НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Н.І. ЛОГІНОВА, Р.Р. ДРОБОЖУР

ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЇ

Навчальний посібник

Одеса
«Фенікс»
2015

ББК 67.404.3:32.973я73
УДК 349:004.056.5
Л694

Друкується за рішенням Вченої ради
Національного університету «Одеська юридична академія»
Протокол № 3 від 29 грудня 2014 р.

Автори:

Н. І. Логінова, доцент кафедри інформаційних технологій, кандидат педагогічних наук, доцент;

Р. Р. Дробожур, асистент кафедри інформаційних технологій.

Технічний редактор:

М. А. Малишев, лаборант кафедри інформаційних технологій.

Рецензенти:

С. А. Положаєнко, *завідувач кафедри комп'ютеризованих систем управління Інституту комп'ютерних систем Одеського національного політехнічного університету, доктор технічних наук, професор.*

Б. А. Кормич, *завідувач кафедри морського та митного права Національного університету «Одеська юридична академія», доктор юридичних наук, професор.*

Посібник призначений для студентів напряму (спеціальності) «правознавство», які вивчають дисципліну «Правовий захист інформації». Посібник охоплює теоретичний і практичний матеріал, необхідний для отримання знань та умінь у сфері інформаційної безпеки та захисту інформації.

Посібник може бути корисним для аспірантів, викладачів та інших спеціалістів гуманітарного профілю, що використовують у своїй діяльності інформаційні технології.

Л694 **Правовий захист інформації**: Навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса: Фенікс, 2015. – 264 с., іл.

ISBN 978-966-438-919-5

ББК 67.404.3:32.973я73
УДК 349:004.056.5

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БТ – банківська таємниця
ГКУ – Господарський кодекс України
ДТ – державна таємниця
ЕОТ – електронно-обчислювальна техніка
ЕОМ – електронно-обчислювальна машина
ЕЦП – електронний цифровий підпис
ЗВДТ – Звід відомостей, що становлять державну таємницю
ЗМІ – засоби масової інформації
ЗУ – Закон України
ІБ – інформаційна безпека
ІзОД – інформація з обмеженим доступом
ІКТ – інформаційно-комунікаційні технології
ІС – інформаційна система
КЗпПУ – Кодекс законів про працю України
ККУ – Кримінальний кодекс України
КПКУ – Кримінальний процесуальний кодекс України
КТ – комерційна таємниця
КУпАП – Кодекс України про адміністративні правопорушення
НІ – носій інформації
НСД – несанкціонований доступ
ОС – операційна система
ПД – персональні дані
ПЗ – програмне забезпечення
ПК – персональний комп'ютер
ПТ – професійна таємниця
СБ – служба безпеки
СЗІ – система захисту інформації
ТДР – таємниця досудового розслідування
ЦКУ – Цивільний кодекс України
ЦПКУ – Цивільний процесуальний кодекс України.

ЗМІСТ

ПЕРЕДМОВА

Сьогодні в умовах переходу від індустріального до інформаційного суспільства в більшості країн світу спостерігаються бурхливі процеси розвитку інформаційних відносин, які є наслідком еволюції інформаційних технологій. Ці процеси несуть як позитивний ефект, що відображається в забезпеченні прав громадян на інформацію та реалізації їх інформаційних потреб, так і потенційну небезпеку зловживання певною інформацією та заподіяння шкоди інформаційним правам та інтересам особи.

Становлення України як правової держави, інтеграція її в європейський простір, реформування економіки та оборони викликало необхідність створення принципово нової системи захисту інформації та законодавчого регулювання інформаційних правовідносин.

Конституція України врахувала загальносвітові тенденції глобалізації та інформатизації суспільства. Тому ряд її статей визначають забезпечення інформаційної безпеки як одну з найважливіших функцій держави і стають основою розвитку інформаційного законодавства.

Ми живемо у світі конкурентної боротьби за сфери впливу на міжнародній арені, світових ринках, за пріоритети у науковій, військово-технічній, економічних галузях. Тож захист інформації, охорона державної таємниці є невід'ємною складовою національної безпеки України.

Актуальність правового захисту інформації зумовлена об'єктивним зростанням кількості інформаційних загроз та шляхів протидії їм в процесі побудови інформаційного суспільства. Тому в багатьох ВНЗ гуманітарного профілю, у тому числі й в Національному університеті «Одеська юридична академія», при підготовці спеціалістів і магістрів викладаються спецкурси, що торкаються різноманітних аспектів захисту інформації, які мають на меті навчити студентів впровадженню організаційно-правових заходів щодо забезпечення інформаційної безпеки в сучасних інформаційних системах та повсякденній діяльності, пов'язаній з отриманням та опрацюванням юридичної інформації.

В навчальному посібнику «Правовий захист інформації» запропоновано систематизований матеріал для детального вивчення теоретичних і практичних аспектів правового захисту інформації.

Автори систематизували праці вчених і фахівців в галузі інформаційного права, інформаційної безпеки та захисту інформації І. Л. Бачило, С. Л. Ємельянова, В. А. Копилова, Б. А. Кормича, В. Н. Лопатіна, А. І. Марущака, І. В. Смолякової, В. С. Цимбалюка, М. Я. Швеця та інших, а також власні дослідження.

В теоретичній частині навчального посібника розглянуто основні поняття інформації та аспекти її правового захисту. Проаналізовано види інформації за порядком доступу. Докладно розглянуто правові інститути таємниць в Україні. Розкрито суть і зміст організаційно-правового захисту персональних даних. Здійснено аналіз міжнародного досвіду в сфері захисту інформації та боротьби з комп'ютерною злочинністю.

Практичні заняття, лабораторні роботи, теми додаткових інформаційних повідомлень і рефератів охоплюють всі питання, розглянуті в теоретичній частині, й спрямовані на формування у студентів навиків аналізу можливих загроз інформації та дій порушників, практичного використання чинного законодавства для захисту різних видів інформації, вмінню здійснювати конкретні організаційні методи з правового захисту інформації.

Також у навчальному посібнику наведено тематичний план дисципліни «Правовий захист інформації», зміст програми за темами, контрольні запитання для самоконтролю, підсумковий тест та бібліографію.

Автори висловлюють щиру вдячність рецензентам за цінні поради та зауваження до рукопису навчального посібника професорам С. А. Положаєнко та Б. А. Кормич.

Шановні читачі!

Якщо ви маєте зауваження та пропозиції щодо змісту навчального посібника, повідомте авторів, надіславши листа на електронноу поштову адресу ***informatics@onua.edu.ua.***

Дякуємо за співпрацю!

ТЕМАТИЧНИЙ ПЛАН ДИСЦИПЛІНИ

№	Тема	Аудиторна робота		Самостійна робота
		Лекції	Практ. заняття	
1.	Поняття інформації та її захист як складова інформаційної безпеки. Правовий захист інформації	**4**	**2**	**4**
2.	Види інформації за порядком доступу. Публічна інформація	**2**	**2**	**6**
3.	Інформація з обмеженим доступом та її види	**2**	**2**	**2**
4.	Інститут державної таємниці	**2**	**2**	**2**
5.	Інститути банківської та комерційної таємниць	**2**	**2**	**2**
6.	Таємниця досудового розслідування та судочинства	**2**	**2**	**2**
7.	Професійна таємниця та інші види таємниць, передбачені законодавством України	**2**	**4**	**4**
8.	Захист персональних даних	**2**		**10**
9.	Міжнародний досвід у сфері захисту інформації та в боротьбі з комп'ютерною злочинністю	**2**		**4**
Загальна кількість годин:		**20**	**16**	**36**
		36		

ЗМІСТ ПРОГРАМИ ЗА ТЕМАМИ

ТЕМА 1.
Поняття інформації та її захист як складова інформаційної безпеки. Правовий захист інформації

Об'єкт, предмет, мета та завдання дисципліни, методи її вивчення.

Поняття «інформація» та підходи до його визначення; інформація і дані. Законодавство про інформацію. Класифікація інформації. Властивості інформації.

Інформаційна безпека як інтегральна проблема: поняття, структура та зміст інформаційної безпеки. Концептуальна модель інформаційної безпеки. Загрози національній безпеці держави в інформаційній сфері.

Інформація як об'єкт захисту. Місцезнаходження інформації. Носії інформації та канали передачі даних. Інформаційні системи та мережі.

Основні загрози інформації та їх класифікація. Комп'ютерна злочинність як комплексна загроза інформації.

Напрями захисту інформації. Поняття та сутність правового захисту інформації та його нормативно-правове забезпечення. Поєднання правових заходів із захисту інформації з організаційними та інженерно-технічними.

Системи захисту інформації (СЗІ). Мета та засади побудови типової СЗІ, її структура. Аналіз та управління ризиками. Контроль ефективності захисту.

ТЕМА 2.
Види інформації за порядком доступу. Публічна інформація

Види інформації за законодавством України. Доступ до інформації. Законодавчі засади поділу інформації на відкриту та інформацію з обмеженим доступом.

Законодавче визначення публічної інформації. Принцип прозорості та відкритості в діяльності суб'єктів владних повноважень. Порядок доступу до публічної інформації та його законодавче регулювання.

Суб'єкти відносин у сфері доступу до публічної інформації. Запитувач та розпорядник інформації, їх правовий статус, права та обов'язки за законодавством України.

Реалізація права на доступ до публічної інформації. Інформаційний запит.

Відповідальність за порушення законодавства про доступ до публічної інформації.

ТЕМА 3.
Інформація з обмеженим доступом та її види

Інформація з обмеженим доступом (ІзОД) за українським законодавством. Законні підстави (вимоги) за якими може бути здійснено обмеження доступу до інформації. Інформація що належить до ІзОД. Інформація що не може бути обмеженою та відомості, які не належать до ІзОД.

Види ІзОД. Поняття конфіденційної інформації, її правові ознаки, відомості, що відносяться до конфіденційної інформації. Поняття таємної інформації, її правові ознаки, види таємниць. Поняття та склад правових інститутів таємниць (за видами). Службова інформація – поняття та відомості що до неї відносяться.

ТЕМА 4.
Інститут державної таємниці

Поняття державної таємниці (ДТ), його законодавче визначення. Складові правового інституту ДТ. Законодавство України про ДТ.

Правові ознаки ДТ. Інформація, що відноситься до ДТ. Інформація, що не відноситься до ДТ.

Охорона ДТ. Основні організаційно-правові заходи щодо охорони ДТ. Ступені та відповідні грифи секретності, категорії режиму секретності. Засекречування та розсекречування матеріальних носіїв інформації, строки засекречування. Державні органи в сфері ДТ. Державний експерт з питань таємниць та його правовий статус. Режимно-секретні органи, їх правовий статус та основні завдання.

Допуск та доступ до ДТ. Режим доступу до ДТ. Порядок надання допуску до ДТ, форми допуску та строки доступу до ДТ.

Контроль за забезпеченням охорони державної таємниці та нагляд за додержанням законодавства про державну таємницю.

Відповідальність за порушення законодавства про державну таємницю.

ТЕМА 5.
Інститути банківської та комерційної таємниць

Інститут банківської таємниці (БТ) та його склад. Проблема міжгалузевого характеру правового інституту БТ та правові норми, що входять до складу інституту.

Поняття БТ, її правові ознаки та основні риси. Інформація, що містить БТ. Співвідношення банківської таємниці із комерційною таємницею.

Заходи з охорони та захисту БТ. Порядок доступу до БТ. Порядок розкриття інформації, що містить БТ.

Відповідальність за розголошення БТ – дисциплінарна, цивільно-правова, кримінальна.

Правовий інститут комерційної таємниці (КТ) та його структура. Поняття КТ, відомості, що до неї відносяться та інформація, що не входить до КТ.

Заходи із охорони та захисту КТ та їх законодавче регулювання. Система загроз та ризиків.

Роль КТ в господарській діяльності.

Відповідальність за розголошення КТ, наслідки розголошення КТ.

ТЕМА 6.
Таємниця досудового розслідування

Поняття таємниці досудового розслідування (ТДР), його законодавче визначення. Правовий інститут ТДР, його особливості. Процесуальні та матеріальні норми права у правовому інституті ТДР.

Інформація, що відноситься до ТДР. Межі застосування ТДР та поширення її дії на судовий розгляд. Таємниця нарадчої кімнати. Закрите судове засідання. Співвідношення дії ТДР у судовому розгляді з принципами публічності та принципом гласності та відкритості судового провадження та його повного фіксування технічними засобами.

Загрози ТДР, заходи з охорони та захисту ТДР.

Недосконаліть законодавства щодо ТДР, пропозиції з його вдосконалення.

ТЕМА 7.
Професійна таємниця та інші види таємниць, передбачені законодавством України

Професійна таємниця (ПТ) – поняття, ознаки, законодавче визначення. Проблема недосконалості правового інституту ПТ. Інформація, що входить до ПТ за законодавством України. Інформація, що за своєю природою та властивостями може входити до ПТ. Заходи із захисту й охорони ПТ.

Інші види таємниць, передбачені законодавством, їх поняття, ознаки, норми, які визначають їх правовий статус; співвідношення їх з ПТ.

Лікарська, нотаріальна, адвокатська, податкова, аудиторська, журналістська, інсайдерська таємниці, таємниця страхування, сповіді, усиновлення, авторства, голосування, зв’язку (листування) – поняття, норми, що визначають їх правовий статус, інформація, що входить до кожного виду таємниць, системи захисту та охорони.

ТЕМА 8.
Захист персональних даних

Персональні дані (ПД), поняття, ознаки та законодавче визначення. Доктринальний та нормативно-правовий підходи до визначення ПД. ПД як складова права на приватність. Інформація, що відноситься до персональних даних.

Інститут ПД, його складові. ПД як об'єкт захисту. Українське законодавство про захист персональних даних. Уповноважений Верховної Ради з прав людини та його повноваження у сфері захисту ПД.

Суб'єкти відносин, пов'язаних із ПД, їх правовий статус, права та обов'язки.

Обробка ПД. Співвідношення понять «використання», «обробка», «збирання» «накопичення та зберігання» ПД. Доступ до ПД.

Конфіденційність інформації в мережі Інтернет та захист ПД в соціальних мережах.

Відповідальність за порушення законодавства про захист персональних даних. Судова практика у справах щодо захисту ПД.

ТЕМА 9.
Міжнародний досвід у сфері захисту інформації та в боротьбі з комп'ютерною злочинністю

Міжнародний досвід у боротьбі з загрозами інформаційній безпеці. Міжнародні нормативно-правові акти та світові стандарти захисту інформації. Політика Європейського Союзу в сфері інформаційної безпеки.

Комп'ютерні злочини як інтегральна міжнародна проблема. Міжнародна правова класифікація кіберзлочинів. Конвенція про кіберзлочинність. Характерні риси комп'ютерної злочинності. Криміналістична характеристика комп'ютерного злочинця.

«Мінімальний» та «необов'язковий» списки комп'ютерних злочинів, рекомендовані до включення до законодавства європейських країн. Аналіз статистики та тенденцій розвитку міжнародної комп'ютерної злочинності.

1 ПОНЯТТЯ ІНФОРМАЦІЇ ТА ЇЇ ЗАХИСТ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЇ

§1.1. Поняття інформації

Одним із найважливіших серед об'єктів захисту в сучасному інформаційному суспільстві стають *інформація та інформаційні ресурси*.

Поняття «***інформація***» (походить від лат. *informatio* – ознайомлення, пояснення) і на сьогоднішній день є одним із поширених і ключових в різних областях знань, проте його загальноприйнятого наукового визначення не існує. Це пояснюється багатоаспектністю інформації (існуванням в живій і неживій природі, в кібернетичних системах, в суспільстві та ін.), різноманітністю її форм проявів в матеріальному світі, особливостями в способах її вивчення і використання різними областями науки і практики[1].

У визначенні поняття ***«інформація»*** в різні роки переважали три основні підходи: ***недетермінований***, ***техноцентричний*** і ***антропоцентричний***.

Недетермінований підхід до поняття інформації (від лат. *determinare* – обмежити, визначити) полягає у відмові від визначення інформації на тій підставі, що вона є фундаментальним поняттям, яке має необмежені рамки. Один із засновників кібернетики Норд Вінер визначав інформацію як позначення змісту, який черпається нами із зовнішнього світу в процесі пристосування до нього і приведення відповідно до нього нашого мислення. Він стверджував, що: *«Інформація є інформація, а не матерія і не енергія»*[2].

У розвитку цієї ідеї ряд дослідників розглядали інформацію як основу всього існуючого, первинну складову всіх явищ і процесів.

---

[1] Використання інформаційних технологій в судах: Навчальний посібник / Ємельянов С. Л., Логінова Н. І., Тодощак О. В., Якутко В. Ф. – Одеса: Фенікс, 2014. – С. 11–15.

[2] Винер Н. Кибернетика, или Управление и связь в животном и машине. / Пер. с англ. И. В. Соловьева и Г. Н. Поварова; Под ред. Г. Н. Поварова. – 2-е издание. – М.: Наука; Главная редакция изданий для зарубежных стран, 1983. – С. 208.

Тобто, інформація поза людської свідомості не існує[3].

Значення ***техноцентричного*** підходу полягає в тому, що інформацію ототожнюють з даними, які мають кількісний вимір (обсяг, швидкість передачі, пропускну здатність каналу тощо). Основоположник теорії інформації Клод Шеннон в 60-х роках XX століття обґрунтував поняття ***«інформації»*** як «*впорядкованої субстанції, яку можна описати математично: кількість інформації тим більше, чим більше невизначеності усувається при отриманні цієї інформації*»[4].

Цей підхід і зараз переважає в точних науках і широко застосовується при розробці та реалізації багатьох, насамперед, апаратно-програмних засобів захисту інформації. Однак в цьому випадку не розглядається змістовний аспект інформації, що не дозволяє використовувати вказаний підхід до правового регулювання інформаційних правовідносин.

Зміст ***антропоцентричного*** підходу полягає в тому, що інформацію ототожнюють з відомостями або фактами, які теоретично можуть бути отримані і засвоєні, тобто перетворені в знання. Саме цей підхід знайшов широке застосування в юридичній науці і чинному законодавстві.

Так, в ст. 1 ЗУ «Про інформацію»[5], прийнятого в 1992 р. було законодавче закріплено таке визначення інформації: «*це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі*».

Але розуміння інформації як відомостей лише про події та явища (статистичне поняття) залишило без уваги відомості про процеси, які можуть тривати в часі.

Одна з основних перешкод введення інформації в цивільний обіг

---

[3] Чубукова С. Г., Элькин В. Д. Основы правовой информатики (юридические и математические вопросы информатики): Учебное пособие. Изд. 2-е, испр., доп. / Под ред. доктора юридических наук, проф. М. М. Рассолова, проф. В. Д. Элькина. – М.: Юридическая фирма «КОНТРАКТ», 2007. – С. 29.

[4] Шеннон К. Работы по теории информации и кибернетике: Математическая теория связи. – М., 1963. – С. 242-332.

[5] Про інформацію: Закон України від 2.10.1992 р. // Відомості Верховної Ради. – 1992. – № 48. – Ст. 650.

та її правового регулювання полягає в *ідеальності* інформації, поки вона існує в свідомості людини. Її перенесення на матеріальний носій (запис на папір, електронний або інший носій) не означає, що інформація матеріалізується, позаяк матеріальним є тільки носій, а не сама інформація. Сама інформація, знову-таки, ідеальна, адже вона залишилася в пам'яті її творця або особи, яка була з нею ознайомлена.

Інформація може існувати в різних формах і видах, і мати різні прояви. Наприклад, за фізичною формою свого прояву інформація поділяється на два основних види: акустичну (зазвичай мовну) і сигнальну. Акустична інформація сприймається органами слуху, а сигнальна – органами зору. Поняття «*сигнальна інформація*» охоплює досить широку кількість можливих схем інформаційного обміну, що існують на практиці. Її можна розділити на аналогово-цифрову (документи на папері або електронних носіях) і об'ємно-видову (графіки, креслення, малюнки тощо).

Ці обставини змусили законодавця шукати нові визначення поняття «інформації», які б відображали можливі матеріальні види та прояви інформації.

Так в ст. 1 ЗУ «Про захист економічної конкуренції»[6] було визначено, що інформація – це *«відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості»*.

А в ст. 1 ЗУ «Про телекомунікації»[7] уточнено: «*Інформація – це відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб»*.

Оскільки недоцільним було б законодавчо перераховувати всі можливі носії та прояви інформації, які мають здатність постійно

[6] Про захист економічної конкуренції: Закон України від 11.01.2001 р. // Відомості Верховної Ради. – 2001. – № 12. – Ст. 64.

[7] Про телекомунікації: Закон України від 18.11.2003 р. // Відомості Верховної Ради. – 2004. – № 12. – Ст. 155.

змінюватися з розвитком інформаційно-комунікаційних технологій (ІКТ), в ЗУ «Про внесення змін до Закону «Про інформацію»[8], прийнятого в 2011 р., дано таке визначення: *«Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді»*.

Це законодавче визначення є найбільш вдалим з точки зору захисту інформації, так як поняття «інформації» як «відомості» дозволяє організувати правовий захист інформації на основі обмежень відомостей, які містять різні види таємниць, передбачені законами. Наприклад: державну, банківську, професійну тощо.[9]

Ототожнення понять «*інформація*» і «*дані*» надає можливість захищати інформацію за допомогою технічних та криптографічних засобів, так як саме у вигляді даних інформація зберігається, обробляється і передається в сучасних інформаційних системах.

Термінологічна конструкція «*будь-які відомості та/або дані*» більш вдала ніж «*відомості про події та явища*», оскільки, наприклад, персональні дані – це не завжди відомості про події та явища, а інформація, що дозволяє ідентифікувати особу. Вказані можливості збереження «*на матеріальних носіях або відтворення в електронному вигляді*» акцентує увагу саме на матеріальних носіях інформації, несанкціонований доступ до яких треба виключити за допомогою систем захисту інформації.

Отже, зараз у чинному законодавстві України відбувається зближення антропоцентричного та техноцентричного підходів до визначення інформації, що є позитивним аспектом правового регулювання інформаційних відносин в суспільстві.

§1.2. Властивості інформації

Як первинна субстанція, інформація має низку властивостей і характеристик, які по-різному визначаються та використовуються в різних галузях знань і життєдіяльності людини.

---

[8] Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 р. // Офіційний вісник України. – 2011. – № 10. – Ст. 445.

[9] Використання інформаційних технологій в судах: Навчальний посібник / Ємельянов С. Л., Логінова Н. І., Тодощак О. В., Якутко В. Ф. – Одеса: Фенікс, 2014. – С. 39.

В інформаційному праві виділяють загальні та юридичні властивості інформації[10]. Також існують властивості інформації, що характеризують її якість для прийняття рішення, що визначають стан безпеки інформації та ін. *(рис. 1.1)*

Рис. 1.1. Основні властивості інформації

До ***загальних властивостей інформації*** належать ті, які властиві будь-якій інформації, що використовується в суспільстві та впливають на всі суспільні відносини інформації, незалежно від наявності чи відсутності правового регулювання:

Системність – властивість інформації, яка вказує на те, що будь-яка інформація, що створюється людиною, має певну внутрішню організаційну структуру, встановлену в суспільстві правилами та законами. Наприклад: фраза, речення, документ мають свої правила побудови, що визначаються граматичними і орфографічними правилами, лексикою, правилами документування та ін.

Селективність (вибірковість) – це залежність інформації від процесів її вибору та відбору. Перетворення сукупності даних та відомостей про інформацію є суб'єктивним процесом, залежним від суб'єкта, що одержує, використовує, поширює та зберігає інформацію. Тому на основі одних і тих самих даних або відомостей різними суб'єктами може бути створена різна за змістом інформація, зроблені різні висновки, про що свідчить, наприклад, судова практика.

[10] Копылов В. А. Информационное право / В. А. Копылов. – М.: Юрист, 2002.– С. 40; Кормич Б. А. Інформаційне право: Підручник / Б. А. Кормич. – Харків: БУРУН і К, 2011. – С. 12.

Субстанційна несамостійність – це властивість обумовлена зв'язком інформації з процесом її відображення. Це дуалізм інформації та її матеріального носія.

Невичерпність інформації полягає в тому, що на відміну від предметів матеріального світу, використання яких призводить до фізичного зносу або виснаження, використання інформації не впливає на її стан і якість, тобто інформація може мати необмежену кількість користувачів, залишаючись при цьому в незмінному стані.

Здатність інформації до поширення зумовлена її невичерпністю і здатністю до безконтрольного розповсюдження, навіть незважаючи на встановлення правових обмежень доступу до певних видів інформації.

Здатність інформації до трансформації полягає в тому, що інформація може зберігатися, накопичуватися на будь-яких придатних для цього носіях, а також як у свідомості окремої людини, так і в масовій свідомості суспільства. Ця властивість означає незалежність змісту інформації від форми її фіксації та способу відображення. Інформація здатна змінюватися, вдосконалюватися, деталізуватися. На її основі можна створювати нову інформацію та ін.

До ***юридичних властивостей інформації*** належать ті, які безпосередньо зумовлюють специфіку правового регулювання суспільних відносин до інформації[11]:

Фізична невідчужуваність інформації пов'язана з її ідеальною природою і полягає в тому, що інформація не здатна відчужуватися від людини – її творця або носія. При передачі інформації від однієї особи до іншої і юридичного закріплення цього факту, процедура відчуження інформації повинна замінюватися передачею прав на її використання і передаватися разом з цими правами.

Необхідність відокремлення показує, що включена в обіг інформація завжди представлена у вигляді символів, знаків, хвиль, внаслідок чого вона відокремлюється від її виробника (творця) та існує

[11] Кормич Б. А. Інформаційне право: Підручник / Б. А. Кормич. – Харків: БУРУН і К, 2011. – С. 13–15; Парошин А. А. Нормативно-правовые аспекты защиты информации: Учебное пособие / А. А. Парошин. – Владивосток: изд-во Дальневост. федер. ун-та, 2010. – С. 15–16.

окремо незалежно від нього.

Незалежність прав на інформацію та її матеріальні носії з’являється через те, що інформація передається і поширюється тільки на матеріальному носії або за допомогою матеріального носія. Тут проявляється дуалізм інформації – її змісту та носія, на якому ця інформація закріплена. Ця властивість дозволяє поширювати на інформаційний об'єкт дію інституту авторського права.

Здатність до тиражування – властивість інформації, безпосередньо пов'язана з такою її характеристикою, як невичерпність. Ця властивість є ключовою для правового регулювання діяльності з поширення інформації, адже її можна копіювати (тиражувати) необмежену кількість разів, і при цьому вона не зменшується за обсягом і не втрачає своїх споживчих якостей.

Якість інформації розглядається як сукупність властивостей інформації, що характеризують міру її відповідності потребам користувачів:

Адекватність інформації – це певний рівень відповідності, що створюється за допомогою отриманої інформації образу, реальному об'єкту, процесу, явищу тощо. В реальному житті практично неможлива ситуація, коли можна розраховувати на повну адекватність інформації. Завжди існує деяка ступінь невизначеності.

Під *достовірністю інформації* розуміється її відповідність об’єктивній дійсності (як поточній, так і минулій). Властивість достовірності має велике значення для прийняття рішень. Недостовірна інформація може привести до рішень, які мають негативні економічні, соціальні, політичні чи юридичні наслідки.

Актуальність інформації – це ступінь відповідності інформації теперішньому моменту часу. Часто саме з актуальністю пов'язують комерційну цінність інформації. Оскільки інформаційні процеси розтягнуті в часі, то достовірна і адекватна, але застаріла інформація може приводити до помилкових рішень. Затримка в отриманні інформації або її старіння ведуть до того, що інформація стає неактуальною.

Повнота інформації означає, що її склад мінімальний, але

достатній для прийняття правильного рішення. Вона залежить як від повноти даних, так і від наявності необхідних методів доступу і обробки.

Суб'єктивність і об'єктивність – ці властивості є відносними. В ході інформаційного процесу ступінь об'єктивність інформації завжди знижується. Наприклад, в результаті перегляду фотографії предмета створюється більш об'єктивна інформація, ніж в результаті перегляду малюнка цього ж предмета.

Надлишковість інформації – це властивість, користь якої ми відчуваємо дуже часто. Нерідко надлишковість інформації людина чисто психологічно сприймає як її якість, тому що вона дозволяє йому менше напружувати свою увагу і менше стомлюватися. Так, текст, надрукований знайомою мовою, має надлишковість близько 20-25%. Якщо відкинути кожну п'яту букву, то отримати інформацію з надрукованого тексту все ж можна, хоча читати його буде достатньо складно.

