.

238. Попов Е.В. Введение в культурологию / Е.В.Попов. – М. : Владос, 1995. – 335 с.

239. Поппер К. Логика и рост научного знания / К.Поппер. – М., 1983. – 368 с.

240. Поппер К. Логика научного исследования / К.Поппер. – М. : Республика, 2004. – 447 с.

241. Потятиник Б.В. Патогенний текст / Б.В.Потятиник. – Львів, 1996. – 295 с.

242. Потятиник Б.В. Патогенний текст у масовій комунікації: ідентифікація, типологія, нейтралізація / Б.В.Потятиник. – Львів, 1996. – 349 с.

243. Почепцов Г.Г. Коммуникативные аспекты семантики / Г.Г.Почепцов. – К., 1987. – 131 с.

244. Почепцов Г.Г. Национальная безопасность стран переходного периода / Г.Г.Почепцов. – К., 1996. – 136 с.

245. Почепцов Г.Г. Стратегический анализ: стратегический анализ для политики, бизнеса и военного дела / Г.Г.Почепцов. – К. : Дзвін, 2004. – 336 с.

246. Почепцов Г.Г. Теорія комунікацій / Г.Г.Почепцов. – К., 1996. – 175 с.

247. Проблемы информационного обеспечения в социологии / [под ред. В.Ф.Сбытова]. – М., 1980. – 186 с.

248. Проблемы сравнительных исследований в социологии: методы сбора данных / [под ред. О.М.Масловой, В.Г.Андреенкова]. – М. : Ин-т социологии, 1988. – 199 с.

249. Прохоров Е.П. Средства массовой информации и информационная безопасность / Е.П.Прохоров // Информационное общество. – 1997. – № 4−6. – С. 36−42.

250. Пушкин В.Г. Информатика, энтропия, интеллект: философские очерки / В.Г.Пушкин, А.Д.Урсул. – Кишинев : Штиинца, 1989. – 293 с.

251. Рабочая книга социолога / [под ред. Г.В.Осипова]. – М. : Наука, 1976. – 511 с.

252. Радвик Б. Военное планирование и анализ систем / Б.Радвик. – М. : Воениздат, 1972. – 480 с.

253. Ракитов А.И. Философия компьютерной революции / А.И.Ракитов. – М. : Политиздат, 1991. – 286 с.

254. Расторгуев С.П. Информационная война как целенаправленное информационное воздействие информационных систем / С.П.Расторгуев // Информационное общество. – 1997. – № 1. – С. 64−66.

255. Ревин В.А. Концепция информационного обеспечения структурных подразделений органов управления / В.А.Ревин. – К., 1993. – 30 с.

256. Редько В.Г. Эволюционная кибернетика / В.Г.Редько. – М. : Наука, 2001. – 157 с.

257. Рейзема Я.В. Информатика социального отражения: информационные и социальные основания общественного разума / Я.В.Рейзема. – М. : Прометей, 1990. – 221 с.

258. Рейтингова система оцінки успішності студентів / [под ред. В.А.Козакова]. – К., 1992. – 203 с.

259. Розенберг Н.М. Проблемы измерений в дидактике / Н.М.Розенберг. – К. : Высшая школа, 1979. – 175 с.

260. Розенберг Н.М. Світ інформації (застосування в психології, лінгвістиці) / Н.М.Розенберг. – К., 1973. – 137 с.

261. Ручкін В.О. Закономірність добування інформації / В.О.Ручкін. – К. : Знання України, 2002. – 45 с.

262. Рыбаков И.А. Философия структур организаций: эволюционный подход / И.А.Рыбаков. – К. : Авторское издание, 1997. – 133 с.

263. Свириденко С.С. Информационные технологии в интеллектуальной деятельности / С.С.Свириденко. – М., 1995. – 240 с.

264. Севастьянов Ю.С. Научные и организационные основы информационной деятельности / Ю.С.Севастьянов. – М. : Радио и связь, 1983. – 184 с.

265. Седов А.В. Методы сбора, обработки и анализа социальной информации / А.В.Седов, Т.Н.Кротова, В.Я.Шмаков. – Л. :ВПШК, 1984. – 80 с.

266. Седов Е.А. Одна формула и весь мир: энтропия / Е.А.Седов. – М., 1982. – 127 с.

267. Седов Е.А. Эволюция и информация / Е.А.Седов. – М., 1976. – 154 с.

268. Семенов В.Е. Метод изучения документов в социально-психологических исследованиях / В.Е.Семенов. – М., 1983. – С. 3.

269. Семенюк Э.П. Информационный подход к познанию действительности / Э.П.Семенюк. – К. : Наукова думка, 1988. – 146 с.

270. Семеняка Г.А. Деякі аспекти короткострокового прогнозування розвитку та аналізу системи / Г.А.Семеняка, Ю.Х.Куценко. – К., 2000. – 27 с.

271. Сидоров Е.В. Аспекты организации высказывания в коммуникативном освещении / Е.В.Сидоров // Текст в коммуникации. – М., 1991. – С. 41−50.

272. Сироткин Л.Ю. Формирование личности: проблема устойчивости / Л.Ю.Сироткин. – Казань, 1992. – 176 с.

273. Ситник В.Ф. Основи інформаційних систем / В.Ф.Ситник. – К. : КНЕУ, 1997. – 252 с.

274. Ситченко Л. Першоджерела комунікативної філософії / Л.Ситченко. – К. : Либідь, 1996. – 170 с.

275. Скороходько Э.Ф. Семантические сети и автоматическая обработка текста / Э.Ф.Скороходько. – К. : Наукова думка, 1983. – 218 с.

276. Сморж Л.О. Особа і суспільство (філософсько-психологічний аспект) / Л.О.Сморж. – К. : МІЛП, 2001. – 384 с.

277. Смысловое восприятие речевого сообщения / [под ред. Т.М.Дридзе]. – М. : Наука, 1976. – 262 с.

278. Современная культура и изменения в содержании образования : методические материалы для преподавателей, аспирантов и студентов II Сибирской конференции “Интеллект, культура и образование” / [под ред. И.С.Ладенко]. – Новосибирск, 1995. – Вып. 3. – 68 с.

279. Современный словарь иностранных слов. – СПб. : Дуэт, 1994. – 740 с.

280. Соловьева Е.А. Методы моделирования и модели понятийных знаний / Е.А.Соловьева, С.И.Маторин // НТИ. – 1989. – Серия 2. – № 4. – С. 2−8.

281. Соловьева Е.А. Естественная классификация: системологические основания / Е.А.Соловьева. – Х. : ХТУРЭ, 1999. – 222 с.

282. Солсо Р. Когнитивная психология / Р.Солсо. - М. : Тривола, 1996. – 598 с.

283. Социальная информатика : сб. тр. – М., 1990. −230 с.

284. Социальная информатика: основания, методы, перспективы / [В.Б.Бритков, А.А.Давыдов, Т.И.Жукова и др.]. – М. : Едиториал УРСС, 2003. – 214 с.

285. Социально-педагогические проблемы формирования личности / [под ред. В.Д.Семенова]. – Свердловск, 1986. – 194 с.

286. Социология : словарь-справочник // Социологические исследования. – М. : Наука, 1991. – Т. 4. – С. 72.

287. Средства формирования всесторонне развитой личности / [под ред. В.С.Ильина] // Сборник научных трудов. – Волгоград, 1987. – 177 с.

288. Старіш О.Г. Теорія відкритих систем як парадигма процесів глобального розвитку / О.Г.Старіш. – Сімферополь : Універсум, 2003. – 240 с.

289. Степанишин Б.І. Викладання української літератури в школі / Б.І.Степанишин. – К. : Проза, 1995. – 255 с.

290. Сулятицький І.В. Проблеми соціопсихології військового управління / І.В.Сулятицький. – К. : Міжнародна фінансова агенція, 1997. – 32 с.

291. Сурмин Ю.П. Теория систем и системный анализ : учеб. пособ. / Ю.П.Сурмин. – К. : МАУП, 2003. – 368 с.

292. Суханов А.П. Информациология на рубеже тысячелетий : сборник / А.П.Суханов. – Новосибирск, 2001. – 187 с.

293. Суханов А.П. Информация и прогресс / А.П.Суханов. – Новосибирск, 1988. – 192 с.

294. Сухина В.Ф. Человек в мире информатики / В.Ф.Сухина. – М. : Радио и связь, 1992. – 112 с.