У рішенні проблем захисту інформації важливу роль відіграють властивості інформації, ***які визначають стан її безпеки***:

Конфіденційність – суб'єктивно визначена властивість інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, які мають доступ до неї. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила її отримання або ознайомлення з нею.

Цілісність – властивість інформації, яка полягає в її існуванні в незмінному вигляді в певний проміжок часу. Інформація зберігає цілісність, якщо підтримуються встановлені правила її модифікації або видалення.

Доступність – властивість інформації бути наданою своєчасно і безперешкодно всім суб'єктам, які мають для цього певні повноваження. Інформація зберігає доступність, якщо протягом певного проміжку часу легітимним (санкціонованим) користувачам немає відмови (блокування) в її отриманні.

Зазначені властивості повинні враховуватися при правовому захисті інформації.

§1.3. Роль інформації в формуванні інформаційного суспільства

У сучасному суспільстві інформація має величезне значення і виконує наступні функції[12]:

- інтегративну, що забезпечує згуртування членів суспільства і соціальних груп в єдине ціле;
- комунікативну, яка сприяє спілкуванню і взаєморозумінню;
- інструментальну, що бере участь в організації виробництва і управління;
- пізнавальну, що є засобом відображення об'єктивної дійсності і передачі даних.

Впровадження інформації в усі сфери життєдіяльності людини сприяє формуванню інформаційного суспільства, можливості якого в різних країнах розглядаються як джерело соціально-економічного розвитку, інтелектуально-технологічної революції, яка приведе в недалекому майбутньому до рішучих змін характеру виробництва, активного формування нового національного і міжнародного інформаційних ринків.

Термін «***інформаційне суспільство***» був введений в обіг на початку 60-х років XX століття одночасно в Японії і США. Інформаційне суспільство – одна з теоретичних моделей, що використовуються для опису якісно нового етапу суспільного розвитку, в який вступили розвинені країни з початком інформаційно-комп'ютерної революції. Технологічною підставою суспільства стають не індустріальні технології, а ІКТ.

З кінця 1990-х років минулого століття концепція інформаційного суспільства знайшла активне застосування в соціальній практиці т проектах, спрямованих на впровадження ІКТ в різні сфери життя суспільства, що особливо проявилося в програмах Європейського Союзу (ЄС). Зокрема, проблематика інформаційного суспільства обговорювалася на нарадах та конференціях, організованих Радою Європи, Європейською Комісією, ЮНЕСКО та

[12] Гаврилов О. А. Курс правовой информатики: Учебник для вузов. – М.: Изд-во НОРМА, 2002. – С. 37–41.

іншими міжнародними і міжурядовими організаціями. У 1998 р. Міжнародний союз електрозв'язку (ITU) виступив з пропозицією про проведення під егідою ООН всесвітнього саміту з інформаційного суспільства. Паралельно здійснювалася аналогічна діяльність в рамках групи G8, яка завершилася підписанням в 2000 р. «Окінавської хартії глобального інформаційного суспільства», де лідери держав, що входять до «вісімки» відзначили готовність до реалізації в своїх країнах програм, спрямованих на розвиток інформаційного суспільства та ліквідації інформаційної нерівності[13]. У цей час і з'явилося поняття «*інформаційного суспільства», як суспільства, заснованого на інформації*.

Характерні риси інформаційного суспільства були сформульовані західним ученим професором Мартіном в якості п'яти критеріїв:

1) *технологічний критерій*: інформаційні технології набули глобального характеру, охопивши всі сфери соціальної діяльності людини;
2) *соціальний критерій*: інформація виступає в якості важливого стимулятора зміни якості життя, формується і затверджується «інформаційна свідомість» при широкому доступі до інформації;
3) *економічний критерій*: інформація є ключовим фактором в економіці в якості ресурсу, послуг, товару, джерела доданої вартості та зайнятості;
4) *політичний критерій*: свобода інформації, що веде до політичного процесу, який характеризується зростаючою участю і консенсусом між різними класами і соціальними верствами населення;
5) *культурний критерій*: визнання культурної цінності інформації шляхом сприяння утвердженню інформаційних цінностей в інтересах розвитку окремого індивіда і суспільства в цілому.

[13] Чугунов А. В. Развитие информационного общества: теории, концепции и программы: Учебное пособие. – СПб.: Ф-т филологии и искусств СПбГУ, 2007. – С. 80–81.

Інформаційне суспільство в Україні задекларовано в розділі 13 Програми інтеграції України до Європейського Союзу[14]. Згідно з цією Програмою розвиток інформаційного простору в нашій країні визначається як станом розвитку інформаційних технологій, так і кількісним та якісним складом доступних інформаційних продуктів.

Матеріалами Парламентських слухань з питань розвитку інформаційного суспільства в Україні[15], ЗУ «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», Постановою Кабінету Міністрів України «Про створення Міжгалузевої ради з питань розвитку електронного урядування»[16], Розпорядженням Кабінету Міністрів України «Стратегія розвитку інформаційного суспільства в Україні»[17] та іншими нормативно-правовими актами, прийнятими за останні десятиліття в нашій країні, визначено необхідність розвитку інформаційного суспільства, орієнтованого на інтереси людей і відкритого для всіх.

Сьогодні інформація перетворилася на потужний ресурс, що володіє більшою цінністю, ніж природні, фінансові, трудові та інші ресурси. Вона стала об'єктом товарно-грошових відносин; перетворилася на зброю, спровокувавши інформаційні війни. Інформація та інформаційні ресурси є об'єктами протиправних посягань. Тому захист інформації, а в першу чергу, правовий, є основоположним аспектом громадської безпеки будь-якої держави.

Слід зазначити, що багато авторів ототожнюють поняття інформації та інформаційного ресурсу, розглядаючи їх як синоніми.

Інформаційний ресурс – систематизована інформація або знання, що мають цінність у певній предметній області та можуть

---

[14] Програма інтеграції України до Європейського Союзу: Указ Президента від 14.09.2000 р. № 1072/2000. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/n0001100-00/card6#Public.

[15] Парламентські слухання з питань розвитку інформаційного суспільства в Україні: Матеріали Парламентських слухань у Верховної Ради України від 21.09.2005 р./ Верховна Рада України; Комітет з питань науки і освіти / М. К. Родіонов (голова редкол., упоряд.), І. Б. Жиляєв (упоряд.). – К.: Парламетн. вид-во, 2006. – 174 с.

[16] Про утворення Міжгалузевої ради з питань розвитку електронного урядування: Постанова Кабінету Міністрів України від 14.01.2009 р. № 4. – Офіційний вісник України. – 2009. – № 3. – С. 52. – Ст. 77.

[17] Стратегія розвитку інформаційного суспільства в Україні: Розпорядження Кабінету міністрів України від 15.05.2013 р. № 386-р // Офіційний вісник України. – 2013. – № 44. – С. 79. – Ст. 1581.

бути використані людиною у своїй діяльності для досягнення певної мети[18].

Основою інформаційного суверенітету України є ***національні інформаційні ресурси***, до яких входить *вся належна країні інформація, незалежно від змісту, форми, часу і місця створення*.[19]

Слід зазначити, що перехід людства до інформаційного суспільства, в якому основним товаром є інформація та інформаційні послуги, супроводжується впровадженням ІКТ в усі сфери людської діяльності, що і спричинило за собою необхідність вирішення питань правового регулювання суспільних відносин в процесі інформатизації.

В ст. 1 ЗУ «Про Національну програму інформатизації» поняття «***інформатизація***» визначено, як *«…сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів і технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки»*[20].

Правове забезпечення інформатизації – це діяльність відповідних суб'єктів суспільних відносин щодо формування комплексу юридичних норм, прав та обов'язків учасників у сфері інформатизації[21].

З метою активізації інформаційного потенціалу суспільства створюється сучасна інформаційна інфраструктура. Її формування передбачає:

---

[18] Стратегія розвитку інформаційного суспільства в Україні: Розпорядження Кабінету міністрів України від 15.05.2013 р. № 386-р // Офіційний вісник України. – 2013. – № 44. – С. 79. – Ст. 1581.

[19] Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9.01.2007 р. // Відомості Верховної Ради. – 2007. – № 12. – Ст. 102.

[20] Про Національну програму інформатизації: Закон України від 04.02.1998 р. // Відомості Верховної Ради України. – 1998. – № 27. – Ст. 181.

[21] Інформатизація управління соціальними системами: Організаційно-правові питання теорії і практики: Навч. посіб. / В. Д. Гавловський, Р. А. Калюжний, В. С. Цимбалюк та ін.: За заг. ред. М. Я. Швеця, Р. А. Калюжного. – К.: МАУП, 2003. – 336 с.

- розвиток національної, галузевих і регіональних інформаційних систем, мереж та електронних ресурсів, електронних інформаційно-аналітичних систем державних органів та органів місцевого самоврядування;
- забезпечення електронної взаємодії державних органів між собою, а також з громадянами та організаціями;
- створення та впровадження єдиної загальнодержавної системи електронного документообігу з використанням електронного цифрового підпису;
- розширення переліку електронних послуг, які можуть надаватися із застосуванням електронних цифрових підписів, у тому числі електронної ідентифікації суб'єктів електронної взаємодії та систем, за допомогою яких здійснюється така взаємодія та ін.[22]

Прикладом інформаційної інфраструктури є глобальна мережа Інтернет, яка активно заповнює інформаційний простір всіх країн. Вона має великий вплив на промисловий і фінансовий ринок, функціонування культури і політики різних держав.

Термін «***глобалізація»*** був введений в термінологію в 1993 р. Давоським форумом міжнародної фінансово-промислової еліти для позначення процесу інтеграції та уніфікації національних економік, політик і культур та побудови світового капіталізму без держави і кордонів. У соціально-економічних і правових областях глобалізація розуміється як узагальнююча подія, що виникає в результаті еволюційних і кардинальних змін в суспільстві[23].

Глобалізація по своїй суті є процес об'єктивний, а його матеріальною основою стає революція в технічній сфері, коли виникають зовсім нові види комунікацій, транспорту та інформаційних технологій. В основному застосування терміну

[22] Стратегія розвитку інформаційного суспільства в Україні: Розпорядження Кабінету міністрів України від 15.05.2013 р. № 386-р // Офіційний вісник України. – 2013. – № 44. – С. 79. – Ст. 1581.

[23] Глобализация и информатизация. – [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/studies/courses/505/361/lecture/8595.

«глобалізація» пов’язане з бурхливим розвитком ІКТ[24].

Процес глобалізації характеризується низкою тенденцій, зокрема:

- інтернаціоналізація всього суспільного життя, поява феноменів «подолання кордонів» і «економічного громадянства», формування інституціональної мережевої взаємодії;
- різке зростання обсягів та інтенсивності трансдержавних перетоків капіталів, інформації, послуг і людських ресурсів;
- формування віртуального простору електронно-комунікаційного спілкування, що різко збільшує можливості для соціалізації особистості, для безпосереднього доступу до загальносвітових інформаційних процесів[25].

Інформатизація і глобалізація призводять до необхідності вирішення багатьох спільних правових проблем. Таких, як проблеми інформатизації і захисту інформації, розвитку високих і нових інформаційних технологій, еволюції інформаційних структур суспільства в глобальну інформаційну та комунікаційну світову структуру. Глобальні інформаційні процеси вимагають правового регулювання, особливо, з точки зору міжнародного інформаційного права, міжнародних інформаційних відносин, все більше актуальних в сучасному суспільстві.

§1.4. Загальні відомості про інформаційну безпеку

Характерною рисою сучасного суспільства є збільшення ролі інформації та інформаційних продуктів у всіх сферах життєдіяльності людини. Перетворення інформації на товар, що має певну цінність і відповідну вартість, привело до появи принципово нового об'єкта безпеки – інформації та інформаційних ресурсів.

Спочатку інформаційну безпеку (ІБ) розуміли як, власне, захист самої інформації від несанкціонованих дій: ознайомлення, копіювання, модифікації, знищення тощо. Потім прийшло розуміння

[24] Понарина Н. Н. Глобализация и информационное общество // Общество: политика, экономика, право. – 2012. – № 1. – С. 19–24.

[25] Информационная безопасность России в условиях глобализации. – [Електронний ресурс]. – Режим доступу: http://www.lawinrussia.ru/informatsionnaya-bezopasnost-rossii-v-usloviyakh-globalizatsii-ch-1.

того, що захищати треба не тільки інформацію та інформаційні ресурси, а й суспільство, громадян та державу від інформації, що має негативний вплив на них.

Збільшення гостроти протиборства держав в інформаційній сфері, прагнення деяких держав, окремих структур, злочинних елементів до протиправного використання інформаційних ресурсів, наявність численних загроз інформації обумовлюють актуальність проблеми ***ІБ*** як складової загальної проблеми інформаційного забезпечення розвитку людини, суспільства, держави[26].

В законодавстві та науковій літературі відзначаються різні підходи до визначення поняття «***інформаційна безпека***».

ЗУ «Про основи національної безпеки України»[27] розглядає ІБ, як один з видів національної безпеки в інформаційній сфері.

В Доктрині інформаційної безпеки України[28] затверджується, що «*ІБ є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави*».

Для подальшого розгляду правового захисту інформації, визначимо поняття «***інформаційна безпека***» як *стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави*[29].

---

[26] Використання інформаційних технологій в судах: Навчальний посібник / Ємельянов С. Л., Логінова Н. І., Тодощак О. В., Якутко В. Ф. – Одеса: Фенікс, 2014. – С. 16–17.

[27] Про основи національної безпеки України: Закон України від 19.07.2003 р. // Відомості Верховної Ради. – 2003. – № 39. – Ст. 351.

[28] Про Доктрину інформаційної безпеки України: проект указу Президента України [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025. – 12.06.2014.

[29] Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О.К. Юдін. – К.: «МК-Прес», 2005. – С. 39.

Згідно з Доктриною інформаційної безпеки, структура і вміст поняття «інформаційної безпеки», а також основні напрямки та принципи державної політики в сфері ІБ наведені на *рис. 1.2*[30].

Рис. 1.2. Структура і склад інформаційної безпеки

[30] Ємельянов С. Л. Основи інформаційної безпеки: Навчальний посібник / С. Л. Ємельянов. – Одеса: «Фенікс», 2014. – С. 19–29.

Основними напрямками державної політики України в сфері ІБ є:

- ***інформаційно-психологічний***, що забезпечує конституційні права і свободи людини і громадянина, створює сприятливий психологічний клімат в національному інформаційному просторі для утвердження загальнолюдських і національних моральних цінностей;
- ***технологічний***, відповідає за розвиток і інноваційне оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, обробки та розповсюдження інформації;
- ***захист інформації***, забезпечує конфіденційність, цілісність і доступність інформації, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

Таким чином, ІБ – досить містка і багатогранна проблема, що має інтегральний характер і охоплює багато аспектів життєдіяльності людини, суспільства, держави *(рис. 1.3.)*

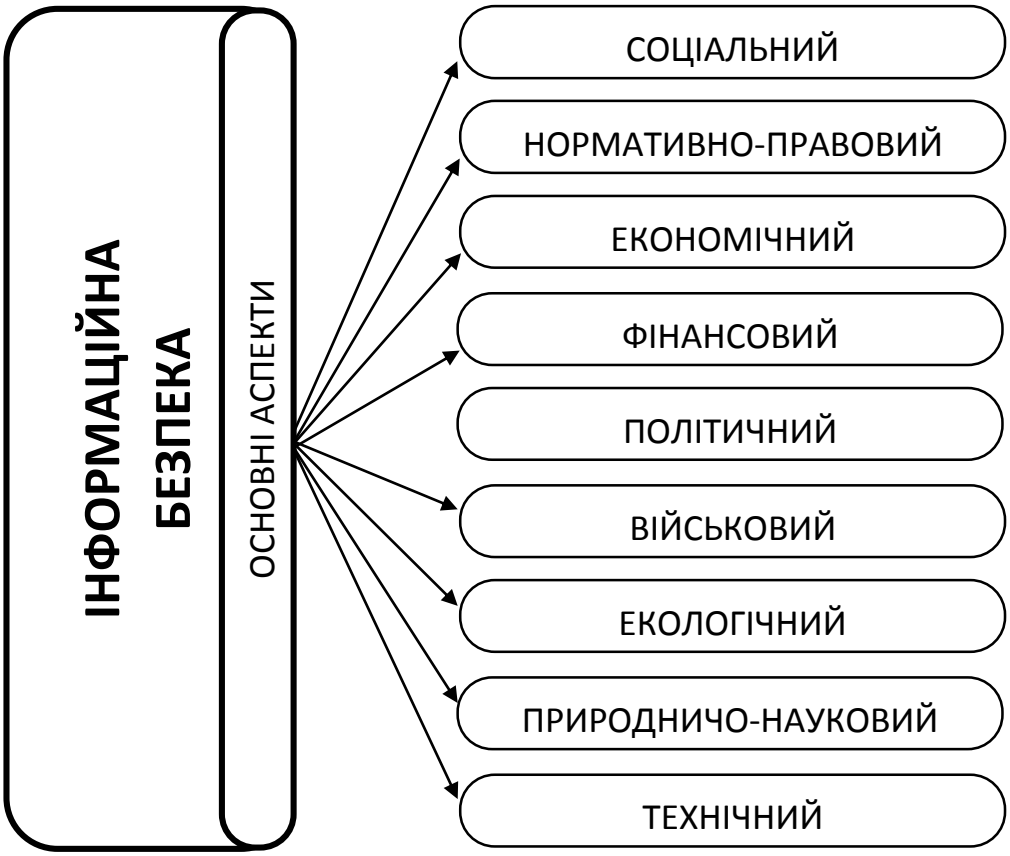

Рис. 1.3. Основні аспекти інформаційної безпеки

Соціальний аспект є одним з показників цивілізованості суспільства та рівня розвитку демократії, розумним балансом між

свободою доступу до відкритої інформації та надійним захистом інформації з обмеженим доступом. Забезпечення безпеки в соціальній сфері включає такі основні напрямки:

- виявлення і усунення причин, що призводять до різкого розшарування суспільства;
- можливість застосування своєчасних заходів щодо протидії кризовим демографічним процесам;
- створення ефективної системи соціального захисту людини, охорони та відновлення її фізичного і духовного здоров'я;
- стимулювання розвитку та забезпечення всебічного захисту освітнього та культурного потенціалу країни;
- захист прав споживачів та ін.

Нормативно-правовий аспект. Правовим фундаментом інформаційного суспільства є відповідне інформаційне законодавство – безліч нормативно-правових актів, прийнятих Верховною Радою України у формі законів і постанов нормативного змісту, які регулюють суспільні відносини щодо інформації.

Сукупність юридичних норм у цій сфері вже досягла критичної маси, що дозволяє на науковому рівні умовно виділити їх в автономну область законодавства (інформаційне законодавство) та юридичний науковий інститут (інформаційне право). Тому актуальним завданням є створення цілісної системи інформаційного законодавства на підставі розробки та прийняття *Інформаційного кодексу України*[31].

Економічний аспект. Економічні аспекти проблеми ІБ можна умовно розділити на два підмножини: інформаційні аспекти безпеки економіки і власне економіка безпеки інформації.

Сьогодні багато підприємців і керівників підприємств розуміють, що без глибокого аналізу інформації, що впливає на ринок їхньої продукції, неможливо успішне ведення бізнесу. Потоки інформації, які генеруються учасниками ділової активності, при їх кваліфікованій обробці, аналізі та синтезі висновків, здатні надати підприємству

[31] Концепція реформування законодавства України у сфері суспільних інформаційних відносин (проект). – [Електронний ресурс]. – Режим доступу: http://bezpeka.com/ru/lib/lavproj\art519.html.

конкурентні переваги і суттєво вплинути на ефективність стратегічного планування економічної діяльності.

В системі економічної безпеки з'явилася і отримала розвиток так звана конкурентна розвідка (економічна, ділова, комерційна та ін.), яка забезпечує постійні процеси збору, обробки, оцінки та накопичення даних, їх аналіз з метою прийняття оптимальних рішень у всіх сферах економіки. Причому, на відміну від комерційного (промислового) шпигунства конкурентна розвідка здійснюється виключно в рамках чинного законодавства, а свої результати отримує завдяки аналітичній обробці величезного числа даних з особистих відкритих джерел інформації. За кордоном вона вже є окремою областю економіки з розвиненим арсеналом засобів і сил ведення розвідувальної інформаційно-аналітичної діяльності[32].

Економіка безпеки інформації також заслуговує на увагу. Якщо, наприклад, розглянути деякий ізольований суб'єкт господарювання, то відсутність у нього адекватного захисту важливої інформації (комерційної таємниці, ноу-хау, іншої інтелектуальної власності тощо.) неминуче призведе до значних економічних втрат, пов'язаних з витоком такий інформації[33].

Фінансовий аспект. Фінансові аспекти ІБ дуже близькі економічним, але не тотожні. Тут мова йде про безпеку фінансово-кредитної і банківської сфери країни, в яких активно застосовуються сучасні ІКТ.

Дослідження експертів США свідчать, що середня вартість втрат складає:

- від разового фізичного пограбування – 3,2 тис. дол.;
- від разового шахрайства – 23 тис. дол.;
- від правопорушення за допомогою ІКТ – 500 тис. дол.

[32] Прескотт Джон Е. Конкурентная разведка: Уроки из окопов. / Джон Е. Прескотт, Стивен Х. Миллер. – М.: Альпина Паблишер, 2003. – 336 с.; Баяндин Н. И. Технологии безопасности бизнеса: введение в конкурентную разведку/ Н. И. Баяндин. – М.: Юристь, 2002. – 320 с.; Доронин А. И. Бизнес-разведка / А. И. Доронин. – М.: Ось-89, 2002. – 288 с.

[33] Баутов А. Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. – № 2. – 2002.

При охопленні автоматизованої платіжною системою усіх регіонів країни будь-яка дестабілізація в її функціонуванні може порушити безпеку фінансово-платіжної системи і, як наслідок, привести до збою всього господарського механізму держави.

Політичний аспект. Його аналіз з точки зору проблеми ІБ показує все більший зсув центру ваги в міжнародній політиці від силових факторів до більш прихованих, заснованих на інформаційному впливі.

Безсумнівно, що технологічно розвинені держави прагнуть збільшити політичну, економічну і військову перевагу за рахунок встановлення та ведення глобального інформаційного контролю над менш розвиненими державами, проведення в світовому інформаційному просторі ідеологічної та культурної експансії.

Тому у вищезгаданій Доктрині визначаються також реальні та потенційні загрози ІБ України у зовнішньополітичній сфері:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України, та створює негативний імідж України, як ненадійного партнера для міжнародних відносин;
- низький рівень інтегрованості України у світовий інформаційний простір;
- прояви кіберзлочинності та кібертероризму, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;
- зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;
- використання інформаційного простору для втручання у внутрішні справи України.

При цьому головними пріоритетами іноземних розвідок є процеси становлення України як самостійної держави на світовій арені, її внутрішні та зовнішні політичні орієнтири, моделі та параметри економічного розвитку, спрямованість і результати

наукових розробок, аналіз всіх сегментів українського ринку товарів і послуг, бойова готовність збройних сил тощо.

Військовий аспект. Офіційно термін «інформаційна війна» вперше був введений в США в грудні 1992 р. і вказував на необхідність всебічного обліку інформаційних ресурсів в системах управління збройними силами в умовах протидії супротивника. Під *інформаційною війною* маються на увазі дії, що вживаються для досягнення інформаційної переваги в підтримці національної військової стратегії, за допомогою впливу на інформацію та інформаційні системи супротивника при одночасному забезпеченні безпеки і захисту власної інформації та інформаційних систем.

Наприкінці 1996 р. була представлена нова військова доктрина Збройних сил США на XXI сторіччя (концепція «Force XXI»), в основі якої лежить поділ театру військових дій на дві складові: традиційний простір і кіберпростір, причому останнє має навіть більш важливе значення. В число сфер ведення бойових дій, крім землі, моря, повітря і космосу тепер включена і інформаційна сфера.

Доктрина інформаційної безпеки України визначає такі реальні і потенційні загрози інформаційній безпеці у військовій сфері:

- використання інформаційного простору для підготовки та здійснення збройної агресії проти України, можливість утягування України в збройні конфлікти чи в протистояння з іншими державами через використання інформаційного простору;
- порушення вимог законодавства щодо збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;
- несанкціонований доступ до національних інформаційних і телекомунікаційних мереж та систем, що може порушити діяльність військових формувань, органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю;
- реалізація програмно-математичних заходів та застосування інформаційних технологій з метою порушення функціонування

систем управління воєнної сфери та сфери оборони;

- навмисні дії, а також помилки персоналу при роботи в інформаційних та інформаційно-телекомунікаційних системах тощо.

Екологічний аспект. Згідно з вищевказаною Доктриною, в екологічній сфері, також існують реальні і потенційні загрози ІБ України:

- приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації або надзвичайні ситуації техногенного та природного характеру;
- недостатня надійність інформаційно-телекомунікаційних систем збору, обробки і передачі інформації в умовах надзвичайних ситуацій;
- низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації.

Таким чином, екологічні аспекти ІБ сьогодні є одними з найважливіших в глобальному масштабі, які пов'язані із захистом інтересів особистості, суспільства і держави від можливого впливу на природне середовище, стихійних лих і катастроф.

Природничо-науковий аспект. Тут проблеми ІБ можна проілюструвати на прикладі того, як інформаційне середовище використовує новітні досягнення прикладних і фундаментальних наук. Так, для реалізації засобів технічної розвідки можуть використовуватися вже відомі науці фізичні поля, в тому числі, електромагнітне, гравітаційне, сейсмічне та ін.

Наприклад, *сейсмічна розвідка* видобуває інформацію шляхом виявлення й аналізу деформацій і зсувів у земній поверхні, що виникають під впливом різних вибухів. Її основний напрямок – розвідка підземних ядерних вибухів і визначення їх параметрів.

Магнітометрична розвідка видобуває інформацію шляхом виявлення й аналізу локальних змін магнітного поля Землі під впливом

об'єкта розвідки з великою магнітною масою. За допомогою магнітометрів різних типів, вимірюють вектор магнітної індукції або його складові, можна визначати «магнітні портрети» об'єктів розвідки з метою їх подальшої класифікації та детального аналізу тощо.

Технічний аспект. Технічний аспект ІБ можна розглядати з кількох позицій. По-перше, це захист інформації, що циркулює в різних автоматизованих інформаційних системах, що мають певне апаратно-програмне забезпечення. Розвиток технічної складової інформаційної інфраструктури неминуче тягне за собою підвищення залежності суспільства, від якості функціонування інформаційних систем різного рівня, тобто створюються критичні елементи інфраструктури, від яких залежить стан ІБ. По-друге, це захист інформації, заснований на застосуванні різних спеціальних інженерно-технічних засобів захисту.

Перелік наведених вище аспектів не є вичерпним, а лише ілюструє складність і багатогранність інформаційної безпеки як інтегральної проблеми.

§1.5. Концептуальна модель інформаційної безпеки

Одним із чинників, що значно ускладнює забезпечення ІБ є постійне протистояння фахівців в області інформаційної безпеки з одного боку, і зловмисників – з іншого.

Зважаючи на необхідність вирішення проблем, що виникають в ході згаданого протистояння, доцільно системно дослідити об'єкти та процеси, ІБ яких необхідно забезпечити, сформувавши умовну ***концептуальну модель інформаційної безпеки***.

Розглядаючи ІБ як стан захищеності інформаційного середовища, в моделі на основі системного підходу доцільно визначити загрози безпеки інформації, джерела цих загроз, способи і цілі їх реалізації.

При цьому слід розглядати і засоби захисту інформації від неправомірних дій, що призводять до нанесення збитку, в контексті їх протиставлення можливим загрозам.

Концептуальна модель інформаційної безпеки складається з наступних елементів: об'єкти захисту; моделі загроз і порушників; джерела інформації; система захисту інформації тощо *(рис. 1.4)*.

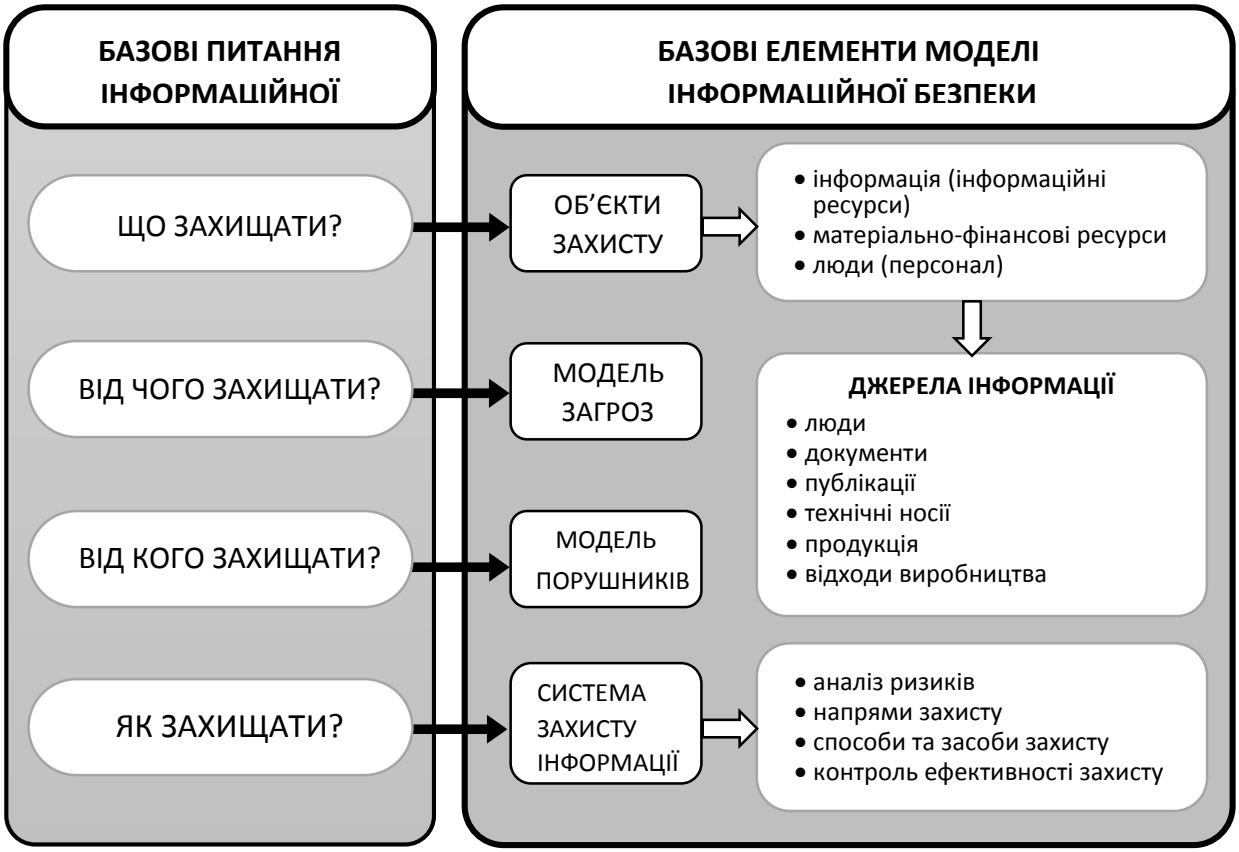

Рис. 1.4. Концептуальна модель інформаційної безпеки

Основним ***об'єктом захисту*** є інформаційна система, яка реалізує автоматизований збір і обробку даних, та включає в себе: інформацію (інформаційні ресурси), матеріально-фінансові ресурси і людей (персонал), які мають санкціонований доступ до цих ресурсів.

Слід звернути увагу на нерозривність інформації та певного матеріального носія. Вираз «отримати доступ до інформації» можна розуміти як отримання доступу саме до певного носія. Відтак, в процесі захисту інформації (даних) необхідно враховувати її місцезнаходження, як наслідок – і стан, в якому вона знаходиться (знаки або сигнали) *(рис. 1.5)*.[34]

[34] Дробожур Р. Р. Слідова картина як елемент криміналістичної характеристики злочинів у сфері електронної обчислювальної техніки. «Віртуальні сліди» // Сучасні проблеми криміналістики: матеріали міжнародної науково-практичної конференції, присвяченої 100-річчю з дня народження доктора юридичних наук, професора В. П. Колмакова (27-28 вересня 2013 року, м. Одеса) / упоряд.: В. В. Тіщенко, О. П. Ващук. – Одеса: Юридична література, 2013. – С. 116.

Рис. 1.5. Місцезнаходження «комп'ютерної інформації

Носій інформації – фізична особа або матеріальний об'єкт, в тому числі фізичне поле, в якому інформація знаходить своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів, кількісних характеристик фізичних величин[35].

Всі носії інформації умовно можна розділити на дві групи.

Перша група – це безпосередні (первинні) носії інформації. Вони є такими за своєю природою, наприклад: людина (фізична особа), військові об'єкти, або спеціально створені для цілей зберігання інформації або передачі інформації за допомогою носія. Такі носії водночас можна вважати *джерелами* інформації.

Друга група – опосередковані (вторинні) носії інформації. Такими носіями, є засоби та системи, що використовуються для

[35] Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов; Алт. гос. техн. ун-т им. И. И. Ползунова. – Барнаул: АлтГТУ, 2011. – С. 97.

обробки інформації (оперативна пам'ять ПК, принтери, сканери тощо), подання (монітори, екрани та ін.), передачі по мережі (комп'ютерні та телекомунікаційні лінії зв'язку) тощо. Опосередкованими носіями також є випромінювання та електромагнітні поля що виникають під час роботи технічних засобів обробки інформації або передачі. В опосередкованих носіях інформація не зберігається (*рис. 1.6*).

Рис. 1.6. Класифікація носіїв інформації, що захищаються

Загроза безпеки інформації є одним з найважливіших елементів концептуальної моделі ІБ. Загроза безпеки – це сукупність умов, чинників, що створюють небезпеку життєве важливим інтересам особистості, суспільства і держави.

Інформаційні загрози (або загрози інформації) – це події або явища, внаслідок дії яких може відбутися негативний вплив на інформацію: її витік, знищення (руйнування), спотворення

(модифікація), блокування доступу до неї санкціонованих користувачів тощо.

Джерелами загроз можуть бути іноземні держави, окремі юридичні або фізичні особи, криміналітет, природні (стихійні лиха та катастрофи) або технічні (стрибки електроживлення, відмова апаратури та ін.) дестабілізуючі чинники.

При відповіді на запитання «*від чого захищати?»* створюється ***модель загроз*** – формалізований або неформалізований опис (перелік) всіх потенційних загроз інформації та їх можливих джерел; уразливих елементів об'єкта захисту, на які вони спрямовані; шляхів (способів) і ймовірності здійснення загроз; рівнів потенційних збитків (матеріальних та моральних) у разі здійснення загроз та ін.

За ***природою походження*** загрози можуть бути природними і штучними.

Природні (об'єктивні) – це загрози, викликані діями або наслідками стихійних природних явищ, незалежних від людини (форс-мажорні обставини).

Штучні (суб'єктивні) – це загрози, викликані діяльністю людини.

За ***мотивацією дій*** поділяються на *навмисні (зловмисні)* та *ненавмисні (випадкові)* загрози.

За ***способами реалізації*** загрози можуть здійснюватися:

- *технічними каналами*, включаючи канали побічних електромагнітних випромінювань, акустичні, оптичні, радіо і радіотехнічні, хімічні та ін.;
- *каналами спеціального впливу* за рахунок формування спеціальних полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- *несанкціонованим доступом* в результаті підключення до апаратури по лініях зв'язку, маскування під зареєстрованих (законних) користувачів, подолання системи захисту для отримання (використання) інформації або нав'язування хибної, вживання заставних пристроїв і вбудованих програм та використання комп'ютерних вірусів.

Носіями загроз безпеки інформації є *джерела загроз*, які можуть знаходитися як всередині організації (внутрішні загрози), так і ззовні – зовнішні загрози. Всі джерела загроз умовно можна розділити на три групи, які обумовлені:

- *діями суб'єктів* (антропогенні джерела загроз – кримінальні структури, хакери, недобросовісні партнери, представники силових структур, програмісти, розробники, охорона та ін.);
- *технічними засобами* (техногенні джерела загроз – засоби зв'язку, мережі інженерних комунікацій, транспорт, сигналізації, телефони, програмні та технічні засоби обробки інформації);
- *стихійними джерелами* (пожежами, землетруси, повені, урагани, різні непередбачувані обставини та ін.).

В результаті відповіді на питання «*від кого захищати*?» створюється ***модель порушників*** – формалізований або неформалізований опис всіх потенційних зловмисників, які можуть створювати певні загрози для інформації, що захищається. При розробці цього елемента, як правило, враховуються відомості про категорії (статусу) порушників, можливого рівня їх кваліфікації та технічного оснащення, цілей, мотивів і характеру їх впливу на захищається інформацію та ін.

Як і джерела загроз, порушники можуть бути як внутрішніми (так звані «інсайдери»), так і зовнішніми (діяти поза об'єктом захисту). Сучасна статистика загроз ІБ[36] свідчить, що саме інсайдери найбільш часто (близько 80% всіх загроз) реалізують спробу несанкціонованого доступу до інформації.

У науковій літературі виділяють чотири типи порушників за рівнем можливостей, що надаються штатними засобами інформаційних систем.

Перший рівень визначає низькі можливості ведення діалогу в інформаційній системі – запуск задач (програм) з фіксованого набору, що реалізують заздалегідь передбачені функції з обробки інформації.

[36] Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб.: Питер, 2008. – 320 с.

Другий рівень визначається можливістю створення і запуску власних програм з новими функціями з обробки інформації.

Третій рівень визначається можливістю управління функціонуванням інформаційних систем.

Четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт елементів і системи в цілому, аж до включення до її складу власних технічних засобів з новими функціями.

Переоцінка можливостей порушників призведе до невиправданого збільшення витрат на побудову системи захисту інформації. І навпаки, недооцінка можливостей порушників збільшить ймовірність загроз і збитку від їх реалізації.

Аналіз вищевказаних моделей дозволяє відповісти на питання «*як захищати*?», тобто побудувати ефективну ***систему захисту інформації*** (СЗІ), яка повинна адекватно відповідати можливим ризикам для всіх або для найбільш небезпечних загроз.

У загальному випадку ***СЗІ*** можна визначити як *організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз*.

Аналіз ризиків – це взаємопов'язаний процес визначення загроз безпеці інформації, уразливих елементів об'єкта захисту, оцінки потенційних збитків від реалізації конкретних загроз і визначення комплексу контрзаходів, що забезпечують достатній рівень захищеності інформації.

Мета мінімізації ризику при побудові СЗІ полягає в тому, щоб застосувати ефективні заходи (засоби) захисту так, щоб залишковий ризик безпеки інформації став прийнятним. При оцінці ризиків враховуються багато факторів: цінність ресурсів, значимість загроз, уразливість об'єкта захисту, ефективність існуючих і передбачуваних засобів захисту, їх вартість тощо.

Як правило, СЗІ комплексно поєднує всі відомі *напрямки захисту*: правовий, організаційний, інженерно-технічний і використовує відповідні способи та засоби захисту, засновані на різних фізичних принципах і механізмах безпеки.

Заключним етапом у побудові СЗІ є організація контролю ефективності захисту. З точки зору безпосередньої організації контролю на об'єкті захисту необхідно поєднати два його варіанти:

- контроль стану параметрів засобів захисту, основних і допоміжних технічних засобів передачі інформації, які безпосередньо впливають на якість стану захищеності інформації;
- контроль всіх проявів типових порушень політики і правил безпеки інформації на об'єкті захисту.

На підставі зазначених елементів концептуальної моделі інформаційної безпеки *(рис. 1.4)* будується захист конкретного об'єкта від можливих зовнішніх і внутрішніх загроз.

§1.6. Поняття і сутність правового захисту інформації

Основним напрямком в СЗІ є правовий захист інформації, актуальність якого зростає в умовах побудови інформаційного суспільства.

Правова форма захисту інформації – це захист інформації, який «*базується на використанні статей Конституції і законів держави, положень цивільного і кримінального кодексів та інших нормативно-правових документів в галузі інформатики, інформаційних відносин та захисту інформації. Вона регламентує права і обов'язки суб'єктів інформаційних відносин, правовий статус органів, технічних засобів і способів захисту інформації і є базою для створення морально-етичних норм в області захисту інформації*»[37].

Правовий захист інформації визнаний як на міжнародному (міжнародні договори, угоди, конвенції, декларації тощо), так і на державному рівні. На державному рівні правовий захист регулюється державними та відомчими нормативно-правовими актами *(рис. 1.7)*.

Система законодавчих актів та розроблених на їх базі нормативних та організаційно-розпорядчих документів повинна забезпечувати організацію ефективного нагляду за їх виконанням з боку правоохоронних органів та реалізацію засобів судового захисту

[37] Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев.– К.: ООО «ТИД «ДС», 2001. – С. 650.

та відповідальності суб'єктів інформаційних відносин. До цієї системи можна віднести і морально-етичні норми поведінки, які склалися традиційно або складаються в міру поширення обчислювальних засобів в суспільстві.

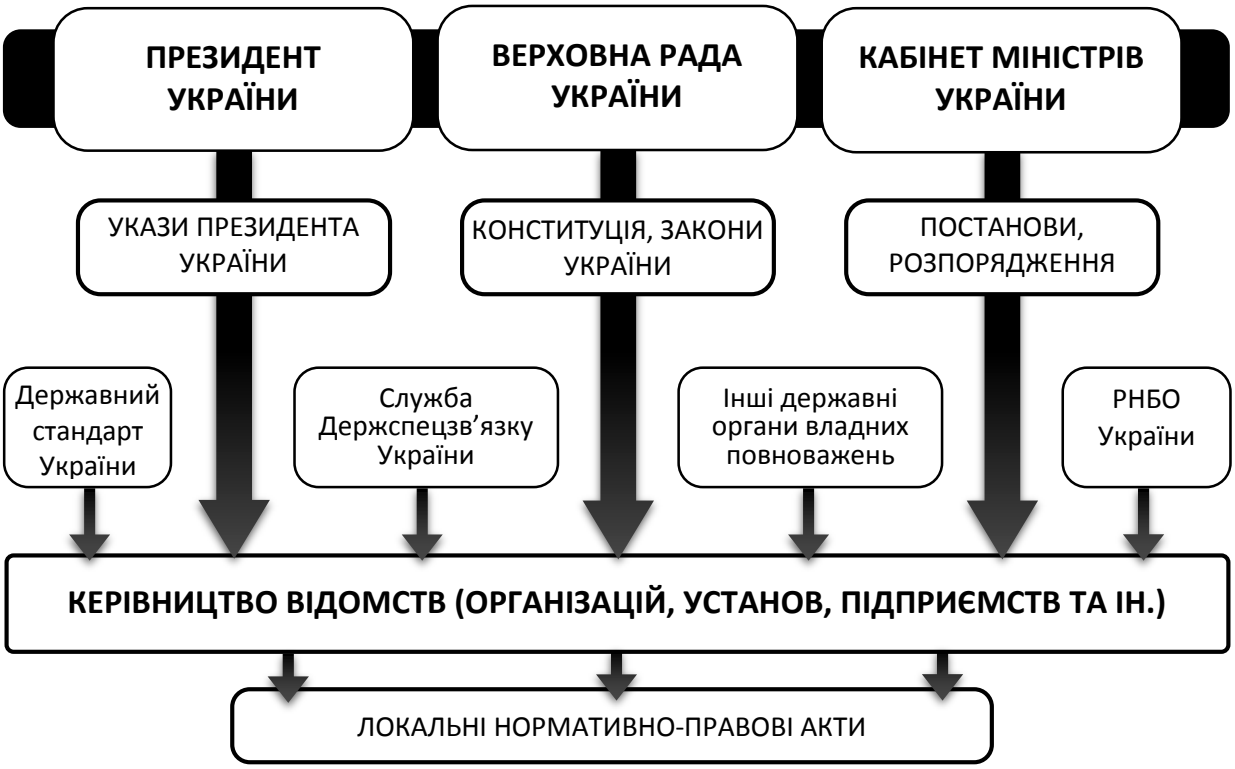

Рис. 1.7. Джерела нормативних вимог у сфері захисту інформації

Отже, на державному рівні правовий захист інформації передбачає, перш за все, організацію ефективної нормотворчої, правоохоронної та правозастосовної діяльності. Тому дуже часто правовий напрямок захисту інформації на рівні держави об'єднують з організаційним напрямком[38].

При розгляді організаційно-правового захисту, як самостійного напрямку захисту інформації, слід сказати, що він охоплює досить велику кількість відносно окремих напрямків *(рис. 1.8)*, кожен з яких вимагає відповідного законодавчого врегулювання.

У широкому сенсі правовим фундаментом для правового захисту інформації виступає національне інформаційне право, предметом

[38] Організаційно-правові основи захисту інформації з обмеженим доступом: Навчальний посібник / А. Б. Стоцький, О. І. Тимошенко, А. М. Гуз та ін., за заг. ред. В. С. Сідака. – К.: Вид–во Європейського університету, 2006. – 232 с.; Аксенов С. Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти / С. Г. Аксенов // Безопасность бизнеса. – 2008. – № 3.

якого саме і є «*суспільні відносини, що виникають з приводу встановлення режимів та форм обігу інформації, реалізації інформаційних прав і правового статусу суб'єктів інформаційних процесів і формування їх правомірної поведінки і зв'язків*»[39].

Рис. 1.8. Основні напрямки організаційно-правового захисту інформації в Україні

В рамках інформаційного права в основному діють три правових способи регулювання, які створюють три можливих види правового обігу інформації *(рис. 1.9)* [40]*:*

- ***відкритий*** – врегульований диспозитивним методом (виключно цивільно-правовими нормами);
- ***закритий*** – регулюється імперативним методом (адміністративно-правові норми);
- ***обмежений*** – до якого застосовуються обидва види правового регулювання.

До цих методів також долучається вільний обіг інформації, який безпосередньо правом не врегульований, але щодо якого можуть

[39] Кормич Б. А. Інформаційне право. Підручник / Б. А. Кормич. – Харків: БУРУН і К, 2011. – С. 37.
[40] Там само. – С. 166–169.

виникати охоронні правовідносини в разі порушення визначених заборон або обмежень.

Рис. 1.9. Види цивільного обігу інформації та їх правові ознаки

У вузькому сенсі мова йде про необхідність створення підсистеми організаційно-правового захисту інформації, яка ґрунтується на базі різних документів *(рис. 1.10)*.

До першої групи (*нормативно-правової*) відносяться документи, що становлять законодавчу базу щодо захисту інформації. Це закони та підзаконні акти, що визначають юридичну відповідальність

учасників процесу захисту та законодавчо регулюють основні питання інформаційної безпеки.

Рис. 1.10. Документальне забезпечення підсистеми організаційно-правового захисту інформації

До другої групи (*довідково-інформаційної*) належать документи, які містять повну інформацію про всі аспекти проблеми захисту і визнані фахівцями в цій галузі (словники, довідники); державні стандарти щодо захисту інформації; технічні описи засобів захисту інформації та ін.

Керуючі методичні матеріали (третя група документів) – це сукупність таких документів, які містять повний і систематизований опис порядку і принципу проведення робіт із захисту інформації, методики вимірювання зон витоку інформації технічними каналами, проектування системи захисту інформації тощо.

До четвертої групи належать *систематизовані набори інструкцій* для різних підрозділів і посадових осіб відповідно до їх повноважень.

До реєстраційних документів (п'ята група) належать облікові документи, що дозволяють контролювати наявність закритої інформації на об'єкті захисту і обмежувати доступ до неї, а також експлуатаційно-технічна документація, що дозволяє реєструвати всі факти і події, що загрожують безпеці інформації.

Отже, сукупність перерахованих вище документів становить правову базу, що забезпечує нормативне регулювання процесів щодо захисту інформації.

Висновки

У визначенні поняття «інформація» в різні роки переважали три основні підходи: недетермінований, техноцентричний і антропоцентричний, кожен з яких має свої переваги і недоліки.

В нормативно-правовому визначенні «інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

Існує безліч властивостей інформації. Суттєвими у вирішенні проблем захисту інформації є властивості, що визначають стан її безпеки: конфіденційність, цілісність і доступність.

В процесі розвитку інформаційного суспільства, будь-який захист інформації, а в першу чергу, правовий, є основоположним аспектом громадської безпеки будь-якої держави.

ІБ – це стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

В основі побудови концептуальної моделі ІБ лежать послідовні відповіді на базові питання: «Що захищати? → Від чого (від кого) захищати? → Як захищати?».

Одним з найважливіших об'єктів захисту в інформаційному суспільстві є інформація (інформаційні ресурси).

2 ВИДИ ІНФОРМАЦІЇ ЗА ПОРЯДКОМ ДОСТУПУ. ПУБЛІЧНА ІНФОРМАЦІЯ

§2.1. Види інформації

Важливим поняттям при роботі з інформацією є її класифікація за видами, яка дозволяє згрупувати об'єкти, що характеризуються загальними властивостями. Класифікація інформації використовується для організації різних систем захисту інформації. Неправильна класифікація може привести до того, що деякі типи даних залишаться поза полем захисту. Або ж, навпаки, витрати будуть неправомірними через необґрунтований захист інформації.

Класифікацію інформації слід проводити у відповідності зі ступенем тяжкості наслідків втрати її властивостей ІБ, зокрема, властивостей доступності, цілісності і конфіденційності[41].

Залежно ***від режиму відображення*** виділяють такі види інформації:

- *числова* – представлена цифрами та відображає результати обчислень;
- *текстова* – представлена у вигляді слів, що складаються із символів;
- *графічна* – представлена графічними об'єктами з урахуванням їх геометричних та оптичних властивостей;
- *акустична* – представлена звуками;
- *відеоінформація* – відео і кінофільми в спеціальних форматах.

Залежно ***від сфери існування*** інформації виділяють наступні види інформації:

- *біологічну* – всередині живих організмів і між ними;
- *машинну* – всередині та між машин;
- *соціальну* – у людському суспільстві.

[41] Лукацький А. Класифікація інформації. Анонс нового дослідження. – [Електронний ресурс]. – Режим доступу: http://bis-expert.ru/sites/default/files/archives/2011/CISCO_for_DLP_Russia_2011.pdf.

За призначенням виділяють два види інформації – *масову* і *спеціальну*.

В рамках вивчення курсу «Правовий захист інформації» будуть розглядатися тільки ті види інформації, які є істотними для правового регулювання інформаційних відносин. Зокрема, види інформації ***за змістом,*** визначені ст. ст. 10-19 в ЗУ «Про інформацію»[42] *(рис. 2.1)*.

Рис. 2.1. Види інформації за змістом

Зміст наведених у законі видів інформації є цілком зрозумілим. Однак, більш детально розглянемо правову інформацію, оскільки вона спрямована на оптимізацію потоків інформації в державних структурах і на підвищення ефективності її використання.

Правова інформація – це відомості (повідомлення, дані) про факти, події, предмети, осіб, явища, що відбуваються у правовій сфері, які містяться в правових джерелах і використовуються для вирішення задач правотворчості, у правозастосовній та правоохоронній діяльності, захисту прав і свобод особистості.

Правова інформація має офіційний і документальний характер. Для неї характерна системність, тобто вся сукупність нормативних правових актів групується навколо Конституції України.

Правова інформація повинна відповідати певним вимогам: бути достовірною і повною, тобто об'єктивно висвітлювати реальність і відображати всі пов’язані з даним випадком факти, явища, процеси.

[42] Про інформацію: Закон України від 13.01.2011 р. // Офіційний вісник України. – 2011. – № 10. – Ст. 445.

Джерела правової інформації бувають нормативні та ненормативні.

До *нормативних* джерел відносять Конституцію України, нормативно-правові акти державних органів, міжнародні договори та угоди, акти вищих судових та арбітражних органів.

Ненормативними джерелами правової інформації є накази керівників організацій, вироки судів, акти нотаріальних органів, повідомлення засобів масової інформації, публічні виступи та інші джерела інформації з правових питань. Ненормативні джерела правової інформації не містять правових норм і тому носять рекомендаційний та інформаційний характер.

Залежно від ***стадії виникнення*** розрізняють *первинну* інформацію, яка виникає безпосередньо в процесі юридичної діяльності, і *вторинну*, яка виникає в результаті обробки первинної та (або) іншої вторинної інформації, до якої відноситься проміжна і результуюча інформація. Отримання результуючої інформації є метою функціонування інформаційних систем.

За стабільністю інформація поділяється на:

- *постійну*, яка не змінює своїх значень;
- *умовно постійну*, для якої це твердження може бути справедливим протягом тривалого періоду;
- *змінну*, значення якої часто змінюються.

За ступенем організованості (впорядкованості) інформацію можна розділити на недокументовану і документовану[43].

Недокументована інформація – це мовна інформація, інформація, виражена у вигляді знаків, символів тощо, яка не має реквізитів. Носієм такої інформації є людина. З точки зору правового регулювання, захист недокументованої інформації не може бути вирішений правовими засобами.

Документована інформація – зафіксована на матеріальному носії шляхом документування інформація з реквізитами, що

[43] Ковалева Н. Н. Информационное право России: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К», 2007. – С. 16–17.

дозволяють визначити таку інформацію або у встановлених законодавством випадках – її матеріальний носій[44].

ЗУ «Про інформацію» вказує, що «***документ***» є «*матеріальним носієм, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі*».[45]

ЗУ «Про бібліотеки і бібліотечну справу»[46] визначає «*документ*» як: «*матеріальну форму одержання, зберігання, використання і поширення інформації, зафіксованої на папері, магнітній, кіно-, фотоплівці, оптичному диску або іншому носієві*».

У державному стандарті ДСТУ 3843-99: «*документ – оформлений згідно з встановленим порядком матеріальний об'єкт, що містить у зафіксованому вигляді інформацію та має відповідно до чинного законодавства юридичну силу*»[47].

Отже, поняття «*документ*» відображає ознаки існуючих предметів, які є об'єктами практичної діяльності щодо створення, збирання, обробки, зберігання, пошуку, розповсюдження та використання документованої інформації в суспільстві.

Стрімкий розвиток і поширення засобів обчислювальної техніки призвели до появи електронних носіїв інформації у вигляді файлів в пам'яті комп'ютера (на жорсткому диску, на флеш-накопичувачах, CD, DVD та ін.). У зв'язку з цим на законодавчому рівні в Україні було введено поняття «*електронний документ*».

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, що включають обов'язкові реквізити документа[48]. Одним з обов'язкових реквізитів електронного документа, що використовується для ідентифікації автора, є електронний цифровий підпис (ЕЦП). Перевірка цілісності

---

[44] Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов; Алт. гос. техн. ун-т им. И. И. Ползунова. – Барнаул: АлтГТУ, 2011. – С. 93.

[45] Про інформацію: Закон України від 13.01.2011 р. // Офіційний вісник України. – 2011. – № 10. – Ст. 445.

[46] Про бібліотеки і бібліотечну справу: Закон України від 21.05.2009 р. // Офіційний вісник України. – 2009. – № 45. – С. 10. – Ст. 1497.

[47] Державна уніфікована система документації. Основні положення: ДСТУ 3843-99. – [Чинний від 2000-07-01]. – К.: Держстандарт України, 2000. – 8 с. – (Національний стандарт України).

[48] Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. // Офіційний вісник України. – 2003. – № 25. – С. 106. – Ст. 1174.

електронного документа проводиться шляхом перевірки ЕЦП. Згідно зі ст. 1 ЗУ «Про електронний цифровий підпис»[49], «*електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації власника цих даних»*. А ЕЦП – «*вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача*».

Однією з важливих форм документованої інформації є ***електронне повідомлення*** – інформація, передана або отримана користувачем інформаційно-телекомунікаційної мережі.

При обробці інформації за допомогою засобів ЕОТ виникають специфічні питання збереження та обмеження доступу до носіїв інформації, які вирішуються на основі поєднання організаційних, правових та програмно-технічних методів захисту, утворюють правовий режим інформації.

§2.2. Правовий режим інформації

У науковій літературі правовий режим визначається, як порядок регулювання, виражений у комплексі правових засобів, що характеризують поєднання взаємодіючих дозволів, заборон, а також позитивних зобов'язань, які створюють особливе спрямування регулювання. Механізм правового режиму пов'язаний, насамперед, із орієнтацією на суб'єкт[50].