295. Сухіна В.Ф. Методологічні і соціокультурні основи інформатики : автореф. дис. на здобуття наук. ступеня канд. філософ. наук / В.Ф.Сухіна. – К., 1993. – 22 с.

296. Сухіна В.Ф. Організація процесу навчання в умовах інформатизації суспільства / В.Ф.Сухіна // Філософські проблеми сучасного природознавства. – 1992. – № 78. – С. 91−96.

297. Сушин Н.С. Педагогічна технологія формування гуманістично-професійних якостей майбутніх фахівців : дис. … канд. пед. наук / Н.С.Сушин. – Луцьк, 1996. – 177 с.

298. Табачковский В.Г. Диалектика деятельности и культура / В.Г.Табачковский. – К. : Наукова думка, 1983. – 296 с.

299. Татарова Г.Г. Типологический анализ в социологии / Г.Г.Татарова. – М. : Наука, 1993. – 103 с.

300. Теория, организация и экономика научно-информационной деятельности : метод. пособ. / [сост. И.А.Бурцева и др.]. – М. : ИПКИР, 1987. – 120 с.

301. Теслер Г.С. Новая кибернетика / Г.С.Теслер. – К. : Логос, 2004. – 404 с.

302. Тесля Ю.Н. Основы теории информационного взаимодействия / Ю.Н.Тесля. – К., 1995. – 46 с.

303. Тимошенко И.И. Мотивация личности и человеческих ресурсов / И.И.Тимошенко, А.С.Соснин. – К. : Изд-во Европейского ун-та, 2004. – 576 с.

304. Тихомиров Б.И. Техника социального анализа / Б.И.Тихомиров. – СПб., 1992. – 104 с.

305. Толковый словарь по основам информационной деятельности / [под ред. Н.Н.Ермоленко]. – К. : УкрИНТЭИ, 1995. – 252 с.

306. Тополянський С.І. Інформаційні правові системи та основи інформатики / С.І.Тополянський. – Ужгород : Мистецька лінія, 2004. – 153 с.

307. Торсуева И.Г. Интонация и смысл высказывания / И.Г.Торсуева. – М., 1979. – 111 с.

308. Тюхтин В.С. Отражение, системы, кибернетика / В.С.Тюхтин. – М. : Наука, 1972. – 212 с.

309. Україна на шляху до інформаційного суспільства / [В.С.Журавський, М.К.Родіонов, І.Б.Жиляєв, М.З.Згуровський]. – К. : Політехніка, 2004. – 482 с.

310. Урсул А.Д. Информация. Методические аспекты / А.Д.Урсул. – М., 1971. – 376 с.

311. Урсул А.Д. Опережающее образование и становление информационной цивилизации / А.Д.Урсул // Вестник Российского общества информатики и вычислительной техники. – 1996. – № 3. – С. 44−47.

312. Усова А.В. Формирование у школьников научных понятий в процессе обучения / А.В.Усова. – М. : Педагогика, 1986. – 174 с.

313. Устич С.І. Системне дослідження суспільства / С.І.Устич. – Львів : Світ, 1992. – 135 с.

314. Ушакова І.О. Системи обробки статистичної інформації / І.О.Ушакова. – Х. : ХНЕУ, 2005. – 160 с.

315. Феоктистов Г.Г. Информационная безопасность общества, личности и средства массовой информации : метод. аспект / Г.Г.Феоктистов // Информатика и вычислительная техника. – 1996. – № 1–2. – С. 32−33.

316. Фридланд А.Я. Информатика: процессы, системы, ресурсы / А.Я.Фридланд. – М. : БИНОМ. Лаборатория знаний, 2003. – 232 с.

317. Фролкин Н.П. Аналитический обзор как форма научно-информационной работы / Н.П.Фролкин. – К., 1989. – 18 с.

318. Хакен Г. Информация и самоорганизация: макроскопический подход к сложным системам / Г.Хакен. – М. : Мир, 1991. – 240 с.

319. Хмельницький О.О. До питання про текстову діяльність фахівця. Проблеми сучасного мистецтва та культури. Проблеми особистісно орієнтованого педагогічного процесу / О.О.Хмельницький // Збірник наукових праць. – 2000. – С.122−129.