Правовий режим інформації [51] включає:

- право використання інформації в якості об'єкта правових відносин;
- право володіння інформацією;

[49] Про електронний цифровий підпис: Закон України від 22.05.2003 р. // Офіційний вісник України. – 2003. – № 25. – С. 111. – Ст. 1175.

[50] Алексеев С. С. Общие дозволения и общие запреты в советском праве. – М., 1989. – С. 185.

[51] Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов [и др.]; под ред. А. А. Стрельцова. – М.: Издательский центр «Академия», 2008. – С. 73–76.

- право доступу до інформації;
- право власності та інші майнові права на різні носії, що містять документовану інформацію;
- право поширення та надання інформації.

Право використання інформації в якості об'єкта правових відносин полягає в можливості встановлення публічних, цивільних та інших правових відносин, об'єктом яких є інформація.

Право володіння інформацією полягає в можливості розпорядження нею (дозвіл або обмеження доступу; використання; поширення; передача іншим особам; правовий захист та інші дії) на розсуд правовласника.

Право доступу до інформації полягає у можливості її вільного отримання та використання, якщо законодавством не встановлені обмеження доступу до інформації, або інші вимоги до порядку її надання або розповсюдження.

Згідно з п. 1 ст. 20 ЗУ «Про інформацію», *за порядком доступу* інформація поділяється на ***відкриту*** та ***інформацію з обмеженим доступом*** *(ІзОД)*.

Відкрита інформація – це інформація, доступ до якої нічим не обмежується. Доступ до такої інформації забезпечується шляхом публікації її в офіційних друкованих виданнях, поширенням її засобами масової інформації (ЗМІ) та безпосереднього надання її зацікавленим особам, громадянам, державним органам.

Порядок і умови надання громадянам, державним органам, юридичним особам за запитами встановлюються ЗУ «Про доступ до публічної інформації» або договорами (угодами), якщо надання відкритої інформації здійснюється на договірній основі.

Відкрита інформація може використовуватися будь-якими особами на їх розсуд при дотриманні встановлених законами обмежень щодо розповсюдження такої інформації. Вона є суспільно значущою інформацією для громадян і суспільства.

Згідно з п. 2 ст. 20 ЗУ «Про інформацію» будь-яка інформація є відкритою, крім тієї, що віднесена законом до ІзОД.

ІзОД докладно буде розглянута в наступному розділі.

Право власності та інші майнові права на матеріальні носії, що містять документовану інформацію, встановлюється цивільним законодавством. Це значить, що носії інформації є об'єктами цивільних прав поряд з іншими речами.

Інформація, є предметом власності і підлягає захисту відповідно до вимог правових документів або вимогами, встановлюваними власником інформації. Власником інформації може бути: фізична або юридична особа, а також держава.

Право поширення і надання інформації полягає у можливості вільного здійснення дій, спрямованих на отримання інформації невизначеним колом осіб або на передачу інформації невизначеному колу осіб (поширення), і дій, спрямованих на отримання або передачу інформації визначеному колу осіб, при дотриманні вимог, встановлених законодавством України .

Отже, правовий режим інформації створює умови для забезпечення інформаційної безпеки.

§2.3. Публічна інформація

Поняття ***«публічна інформація»*** є ключовим у ЗУ «Про доступ до публічної інформації», який і визначає механізм доступу до даного виду інформації.

У 1995 р. Україна приєдналась до Ради Європи. При вступі Україна зобов'язалась дотримуватись зобов'язань, що випливають із Статуту Ради Європи, а саме, принципів плюралістичної демократії, верховенства права та захисту прав людини і основних свобод усіх осіб, які перебувають під юрисдикцією країни. Зокрема, Резолюцією Парламентської Асамблеї Ради Європи від 5 жовтня 2005 р. № 1466 «Про виконання обов'язків та зобов'язань Україною»[52] були підведені підсумки реалізації ключових реформ, які Україна зобов'язалася реалізувати. Зокрема, органи державної влади України повинні поліпшити правове регулювання доступу до інформації, а також

[52] Об исполнении обязанностей и обязательств Украиной: Резолюция 1466 (2005) Парламентской Ассамблеи Совета Европы от 05.10.2005 г. – [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/ l_doc2.nsf/link1/MU05122.html.

суворо дотримуватися ст. 34 Конституції України[53] стосовно свободи інформації під час засекречування документів, і розсекретити всі офіційні документи, які були закриті для загального доступу з порушенням законодавства.[54]

Для виконання зазначеної резолюції Парламентської Асамблеї Ради Європи та з метою забезпечення реалізації положень ст. 34 Конституції України, ст. 10 Конвенції про захист прав людини і основних свобод 1950 р.[55], ст. 19 Міжнародного пакту про громадянські і політичні права[56], а також для забезпечення ефективної реалізації права кожного на свободу вираження поглядів та доступ до інформації, права на вільне збирання, зберігання, використання та поширення інформації усно, письмово або іншим способом, Верховною Радою України в 2011 р. були прийняті Закони України «Про доступ до публічної інформації»[57] (далі Закон) та «Про інформацію».

В ЗУ «Про інформацію» визначено основні принципи, суб'єкти та об'єкти інформаційних відносин в нашій країні, дано визначення інформації та розглянуто види інформації. Закон України «Про доступ до публічної інформації» визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим законом, та інформації, яка становить суспільний інтерес.

Правове визначення поняття «***публічна інформація***» наведено у ст. 1 ЗУ «Про доступ до публічної інформації»: «*...це відображена та задокументована будь-якими засобами та на будь-яких носіях*

---

[53] Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. –1996. – № 30. – Ст. 141.

[54] Разъяснения Министерства юстиции Украины «Закон Украины «О доступе к публичной информации»: информационный прорыв в Украине». – [Електронний ресурс]. – Режим доступу: http://www.medlawcenter.com.ua/ru/105/495.html

[55] Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.). – [Електронний ресурс]. – Режим доступу: http://base.garant.ru/2540800/.

[56] О гражданских и политических правах: Международный пакт от 16.12.1966 г. – [Електронний ресурс]. – Режим доступу: http://zakonbase.ru/content/base/5683.

[57] Про доступ до публічної інформації: Закон України від 13.01.2011 р. // Офіційний вісник України. – 2011. – № 10. – С. 29. – Ст. 446.

інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом».

Слід врахувати, що інформація вважається публічною у зв'язку з тим, що вона створюється, збирається, обробляється і зберігається за рахунок бюджетних коштів, призначених для забезпечення діяльності відповідного органу влади.

В ст. 4 Закону встановлено принципи забезпечення доступу громадян до публічної інформації:

1) прозорості та відкритості діяльності суб'єктів владних повноважень;
2) вільного отримання та поширення інформації, крім обмежень, встановлених законом;
3) рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак.

Закон визначає два способи доступу до публічної інформації – ***активний*** і ***пасивний.***

Активний доступ передбачає безпосереднє звернення особи та групи осіб до розпорядника інформації за необхідною йому (їм) інформацією шляхом відправки відповідного запиту. В цьому випадку розпорядник надає інформацію лише в рамках запиту, а запитувач може понести додаткові витрати на компенсацію витрат на роздруківку або копіювання.

Пасивний доступ забезпечує відповідний розпорядник публічної інформації шляхом її оприлюднення.

Активний доступ є більш інформативним – особа може отримати відкриту публічну інформацію, щодо якої не встановлено обов'язковість оприлюднення. Наприклад: службова переписка, яка стала відкритою після закінчення реалізації певної програми, прийняття рішень та ін.

Публічна інформація може бути представлена у вигляді текстових, числових, графічних висловів чи виражена вербально. Вона може бути зафіксована на будь-якому матеріальному носії інформації, а не тільки на паперовому носії.

Публічна інформація завжди є відкритою, крім випадків, встановлених законом. Доступ до неї забезпечується шляхом систематичного і оперативного оприлюднення її в офіційних друкованих виданнях, на офіційних веб-сайтах в мережі Інтернет, на інформаційних стендах та будь-яким іншим способом, а також шляхом надання інформації за запитами.

Суб'єктами відносин у сфері доступу до публічної інформації є:

1) запитувачі інформації – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;
2) розпорядники інформації – суб'єкти, визначені в ст. 13 цього Закону;
3) структурний підрозділ або відповідальна особа з питань запитів на інформацію розпорядників інформації.

Запитувачами інформації є:

- фізична особа – будь-яка людина незалежно від віку, громадянства та інших ознак;
- юридична особа – будь-яка організація, створена і зареєстрована у встановленому законом порядку;
- об'єднання громадян без статусу юридичної особи – спільноти, передбачені ЗУ «Про об'єднання громадян», які були легалізовані шляхом повідомлення про утворення без державної реєстрації, та про будь-які інші об'єднання людей, які виступають під спільною назвою. Крім того, фізичні особи можуть подавати колективні запити на інформацію, вказуючи свої персональні дані окремо.

Перелік розпорядників публічної інформації наведено на *рис. 2.2*.[58]

[58] Методичні рекомендації щодо практичного впровадження Закону України «Про доступ до публічної інформації» / М. В. Лациба, О. С. Хмара, В. В. Андрусів [та ін.]; Укр. незалеж. центр політ. дослідж. – К. : Агентство «Україна», 2011. – С. 10.

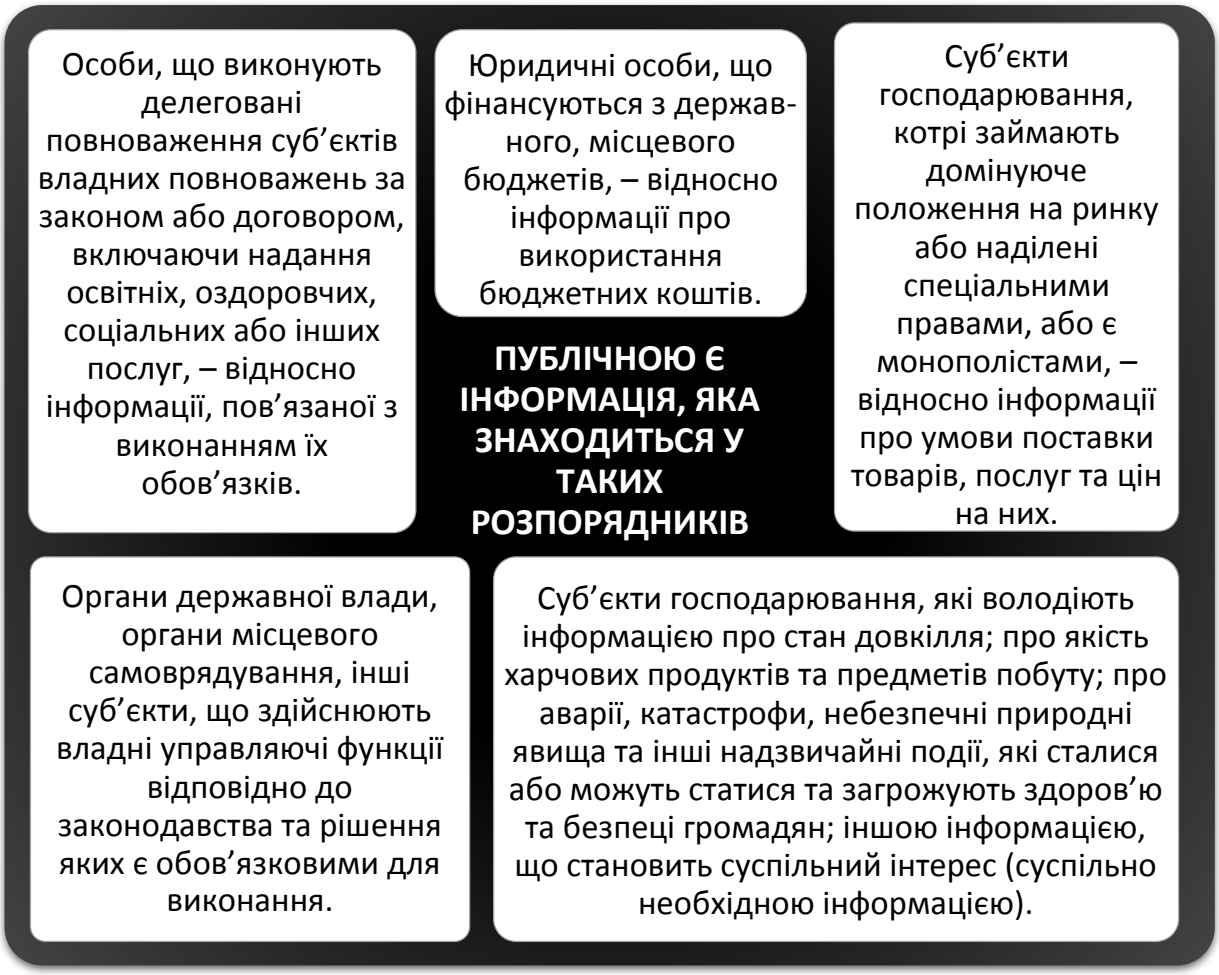

Рис. 2.2. Розпорядники публічної інформації

До розпорядників інформації, що зобов'язані оприлюднювати та надавати за запитами інформацію, у порядку, передбаченому цим Законом, прирівнюються суб'єкти господарювання, які володіють:

- інформацією про стан довкілля;
- інформацією про якість харчових продуктів і предметів побуту;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян;
- іншою інформацією, що становить суспільний інтерес (суспільно необхідною інформацією).

Розпорядники інформації зобов'язані (ст. 14):

1) оприлюднювати інформацію про свою діяльність та прийняті рішення;
2) систематично вести облік документів, що знаходяться в їх володінні;

3) вести облік запитів на інформацію;
4) визначати спеціальні місця для роботи запитувачів з документами чи їх копіями, а також надавати право запитувачам робити виписки з них, фотографувати, копіювати, сканувати їх, записувати на будь-які носії інформації тощо;
5) мати спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації;
6) надавати достовірну, точну та повну інформацію, а також у разі потреби перевіряти правильність та об'єктивність наданої інформації.

Розпорядник інформації відповідає за визначення завдань та забезпечення діяльності структурного підрозділу або відповідальної особи з питань запитів на інформацію розпорядників інформації, відповідальних за обробку, систематизацію, аналіз та контроль щодо задоволення запиту на інформацію та надання консультацій під час оформлення запиту.

В Законі введена трьохскладена формула, що застосовується для обмеження доступу до інформації – обмеження доступу до інформації можливо лише на підставі закону при сукупності трьох вимог: мати легітимну мету; розголошення інформації може завдати шкоди законним інтересам; шкода від оприлюднення інформації переважає суспільний інтерес в її отриманні[59].

Передбачено захист джерел інформації (викривачів) – ст. 11 «Захист особи, яка оприлюднює інформацію».

Крім того, Законом передбачається неможливість обмеження доступу до такої інформації:

- про розпорядження бюджетними коштами;
- про володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна;

[59] Доступ к публичной информации на Украине тянет на троечку. – [Електронний ресурс]. – Режим доступу: http://svobodainfo.org/ru/node/2742.

- про прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно, якщо оприлюднення або надання такої інформації не може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину.

Основним способом доступу до інформації ЗУ «Про інформацію» визначає ***інформаційний запит*** (ст. 32). Предметом інформаційного запиту є офіційні документи, письмова або усна інформація про діяльність органів законодавчої, виконавчої та судової влади України, їх посадових осіб з певних питань.

Запит на отримання інформації має чітко визначений предмет: надання публічної інформації, якою володіє або повинен володіти її розпорядник[60].

Слід розмежовувати поняття «*інформаційного запиту»* та *«звернення громадян»,* які на перший погляд є схожими, проте мають різну правову природу.

Так, ***зверненнями громадян*** є виражені в письмовій чи усній формі пропозиції (зауваження), заяви (клопотання) і скарги (ст. 3 ЗУ «Про звернення громадян»[61]) *(рис. 2.3)*.

Запит на інформацію − це вимоги особи до розпорядника інформації надати публічну інформацію, яка знаходиться в його володінні.

Крім того, розмежування звернень і запитів органів влади передбачають застосування окремих процедур реєстрації та обліку, а також різні строки надання відповіді.

В Законі особливої уваги заслуговують положення, що визначають порядок реалізації права на доступ до інформації за інформаційним запитом − прохання особи до розпорядника інформації надати публічну інформацію, що знаходиться у його володінні.

---

[60] Доступ до публічної інформації: Навчально-метод. матеріали для тематичного короткотермінового семінару / В. І. Малімон, С. В. Онищук. – Івано-Франківськ: «Місто НВ», 2012. – С. 23–28.

[61] Про звернення громадян: Закон України від 02.10.1996 р. // Відомості Верховної Ради. – 1996. – № 47. – Ст. 256.

Рис. 2.3. Основні форми звернення громадян

Закон передбачає, що запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту.

Спрощено порядок подання запитів, передбачена максимально проста форма, запит можна подати поштою, факсом, електронною поштою.

Запит на інформацію повинен містити:

- ім'я (назву) запитувача, поштову адресу або адресу електронної пошти, номер засобу зв'язку;
- загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит (якщо це відомо);
- підпис і дату, за умови подання запиту в письмовій формі.

З метою спрощення процедури оформлення письмових запитів на інформацію особа може подавати запит шляхом заповнення форм запитів на інформацію, затверджених розпорядженням голови, яку можна отримати у відповідальної особи за організацію доступу запитувачів публічну інформацію або на офіційному сайті.

Вся *відкрита інформація* повинна надаватися за запитами.

При подачі інформаційного запиту, запитувач зазначає зручну для нього форму отримання інформації.

Наявність в документі, що запитувався, частини ІзОД не повинно перешкоджати наданню відкритої інформації з нього (ч. 7 ст. 6 Закону).

Публічна ІзОД (що містить її документ), по якій прийшов запит, підлягає розгляду на предмет існування в даний момент формальних підстав для обмеження доступу до неї. Наприклад, закінчення строків засекречування, скасування законодавчих норм про обмеження доступу, прийняття рішення або початок публічного обговорення у випадках, визначених п. 1 ч. 1 ст. 9 Закону. У разі відсутності на момент розгляду таких формальних підстав для обмеження доступу до інформації вона підлягає наданню на запит (ч. 4 ст. 6 Закону).

Згідно зі ст. 20 Закону відповідь на інформаційний запит має бути надано *не пізніше п'яти робочих днів* з дня отримання запиту.

Якщо запит стосується надання великого обсягу інформації або вимагає пошуку інформації серед значної кількості даних, розпорядник інформації *може продовжити строк розгляду запиту до 20 робочих днів* з обґрунтуванням такого продовження. При продовженні терміну розпорядник інформації повідомляє запитуючу особу в письмовій формі не *пізніше п'яти робочих днів* з дня отримання запиту.

Інформація на запит надається *безкоштовно*.

У разі, коли запитувана інформація містить документи обсягом більше 10 сторінок, про це протягом п'яти робочих днів з дня отримання запиту повідомляється запитувачу із зазначенням фактичних витрат, пов'язаних із копіюванням або друком документів, та реквізитів і порядку відшкодування таких витрат. Надання інформації здійснюється протягом трьох робочих днів після підтвердження оплати вартості фактичних витрат.

Для суб'єктів владних повноважень встановлені обов'язки по створенню систем обліку всієї інформації, яка знаходяться у віданні розпорядника. Зазначено перелік обов'язкової для розміщення на

веб-сайтах органів влади інформації. Для роботи з інформаційними запитами створені спеціальні відділи.

За порушення Закону передбачені дисциплінарна, адміністративна та кримінальна відповідальності.

Дисциплінарна відповідальність державних службовців полягає в їх обов'язки відповісти за вчинене ними порушення трудової дисципліни. Правовою підставою притягнення до дисциплінарної відповідальності є вчинення дисциплінарного проступку.

Згідно зі ст. 14 ЗУ «Про державну службу»[62] дисциплінарні стягнення застосовуються до державного службовця за невиконання або неналежне виконання службових обов'язків, перевищення своїх повноважень, порушення обмежень, пов'язаних з проходженням державної служби, а також за вчинок, який порочить його як державного службовця або дискредитує державний орган, в якому він працює.

Адміністративна відповідальність державного службовця полягає в обов'язку відповідати за вчинення адміністративного правопорушення і понести адміністративне стягнення.

Державний службовець може бути притягнутий до адміністративної відповідальності за порушення (недотримання) Закону, якщо він вчинив діяння (дія або бездіяльність), передбаченого статтями КУпАП[63], і якщо при цьому він порушив правила, забезпечення яких входить до його службових обов'язків.

Кримінальна відповідальність державного службовця наступає за вчинення злочину, тобто діяння, передбаченого ККУ. Зокрема, кодексом передбачено відповідальність за приховування або перекручення відомостей про екологічний стан або захворюваність населення (ст. 238 ККУ[64]).

---

[62] Про державну службу: Закон України від 16.12.1993 р. // Відомості Верховної Ради України. – 1993. – № 52. – Ст. 490.

[63] Кодекс України про адміністративні правопорушення (статті 1 – 212-20): Кодекс від 07.12.1984 р.// Відомості Верховної Ради України. – 1984. – № 512. – Ст. 1122.

[64] Кримінальний кодекс України: Кодекс від 05.04.2001 р.// Відомості Верховної Ради України. – 2001. – № 25. – Ст. 131.

На виконання ЗУ «Про доступ до публічної інформації» було видано Укази Президента України – «Питання забезпечення органами виконавчої влади доступу до публічної інформації»[65] та «Про першочергові заходи щодо забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України»[66], спрямовані на забезпечення реалізації конституційного права громадян вільно збирати, зберігати, використовувати і поширювати інформацію.

У квітні 2014 р. набрав чинності ЗУ «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Законів України «Про інформацію» та «Про доступ до публічної інформації»[67], який створює прозорі умови для доступу ЗМІ до інформації, яка має гриф «для службового користування» і зобов'язує органи державної влади публікувати всі свої рішення. Передбачається також значне розширення інформації, до якої громадяни матимуть право доступу. Також вводяться різні штрафи. Так, відповідно до закону, накладення штрафу на посадову особу від 25 до 50 неоподатковуваних мінімумів доходів громадян передбачено за:

- не опублікування інформації, обов'язкове оприлюднення якої передбачено Законами України «Про доступ до публічної інформації» та «Про засади запобігання та протидії корупції»;
- необґрунтоване віднесення інформації до інформації з обмеженим доступом, ненадання відповіді на запит на інформацію, не надання інформації, неправомірну відмову в наданні інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації;
- неправомірну відмову в наданні інформації, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає

[65] Питання забезпечення органами виконавчої влади доступу до публічної інформації: Указ Президента України від 05.05.2011 р. № 547/2011 // Офіційний вісник України. – 2011. – № 35. – С. 14. – Ст. 1433.

[66] Про першочергові заходи щодо забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України: Указ Президента України від 05.05.2011 р. № 548/2011 // Офіційний вісник України. – 2011. – № 35. – С. 15. – Ст. 1434.

[67] Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації»: Закон України від 27.03.2014 р. // Відомості Верховної Ради. – 2014. – № 22. – С. 1950. – Ст. 816.

дійсності, у відповідь на адвокатський запит, запит кваліфікаційно-дисциплінарної комісії адвокатури, її палати або члена відповідно до ЗУ «Про адвокатуру та адвокатську діяльність»;

- не надання доступу до судового рішення або матеріалами справи за заявою особи, а також інше порушення ЗУ «Про доступ до судових рішень»;
- незаконну відмову в прийнятті та розгляді звернення, інше порушення ЗУ «Про звернення громадян».

Повторне протягом року вчинення будь-якого з перелічених порушень, за яке особу вже було піддано адміністративному стягненню, тягне за собою накладення штрафу на посадових осіб від 60 до 80 неоподатковуваних мінімумів доходів громадян.

Крім того, обмеження доступу до інформації або віднесення інформації до ІзОД, якщо це прямо заборонено законом тягне за собою накладення штрафу на посадових осіб від 60 до 80 неоподатковуваних мінімумів доходів громадян.

Разом з тим, незаконне надання доступу до певних видів інформації так само тягне за собою відповідальність посадової особи, неправомірно надав такий доступ, в тому числі і кримінальну, за:

- розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132 ККУ);
- порушення авторського права і суміжних прав (ст. 176 ККУ);
- незаконне розповсюдження інформації про особу без її згоди (ст. 182 ККУ);
- розголошення в будь-якому вигляді інформації, яка відповідно до Закону надається спеціально уповноваженому центральному органу виконавчої влади із спеціальним статусом з питань фінансового моніторингу, особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю, якщо такі дії заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб (ч. 2 ст. 209-1 ККУ) та інші.

Висновки

Існує безліч класифікацій інформації. Основними для правового регулювання інформаційних відносин є класифікація інформації за змістом і за режимом доступу до неї.

Види інформації за змістом, визначені ст. ст. 10-19 Закону України «Про внесення змін до Закону «Про інформацію».

По порядку доступу інформація поділяється на відкриту і ІзОД.

Відкрита інформація – ця інформація, доступ до якої нічим не обмежується. Доступ до такої інформації забезпечується шляхом публікації її в офіційних друкованих виданнях, поширенням її ЗМІ та безпосереднього надання її зацікавленим особам, громадянам, державним органам.

До публічної інформації відноситься інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених ЗУ «Про доступ до публічної інформації».

3 ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ ТА ЇЇ ВИДИ

§3.1. Правовий порядок доступу до інформації

Розвиток сучасного інформаційного суспільства визначається стрімким зростанням ролі інформації в багатьох сферах суспільних відносин. В рамках інформаційних відносин відбувається реалізація прав суб'єктів на інформацію. У ст. 34 Конституції України закріплено право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово чи будь-яким іншим способом і на свій вибір. Однак на законодавчому рівні встановлено обмеження доступу до певних видів інформації, яке зумовлене необхідністю правового забезпечення захисту окремих видів інформації.

Доступ фактично є певною дозвільною процедурою, яка полягає в отриманні згоди компетентного органу (особи) на одержання документа або інформації, отримання якої безпосередньо пов'язане з реалізацією права на інформацію, і, відповідно, обмежує це право[68].

Відповідно до ЗУ «Про інформацію», вчинення права на отримання інформації пов'язане з поняттям доступу до інформації.

Доступ до інформації – це передбачений правовими нормами порядок отримання, використання, поширення та зберігання інформації.

По суті, порядок доступу до інформації є різновидом спеціальних правових режимів, які встановлюють сукупність правил, закріплених в юридичних нормах, що регулюють певну діяльність людей. Правові режими існують в межах багатьох галузей права. Захист інформації в цілях інформаційної безпеки здійснюється на основі імперативного методу правового регулювання, тому відповідні режими доступу до інформації за своїми характеристиками найбільш близькі до

[68] Доступ до інформації та електронне урядування / Автори-упорядники М. С. Демкова, М. В. Фігель. – К.: Факт, 2004. – С. 27.

адміністративно-правових режимів.[69]

Головними *характеристиками порядку доступу до інформації* є[70]:

- суб'єкт визначення доступності цієї інформації;
- коло суб'єктів, які мають доступ до цієї інформації;
- особливі вимоги і правила збереження та поширення цієї інформації;
- термін дії порядку.

Суб'єктом визначення доступності інформації є особа, в компетенцію якої входить вирішення питань щодо встановлення обмежень на доступ до інформації та її матеріальних носіїв, а також надання права доступу до такої інформації.

Суб'єкт, який має доступ до інформації − це особа, якій надано право ознайомлення з матеріальними носіями інформації або їх використання. Надання особі права доступу до інформації, зазвичай пов'язане з взяттям нею на себе зобов'язань з нерозголошення отриманої інформації.

Порядок доступу до інформації означає певну сукупність правил, якими позначені особливі вимоги і правила зберігання та поширення інформації. Ці правила визначають діяльність осіб, на яких покладено відповідальність за зберігання матеріальних носіїв інформації, встановлюють необхідність застосування певних правових, організаційних, технічних та криптографічних засобів захисту інформації. Ці правила також визначають порядок надання доступу до такої інформації.

Більшість видів ІзОД мають визначений законодавством або власником інформації термін дії режиму обмеження доступу до інформації. Цей термін визначають, як правило, при ухваленні рішення про обмеження доступу до інформації або її матеріальних носіїв. Після закінчення цього терміну може бути ухвалено рішення

[69] Інформаційне право. Тексти лекцій (для студентів денного та заочного відділення спеціальності «Правознавство») / Укладач: Є. А. Таликін. – Луганськ: вид-во СНУ ім. В. Даля, 2013. – С. 32–34.