320. Хмельницький О.О. Особливості текстової діяльності та сприйняття інформації у професійній підготовці спеціаліста / О.О.Хмельницький // Педагогіка і психологія професійної освіти. – 2000. – № 2. – С. 107−117.

321. Хмельницький О.О. Психолого-педагогічні механізми інформаційного впливу суспільства на формування особистості спеціаліста / О.О.Хмельницький // Педагогіка і психологія професійної освіти. – 1999. – № 3. – С. 195−203.

322. Ходаков В.Е. Системы информационного обслуживания / В.Е.Ходаков. – К., 1983. – 175 с.

323. Хомский Н. Язык и мышление / Н.Хомский. – М. : Изд-во Московского ун-та, 1972. – 122 с.

324. Хурсин Л.А. Начала теории систем общественного типа / Л.А.Хурсин // Информационно-психологические вопросы теории систем общественного типа. – К. : Світ, 2001. – 276 с.

325. Циба В.Т. Соціологія особистості: системний підхід (соціально-психологічний аналіз) : навч. посіб. – К. : МАУП, 2000. – 149 с.

326. Цырдя Ф.Н. Информатизация, познание, социальное управление / Ф.Н.Цырдя. – Кишинев, 1992. – 138 с.

327. Цырдя Ф.Н. Социальная информация – важный инструмент руководства и средство воспитания / Ф.Н.Цырдя // Роль социальной информации в образовании и воспитании молодежи. – Волгоград, 1977. – 56 с.

328. Чавчавадзе Н.З. Культура и ценности / Н.З.Чавчавадзе. – Тбилиси : Мецниереба, 1984. – 171 с.

329. Чепелєва Н.В. Психологія читання навчальної та наукової літератури в системі професійної підготовки студентів / Н.В.Чепелєва. – К., 1992. – 397 с.

330. Червінська Л.П. Мотивація персоналу в менеджменті: стан, проблеми, напрями розвитку / Л.П.Червінська. – К., 1997. – 203 с.

331. Чернавский Д.С. Синергетика и информация: динамическая теория информации / Д.С.Чернавский. – М. : Наука, 2001. – 244 с.

332. Чернилевский Д.В. Технология обучения в высшей школе / Д.В.Чернилевский, О.К.Филатов. - М. : Экспедитор, 1996. – 228 с.

333. Чернов А.А. Становление глобального информационного общества: проблемы и перспективы / А.А.Чернов. – М. : Изд.-торговая корпорация “Дашков и Ко”, 2003. – 232 с.

334. Черняк О.І. Техніка вибіркових досліджень / О.І.Черняк. – К. : МІВВЦ, 2001. – 248 с.

335. Черри К. Человек и информация (критика и обзор) / К.Черри. – М., 1972. – 488 с.

336. Чистякова Г.Д. Исследование понимания текста как функции его смысловой структуры / Г.Д.Чистякова. – М., 1975. – 24 с.

337. Шапиро Э.Л. Знания о мире и их информационные модели / Э.Л.Шапиро // НТИ. – 1989. – Серия 1. – № 9. – С. 2−5.

338. Шаров А.А. Биосемиотика: функционально-эволюционный подход к анализу смысла информации / А.А.Шаров // НТИ. – 1990. – Серия 2. – № 12. – С. 10−20.

339. Швець М.Я. Правова інформатика : підруч. / [М.Я.Швець, В.М.Фурашев, М.І.Коваль та ін.]. – К. : Парламентське вид-во, 2004. – Т. 1. – 416 с.

340. Шевченко Т.И. Современные дидактические концепции в образовании / Т.И.Шевченко. – К., 1995. – 158 с.

341. Шевчук В.П. До питання методологічних підходів до формування гуманітарної культури сучасного спеціаліста / В.П.Шевчук ; за ред. В.Д.Базилевича // Актуальні проблеми формування професійної та гуманітарної культури сучасного спеціаліста. – К., 1994. – Ч. 1. – С. 38−41.

342. Шемшученко Ю.С. Інформаційне законодавство : зб. законодавчих актів / Ю.С.Шемшученко, І.С.Чиж. – К. : Вид-во “Юр. думка”, 2005. – Т. 1. – 414 с.

343. Шенк Р. Обработка концептуальной информации / Р.Шенк. – М., 1980. – 361 с.

344. Шеннон К. Работы по теории информации и кибернетике / К.Шеннон. – М., 1963. – 820 с.