[70] Кормич Б. А. Інформаційне право. Підручник / Б. А. Кормич. – Харків: БУРУН і К, 2011. – С. 161.

або про його відновлення, або про надання інформації статусу відкритої.

Згідно зі п. 1 ст. 20 ЗУ «Про інформацію», в залежності від ***порядку доступу*** інформація поділяється на ***відкриту*** **та** ***інформацію з обмеженим доступом*** (ІзОД) *(рис. 3.1)*.

Рис. 3.1. Види інформації за порядком доступу

Будь-яка інформація є *відкритою,* крім тієї, яка відноситься законом до ІзОД.

Визначення ІзОД наводиться в багатьох наукових публікаціях, проте в законодавчих актах точного визначення ІзОД не існує, воно зустрічається тільки в міжнародних угодах.

Так, в ст. 1 Угоди між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону ІзОД визначено, що ІзОД – це «*інформація і матеріали незалежно від їх форми, природи та способу передачі, яким встановлені певні ступені обмеження та надані відповідні грифи обмеження доступу, і які в інтересах національної безпеки і згідно з національним законодавством Сторін підлягають охороні від несанкціонованого доступу*»[71] .

В ст. 2 Угоди між Кабінетом Міністрів України та Урядом Королівства Норвегії про захист ІзОД визначено, що ІзОД – це «*інформація в будь-якій формі, зокрема, в усній, і будь-який документ, матеріал, виріб, речовина або фізичне поле, на / в яких*

[71] Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом: Угода ратифіковано Законом України від 04.06.2004 р. № 1761-IV // Офіційний вісник України. – 2004. – № 33. – С. 192. – Ст. 2239.

інформація міститься або може бути записана, і до якої обмежений доступ згідно з національним законодавством Сторін»[72].

ІзОД – це відомі тільки певному колу осіб відомості, дані та знання, які мають особливу цінність, щодо яких вживаються заходи, спрямовані на обмеження вільного доступу третіх осіб, поширення яких може принести істотну шкоду заінтересованим особам[73] .

ІзОД становлять відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено відповідно до законодавства України її власником або сумлінним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) у зв'язку з її особливою цінності для них на законних підставах[74].

Це відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, визнаних такими відповідно до встановлених юридичних процедур і доступ до яких обмежений власником таких відомостей[75].

Таким чином, ІзОД визначається такими основними ознаками[76]:

- доступ обмежений відповідно до закону;
- мета обмеження – захист основ конституційного ладу, моральності, здоров'я, прав і законних інтересів інших осіб, забезпечення оборони країни і безпеки держави.

Згідно ст. 3 ЗУ «Про інформацію» одним з напрямків державної інформаційної політики є забезпечення ІБ України, яка й визначає мету правового режиму ІзОД.

Питання *обмеження доступу до інформації* регулюються різними нормативно-правовими актами України, серед яких:

---

[72] Угода між Кабінетом Міністрів України та Урядом Королівства Норвегія про захист інформації з обмеженим доступом: Угода ратифіковано Законом України від 30.10.2008 р. № 636-VI // Офіційний вісник України. – 2009. – № 27. – С. 163. – Ст. 916.

[73] Кулініч О. О. Інформація з обмеженим доступом як об'єкт цивільних прав: Дис… к.ю.н.: 12.00.03 – Одеса, 2006. – С. 30.

[74] Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / В. Ю. Баскаков. – К., 2012. – С. 7.

[75] Марущак А. І. Інформаційне право: Доступ до інформації: Навчальний посібник. – К.: КНТ, 2007. – С. 24.

[76] Ковалева Н. Н. Информационное право России: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К°», 2007. – С. 95–96.

Конституція України, Закони України «Про інформацію», «Про доступ до публічної інформації» та ін.

Так, відповідно до п. 2 ст. 6 ЗУ «Про доступ до публічної інформації» обмеження доступу до інформації здійснюється при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;
2) розголошення інформації може завдати істотної шкоди цим інтересам;
3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

ІзОД може бути поширена, якщо вона є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення (ст. 29 ЗУ «Про інформацію»).

Предметом суспільного інтересу вважається інформація, яка:

- свідчить про загрозу державному суверенітету, територіальної цілісності України;
- забезпечує реалізацію конституційних прав, свобод і обов'язків;
- свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

Відповідно до ч. 7 ст. 6 ЗУ «Про доступ до публічної інформації» обмеженню доступу підлягає інформація, а не документ. Якщо документ містить ІзОД, для ознайомлення надається інформація, доступ до якої необмежений.

Відповідно до п. 4 ст. 21 ЗУ «Про інформацію» до *ІзОД не можуть бути віднесені* такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечних природних явищах та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

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

4) про факти порушення прав і свобод людини і громадянина;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб;

6) інші відомості, доступ до яких не може бути обмежений відповідно до законів та міжнародних договорів України, згода на обов’язковість яких представлено Верховною Радою України.

Відповідно до ч. 5 ст. 6 ЗУ «Про доступ до публічної інформації» *не може бути обмежено доступ* до інформації про розпорядження бюджетними коштами; володіння, використання чи розпорядження державним, комунальним майном, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. При дотриманні вимог, передбачених ч. 2 ст. 6 цього Закону (перераховані вище), зазначене положення не поширюється на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину.

Також *не відносяться до ІзОД* декларації про доходи осіб та членів їхніх сімей, які претендують на зайняття чи займають виборну посаду в органах влади або обіймають посади державного службовця, службовця органу місцевого самоврядування першої або другої категорії (ч. 6 ст. 6 ЗУ «Про доступ до публічної інформації»).

На підставі п. 1 ст. 13 ЗУ «Про доступ до публічної інформації» *не є ІзОД:*

- інформація, пов'язана з виконанням обов'язків осіб, що виконують делеговані повноваження суб'єктів владних повноважень

відповідно до закону або договору, включаючи надання освітніх, оздоровчих, соціальних або інших державі н них послуг;

- інформація про умови поставок товарів та послуг суб'єктами господарювання, які займають домінуюче положення на ринку або наділені спеціальними чи виключними правами, або є природними монополіями.

Не можуть відноситись до ІзОД всі персональні дані фізичної особи, яка претендує зайняти чи займає виборну посаду (у представницьких органах) або посаду державного службовця першої категорії, не належать до ІзОД, за винятком інформації, яка визначена такою відповідно до ЗУ «Про доступ до публічної інформації» (п. 3 ст. 5 ЗУ «Про захист персональних даних»).

Не належать до ІзОД відомості, зазначені в деклараціях про майно, доходи, витрати і зобов'язання фінансового характеру, оформленої за формою і в порядку, встановлених Законом України «Про засади запобігання та протидії корупції»[77], крім відомостей про дохід від викладацької, наукової і творчої діяльності, медичної практики, інструкторської та суддівської практики із спорту.

Отже, на законодавчому рівні проведено поділ інформації на ІзОД та інформації, яка є строго відкритою і не може належати ІзОД.

§3.2. Види інформації з обмеженим доступом

Згідно з п. 1 ст. 21 ЗУ «Про інформацію» ІзОД поділяється на ***конфіденційну, таємну*** та ***службову*** інформацію.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку, відповідно до передбачених нею умов, а також в інших випадках, визначених законом (п. 2 ст. 21 ЗУ «Про інформацію»).

[77] Про засади запобігання і протидії корупції: Закон України від 07.04 2011 р. // Відомості Верховної Ради. – 2011. – № 40.– Ст. 404.

Конфіденційна інформація – це інформація виключно приватних суб'єктів, яка може бути різною. До конфіденційної інформації може належати як інформація про її власника, так і інша інформація, що потрапила у володіння приватного суб'єкта (відомості про непублічну подію, властивості природних об'єктів, місце їх знаходження та ін.)[78].

Отже, будь-яка інформація може бути віднесена до конфіденційної, якщо це не заборонено законом.

До конфіденційної інформації належать персональні дані (п. 2 ст. 5 ЗУ «Про захист персональних даних»[79]).

Особливим видом конфіденційної інформації є комерційна таємниця: згідно зі ст. 36 ГКУ[80] юридична або фізична особа-підприємець (суб'єкт господарювання) самостійно визначають склад і обсяг відомостей, що становлять комерційну таємницю. Це і є головна ознака, яка відрізняє «комерційну таємницю» від таємної інформації, склад і режим захисту якої визначається законом.

Також, конфіденційною інформацією є інформація про споживачів телекомунікаційних послуг. Відповідно до п. 1 ст. 34 ЗУ «Про телекомунікації»[81] оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

До конфіденційної інформації у сфері господарської (підприємницької) діяльності відноситься інформація, яка визначається ст. 862 ЦКУ та «ноу-хау» (таємниці виробництва) (ст. 1 ЗУ «Про інвестиційну діяльність»[82]).

---

[78] Золотар О. О. Обмеження доступу до інформації: інформаційно-правовий аспект. – [Електронний ресурс]. – Режим доступе : http://archive.nbuv.gov.ua/portal/soc_gum/iblsd/2012_1/_private/13zooala.pdf

[79] Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради. – 2010. – № 34. – Ст. 481.

[80] Господарський кодекс України від 16.01.2003 р. № 436-IV // Відомості Верховної Ради. – 2003. – № 18–22. – Ст. 144.

[81] Про телекомунікації: Закон України від 18.11.2003 р. // Відомості Верховної Ради. – 2004.– № 12.– Ст. 155.

[82] Про інвестиційну діяльність: Закон України від 18.09.1991 р. // Відомості Верховної Ради. – 1991.– № 47.– Ст. 646.

Згідно зі ст. ст. 60-61 ЗУ «Про банки і банківську діяльність»[83] банківська таємниця також відноситься до конфіденційної інформації.

Таким чином, конфіденційна інформація включає в себе наступні види, що не мають ознак державної таємниці: таємниця особистого життя, комерційна, банківська та професійні таємниці.

Винятком є інформація, для якої встановлені правові обмеження щодо можливості її віднесення до категорії конфіденційної. Це окремі відомості комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо).

Розпорядники, що володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – «*лише в інтересах національної безпеки, економічного добробуту та прав людини*» (ст. 7 ЗУ «Про доступ до публічної інформації»).

На підставі вище викладеного, можна виділити правові ознаки конфіденційної інформації:

- визнана конфіденційною законом;
- по об'єкту – це інформація про фізичному особу (персональні дані), інформація, доступ до якої обмежено правовласником;
- за суб'єктом – фізична або юридична особа, яка не є суб'єктом владних повноважень;
- поширюється за власним бажанням і розсуд суб'єктів незалежно від правовласників.

Другим видом ІзОД є ***таємна інформація***.

Відповідно до ст. ст. 6 і 8 ЗУ «Про доступ до публічної інформації» ***таємна інформація*** – це інформація, розголошення якої може завдати шкоди особі, суспільству і державі, доступ до якої обмежується виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку для запобігання

[83] Про банки і банківську діяльність: Закон України від 07.12.2000 р. // Відомості Верховної Ради. – 2001.– № 5-6.– Ст. 30.

заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Її розголошення може завдати істотної шкоди цим інтересам. Шкода від оприлюднення такої інформації переважає над суспільним інтересом в її отриманні. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

Крім ЗУ «Про доступ до публічної інформації» поняття «таємна інформація» розкривається в багатьох нормативно-правових актах.

Положення про роботу із засобами обчислювальної техніки і телекомунікаційною мережею Міністерства економіки України визначають таємну інформацію, як «*інформацію, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю*»[84].

Основними характеристиками таємної інформації є те, що: відношення її до категорії таємних відомостей, доступ до неї громадян, порядок обігу та захисту, порядок і строки її опублікування визначаються законодавчо.

Обмеження доступу до таємної інформації встановлюється законодавством у разі відповідності інформації певним критеріям. Засекречується інформація незалежно від бажання чи небажання її власника, більш того власник інформації зобов'язаний реалізувати своє право власності на інформацію з урахуванням встановлених законом обмежень. А у випадку їх порушення, може бути позбавлений права власності на інформацію та її матеріальні носії. Рішення про засекречування інформації приймають уповноважені органи державної влади, а вміст режиму доступу до інформації, засоби її

[84] Положення про роботу із засобами обчислювальної техніки і телекомунікаційною мережею Міністерства економіки України: Наказ Міністерства економіки України від 08.06.2010 р. № 630. – [Електронний ресурс]. – Режим доступу: http://www.uapravo.net/akty/administraciya-osnovni/akt8teoz4b.htm.

захисту та юридичну відповідальність за порушення режиму визначаються законодавчо[85].

Таємна інформація не є однорідною та відрізняється по предмету інформації, що захищається; по суб'єктам, на яких поширюються обов'язки не порушувати таємницю у зв'язку з професійною або службовою діяльністю.

Порядок доступу до таємної інформації та її правові ознаки визначені ЗУ «Про доступ до публічної інформації».

Між таємною інформацією та конфіденційною інформацією існують відмінності. Полягають вони в тому, що обмеження доступу до таємної інформації встановлюється законом і не вимагає волевиявлення особи, якого така інформація стосується. Тоді як підставою для визнання інформації конфіденційною є, насамперед, бажання фізичної або юридичної особи вважати певну інформацію про нього або інформацію, яка знаходиться в його володінні, конфіденційною. Друга відмінність – режим доступу до таємної інформації визначається законом, а доступ до конфіденційної – особою, яка цей доступ і обмежила[86].

Третій вид ІзОД – ***службова інформація.***

До *службової інформації* може належати така інформація (ст. 9 ЗУ «Про доступ до публічної інформації»), яка:

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

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яка не відноситься до державної таємниці. Документам, які містять інформацію, що становить

[85] Кормич Б. А. Інформаційне право. Підручник. – Харків: БУРУН і К, 2011. – С. 163.

[86] Науково-практичний коментар до Закону України «Про доступ до публічної інформації» / Під заг. ред. Д. Котляр. – К., 2012. – С. 144.

службову інформацію, присвоюється гриф «для службового користування» (ДСК).

Обов'язковість присвоєння грифу пояснюється необхідністю особливого обліку та зберігання таких документів, зокрема, для забезпечення відповідної реєстрації таких документів в систему обліку публічної інформації, передбаченої в ст. 18 ЗУ «Про доступ до публічної інформації». Гриф представляється як матеріальним носіям службової інформації, так і документам в електронній формі.

Робота з такими документами здійснюється відповідно до Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, затвердженої постановою Кабінету Міністрів України від 27 листопада 1998 р. № 1893 (із змінами)[87]. Тому віднесення до службової інформації повинно бути дійсно необхідним і не повинно бути автоматичним (не треба в кожній службової записки застосовувати гриф ДСК).

Перелік відомостей, що становлять службову інформацію, складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмежений у доступі.

Відомості, що становлять службову інформацію, містяться в внутрішньовідомчої службової кореспонденції, доповідних записках, рекомендаціях. Ці відомості визначаються не через зміст інформації, а через документи, в яких вони містяться. При цьому мова йде тільки про документи суб'єктів владних повноважень, визначених у ст. 13 ЗУ «Про доступ до публічної інформації». Такі документи повинні бути пов'язані з розробкою напряму діяльності існуючого органу або із здійсненням його контрольних або наглядових функцій.

До службової інформації не відноситься інформація, що міститься в міжвідомчій кореспонденції.

[87] Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію: затверджено постановою Кабінету Міністрів України від 27.11.1998 р. № 1893 // Офіційний вісник України. – 1998. – № 48. – С. 31.

В п. 2 ст. 6 ЗУ «Про доступ до публічної інформації» визначено три загальних умови обмеження доступу до інформації. При наявності одночасно всіх цих умов суб'єкт владних повноважень може обмежити доступ до певної інформації і надати документів, що містять її гриф ДСК.

П. 3 ст. 21 ЗУ «Про інформацію» встановлює, що «*порядок віднесення до ... службової інформації, а також порядок доступу до неї регулюється законом*». Порядок віднесення інформації до службової інформації визначається різними нормативно-правовими актами, які можна об'єднати в кілька груп[88]:

- відомчі положення та інструкції про забезпечення доступу до публічної інформації;
- нормативно-правові акти, що визначають обов'язок не розголошувати службову інформацію;
- відомчі переліки відомостей, що становлять службову інформацію;
- відомчі інструкції і положення про порядок використання службової інформації в окремих службах і органах;
- акти про ведення загального діловодства за зверненням службових листів, службових документів, записок;
- нормативно-правові акти, що передбачають проведення службових розслідувань за порушення правил використання службової інформації та дисциплінарну відповідальність.

Підсумовуючи можна зробити висновок, що правовими ознаками службової інформації є:

- визнана службовою законом;
- міститься в документах суб'єктів владних повноважень;
- зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності або в сфері оборони;
- не є державною таємницею;
- є власністю держави (створена на державні кошти).

[88] Блінова Г. О. Службова таємниця як вид публічної інформації з обмеженим доступом. – [Електронний ресурс]. – Режим доступу: http://pravoisuspilstvo.org.ua/archive/2013/3_2013/07.pdf.

Отже, до службової інформації можуть відноситися такі види таємниць: податкова, нарадчої кімнати, а також інформація військового характеру, що не є державною таємницею.

Слід зауважити, що наведена класифікація видів ІзОД за порядком доступу залишається дещо складною та заплутаною і має певні недоліки[89].

§3.3. Поняття і склад правових інститутів таємниць

Інститут таємниці – один з найважливіших інститутів, що визначають співвідношення інтересів особистості, суспільства і держави, приватного і публічного права, підстави та межі втручання держави в недержавну сферу, ступінь інформаційної захищеності. Він охоплює широке коло досить різнорідних суспільних відносин, що виникають у різних сферах діяльності особистості, суспільства і держави.

Зміст будь-якої таємниці, незалежно від специфіки її різновидів, полягає в тому, що предмет таємниці утворюють відомості, не призначені для широкого кола осіб, їх розголошення може спричинити небажані наслідки для зберігачів і носіїв таємниці[90].

У правовому відношенні інститут таємниці становить інтерес з позиції обмеження гласності та визначення меж втручання в сферу його дії, розробки гарантій його захисту.

Правовий інститут будь-якої таємниці можна умовно представити у вигляді трьох складових *(рис. 3.2):*

- ***загальна частина*** – визначення таємниці, принципи і критерії віднесення інформації до таємниці, обмеження по включенню певної інформації до таємниці, правові ознаки таємниці тощо;
- ***режим таємниці*** – правовий механізм обмеження доступу до інформації, що становить таємницю;

[89] Бєляков К. І. Інформація з обмеженим доступом: проблеми законодавчого регулювання / К. І. Бєляков // Науковий вісник Національної академії внутрішніх справ України. – 2004. – № 6.– С. 267–277.

[90] Смолькова И. В. Проблемы охраняемой законом тайны в уголовном процессе. – М.: Изд-во «Луч», 1999. – С. 14–17.

• ***санкції*** – юридична відповідальність за протиправні дії з інформацією, що складає таємницю[91].

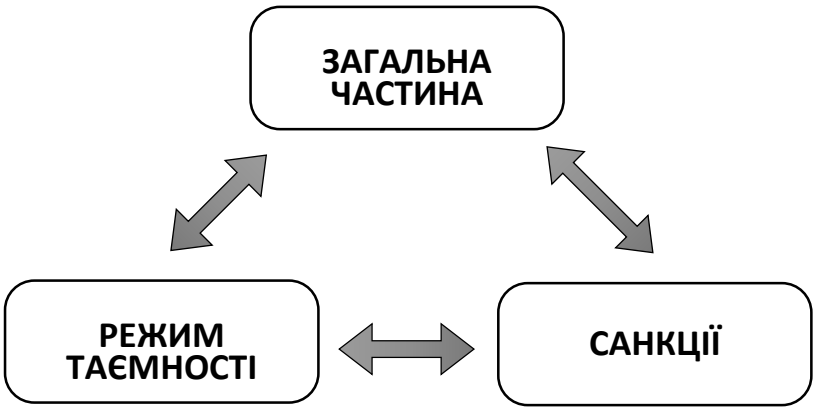

Рис. 3.2. Склад правового інституту таємниці

Сукупність правових норм, яка регламентує інформаційні відносини в сфері обігу інформації, що становить таємницю, і утворює *окремий правовий інститут*, оскільки їй притаманні однорідність фактичного змісту, єдність правових норм.

Відзначимо, що до правових інститутів, які регулюють сукупність однорідних суспільних відносин, пов'язаних з обігом ІзОД і мають всі зазначені складові зараз відносять правові інститути таємниць: державної, банківської, комерційної, професійної, особистого життя, нарадчої кімнати тощо.

З урахуванням правових інститутів таємниць можна докладно представити класифікацію ІзОД *(рис. 3.3)*.

[91] Ємельянов С. Л. Проблема формування правових інститутів таємниць в Україні / С. Л. Ємельянов // Наукові праці Національного університету «Одеська юридична академія». – 2012. – Т. XII. – С. 130–140.

Рис. 3.3. Класифікація ІзОД

Висновки

Відповідно до Закону України «Про інформацію», вчинення права на отримання інформації безпосередньо пов'язане з поняттям режиму доступу до інформації, який є передбаченим правовими нормами порядком отримання, використання, поширення та зберігання інформації.

Залежно від порядку доступу інформація поділяється на відкриту і ІзОД.

В свою чергу, ІзОД поділяється на конфіденційну, таємну і службову інформацію.

Правовий інститут таємниці утворює сукупність правових норм, що регламентує інформаційні відносини в сфері обігу інформації.

4 ІНСТИТУТ ДЕРЖАВНОЇ ТАЄМНИЦІ

§4.1. Поняття і правовий режим державної таємниці

В системі правовідносин, що виникають при обігу інформації, особливе місце займає *інститут державної таємниці* (ДТ). Важливість і значимість цього інституту під час розвитку інформаційного суспільства, коли інформація стає основним і цінним ресурсом, зростає на багато разів. Інститут ДТ існує в усіх країнах світу[92] і сьогодні є основною складовою системи інформаційної безпеки, яка займає провідне місце в системі національної безпеки держави[93].

Сьогодні в Україні сформована досить чітка система охорони ДТ, яка включає в себе *комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів,* спрямованих на запобігання розголошенню таємної інформації та втрати її матеріальних носіїв[94].

Правовий інститут ДТ в Україні представлений трьома складовими:

- загальна частина: визначення таємниці, принципи і критерії віднесення інформації до ДТ, правові ознаки ДТ;
- режим ДТ: механізм обмеження доступу до зазначених відомостей, тобто механізм їх організаційно-правового захисту;
- санкції за неправомірне поводження з відомостями, що становлять ДТ.

[92] Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В. С. Сідак, В. Ю. Артемов. – К.: КНТ, 2007. – 160 с.

[93] Про основи національної безпеки України: Закон України від 19.06.2003 р. // Відомості Верховної Ради. – 2003. – № 39.– Ст. 351; Про доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514 // Офіційний вісник України. – 2009. – № 52. – Ст. 1783.

[94] Головань С. М. Системи охорони державної таємниці. підручник / С. М. Головань, С. Б. Гордієнко, О. В. Корнейко, А. О. Петров. – Луганськ: вид-во СНУ ім. В. Даля, 2012. – 296 с.

Базовим законом, що регулює *перші дві складові* (загальну частину та режим ДТ), є ЗУ «Про державну таємницю»[95]. Також одним з основних, є ЗУ «Про службу безпеки України»[96], оскільки Служба безпеки України (СБУ) виступає основною спеціальною службою, що здійснює охорону ДТ. Третя складова (санкції) прописана в ККУ[97], в КУпАП[98] і в інших нормативно-правових актах.

Відповідно до ст. 1 ЗУ «Про державну таємницю»: ***«державна таємниця*** *(далі також – секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою*». З цього визначення випливають найважливіші ***правові ознаки ДТ:***

1) ДТ – це вид таємної інформації, який регулюється ЗУ «Про державну таємницю»;
2) ДТ становлять лише відомості в чітко зазначених сферах;
3) розголошення ДТ може завдати шкоди національній безпеці України;
4) існує організаційно-правовий механізм віднесення інформації до ДТ;
5) охорона ДТ здійснюється державою.

Інформація, яка може бути віднесена до ДТ, визначається відповідно до норм ст. 8 ЗУ «Про державну таємницю» та викладена в Зводі відомостей, що становлять державну таємницю в Україні (ЗВДТ)[99]. ЗВДТ є *«єдиною формою реєстрації цих відомостей в Україні. З моменту опублікування ЗВДТ держава забезпечує захист і правову*

[95] Про державну таємницю: Закон України від 21 січня 1994 р. // Відомості Верховної Ради. – 1994. – № 16.–Ст. 93.
[96] Про Службу безпеки України: Закон України від 25.03.1992 р. // Відомості Верховної Ради. – 1994. – № 27. – Ст. 382.
[97] Кримінальний кодекс України від 5.04.2001 р. // Відомості Верховної Ради. – 2001. – № 25–26. –Ст. 131.
[98] Кодекс України про адміністративні правопорушення від 7.12.1984 р. // Відомості Верховної Ради Української РСР. – 1984. – Додаток до № 51. – Ст. 1122.
[99] Звід відомостей, що становлять державну таємницю, затв. Наказом Служби безпеки України від 12.08.2005 р. № 440 // Офіційний Вісник України. – 2005. – № 34. – Ст. 2089.

охорону відомостей, зареєстрованих в ньому». ЗВДТ – це систематизований перелік відомостей, віднесених до ДТ, що складається з статей, пунктів і підпунктів.

ДТ становлять:

1. У сфері оборони:

- інформація, що стосується безпосередньо Збройних Сил України;
- інформація військово-технічного характеру;
- інформація про заходи захисту населення в умовах можливих конфліктів;
- відомості географічно-топологічного характеру, які мають значення для оборони країни;

2. У сфері економіки, науки і техніки:

- інформація військово-економічного характеру;
- стратегічна економічна інформація;
- фінансово-економічна інформація;
- науково-технічна інформація;

3. У сфері зовнішніх відносин:

- окремі аспекти зовнішньополітичної і зовнішньоекономічної діяльності;
- окремі аспекти міждержавного військово-економічного співробітництва;
- відомості про експорт та імпорт озброєння, військової та спеціальної техніки, окремих стратегічних видів сировини і продукції;

4. У сфері державної безпеки та охорони правопорядку:

- окремі аспекти негласної правоохоронної діяльності;
- заходи щодо захисту різного роду режимних об'єктів;
- відомості щодо безпосереднього здійснення заходів з захисту інформації.

Отже, до ДТ відноситься інформація в різних сферах діяльності, а саме: оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

В останні роки були внесені зміни в національне законодавство з метою впорядкування та попередження зловживань в

засекречування інформації. Так, згідно зі ст. 8 ЗУ «Про державну таємницю» забороняється відносити до ДТ будь-які відомості, якщо цим будуть обмежуватися конституційні права і свободи людини і громадянина, буде наноситися шкода здоров'ю та безпеці населення.

Не відноситься до ДТ наступна інформація**:**

- про стан довкілля, про якість харчових продуктів і предметів побуту, про впливі товару (роботи, послуги) на життя і здоров'я людини;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що 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 соціально-демографічні показники, стан правопорядку, освіти і культури населення;
- про факти порушень прав і свобод людини і громадянина;
- про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових і службових осіб;
- інша інформація, доступ до якої, відповідно до законів і міжнародних договорів, згода на обов'язковість яких надається Верховною Радою України, не може бути обмежений.

Віднесення відомостей до ДТ здійснюється відповідно до їх галузевої, відомчої або цільової приналежності, а також відповідно до законодавства.

Обґрунтування необхідності віднесення відомостей до ДТ покладається на органи державної влади, підприємства, установи та організації, які ці відомості отримано і розроблені.

§4.2. Організаційно-правові методи охорони державної таємниці

Національна система охорони ДТ створювалася з урахуванням досвіду розвинених демократичних країн і перевірених на практиці традиційних засобів і методів. Значною мірою сучасна Україна є спадкоємицею системи захисту секретної інформації, яка існувала ще

під час Радянського Союзу. Більшість елементів цієї структури було збережено, а внаслідок – розвинуто і вдосконалено.

Заходи, які вживає держава, охороняючи свої таємниці, повинні бути адекватні існуючим в даний момент загрозам (як зовнішнім, так і внутрішнім). Ефективне вирішення цього питання можливе лише за умови комплексного підходу, який включає дослідження виникнення потреби в охороні ДТ взагалі, та особливостей формування цієї системи на території України, зокрема.

Формування системи охорони ДТ передбачає введення системи взаємодіючих адміністративно-правових режимів, функції яких, в тій чи іншій мірі, спрямовані на охорону ДТ. Введення відповідних режимів передбачає нормативно-правове регулювання відносин у цій сфері та створення державних органів, діяльність яких спрямована на вирішення конкретних задач з забезпечення зазначених режимів.[100]

Щодо *другої складової правового інституту ДТ* (режиму ДТ) відзначимо, що в цілях захисту ДТ використовуються наступні основні ***організаційно-правові методи*** (ст. 18 ЗУ «Про державну таємницю»):

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
- дозвільний порядок здійснюється органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з ДТ;
- обмеження оприлюднення, передачі 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 ДТ, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

[100] Ботвінкін О. Система охорони Державної таємниці в Україні. Історичний аспект / О. Ботвінкін. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2 (13). – 2006. – С. 83-88.

- особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з ДТ;
- режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з ДТ;
- спеціальний порядок допуску та доступу громадян до ДТ;
- технічний та криптографічний захист секретної інформації.

Відомості ДТ можуть мати різну ***ступінь секретності,*** яка є категорією, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її захисту державою. За ступенем секретності виділяють три категорії: **Т –** *таємно;* **ЦТ –** *цілком таємно;* **ОВ** – *особливої важливості*.

Конкретні дані можуть відноситися до певної категорії відомостей, які містять ДТ тільки за умови, що їх розголошення завдасть шкоди інтересам національній безпеці України. При цьому обов'язково враховується ступінь секретності інформації, критерії визначення якої встановлюються СБУ. Термін, протягом якого діє рішення про віднесення інформації до ДТ, не може перевищувати для інформації із ступенем секретності «Т» – 5 років, для інформації «ЦТ» – 10 років і для інформації «ОВ» – 30 років (ч. 1 ст. 13 ЗУ «Про державну таємницю»).

Після закінчення передбаченого терміну дії рішення про віднесення інформації до ДТ, приймається рішення про скасування рішення про віднесення її до ДТ або приймається рішення про продовження терміну дії певного рішення в рамках вище зазначених строків.

Президент України з власної ініціативи або за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до ДТ, ніж строки, встановлені ч. 1 ст. 13.

Встановлення терміну дії рішення про віднесення інформації до ДТ, прийняття рішення про його продовження здійснюються з дотриманням вимог ст. 6 ЗУ «Про доступ до публічної інформації».

Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до ДТ здійснюється на основі рішення державного експерта з питань таємниць або на підставі рішення суду у випадках, передбачених ст. 12 ЗУ «Про державну таємницю», і оформляються СБУ шляхом внесення відповідних змін до ЗВДТ. Інформація вважається ДТ з вищою або нижчою ступенем секретності або не складає ДТ, з моменту опублікування відповідних змін до СС ДТ.

Інформація, включена в ЗВДТ, подається за формою *(рис. 4.1)*[101]*:*

Відомості, що становлять державну таємницю

Номер статті ЗВДТ	**Склад відомостей, що складають ДТ**	**Ступінь секретності**	**Термін дії рішення про віднесення інформації до ДТ в роках**	**Реєстраційний номер і дата рішення державного експерта з питань таємності**
1	**2**	**3**	**4**	**5**

Рис. 4.1. Форма подачі відомостей, що становлять ДТ

Рішення про віднесення інформації до ДТ приймається державним експертом з питань таємниць не пізніше одного місяця з дня отримання звернення відповідного органу державної влади, органу місцевого самоврядування, підприємств, установ, організацій чи громадянина, після чого воно підлягає реєстрації СБУ в ЗВДТ.

Інформація також може бути вилучена з ЗВДТ. Підставою для цього є висновок державного експерта з питань таємниць про скасування рішення про віднесення інформації до ДТ. Цей висновок набирає чинності з моменту внесення СБУ змін до ЗВДТ, які згідно зі ст. 12 ЗУ «Про державну таємницю» формуються та публікуються в

[101] Іванова Т. В., Піддубна Л. П. Діловодство в органах державного управління та місцевого самоврядування: Навчальний посібник. – К.: Центр учбової літератури, 2007. – С. 231.

офіційних виданнях СБУ на підставі рішень державних експертів з питань таємниць.

Зразки форм рішень (висновків) державних експертів з питань таємниць, порядок і механізм формування ЗВДТ, і їх публікація визначаються Кабінетом Міністрів України.

Важливою справою є ***засекречування та розсекречування матеріальних носіїв,*** які містять ДТ.

Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі ЗВДТ (розгорнутих переліків відомостей, що становлять ДТ), відповідному документу, виробу або іншому матеріальному носію інформації грифу секретності посадовою особою, який готує або створює їх. Засекречування документів здійснюється тільки в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується до незасекреченої частини.

Гриф секретності кожного матеріального носія таємної інформації повинен відповідати ступеню секретності міститься інформації, відповідно до ЗВДТ, – «ОВ», «ЦТ» або «Т». Реквізити кожного матеріального носія секретної інформації складаються з:

- грифу секретності;
- номера примірника;
- статті ЗВДТ, на підставі якої здійснюється засекречення;
- найменування посади та підпису особи, яка надала гриф секретності.

Якщо перераховані реквізити неможливо нанести безпосередньо на матеріальний носій секретної інформації, то вони повинні бути визначені в супровідних документах.

Забороняється надавати гриф секретності, матеріальним носіям іншої таємної інформації, яка не складає ДТ.

Перелік посад, перебування на яких дає посадовим особам право надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником державного органу, органу

місцевого самоврядування, підприємства, установи, організації, здійснює діяльність, пов'язану з ДТ.

Ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт, виконуваних в інтересах забезпечення національної безпеки та оборони держави, встановлюються шляхом винесення відповідного висновку державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації, а також в разі підвищення або зниження ступеня секретності такої інформації або скасування рішення про віднесення її до ДТ, керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну грифу секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників державних органів, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі матеріальні носії секретної інформації.

Термін засекречування матеріальних носіїв інформації має відповідати терміну дії рішення про віднесення інформації до ДТ, встановленого рішенням державного експерта.

Термін дії засекречування матеріальних носіїв інформації починається з моменту надання їм грифу секретності.

Громадяни та юридичні особи мають право внести посадовим особам, які надали гриф секретності матеріальному носію таємної інформації, обов'язкову для розгляду мотивовану пропозицію про розсекречування цього носія інформації. Зазначені посадові особи повинні протягом одного місяця надати письмову відповідь з цього приводу.

Рішення про засекречування матеріального носія інформації може бути оскаржено громадянином чи юридичною особою в порядку підлеглості вищому органу або посадовій особі, а також у суді. У разі незадоволення скарги, поданої в порядку підлеглості, громадянин або юридична особа мають право оскаржити рішення вищого органу або посадової особи в суді.

Питання віднесення інформації у зазначених вище сферах, зміни ступеня секретності інформації та її розсекречування, покладено на ***державних експертів з питань таємниць***. Ці експерти призначаються у Верховній Раді – Головою Верховної Ради, в інших органах державної влади – Президентом України за поданням керівника відповідного державного органу.

Державний експерт з питань таємниць відповідно до покладених на нього завдань визначає підстави, за якими інформація може бути віднесена до ДТ, ступінь секретності інформації та державні органи, яким надається право приймати рішення про доступ осіб до таємної інформації, що становить ДТ та виконує інші функції, передбачені законодавством.

Державний експерт з питань таємниць при виконанні покладених на нього функцій ***зобов'язаний***:

- погоджувати з представником СБУ свої висновки про скасування рішень про віднесення інформації до міждержавних таємниць з відповідними посадовими особами держав-учасників міжнародних договорів України;
- представляти СБУ не пізніше ніж через десять днів з моменту підписання рішення про віднесення відомостей до ДТ або про скасування цих рішень, а розгорнуті переліки відомостей, що становлять державну таємницю, – в той же термін з моменту їх затвердження;
- розглядати протягом одного місяця пропозиції СБУ про віднесення інформації до державної таємниці, скасування чи продовження терміну дії раніше прийнятого рішення про віднесення інформації до ДТ;

- надавати відповідний гриф секретності рішенням про віднесення інформації до ДТ і про скасування цих рішень в залежності від важливості їх отримання;
- брати участь в засіданнях державних експертів з питань таємниць;
- ініціювати питання про притягнення до відповідальності посадових осіб, які порушують законодавство України про ДТ.

Державний експерт з питань таємниць ***має право***:

- безперешкодно проводити перевірку виконання державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями, що перебувають у сфері його діяльності, рішень про віднесення інформації до ДТ, скасування цих рішень, додержання порядку засекречення інформації та у разі виявлення порушень давати обов'язкові для виконання приписи про їх усунення;
- створювати експертні комісії з фахівців і вчених, що мають допуск до ДТ, для підготовки проектів рішень про віднесення інформації до ДТ, зниження ступеня її секретності та скасування зазначених рішень, висновків по обізнаності про ДТ громадян, котрі мають або мали допуск до ДТ, а також для підготовки відповідних висновків в випадку розголошення секретної інформації або втрати матеріальних носіїв такої інформації;
- скасовувати безпідставні рішення про надання носію інформації грифу секретності, зміну або скасування цього грифу;
- клопотати про притягнення до відповідальності посадових осіб, які порушують законодавство України про ДТ;
- отримувати в установленому порядку від державних органів, органів місцевого самоврядування, підприємств, установ та організацій дані, необхідні для виконання своїх функцій.

Державний експерт з питань таємниць несе персональну відповідальність за законність і обґрунтованість свого рішення про віднесення інформації до ДТ або про зниження її ступеня секретності, або скасування рішення про віднесення її до ДТ, а також за умисне

невжиття рішення про віднесення до ДТ інформації, розголошення якої може нанести шкоду інтересам національної безпеки України.

Для віднесення інформації до ДТ державним експертом з питань таємниць видається мотивоване рішення, яке може бути видано як за його ініціативою, так і за зверненнями громадян, керівників відповідних органів і організацій. У цьому рішенні зазначаються:

- інформація, яка повинна становити ДТ та її відповідність категоріям і вимогам, передбачених законодавством;
- підстави для віднесення інформації до ДТ і обґрунтування збитку, котрий може бути завдано національній безпеці країни у разі її розголошення;
- ступінь секретності зазначеної інформації;
- орган державної влади, орган місцевого самоврядування, підприємство, установа, організація або громадянин, який зробив пропозиції про віднесення цієї інформації до ДТ, і орган державної влади, який має право визначати коло суб'єктів, що мають доступ до цієї інформації;
- термін дії рішення про віднесення інформації до ДТ.

Рішення про віднесення інформації до ДТ, продовження терміну дії раніше прийнятого рішення про віднесення інформації до ДТ, зміна ступеня секретності інформації, скасування раніше прийнятого рішення про віднесення інформації до ДТ приймаються державним експертом з питань таємниць протягом одного місяця з моменту надходження звернення державного органу, органу місцевого самоврядування, підприємства, установи, організації чи громадянина. Такі рішення підлягають реєстрації СБУ і є підставою для формування ЗВДТ, та внесення змін до зазначеного Зводу, галузевих або відомчих розгорнутих переліків відомостей, що становлять ДТ. Порядок реєстрації рішень державних експертів з питань таємниць визначається Кабінетом Міністрів України.

У державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що здійснюють діяльність, пов'язану з ДТ, з метою розробки і здійснення заходів щодо

забезпечення режиму секретності, постійного контролю над їх виконанням, створюються на правах окремих структурних підрозділів ***режимно-секретні органи*** (РСО), які підпорядковуються безпосередньо керівникові цих установ.

Створення, реорганізація або ліквідація РСО здійснюються за погодженням із СБУ.

До складу РСО входять підрозділи режиму, криптографічного, технічного захисту інформації, таємного діловодства та інші підрозділи, що безпосередньо забезпечують охорону ДТ, в залежності від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

РСО комплектуються спеціалістами, яким надано допуск до ДТ зі ступенем секретності «ЦТ», якщо характер робіт не потребує іншого. Прийняття в ці структурні підрозділи тимчасових працівників не допускається.

Основними завданнями РСО є:

- недопущення необґрунтованого допуску та доступу осіб до таємної інформації;
- своєчасна розробка і реалізація заходів, що забезпечують охорону ДТ, спільно з іншими структурними підрозділами державних органів, органів місцевого самоврядування, підприємств і організацій;
- запобігання розголошенню секретної інформації, випадків втрат матеріальних носіїв цієї інформації, заволодіння секретною інформацією іноземними державами та громадянами України, яким надано допуску та доступу до неї;
- виявлення та закриття каналів витоку секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;
- забезпечення впровадження заходів режиму таємності при виконанні всіх видів робіт, пов'язаних з ДТ, і при здійсненні зовнішніх відносин;
- організація та ведення таємного діловодства;

- здійснення контролю над станом режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

РСО *має право:*

- вимагати від усіх безпосередніх учасників роботи з ДТ неухильного виконання вимог законодавства щодо забезпечення захисту ДТ;
- здійснювати перевірку стану та організації роботи з питань захисту ДТ і забезпечення режимів секретності;
- брати участь в службових розслідуваннях;
- отримувати від громадян, яким оформляються документи на допуск до секретної інформації, анкетні дані;
- використовувати засоби зв'язку та вести в установленому порядку поштово-телеграфне листування з питань забезпечення режиму таємності та ін.

Передача функцій РСО будь-яким іншим підрозділам державного органу, органів місцевого самоврядування, підприємств, установ та організацією не допускається.

Залежно від ступеня секретності інформації встановлено такі ***форми допуску*** до ДТ:

форма 1 – для роботи з таємною інформацією, що має ступінь секретності «ОВ», «ЦТ» і «Т», термін дії – 5 років;

форма 2 – для роботи з таємною інформацією, що має ступінь секретності «ЦТ» і «Т», термін дії – 7 років;

форма 3 – для роботи з таємною інформацією, що має ступінь секретності «Т», термін дії – 10 років.

Органами СБУ надається допуск до ДТ дієздатним громадянам України віком від 18 років, яким він необхідний при виконанні службової, виробничої, наукової чи науково-дослідної діяльності або навчанні. В окремих випадках, які визначаються міністерствами, іншими центральними органами виконавчої влади, з угодою з СБУ громадянам України може надаватися допуск до ДТ зі ступенем

секретності «Т» і «ЦТ», а з 17 років – також до ДТ зі ступенем секретності «ОВ» .

Надання допуску до роботи з документами, що містять ДТ, здійснюється відповідно до Положення з питань державної таємниці, затвердженого постановою КМУ від 29 листопада 2001 р. № 1601[102]. При цьому заповнюється облікова карта громадянина про надання допуску до ДТ форма, якої затверджена СБУ[103].

Всі облікові картки громадянина про надання допуску до ДТ реєструються в журналі реєстрації облікових карток.

Згідно зі ст. 23 ЗУ «Про державну таємницю» надання допуску передбачає:

- визначення необхідності роботи громадянина із секретною інформацією;
- перевірку громадянина у зв'язку з допуском до ДТ;
- взяття громадянином письмового зобов'язання щодо збереження довіреної йому ДТ;
- отримання в письмовій формі згоди громадянина на передбачене законом обмеження прав у зв'язку з його допуском до ДТ;
- ознайомлення громадянина з мірою відповідальності за порушення законодавства про ДТ.

Безпосередньо перелік відомостей, які надає громадянин для оформлення допуску до ДТ, а також текст зобов'язання, яке він дає, затверджено Указом Голови СБУ «Про затвердження зобов'язання громадянина України у зв'язку з допуском до ДТ і анкети для оформлення допуску до ДТ»[104].

---

[102] Про затвердження положень з питань державної таємниці та внесення змін до деяких постанов Кабінету Міністрів України: Постанова Кабінету Міністрів України від 29.11.2001 р. № 1601 // Офіційний вісник України. – 2001. – № 49 / № 66. – 2010, ст. 2348. – С. 56. – Ст. 2190.

[103] Про затвердження форм документів для оформлення громадянам допуску до державної таємниці та порядку їх заповнення: Наказ Служби безпеки України від 04.02.2002 р. № 26 // Офіційний вісник України. – 2002. – № 9. – С. 163. – Ст. 424.

[104] Про затвердження зобов'язання громадянина України у зв'язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці: Наказ Служби безпеки України від 18.06.2001 р. № 190 // Офіційний вісник України. – 2001. – № 35. – С. 421. – Ст. 1655.

Доступ до ДТ надається вищим державним посадовим особам за фактом вступу на посаду: Президенту, Голові Верховної Ради України, Прем'єр-міністру, Голові Верховного Суду, Голові Конституційного Суду, Генеральному прокурору, Голові СБУ (з письмовим зобов'язанням про нерозголошення ДТ).

Громадяни, які мають допуск до ДТ обмежуються частково в своїх правах: це стосується виїзду за кордон на ПМП, свободи інформаційної діяльності.

Секретна інформація може передаватися за кордон іноземній державі чи організації тільки за міжнародними угодами, за згодою Верховної Ради України, Президента, за пропозицією Ради національної безпеки і оборони (РНБО).

Ст. 23 ЗУ «Про державну таємницю» визначає перелік, на підставі якого громадянину може бути відмовлено в наданні допуску до ДТ:

- відсутності у громадянина обґрунтованої необхідності в роботі із секретною інформацією;
- сприяння громадянином діяльності іноземної держави, іноземної організації або їх представників, а також окремих іноземців або осіб без громадянства, що наносить збиток інтересам національної безпеці України, або участь громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;
- відмова громадянина взяти на себе письмове зобов'язання по збереженню ДТ, яка буде йому довірено, а також при відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до ДТ;
- наявність у громадянина судимості за тяжкі або особливо тяжкі злочини, чи не погашеної або не знятої в установленому порядку;
- наявність у громадянина психічних розладів, які можуть нанести шкоду охороні ДТ, у відповідності з переліком, затвердженого Міністерством охорони здоров'я України та СБУ.

Крім того, в наданні допуску також може бути відмовлено в разі:

- повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;
- постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;
- невиконання громадянином обов'язків щодо збереження ДТ, яка йому довірена або довірялася раніше.

§4.3. Контроль над забезпеченням охорони та відповідальність за порушення державної таємниці

Керівники органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль над забезпеченням захисту ДТ (ст. 37 ЗУ «Про державну таємницю»).

Контроль над дотриманням законодавства про ДТ в системі СБУ здійснюється відповідно до ЗУ «Про Службу безпеки України».

СБУ має право контролювати стан захисту ДТ в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення захисту ДТ.

Посадові особи та громадяни, винні у розголошенні ДТ, втраті документів та інших матеріальних носіїв таємної інформації, недотриманні встановленого законодавством порядку передачі ДТ іншій державі чи міжнародній організації, порушенні встановленого законодавством режиму таємності та невиконанні обов'язків по збереженню ДТ, порушенні встановленого законодавством порядку надання допуску та доступу до ДТ та ін., несуть *дисциплінарну*, *адміністративну* та *кримінальну* відповідальність відповідно до ЗУ «Про державну таємницю», що і є *третьою складовою правового інституту ДТ*.

Дисциплінарна відповідальність настає за порушення правил використання документів, що містять ДТ, що не потрапляють під дію кримінальної відповідальності.

У чинному ККУ[105] ***кримінальна відповідальність*** за посягання на ДТ, за порушення встановленого порядку її зберігання передбачена в п'яти статтях*: ч. 1 ст. 111 – державна зрада; ст. 114 – шпигунство; ст. 328 – розголошення ДТ; ст. 329 – втрата документів, що містять ДТ; ст. 422 – розголошення відомостей військового характеру, що становлять ДТ, або втрата документів чи матеріалів, що містять такі відомості.*

Адміністративна відповідальність за порушення законодавства про ДТ визначена в ст. 212-2 КУпАП[106]: «*Порушення законодавства про ДТ»*, яка передбачає відповідальність за:

- недодержання встановленого законодавством порядку передачі ДТ іншій державі чи міжнародній організації;
- засекречування інформації, що не може бути засекречена, згідно ЗУ «Про державну таємницю»;
- необґрунтоване засекречування інформації;
- надання грифу секретності матеріальним носіям конфіденційної чи іншої секретної інформації, яка не становить ДТ або не надання грифу секретності матеріальним носіям інформації, що складають ДТ, а також безпідставне скасування або зменшення грифу секретності матеріальних носіїв таємної інформації;
- порушення встановленого законодавством порядку надання допуску та доступу до ДТ;
- невжиття заходів щодо забезпечення охорони ДТ і незабезпечення контролю над охороною ДТ;
- здійснення діяльності, пов'язаної з ДТ, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності;

[105] Кримінальний кодекс України від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131.

[106] Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8073-X // Відомості Верховної Ради України. – 1984. – № 51. – Ст. 1122.

- недотримання вимог законодавства щодо забезпечення охорони ДТ при здійсненні міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведенні роботи з ними;
- невиконання норм і вимог криптографічного та технічного захисту таємної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності.

В цілому створена в Україні власна система організаційно-правового захисту ДТ відповідає світовим стандартам, хоча і має окремі недоліки[107].

Отже, в Україні створена власна система захисту ДТ, стан і тенденції розвитку якої, є цілком позитивними і відповідають світовим стандартам. Триває усунення окремих недоліків в системі організаційно-правового захисту ДТ.

На підставі вище викладеного можна побудувати концептуальну модель захисту ДТ *(рис. 4.2)*.

Висновки

Система захисту ДТ є найбільш розробленою національним законодавством.

ДТ – вид секретної інформації, яка охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки, охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України.

Відомості ДТ можуть мати різну ступінь таємності, яка є категорією, що характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її захисту державою.

[107] Ємельянов С. Л. Проблемні аспекти організаційно-правового захисту державної таємниці в Україні / С. Л. Ємельянов // Інформаційна безпека. – 2011.– Вип. 1(5), м. Луганськ: СНУ ім. В. Даля. – С. 36–44; Організаційно-правові засади політики інформаційної безпеки України: Монографія / Б. А. Кормич. – Одеса: Юридична література, 2003.– С. 353–357.

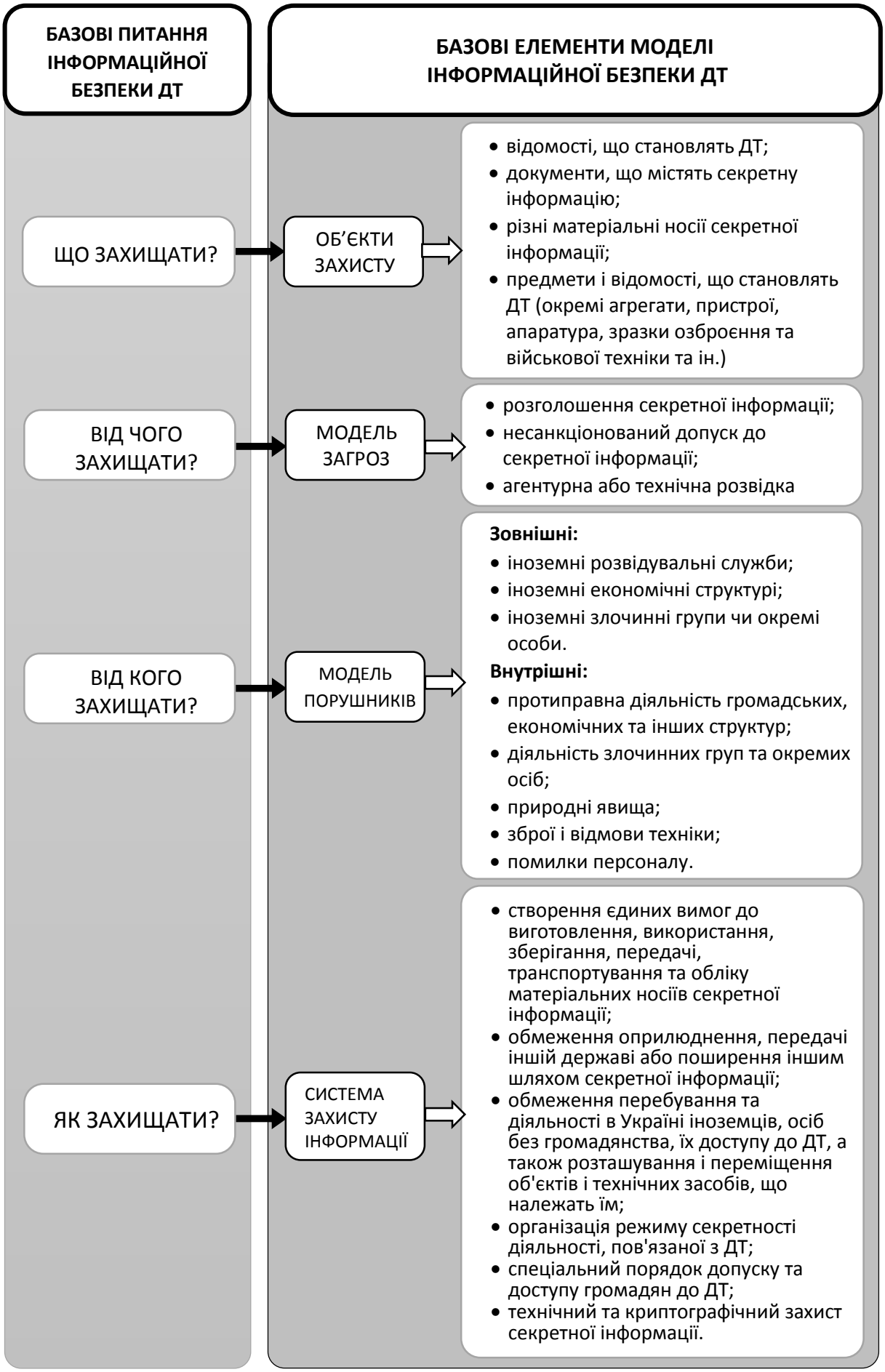

Рис. 4.2. Концептуальна модель захисту ДТ

5 ІНСТИТУТИ БАНКІВСЬКОЇ ТА КОМЕРЦІЙНОЇ ТАЄМНИЦЬ

§5.1. Поняття і правовий режим банківської таємниці

Банківська система в будь-якій країні є важливою складовою економіко-господарського механізму. З метою забезпечення її стабільного та ефективного функціонування держава створює ряд гарантій банківської діяльності, чинне місце серед яких займає *банківська таємниця* (БТ)[108].

Інститут БТ є складовою частиною правової системи будь-якої розвиненої країни світу, зміст якої обумовлено особливостями економіко-правової доктрини держави та формування нормативної бази, що забезпечує правовий захист інформації з обмеженим доступом[109].

Правовий інститут БТ, як і будь-який інший таємниці, можна умовно представити трьома складовими:

- загальна частина: визначення БТ, принципи і критерії інформації, котра відноситься до БТ, правові ознаки БТ;
- режим БТ: правовий механізм обмеження доступу до інформації, складової БТ;
- санкції: юридична відповідальність за протиправні дії з інформацією, що складає БТ.

Щодо *першої складової правового інституту БТ* відзначимо, що в юридичній науці та в чинному законодавстві досі немає єдиного розуміння поняття, правової природи і змісту БТ, її співвідношення з іншими видами таємниць (комерційної, службової, професійної тощо).

---

[108] Банківське право України: Навч. посібник. Кол. авт.: Жуков А. М., Іоффе А. Ю., Кротюк В. Л., Пасічник В. В., Селіванов А. О. та ін. / За заг. ред. А. О. Селіванова. – К.: Видавничий Дім «Ін Юре», 2000. – 384 с.

[109] Гетманцев Д. О. Банківська таємниця: особливості її нормативно-правового регулювання в Україні та в законодавстві зарубіжних країн. Автореф. дис…канд.юр. наук: 12.00.07 / КНУ ім. Т. Шевченка. – К., 2003. – 23 с.

Ряд авторів[110] вважають, що БТ є різновидом комерційної таємниці (КТ), оскільки склад БТ утворює КТ клієнта, що стала відомою банку в силу наявності договірних відносин між ним і банком, і КТ самого банку як самостійного суб'єкта господарювання. Інші автори[111] розглядають БТ як різновид службової таємниці: *«БТ визначається як інформація про операції, рахунки і вклади клієнтів і кореспондентів банку. Носії такої інформації мають гриф секретності, оскільки вона є різновидом службової таємниці»*.