345. Шерковин Ю.А. Психологические проблемы массовых информационных процессов / Ю.А.Шерковин. – М., 1973. – 216 с.

346. Шрейдер Ю.А. Системы и модели / Ю.А.Шрейдер, А.А.Шаров. – М. : Радио и связь, 1982. – 152 с.

347. Штанько В.С. Информация. Мышление. Целостность / В.С.Штанько. – Х., 1992. – 144 с.

348. Щедрин А.Н. Электронные информационные ресурсы в информационной экономике / А.Н.Щедрин. – Донецк : Ин-т экономики промышленности, 2003. – 232 с.

349. Щерба Л.В. Языковая система и речевая деятельность / Л.В.Щерба. – Л. : Наука, 1974. – 428 с.

350. Щербицкий Г.И. Информация и познавательные потребности / Г.И.Щербицкий. – Минск, 1983. – 160 с.

351. Щербицкий Г.И. Системный характер информации / Г.И.Щербицкий. – Минск, 1978. – 173 с.

352. Экспертные оценки в социологических исследованиях / [С.Б.Крымский и др.]. – К. : Наукова думка, 1990. – 320 с.

353. Энциклопедия кибернетики. – К., 1974. – Т. 1. – 608 с.

354. Эстетика: информационный подход / [под ред. Ю.С.Зубова, В.Л.Петрова]. – М. : Смысл, 1997. – 205 с.

355. Юдин Э.Г. Методология науки. Системность. Деятельность / Э.Г.Юдин. – М. : Эдиториал УРСС, 1997. – 444 с.

356. Юзвишин И.И. Энциклопедия информациологии : учеб. пособ. / И.И.Юзвишин. – М. : Информациология, 2000. – 466 с.

357. Юзвішин І.Й. Інформаціологія або закономірності інформаційних процесів та технологій в мікро- та макросвітах всесвіту / І.Й.Юзвішин. – Луганськ, 1999. – 204 с.

358. Юсупова Н.И. Основы теории информации для информатиков : учеб. пособ. / Н.И.Юсупова, В.В.Миронов. – Уфа, 2001. – 159 с.

359. Ягодзинський А.Й. Оцінка знань студентів та якості підготовки фахівців / А.Й.Ягодзинський, А.О.Муромцева. – К., 1997. – 216 с.

360. Ядов В.А. Социологическое исследование: методология, программа, методы / В.А.Ядов. – Самара : Самарский ун-т, 1995. – 331 с.

361. Яковенко В.Я. Інформаційні ресурси / В.Я.Яковенко. – Донецьк : ДонНУ, 2005. – 202 с.

362. Яковец Ю.В. Циклы. Кризисы. Прогнозы / Ю.В.Яковец. – М. : Наука, 1999. – 448 с.

363. Bollnow J.F. Existenzphilosophi und Padagogik / J.F.Bollnow. – Stutgart, 1962. – 189 s.

364. Linton R. The Cultural Background of Profesionality / R.Linton. – N.Y. Appleton-Groffs, 1945. – 337 p.

365. Popper K. Evolutionary Epistemology. Open Questions of Quantum Physics Invit. / K.Popper. – Pap. : Foundation Microphys, May, 1983; Dordreht et. al., 1985.

ПІСЛЯМОВА

Ви закінчили вивчати курс, який, сподіваємося, стане в пригоді на першому етапі вашого становлення як фахівця із захисту інформації. До цього часу в Україні не було підручника, який би забезпечував комплексне вивчення систем захисту інформації. Утім, відразу зауважимо, що внаслідок об'єктивних причин ми не ставили за мету узагальнити весь передовий досвід із зазначеного питання. Ми відкриті для діалогу та дискусії й будемо раді кожній пропозиції, щоб в перспективі значно поліпшити, удосконалити зміст видання.

Мета цієї праці значно скромніша – забезпечити програмний курс "Організаційно-правові основи захисту інформації з обмеженим доступом" виданням, за яким би студенти як майбутні фахівці могли вивчити основи предмета.

Зокрема фахівець з організації захисту інформації з обмеженим доступом повинен знати: положення чинного законодавства України щодо захисту інформації з обмеженим доступом; організаційно-технічні заходи для забезпечення захисту інформації з обмеженим доступом на всіх етапах виробництва товарів, надання послуг, виконання робіт; правові засоби захисту інтересів власників інформації з обмеженим доступом та правила проведення службових розслідувань; організацію та оснащення системи охорони установ, підприємств, їх режимних приміщень; основні положення трудового законодавства, вимоги з охорони праці та техніки безпеки, пожежної безпеки, внутрішньооб'єктового й перепускного режиму, трудовий розпорядок, правила та засоби проведення профілактичної роботи на підприємстві, в установі, організації різних форм власності.

Ми також сподіваємося, що цей підручник допоможе вибудувати ваші знання в систему, що стане запорукою успішної майбутьої професійної діяльності.

ЗМІСТ

ПЕРЕДМОВА 3

Розділ 1. Інформаційна безпека держави як стратегічна основа організаційних процесів захисту інформації 6

1.1. Основні визначення, категорії інформаційної безпеки та їхній зміст, принципи забезпечення 6

1.2. Національні інтереси в інформаційній сфері. Інформаційні загрози 9

1.3. Державна політика в інформаційній сфері. Характеристика напрямів забезпечення інформаційної безпеки 13

1.4. Характеристика, основні засоби здійснення можливих інформаційних впливів (операцій) 16

Запитання і завдання для самоперевірки 19

Перелік використаних джерел 19

Розділ 2. Історичний досвід організації захисту інформації з обмеженим доступом 21

2.1. Захист інформації на території України в складі Російської імперії (XVII – поч. XX ст.) 21

2.1.1. Організація захисту інформації на території України в XVII – XIX ст. 21

2.1.2. Організація захисту інформації в російській армії (XIX – поч. XX ст.) 27

2.2. Формування національної системи захисту інформації в період відродження української національної державності (1917–1921 рр.) 41

2.2.1. Організація захисту інформації в період Центральної Ради 41

2.2.2. Організація захисту інформації в українській державі гетьмана П.Скоропадського 44

2.2.3. Організація захисту інформації в період Директорії.....47

2.2.4. Специфіка та особливості організації захисту інформації в Західноукраїнській Народній Республіці 48

2.2.5. Особливості захисту інформації органами МВС Державного центру УНР в екзилі 50

2.3. Формування української радянської системи захисту інформації (1920–1930 рр.) 53

2.3.1. Організація захисту державної таємниці 53

2.3.2. Організація захисту інформації в пресі та видавничий галузі 62

2.3.3. Організація захисту рішень партії 66

2.3.4. Правові основи забезпечення захисту інформації органами ДПУ УСРР 67

2.3.5. Організація захисту військової інформації 71

2.4. Розвиток радянської системи захисту інформації в 40–80-х рр. XX ст. ... 71

2.4.1. Організаційно-правові основи забезпечення охорони державної таємниці органами КДБ 71

2.4.2. Організаційно-правові основи діяльності цензури та технічного захисту інформації 73

2.5. Забезпечення охорони державної таємниці в Україні в 90-х рр. XX ст. 75

2.5.1. Нормативно-правове забезпечення діяльності органів охорони державної таємниці 75

2.5.2. Забезпечення контролю за режимом секретності в органах державної влади, місцевого самоврядування, на підприємствах, в установах та організаціях 79

2.5.3. Забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва 80

2.6. Формування національної системи захисту інформації в 1991–2008 рр. 82

2.6.1. Характеристика законодавства України, яке визначило систему захисту інформації з обмеженим доступом 82

2.6.2. Відомчі нормативно-правові акти з питань організації захисту інформації з обмеженим доступом 95

2.7. Гармонізація законодавства про захист інформації в Україні відповідно до критеріїв і цінностей країн – членів НАТО 97

2.7.1. Характеристика етапів відносин України із структурами НАТО 97

2.7.2. Загальна характеристика законодавства про інформаційну безпеку країн – членів НАТО 106

Запитання і завдання для самоперевірки 112

Перелік використаних джерел 114

Розділ 3. Поняття та зміст інформації з обмеженим доступом 122

3.1. Зміст поняття “інформація з обмеженим доступом” 122
3.2. Види інформації з обмеженим доступом та їхні особливості 123
3.3. Місце інформації з обмеженим доступом у діяльності органів державної влади України 129
3.4. Правові особливості обігу інформації з обмеженим доступом у діяльності суб’єктів господарювання 131