Треті[112] визначають БТ, як *«встановлену законом і гарантовану банком систему правових та спеціальних технічних засобів, що забезпечують правовий режим обмеженого доступу до інформації про банківський рахунок, операції за рахунком і відомості про клієнта»*.

Не додає ясності й норма ст. 1076 ЦКУ, згідно з якою *«банк гарантує таємницю банківського рахунку, операцій за рахунком і відомостей про клієнта»*[113]. Ця норма носить загальний характер, адже в ній не наводиться перелік відомостей про клієнта, які можуть становити БТ.

Якщо клієнт – *фізична особа,* то БТ є його паспортні дані, відомості про внесення третіми особами грошей на рахунок вкладника, номер рахунку тощо. А також будь-які відомості, які стали відомі банку в процесі обслуговування клієнта.

Якщо клієнт – *юридична особа,* то БТ складають всі відомості, які зберігаються в справі клієнта, в тому числі довідки та свідоцтва державних органів про реєстрацію та облік, установчі документи, інформація, що міститься в документах, що дають право займатися підприємницькою діяльністю (ліцензії та ін.), в різних формах

---

[110] Стрельбицька Л. М. Правові засади захисту банківської таємниці / Л. М. Стрельбицька // Юридична Україна. – 2005. – № 4. – С. 64-69; Банківська енциклопедія / За заг. ред. докт. екон. наук, проф. А. М. Мороза. – К.: Фірма «Ельтон», 1993. – С. 22; Гвирцман М. В. Правовое регулирование банковской тайны / М. В. Гвирцман // Деньги и кредит. – 1992. – № 6. – С. 57.

[111] Юридична енциклопедія. – К.: Українська енциклопедія, 1998. – Т 1. – С. 190; Викулин А. Ю. Категории «банковская тайна» и «коммерческая тайна банка» и их соотношение / А. Ю. Викулин // Банковское дело. – 1997. – № 12. – С. 36.

[112] Безклубий І. Поняття банківської таємниці / І. Безклубий // Підприємництво, господарство і право. – 2005. – № 4. – С. 16–19.

[113] Цивільний кодекс України // Відомості Верховної Ради України. – 2003. – № 40-44. – Ст. 356.

бухгалтерської звітності та в інших документах, відомості про кредитну історію клієнта, про зміст і умови кредитного договору та договору про забезпечення виконання зобов'язань тощо.

Безумовно таємниця вкладів, рахунків та операцій по ним і персональні дані клієнтів є елементом таємниці особистого (сімейної) життя і відносяться до персональної інформації про особу, поширення якої без згоди її власника заборонено законодавством. Але поняття *«відомості про клієнта»* є необмеженим і вимагає, законодавчого уточнення.

Обсяг інформації, що становить БТ (не обмежуючи її обсягу, визначеного ЦКУ), конкретизують норми ч. 1 ст. 60 ЗУ «Про банки і банківську діяльність»[114], який є основоположним документом, що визначає правовий режим БТ в Україні. Тут визначено, що *«інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку, є БТ»*.

Повний перелік цієї інформації наступний:

- відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;
- операції, проведені на користь чи за дорученням клієнта, здійснені ним угоди;
- фінансово-економічний стан клієнтів;
- системи охорони банку та клієнтів;
- інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;
- відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша інформація;
- інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

[114] Про банки і банківську діяльність: Закон України від 07.12.2000 р. // Відомості Верховної Ради. – 2001.– № 5-6.– Ст. 30.

- коди, що використовуються банками для захисту інформації.

До цього списку не входить інформація, що підлягає розголосу, а саме: дата реєстрації, кількість балансових філій, кількість працюючих на кінець року, кількість рахунків, валюта балансу, обсяг кредитного портфеля, обсяг вкладів громадян, капітал банку згідно з інструкцією про порядок регулювання та аналіз діяльності комерційних банків, оплачений статутний фонд, сума доходів, сума витрат, прибуток, рентабельність власного капіталу в процентах та інші відомості, що визначаються Державним комітетом статистики України, Національним банком України і самим банком (на власний розсуд) відповідно до законодавства України.

Інформація про банки чи клієнтів, яка збирається під час проведення банківського нагляду, також становить БТ. Можна стверджувати, що до БТ певного банку також належить інформація про клієнтів інших банків, яка стала відома з документів, угод та операцій клієнта банку.

З теоретичної точки зору неоднозначним є визначення місця БТ серед видів ІзОД.

Зміст глави 10 ЗУ «Про банки і банківську діяльність» недостатньо точно розподіляє співвідношення БТ з категорією конфіденційної інформації. Аналіз положень ч. 2 і 3 ст. 61 цього Закону дає підстави вважати, що конфіденційна інформація співвідноситься з БТ як загальне і окреме. Так, назва ст. 61 говорить: *«зобов'язання щодо збереження банківської таємниці*", а в ч. 4 даної статті наголошується, що *«приватні особи та організації, які при виконанні своїх функцій або наданні послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб*».

Отже, можна зробити висновок, що законодавець розглядає БТ не як окремий вид ІзОД, а як підвид конфіденційної інформації.

Також й вчені відносять БТ до конфіденційної інформації: *«БТ є специфічним видом конфіденційної інформації, яка пов'язана з виконанням юридичними особами банківської діяльності та*

приналежністю фізичних осіб до відповідної професії – банківських службовців»[115].

Однак, відповідно до ст. 8 ЗУ «Про доступ до публічної інформації», БТ належить до категорії таємної інформації, в силу своєї назви – таємниця.

Поширення конфіденційної інформації здійснюється за бажанням юридичних і фізичних осіб у володінні, користуванні або розпорядженні яких така інформація знаходиться. А поширення (або розголошення) БТ здійснюється в чітко встановлених законодавством межах, порядку та за оформленим запитом належних суб'єктів.

Володілець (власник) конфіденційної інформації самостійно визначає режим доступу до неї. У той же час порядок доступу та зобов'язання щодо збереження БТ чітко визначені законодавством[116].

Різниця між цими поняттями проводить і сам законодавець. Так, глава 10 ЗУ «Про банки і банківську діяльність» називається «Банківська таємниця та конфіденційність інформації». Тобто, БТ відноситься не тільки до конфіденційної категорії, але й до таємної.

З вище сказаного випливають ***правові ознаки БТ:***

- це конфіденційна інформація, отримана банком від його клієнтів у зв'язку з наданням банківських послуг;
- розголошення інформації, що становить БТ, заборонено законом;
- ця інформація не відноситься до державної таємниці, але є таємною.

Практичний інтерес представляє також *порівняння БТ* з іншого різновидом таємної інформації – *комерційною таємницею* (КТ).

Правовий режим КТ регламентується ГКУ, ЦКУ, ЗУ «Про господарські товариства» та деякими підзаконними нормативними актами. Незважаючи на загальну правову природу БТ і КТ, з практичної

[115] Кормич Б. А. Інформаційне право. Підручник. – Харків: БУРУН і К, 2011. – С. 212.

[116] Гавдьо Ю. Банківська таємниця як окремий вид інформації з обмеженим доступом // Юридичний радник. – 2007. – № 4 (18). – С. 9-12; Тітомер Є. В. Банківська таємниця як предмет кримінально-правової охорони // Актуальні проблеми держави і права: Збірник наукових праць. – 2008. – Вип. 44. – Одеса: «Юридична література». – С. 311–316.

точки зору досить важливим є проведення чіткого розмежування цих двох категорій в чинному законодавстві та в науковій літературі, і виділення принципових відмінностей[117]:

- на відміну від КТ, зміст і обсяг якої встановлюється керівником підприємства на свій розсуд, перелік відомостей, що складають БТ, встановлений ЗУ «Про банки і банківську діяльність». Це, до речі, і об'єднує банківську і державну таємницю, оскільки склад і обсяг останньої, також визначений на рівні закону;
- БТ складають чужі відомості, тобто відомості про клієнтів і кореспондентів банку, що знаходяться в банку на правовому титулі володіння. Тому банк не має права використовувати і розпоряджатися такими відомостями без спеціальної згоди клієнта. У той самий час відомості, що становлять КТ банку, знаходяться у власності банку;
- правовий режим КТ визначається ГКУ та ЦКУ, а правовий режим БТ визначається ЗУ «Про банки і банківську діяльність».

Отже, БТ є окремим самостійним видом таємниці, що належить до ІзОД.

§5.2. Організаційно-правовий захист банківської таємниці

Режим БТ – це правовий механізм її захисту, який ґрунтується на законодавчих підставах обмеження доступу до інформації, що становить таємницю, чіткої регламентації процесу обороту цієї інформації (отримання, засекречування, збереження, передачі, розсекречення та ін.). Саме ця складова БТ та її практична реалізація має багато спільного з режимами комерційної, службової та професійної таємниць.

Специфічні риси правового режиму БТ полягають у тому, що його встановлення не вимагає додаткового оформлення локальними актами.

[117] Тітомер Є. В. Банківська таємниця як предмет кримінально-правової охорони // Актуальні проблеми держави і права: Збірник наукових праць. – 2008. – Вип. 44. – Одесса: «Юридична література». – С. 311-316

Конкретні шляхи реалізації *організаційно-правового захисту БТ* згідно зі ст. 61 ЗУ «Про банки і банківську діяльність» полягають у наступному:

- обмеження кола осіб, що мають доступ до інформації, що становить БТ;
- організація спеціального діловодства з документами, що містять БТ;
- застосування технічних засобів щодо запобігання несанкціонованого доступу до електронних та інших носіїв інформації;
- застосування застережень щодо збереження БТ та відповідальності за її порушення в договорах і угодах між банком і клієнтом.

З метою *запобігання несанкціонованому доступу* до інформації, що містить БТ, суб'єкти, які мають доступ до такої інформації, у власних інструкціях з діловодства встановлюють особливий порядок реєстрації, використання, зберігання та доступу до документів, що містить БТ[118].

При обробці вихідних документів виконавець документа визначає потребу проставляння на ньому *грифу «Банківська таємниця»,* з урахуванням вимог ст. 1076 ЦКУ та ст. 60 ЗУ «Про банки і банківську діяльність».

Гриф «Банківська таємниця» не проставляється на документах, які банки надають клієнтам − власникам інформації, яка містить БТ. Забороняється відправлення документів з грифом «Банківська таємниця» з використанням факсимільного зв'язку або іншими каналами зв'язку, що не забезпечують захист інформації.

Роздруківка документів з грифом «Банківська таємниця» у технологічних автоматизованих робочих місцях (АРМ) здійснюється згідно з технологічними схемами роботи відповідних АРМ банку. На роздрукованих документах проставляється гриф «Банківська таємниця», і вони обліковуються відповідно до вимог з обліку паперових документів.

---

[118] Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова Національного банка від 14.07.2006 р. // Офіційний вісник України. – 2006. – № 32. – С. 137. – Ст. 2330.

Важливим елементом правового режиму БТ є законодавчо визначений *порядок розкриття банкам* БТ, який встановлений ст. 62 ЗУ «Про банки і банківську діяльність».

Порядок розголошення банкам інформації, яка містить БТ, можна умовно показати трьома основними елементами[119] *(рис. 5.1)*.

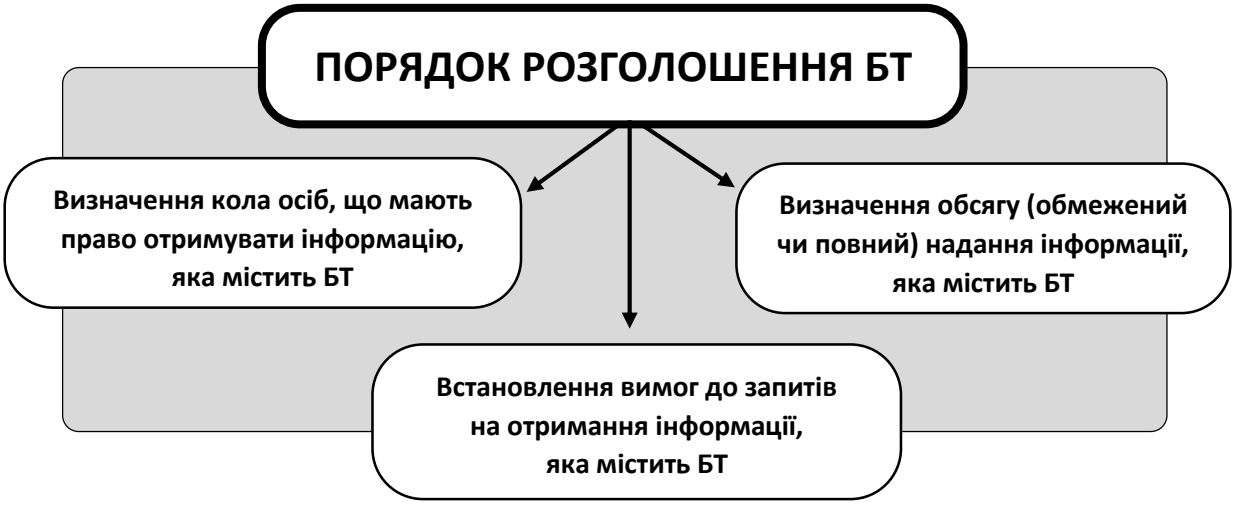

Рис. 5.1. Основні елементи процедури розголошення БТ

Коло осіб або перелік суб'єктів, які мають право вимагати безпосередньо від банку в тому чи іншому обсязі розкриття інформації, що містить БТ, є вичерпним і певним ст. 62 ЗУ «Про банки і банківську діяльність», а саме:

- власник такої інформації;
- суд (на його рішенню);
- органи прокуратури України, СБУ, Міністерства внутрішніх справ України, Національне антикорупційне бюро України, Антимонопольний комітет України;
- центральний орган виконавчої влади, що реалізує державну податкову політику;
- центральний орган виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму;

[119] Ємельянов С. Л. Основи інформаційної безпеки: Навчальний посібник / С. Л. Ємельянов. – Одеса: «Фенікс», 2014. – С. 139-150.

- органи державної виконавчої служби;
- Національна комісія з цінних паперів та фондового ринку;
- Національне агентство з питань запобігання корупції;
- інші банки;
- інші особи, зазначені власником рахунку (вкладу) в заповідальному розпорядженні банку;
- Фонд гарантування вкладів фізичних осіб;
- державні нотаріальні контори чи приватні нотаріуси, іноземні консульські установи по справах спадщини за рахунками (вкладами) померлих власників рахунків (вкладів);
- службовці Нацбанку України або уповноважені ними особи;
- особа (у тому числі, уповноважена діяти від імені держави), на користь якої відчужуються активи та зобов'язання, банку при виконанні заходів, передбачених програмою фінансового оздоровлення банку, або під час здійснення процедури ліквідації.

Цей перелік суб'єктів БТ є повним і вичерпним, що свідчить про те, що інші фізичні та юридичні особи, в тому числі і державні органи, мають право отримувати відповідну інформацію виключно за рішенням суду, а не безпосередньо в банку.

Однак аналіз норм спеціального законодавства та матеріалів судової практики свідчить, що право вимагати від банків розкриття інформації, яка містить БТ, мають також інші, прямо не зазначені в законі суб'єкти владних повноважень.

Так, Рахункова палата України в межах повноважень, визначених у ч. 5 ст. 7 ЗУ «Про Рахункову палату» може *«отримувати від Національного банку України, уповноважених банків та інших кредитних установ необхідні відомості про здійснювані ними операції та стан рахунків установ та організацій, що перевіряються, від інших підприємств і організацій – довідки, копії документів по операціях і рахунках цих підприємств та організацій»*[120].

[120] Про Рахункову палату: Закон України від 11.07.1996 р. // Відомості Верховної Ради. – 1996.– № 43. – Ст. 212.

Відповідно зі ст. 12 ЗУ «Про організаційно-правові основи боротьби з організованою злочинністю» створена система спеціальних органів, які здійснюють боротьбу з організованою злочинністю. Вони мають право «*одержувати від банків, а також кредитних, митних, фінансових та інших установ, підприємств, організацій (незалежно від форм власності) інформацію і документи про операції, рахунки, вклади, внутрішні та зовнішні економічні угоди фізичних і юридичних осіб*»[121].

Отже, з усіх зазначених спеціальних законів випливає, що відповідні державні органи мають право отримувати від банків інформацію, яка містить БТ, але тільки на підставі та в межах ЗУ «Про банки і банківську діяльність», в якому ці суб'єкти не вказані, що й обумовлює цей проблемний аспект.

Аналогічна ситуація склалася ще з одним суб'єктом, який має право на запит (звернення) в Національний банк України про надання інформації, що містить БТ – народні депутати України, якщо це пов'язано з їх депутатською діяльністю, і комітети Верховної Ради України, якщо це стосується їх законопроектної роботи[122].

Іншою проблемою в порядку розкриття БТ стосується визначення *обсягу надання інформації*, яка містить БТ. Аналіз норм чинного законодавства показує, що розкриття інформації, яка містить БТ, зазначеним вище суб'єктам може здійснюватися *(рис. 5.2):*

- ***в повному обсязі*** БТ розкривається банком:

1) за письмовим запитом або з письмового дозволу власника такої інформації;

2) на письмову вимогу суду або за рішенням суду;

3) спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу (в тому числі без їх письмового запиту щодо фінансових операцій, що стали об'єктами фінансового моніторингу);

[121] Про організаційно-правові основи боротьби із організованою злочинністю: Закон України від 30.06.1993 р. // Відомості Верховної Ради .– 1993.– № 35. – Ст. 358.

[122] Рішення Конституційного суду України № 5-рп/2003 від 05.03.2003 р.(справа про звернення народних депутатів України до Національного банку України) // Урядовий кур'єр. – 2003. – № 51.

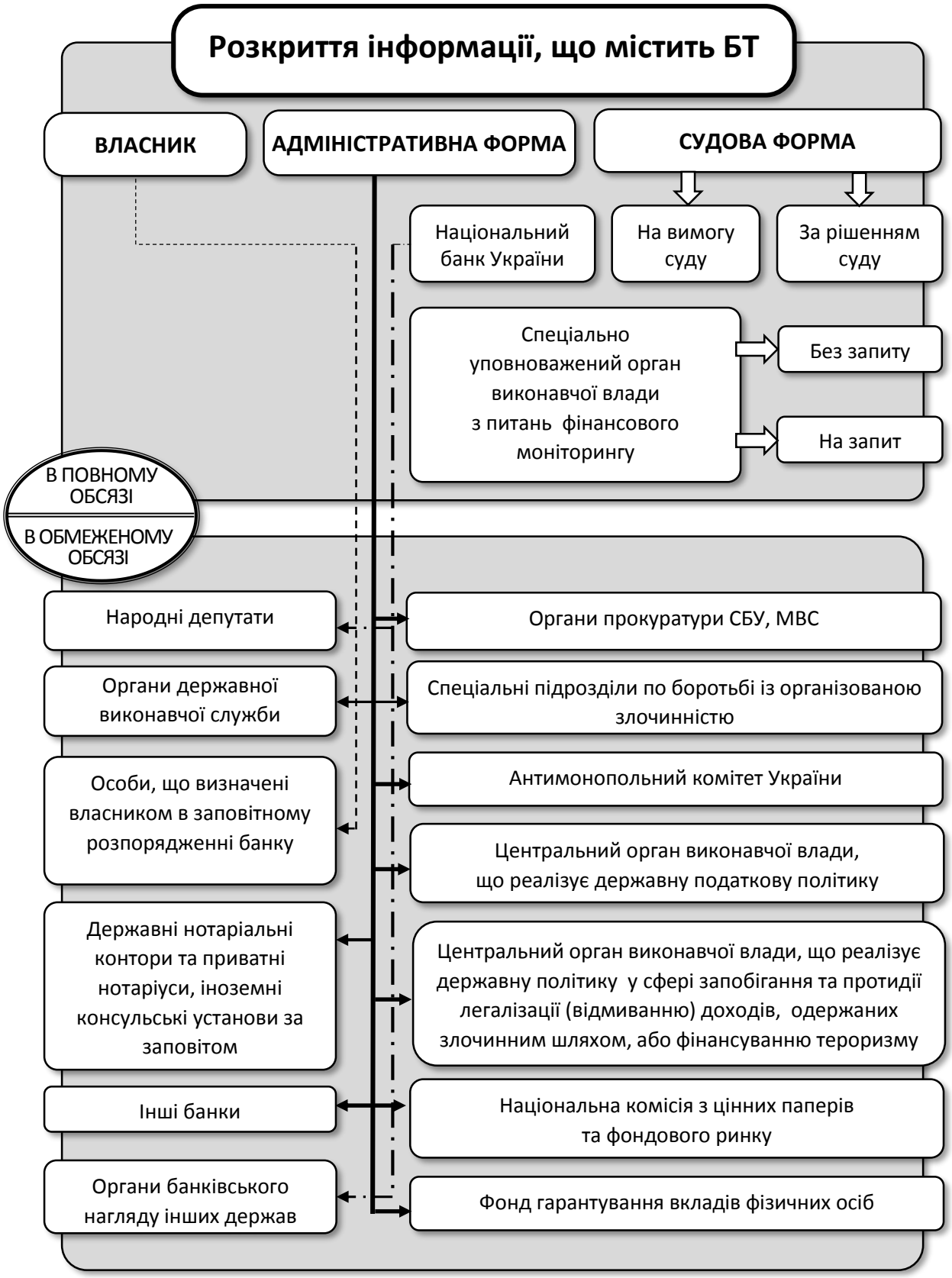

Рис. 5.2. Розкриття інформації, що містить БТ

4) на вимогу службовців Національного банку України або уповноважених ними осіб, в рамках, наданих ЗУ «Про Національний банк України»[123] повноважень, які здійснюють функції банківського нагляду або валютного контролю.

- ***в обмеженому обсязі*** (в межах повноважень кожного з суб'єктів звернення, за конкретний проміжок часу і тільки щодо операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єктів незалежно від підприємницької діяльності) на письмову вимогу органів, визначених ст. 62 ЗУ «Про банки та банківську діяльності».

Інформація, яка містить БТ в відношенні фізичної особи – громадянина, котрий не є суб'єктом підприємницької діяльності, може бути розкрита банком виключно на письмову вимогу суду або за рішенням суду. Отже, законом не передбачається, щоб зазначені вище суб'єкти на їх письмову вимогу, отримували від банків таку інформацію в повному об'ємі.

Щодо третього елементу в процедурі розкриття БТ – встановлення вимог до запитів державних органів на отримання інформації, яка містить БТ, то вони викладені в ч. 2 ст. 62 ЗУ «Про банки і банківську діяльність». Так, вимога відповідного державного органу на отримання інформації, яка містить БТ, повинна:

- бути викладена на бланку державного органу встановленої форми;
- бути подана за підписом керівника державного органу (або його заступника), скріпленим гербовою печаткою;
- містити передбачені законом підстави для отримання цієї інформації;
- містити посилання на норми спеціальних законів, відповідно до яких державний орган має право на отримання такої інформації.

Певні суперечності в цьому елементі полягають в тому, що відповідні державні органи зобов'язані використовувати тільки

[123] Про Національний банк України: Закон України від 20.05.1999 р. // Відомості Верховної Ради. – 1999. – № 29. – Ст. 238.

паперову форму запиту інформації від банку, але останнім дозволяється надавати цю інформацію, як в паперовому вигляді, так і в електронному. Хоча «*передача інформації, яка містить БТ, електронною поштою або в режимі on-line здійснюється лише в захищеному (зашифрованому) вигляді з контролем цілісності та з обов'язковим наданням підтвердження про її надходження з електронним підписом одержувача з використанням засобів захисту*»[124].

Слід також зазначити, що режим таємності певного обсягу банківської інформації, що входить до складу БТ, має кінцевий, а не абсолютний характер. Припинення режиму конфіденційності даної інформації пов'язується з настанням певної події в часі, а саме: на стадії ліквідації банку, призначення ліквідатора, відомості про фінансове становище банку перестають бути конфіденційними чи становити БТ. Проте решта відомостей, що становлять БТ, зберігають режим таємниці, навіть після завершення угоди про банківське обслуговування клієнта.

Щодо ***третьої складової правового інституту*** *БТ* – ***санкцій***, зазначимо таке: основними видами відповідальності за розголошення БТ є дисциплінарна, цивільно-правова і кримінальна.

До посадових і службових осіб банків можуть бути застосовані заходи ***дисциплінарної відповідальності***, згідно із загальним трудовим законодавством, або спеціальним законодавством, яке визначає правовий статус тих чи інших категорій осіб, наприклад, державних службовців.

Застосування одного з видів відповідальності (наприклад, дисциплінарної) не виключає можливості застосування та інших її видів (цивільно-правової, кримінальної).

У разі розголошення банком відомостей, що становлять БТ, клієнт має право вимагати від банку відшкодування завданих збитків та моральної шкоди. Положення ч. 1 ст. 22 ЦКУ[125] встановлюють

[124] Про затвердження правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова Правління Національного банку України від 14 липня 2006 р. № 267 // Офіційний вісник України. – 2006. – № 32. – Ст. 2330.

[125] Цивільний кодекс України // Відомості Верховної Ради України. – 2003. – № 40-44. – Ст. 356.

загальне правило про право особи на відшкодування збитків, завданих порушенням її цивільного права.

В ч. 2 ст. 22 ЦКУ законодавець розділяє збитки на два види:

- *реальний збиток* – втрати, які особа понесла в зв'язку з знищенням або пошкодженням речі, а також витрати, які особа зробила або мусить зробити для відновлення свого порушеного права;
- *втрачена вигода* – доходи, які особа могла отримати при звичайних обставинах, якби її право не було порушене.

Відповідно до ч. 4 ст. 61 ЗУ «Про банки і банківську діяльність», у разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, уповноважених здійснювати банківський нагляд, збитки відшкодовуються винними органами.

Що стосується ***кримінальної відповідальності***, то вона настає відповідно до чинного ККУ за вчинення таких злочинів, як «*незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю*» (ст. 231) та «*розголошення комерційної або банківської таємниці*» (ст. 232).

Слід зауважити, що притягнення особи до кримінальної відповідальності за ст. ст. 231, 232 ККУ можливо тільки у випадку, якщо використання чи розголошення відомостей, що становлять БТ, завдало істотної шкоди суб'єкту господарювання. Під «*істотною*» слід розуміти шкоду, яка в 100 і більше разів перевищує неоподатковуваний мінімум доходів громадян. Максимальне покарання, передбачене ст. 231 ККУ, – позбавлення волі на строк до трьох років, а за ст. 232 – позбавлення волі на строк до двох років.

На підставі проведеного аналізу, можна побудувати концептуальну модель захисту БТ *(рис. 5.3)*.

Отже, БТ є самостійним видом ІзОД і має свій специфічний режим захисту, не тотожний ніякому іншому правовому режиму конфіденційності.