Запитання і завдання для самоперевірки 135
Перелік використаних джерел 135

Розділ 4. Охорона державної таємниці в Україні 136

4.1. Правовий статус державної таємниці в Україні 136
4.2. Зміст поняття “охорона державної таємниці” 140
4.3. Звід відомостей, що становлять державну таємницю 142
4.4. Поняття допуску та доступу до державної таємниці 144
4.5. Повноваження органів, котрі забезпечують охорону державної таємниці відповідно до законодавства України 146

Запитання і завдання для самоперевірки 151
Перелік використаних джерел 151

Розділ 5. Організація захисту конфіденційної інформації та комерційної таємниці на підприємстві 152

5.1. Види інформації з обмеженим доступом на підприємстві 152
5.2. Конфіденційна інформація про особу на підприємстві 154
5.3. Режим комерційної таємниці на підприємстві 157

Запитання і завдання для самоперевірки 175
Перелік використаних джерел 176

Розділ 6. Правові засоби охорони персональних даних в Україні.....177

6.1. Зміст персональних даних як об'єкта охорони та перелік правових механізмів їхнього захисту……177

6.2. Порядок функціонування баз персональних даних……179

6.3. Перелік та основний зміст інститутів інформаційного права, які задіяні в захисті персональних даних……..182

Запитання і завдання для самоперевірки 188

Перелік використаних джерел 188

Розділ 7. Формування та експлуатація систем технічного захисту інформації з обмеженим доступом 190

7.1. Основні положення технічного захисту інформації 190

7.2. Ліцензування діяльності в галузі технічного захисту інформації 201

7.3. Сертифікація засобів та державна експертиза у сфері технічного захисту інформації 202

7.4. Основна термінологія в галузі технічного захисту інформації 205

7.5. Перелік нормативно-правових актів та нормативних документів, що регламентують діяльність у сфері технічного захисту інформації 207

Запитання і завдання для самоперевірки 224

Перелік використаних джерел 224

Розділ 8. Організаційно-правові засади захисту інформації з обмеженим доступом у провідних країнах світу 225

8.1. Концептуальні засади захисту інформації з обмеженим доступом у країнах НАТО та ЄС 225

8.2. Політика безпеки й сутність організаційно-правових аспектів захисту інформації з обмеженим доступом у країнах НАТО та ЄС 229

8.3. Зміст організаційно-правових основ захисту інформації з обмеженим доступом у країнах НАТО і ЄС 242

8.4. Міжнародні стандарти захисту інформації 257

Запитання і завдання для самоперевірки 272

Перелік використаних джерел 273

Розділ 9. Інформаційно-аналітичне забезпечення управлінської діяльності фахівця у галузі захисту інформації з обмеженим доступом 287

9.1. Теоретичне обґрунтування змісту інформаційної діяльності 287

9.2. Інформаційний вплив суспільства на формування особистості фахівця із захисту інформації.....308

9.3. Методики формування умінь і навичок роботи з інформацією.....329

Запитання і завдання для самоперевірки 345

Перелік використаних джерел 345

ПІСЛЯМОВА 370

ЗМІСТ 371

Навчальне видання

ГУЗ *Анатолій Михайлович*
Довгань *Олександр Дмитрович*
МАРУЩАК *Анатолій Іванович*
СОЛОДКА *Олена Маркіянівна*
КАСПЕРСЬКИЙ *Ігор Петрович*
ВОЛОЩЕНКО *Андрій сергійович*
АРТЕМОВ *Володимир Юрійович*
ХМЕЛЬНИЦЬКИЙ *ОлексійОлексійович*

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

П І Д Р У Ч Н И К

За редакцією Є.Д.Скулиша

Редактор *Н.М.Мармоленко*
Художньо-технічний редактор *О.В.Денисова*

Підписано до друку 00.12.2011. Формат 60х84/16. Папір офсетний № 1.
Гарнітура Times New Roman. Друк офсетний. Ум. друк. арк.00,00.
Обл.-вид. арк. 00,00. Тираж 00 пр. Зам. №

Рег. № 29/4-299 від 07.09.2009 р.

Копіювально-розмножувальний сектор науково-видавничого відділу
Національної академії Служби безпеки України,
03022, Київ, вул. Трутенка, 22.