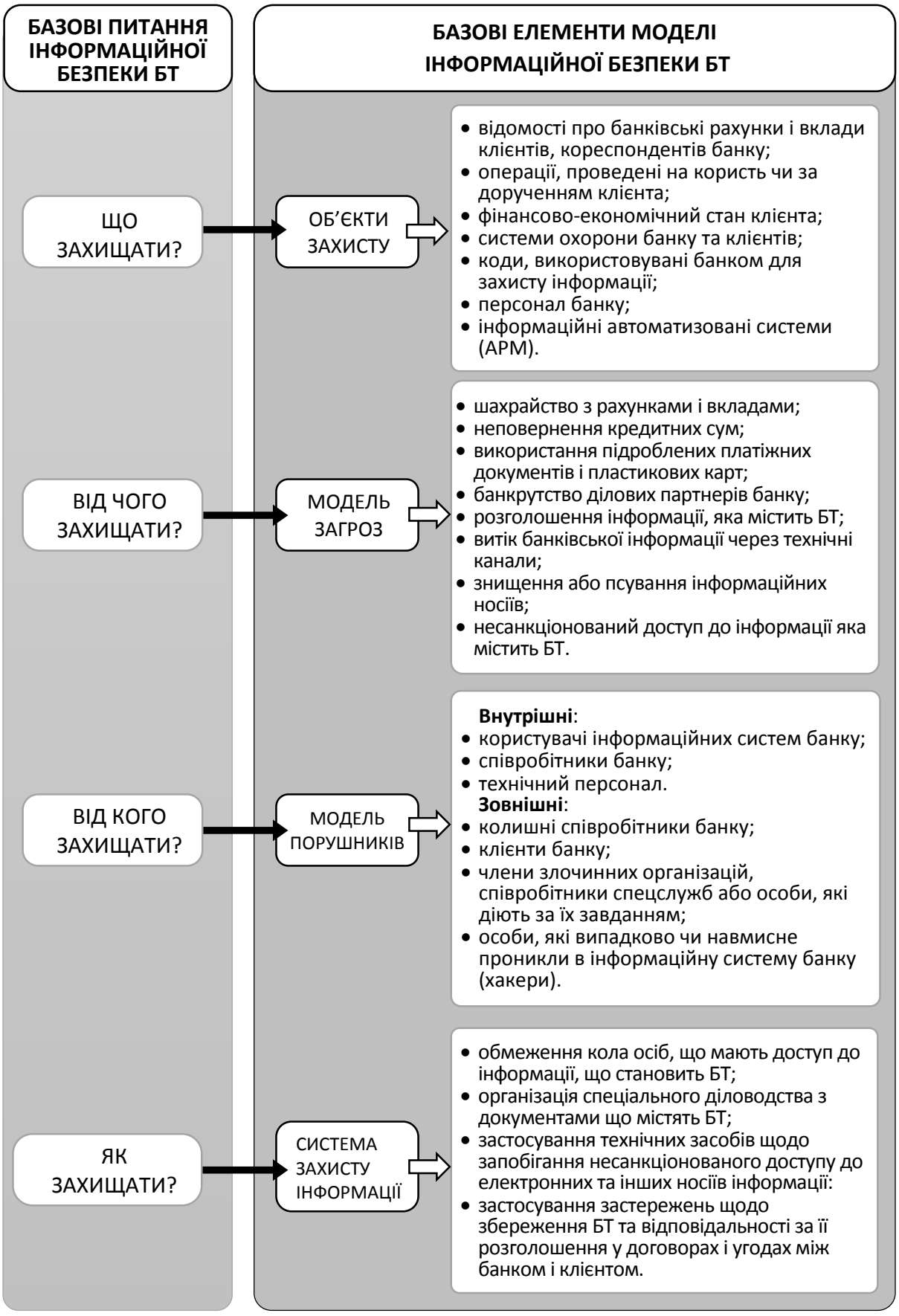

Рис. 5.3. Концептуальна модель захисту БТ

§5.3. Поняття і ознаки комерційної таємниці

Аналогічно розглянутим двом таємницям, правовий інститут комерційної таємниці (КТ) в Україні також представлений трьома складовими[126].

Щодо *першої складової* слід відзначити, що в світі не існує єдиного підходу до визначення поняття КТ. Застосовуються різні визначення інформації, що містить КТ[127]: «*ділові таємниці*», «*виробничі таємниці*», «*торговельні таємниці*», «*ноу – хау*» та інші. В Україні всі вищевказані види таємниць об'єднані в один узагальнюючий термін – КТ, який знайшов своє відображення у чинному законодавстві, хоча й неоднозначне.

В ст. 505 ЦКУ КТ – «*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*».

У наведеному визначенні КТ викликає сумнів термін «секретна інформація», який не вписується в традиційну класифікацію інформації в українському законодавстві (ст. 8 ЗУ «Про доступ до публічної інформації»). Секретною (таємною) інформацією є інформація, яка становить державну, професійну, БТ та ін. КТ являє собою вид конфіденційної інформації.

Нормами ст. 506 ЦКУ передбачено виключне право власника інформації, що становить КТ на встановлення режиму доступу до цієї інформації, надання права на використання та перешкоджання розголошенню, збиранню та використання.

---

[126] Ємельянов С. Л. Основи інформаційної безпеки: Навчальний посібник / С. Л. Ємельянов. – Одеса: «Фенікс», 2014. – С. 150–159.

[127] Брединский А. Правовой режим защиты коммерческой тайны в США и Великобритании / А. Брединский. – [Електронний ресурс].– Режим доступу: http://www.real-voice.info/modules/myarticles/article.php?storyid=503.

Тобто суб'єктом визначення доступу до інформації, яка містить КТ, є власник відповідної інформації або особа, якій надано права розпоряджатися цією інформацією.

Глава 46 ЦКУ встановлює майнові права інтелектуальної власності на КТ, охорону КТ органами державної влади, а також термін дії права інтелектуальної власності на КТ.

Ст. 162 ГКУ[128] трохи дає дещо інакше визначення КТ, включаючи її до об'єктів прав інтелектуальної власності: «*технічна, організаційна або інша комерційна інформація ... 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 з охорони її конфіденційності*».

На рівні окремого закону визначення конкретних сфер або видів господарської діяльності і категорій (перелік) відомостей, які можуть становити КТ, в Україні досі не існує. Згідно зі ст. 36 ГКУ склад і обсяг відомостей, що становлять КТ і спосіб їх захисту, самостійно визначаються суб'єктом господарської діяльності.

У той же час, відповідно до ч. 2 ст. 505 ЦКУ, певні відомості «*технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих з них, які відповідно до закону не можуть бути віднесені до КТ, можуть становити КТ*».

Не може бути віднесена до КТ інформація, що відповідно до ЗУ «Про інформацію» підпадає під режим ДТ або, навпаки, відкритої інформації, наприклад, правила страхування, розроблені страховиком (ЗУ «Про страхування»[129]).

Так само не можуть становити КТ відомості, які підлягають обов'язковому опублікуванню, наданню на запит необмеженого кола зацікавлених осіб, а також відомості, про які в законодавстві міститься пряма заборона на поширення на них режиму обмеженого доступу. Наприклад, ЗУ «Про бухгалтерський облік та фінансову звітність в

[128] Господарський кодекс України // Відомості Верховної Ради. – 2003.– № 18-22. – Ст. 144.

[129] Про страхування: Закон України від 07.03.1996 р.// Відомості Верховної Ради. – 1996.– № 18. – Ст. 78.

Україні»[130] передбачає, що фінансова звітність підприємств не становить КТ, крім випадків, передбачених законодавством. В ЗУ «Про сертифіковані товарні склади та прості і подвійні складські свідоцтва»[131] закріплена норма про те, що регламент сертифікованого складу не може становити КТ.

Перелік відомостей, що не становлять КТ, наведено не в законі, а в підзаконному акті[132], який був прийнятий для виконання ЗУ «Про підприємства в Україні», і втратив чинність у зв'язку з прийняттям ГКУ.

Це також свідчить про необхідність перегляду переліку на предмет відповідності існуючим реаліям розвитку конкурентного ринкового середовища.

Щодо принципів та критеріїв віднесення інформації до КТ також існують певні труднощі, тому однією з ознак КТ є *комерційна цінність*, тобто цінова визначеність (вартість) такої інформації, методику підрахунку якої в кількісному вимірі до цих пір не розроблено.

Інформація, складова КТ, повинна бути предметом адекватних існуючим обставинам заходів щодо збереження її конфіденційності, вжитих особою, яка законно контролює цю інформацію.

Як форму КТ можна розглядати *комерційні таємниці*, які є інформацією у вигляді документів, схем, виробів. Вони підлягають захисту від можливого посягання через викрадення, вивідування, витік інформації.

Їх розрізняють за такими ознаками[133]:

- за природою КТ (технологічні, виробничі, організаційні, маркетингові, інтелектуальні, рекламні);
- за власністю (власність підприємства, групи підприємств, окремої особи, групи осіб тощо);

---

[130] Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16.07.1999 р.// Відомості Верховної Ради. – 1999.– № 40. – Ст. 365.

[131] Про сертифіковані товарні склади та прості і подвійні складські свідоцтва: Закон України від 23.12.2004 р. // Відомості Верховної Ради. – 2005.– № 6. – Ст. 136.

[132] Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 09.08.1993 р. № 611. – [Електронний ресурс].– Режим доступу: http://zakon4.rada.gov.ua/laws/show/611-93-п.

[133] Юсупова Д. Комерційна таємниця як об'єкт трудових відносин: поняття та ознаки / Д. Юсупова // Публічне право. – № 2(10). – 2013. – С. 336-343.

- за колом осіб, які мають до них доступ;
- за призначенням.

Інформація, яку можна віднести до КТ, повинна містити наступні *ознаки*: не бути державною таємницею (секретними даними); стосуватися торгово-виробничої діяльності підприємства; не завдавати шкоди інтересам суспільства; мати комерційну цінність та створювати переваги в конкурентній боротьбі; мати встановлені власником інформації обмеження в доступі.

До числа основних *об'єктів правовідносин КТ* відносяться[134]:

- **володілець КТ:** фізична або юридична особа, що володіє на законній підставі інформацією, що становить КТ;
- **конфідент КТ:** фізична або юридична особа, якій в силу службового становища, договору або на іншій законній підставі відома КТ іншої особи;
- **носії КТ:** матеріальні об'єкти, в тому числі і фізичні поля, в яких інформація, складова КТ, знаходить відображення у вигляді символів, сигналів, технічних рішень і процесів.

Отже, до ***правових ознак КТ*** можна віднести:

- конфіденційність інформації, що є КТ, яка полягає в тому, що вона є невідомою та не є легкодоступною;
- інформація, складова КТ, має комерційну цінність (цінову визначеність);
- склад і обсяг відомостей, що становлять КТ, визначені суб'єктом господарювання або уповноваженим на це органом;
- власник КТ повинен застосовувати відповідні засоби для охорони цієї інформації.

§5.4. Захист комерційної таємниці

Щодо *другої складової правового інституту КТ* (режиму таємності) слід зазначити, що згідно зі ст. 20 редакції ЗУ «Про інформацію» КТ відноситься до ІзОД. При цьому конфіденційна інформація − це відомості, які знаходяться у володінні, користуванні

[134] Копылов В. А. Информационное право / В. А. Копылов. – М.: Юрист, 2002.– С. 221

або розпорядженні окремих фізичних чи юридичних осіб і поширюється за їх бажанням відповідно до передбачених ними умов.

КТ постійно піддається різним загрозам, під якими розуміється окремі явища, події, процеси, настання яких може вплинути на захищеність КТ і привести до негативних наслідків (прямих збитків, неотримання прибутку, підриву іміджу, зміна в планах, тимчасових втрат та ін.).

Класифікація загроз КТ представлена різними ознаками і критеріями[135] *(таблиця 6.1)*.

Таблиця 6.1.

Класифікація загроз КТ

Критерії	**Різновиди**
За джерелами загрози	Зовнішні (промислове шпигунство, незаконні дії конкурентів, крадіжка матеріальних цінностей);внутрішні (розголошення працівниками конфіденційної інформації, низька мотивація персоналу, низька ефективність діяльності служби безпеки).
За ступенем тяжкості наслідків	Загрози з високою тяжкістю наслідків призводять до різкого погіршення всіх фінансово-економічних показників та припинення діяльності фірми; середньої – подолання наслідків вимагає великих витрат, але не вимагає тривалого часу; низькою – не завдають значної деструктивного впливу.
За ступенем імовірності загрози	Малоймовірні небезпеки (потенційні), які потенційно не мають реальної можливості наступити; реальні.
За стадії функціонування підприємства	На стадії створення підприємства; на стадії функціонування.
За об'єктом посягань	Інформаційні; фінансові; матеріальні; загрози престижу, авторитету, іміджу підприємства.
По суб'єкту загроз	Загрози з боку організованих злочинних угруповань; недобросовісних конкурентів; власних працівників; державних структур.
За характером напрямку	Прямі; непрямі.
По об'єкту напрямку	Виробничі таємниці; відомості про фінансову діяльність; відомості про управління; відомості про клієнтів і т. д.
За тривалістю дії	Тимчасові; постійні.

[135] Лічман Т. В. Класифікація та аналіз загроз безпеці комерційної таємниці підприємства / Т. В. Лічман // Вісник ОНУ ім. І. І. Мечникова. – 2013. – Т. 18. – Вип. 1/1. – С. 230-233.

Критерії	Різновиди
За рівнем суб'єктивного сприйняття	Неусвідомлені; із завищеним (заниженим) рівнем сприйняття; мнимі; адекватні.
При наявності людського фактору	Пов'язані з діяльністю людини; не пов'язані з діяльністю людини
За характером відповідальності суб'єктів загроз щодо їх наслідки	Дисциплінарна, цивільно-правова, адміністративна, кримінально-правова.
По виду збитків	Прямі; упущена вигода

Система захисту повинна комплексно поєднувати правові, організаційні, технічні та інші заходи, які приймає власник КТ з охорони її конфіденційності[136] *(рис. 5.4)*.

Рис. 5.4. Заходи по забезпеченню захисту КТ

Слід зазначити, що в умовах недосконалості чинного законодавства щодо КТ і з урахуванням останніх тенденцій світового досвіду багато фахівців вважають, що основних в реалізації правового

[136] Кришталюк А. Н. Защита коммерческой тайны: Курс лекций. – [Електронний ресурс].– Режим доступу: http://nauka2020.ru/Krishtaluk_40213.pdf.

механізму захисту КТ доцільно перенести *в сферу локальних нормативно-правових актів і правового регулювання відносин в сфері «роботодавець-працівник»*.[137]

Зокрема, в якості таких актів можуть розглядатися: Статут підприємства; Установчий договір; Колективний договір; Правила внутрішнього розпорядку, посадові інструкції тощо. На підставі вище викладеного можна побудувати концептуальну модель захисту КТ *(рис. 5.5)*.

Щодо ***третьої складової інституту КТ*** зазначимо, що за порушення права суб'єкта господарської діяльності на КТ до винної особи може бути застосована юридична відповідальність різної приналежності:

- *цивільно-правова відповідальність* в вигляді відшкодування збитків, заподіяних суб'єкту, на підставі ГКУ;
- *дисциплінарна і матеріальна відповідальність* , передбачена КЗпПУ;
- *адміністративна відповідальність* , встановлена ч. 3 ст. 164-3 КУпАП;
- *кримінальна відповідальність* в Згідно зі ст. ст. 231, 232 ККУ.

Крім цього, адміністративно-господарські штрафи передбачені за недобросовісну конкуренцію у вигляді неправомірного збору, розголошення, схилення до розголошення та використання КТ (Глава 4 ЗУ «Про захист від недобросовісної конкуренції»[138]).

Адміністративна відповідальність юридичних і фізичних осіб за отримання, використання, розголошення КТ передбачена, по-перше, ст. 164-3 «Недобросовісна конкуренція» КУпАП, а також ст. 16 «Неправомірне збирання КТ», ст. 17 «Розголошення КТ», ст. 18 «Схиляння до розголошення КТ» і ст. 19 «Неправомірне використання КТ» ЗУ «Про захист від недобросовісної конкуренції».

---

[137] Сляднєва Г. О. Право суб'єкта господарювання на комерційну таємницю та його захист: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.04 «Господарське право» / Г. О. Сляднєва. – Донецьк, 2005. – 19 с.; Янина Е. В. Актуальные вопросы информационной безопасности: защита коммерческой тайны хозяйствующего субъекта в рамках локального нормативного акта / Е. В. Янина // Актуальные проблемы современной науки. – 2003. – № 2.– С. 109-111.

[138] Про захист від недобросовісної конкуренції: Закон України від 07.06.1996 р. // Відомості Верховної Ради.– 1996. – № 36. – Ст. 164.

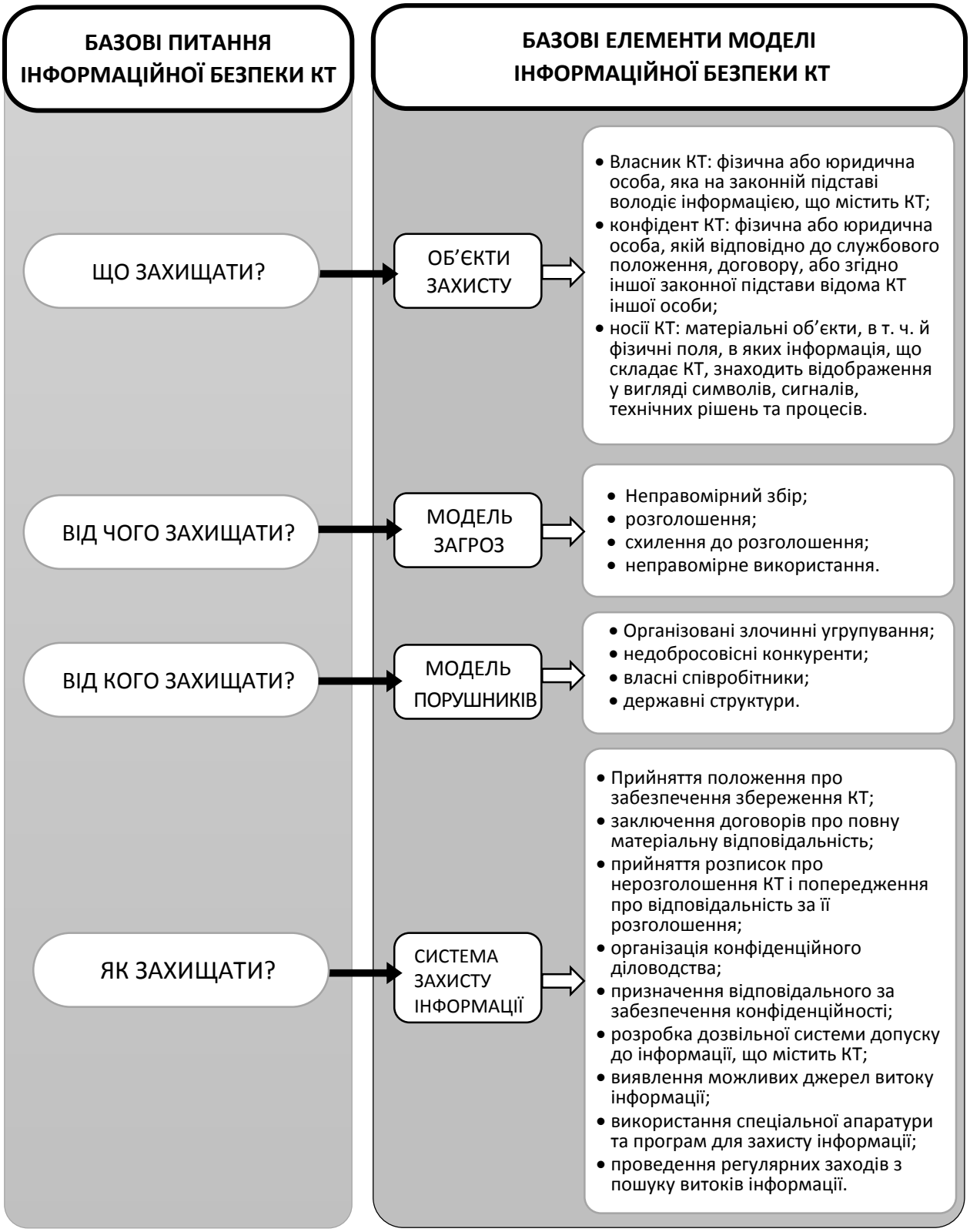

Рис. 5.5. Концептуальна модель захисту КТ

Неправомірним збиранням КТ вважається добування протиправним способом відомостей, відповідно до законодавства України КТ, якщо це завдало чи могло завдати шкоди суб'єкту господарської діяльності.

Розголошенням КТ є ознайомлення іншої особи без дозволу особи, уповноваженої на те, з відомостями, які відповідно до законодавства України КТ складають КТ, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням відповідних обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

*Схилянням до розголошення КТ я*вляється примус особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням відповідних обов'язків відомості, які відповідно до законодавства України становлять КТ, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

Неправомірним використанням КТ є впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу уповноваженої на те особи відомостей, що становлять відповідно до законодавства України КТ.

Кримінальна відповідальність за порушення законодавства про захист КТ передбачена в розділі VII ККУ – «*Злочини у сфері господарської діяльності*». Так, ст. 231 ККУ передбачає притягнення до відповідальності за такі злочинні дії як незаконне збирання з метою використання або використання відомостей, що становлять КТ. Злочином у сфері посягань на КТ є її розголошення (ст. 232 ККУ).

Зазначені злочинні дії відбуваються у відношенні предмета злочину і для отримання переваг в конкурентній боротьбі всупереч волі власника КТ і наносять останньому істотну шкоду, тим самим посягаючи на відносини добросовісної конкуренції.

Зараз у Верховній Раді України триває розгляд двох законопроектів: № 5180 «Про комерційну таємницю» та № 5180-1 «Про основні положення охорони комерційної таємниці в Україні»[139], в яких законодавець спробує усунути деякі з зазначених недоліків.

Однак, незважаючи на їх окремі позитивні аспекти, жоден з цих актів не відповідає повністю Концепції проекту ЗУ «Про охорону прав

[139] Гончар И. Режим коммерческой тайны. Анализ правового статуса института коммерческой тайны в аспекте его реформирования.– [Електронний ресурс].– Режим доступу: http://www.e-news.com.ua/print/124720.html.

на комерційну таємницю»[140]. Остання визначає в якості основних завдань:

- проведення та систематизація законодавства з питань КТ, його уточнення та доповнення;
- забезпечення єдиного підходу до охорони КТ як складової законодавства з питань інтелектуальної власності;
- визначення правових основ віднесення інформації до КТ;
- встановлення відповідальності за порушення прав інтелектуальної власності на КТ та ін.

Отже, в Україні створено основні елементи правового інституту КТ, але відсутній єдиний правовий механізм захисту КТ, хоча тенденції його розвитку цілком позитивні та відповідають світовим стандартам.

Висновки

БТ та КТ є окремими самостійними видами таємниць, що належать до ІзОД.

БТ – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку.

КТ – відомості економічного, виробничого, технічного, організаційного характеру, що стали відомі працівнику в процесі виконання ним посадових обов'язків, які зберігаються в таємниці, а їх розголошення має спричинити для працівника негативні наслідки згідно із законом.

Основними видами відповідальності за розголошення цих видів таємниць є дисциплінарна, цивільно-правова та кримінальна відповідальність.

[140] Концепція проекту Закону України «Про охорону прав на комерційну таємницю».– [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1404-2008-%F0.

6 ТАЄМНИЦЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА СУДОЧИНСТВА

§6.1. Поняття та правові ознаки таємниці досудового розслідування

Одним з видів таємниць, прямо зазначених у ч. 1 ст. 8 ЗУ «Про доступ до публічної інформації»[141] є ***таємниця досудового розслідування*** (ТДР).

ТДР є різновидом професійної таємниці та однією з умов, що сприяє успішному розкриттю злочинів і викриттю обвинуваченого. Передчасне її розголошення може негативно вплинути на хід розслідування, надасть можливість обвинуваченому приховати або знищити сліди злочину, предмети і документи, які можуть стати доказами, ухилитися від слідчого та судді, іноді також заподіяти шкоду обвинуваченому, потерпілому та іншим особам[142].

Побудова демократичного та правового суспільства передбачає необхідність правового захисту особистості та сімейної таємниці громадян, відомості про яких можуть бути отримані в ході досудового розслідування на підставі гласних або негласних оперативно-розшукових заходів, які проводять органи, що здійснюють дізнання і досудове слідство.

До основних фундаментальних прав людини, які в результаті застосування кримінально-процесуального законодавства та інших нормативно-правових актів в процесі досудового розслідування підлягають безпосередньому захисту, Конституція України відносить такі права:

- на життя (ст. 27);
- на свободу та особисту недоторканність (ст. 29);

---

[141] Про доступ до публічної інформації: Закон України від 13.01.2011 р. // Відомості Верховної Ради – 2011. – № 32. – Ст. 314.

[142] Ємельянов С. Л. Таємниця слідства та судочинства в України / С. Л. Ємельянов // Ученые записки Таврического национального университета им. В. И. Вернадского. – Серия «Юридические науки». – Том 26 (65). – 2013. – № 2-1 (Ч. 2). – С. 310–316.

- на недоторканність житла (ст. 30);
- на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31);
- на недоторканність приватного та сімейного життя (ст. 32);
- на свободу пересування, вільного вибору місця проживання (ст. 33);
- на свободу думки і слова, на вільне вираження своїх поглядів і переконань (ст. 34);
- на судовий захист (ст. 55);
- на правову допомогу (ст. 59);
- не доводити свою невинуватість у вчиненні злочину (ст. 62);
- не свідчити проти самого себе, членів сім'ї та чи близьких родичів (ст. 63) та ін.

В процесі забезпечення прав і свобод людини та громадянина необхідно враховувати, що при реалізації органами досудового розслідування законодавчих норм про захист прав і законних інтересів учасників кримінального процесу виникають суперечності, зумовлені різними інтересами суб'єктів цих прав, інших осіб, суспільства і держави в цілому. При цьому необхідно враховувати положення ст. ст. 1, 2 і 7 Загальної декларації прав людини, які покликані однаково захищати як права особистості, що здійснила злочин, так і права особистості, що стала жертвою злочину, а також інтереси суспільства і держави, в цілому, виступаючого в якості інструменту, що реалізує державну функцію захисту прав особистості і суспільства[143].

Правовий інститут ТДР містить:

- **загальну частину:** визначення, принципи і критерії відносини інформації до ТДР, правові ознаки ТДР;
- **режим ТДР:** механізм обмежень доступу до даних, що становить ТДР;
- **санкції** за неправомірне використання відомостей, що становлять ТДР.

[143] Гаврилов Б. Я. Реализация органами предварительного следствия правовых норм о защите конституционных прав и свобод человека и гражданина. – [Електронний ресурс]. – Режим доступу: http://www.cfin.ru/press/black/2001-1/05_01_gavriloff.shtml.

Розглянемо першу складову правового інституту ТДР.

Точного визначення поняття ТДР немає ні в законодавстві України, ні в юридичній літературі. Далі наведемо різні підходи до визначення терміну «таємниця досудового розслідування».

ТДР – це обмежені терміном досудового розслідування відомості, що стосуються обставин, які підлягають доведенню в кримінальній справі та що знаходяться в провадженні слідчого, приховувані від інших, відомі не всім, і які можуть бути розголошені в суді лише з дозволу слідчого[144].

ТДР – службова інформація, що створюється та збирається в системі діяльності з виявлення та розкриття злочинів, і використовується співробітниками правоохоронних органів, що здійснюють зазначену діяльність з метою попереднього розслідування подій злочину та протидії їм[145].

Об'єкт ТДР – це сукупність відомостей про діяльність слідчих і судових органів, заплановані заходи, результати роботи, шляхи вдосконалення боротьби зі злочинністю, методи та засоби реалізації покладених завдань, а також відомості про осіб, предмети, події, процеси, необхідні для ефективної правоохоронної діяльності[146].

Предмет ТДР може бути обмежений доказовою інформацією та слідчими версіями, що потребують перевірки, а також тактичної інформацією, яка стосується умов збирання доказів[147].

Отже, в наведених визначеннях вказуються різні поняття, що характеризують ТДР.

Також у науковій літературі визначено ***систему відомостей***, які можуть ***становити ТДР***:

---

[144] Игнатов С. Д. Следственная тайна и ее пределы / С. Д. Игнатов // Правовая реформа и проблемы ее реализации. – Краснодар, 1989. – С. 257–258.

[145] Камалова Г. Г. Анализ понятия и содержания тайны следствия / Г. Г. Камалова // Вестник Удмурского университета. – Серия «Экономика и право». – 2013. – Вып. 1. – С. 156.

[146] Кузьмічов В. С., Лісогор В. Г. Розголошення інформації, що становить таємницю досудового слідства / В. С. Кузьмічов, В. Г. Лісогор // Боротьба з організованою злочинністю й корупцією (теорія і практика) : наук.-практ. журнал. – К. : Міжвід. наук.-дослід. центр із проблем боротьби з організованою злочинністю, 2001. – № 4. – С. 176.

[147] Бойков А. Д. Предмет и пределы гласности уголовного судопроизводства / А. Д. Бойков // Охрана прав граждан в уголовном судопроизводстве: Сб. науч. тр. / ВНИИ проблем укрепления законности и правопорядка. – М.: ВНИИ проблем укрепления законности и правопорядка, 1989. – С. 8.

1. *По відношенню до об'єктів захисту:*

- відомості, що відносяться до посадових осіб правоохоронних органів (слідчий, дізнавач, прокурор) та інших учасників кримінального процесу.

2. *Залежно від необхідності засекречування:*

- відомості, що становлять таємницю слідства під час розслідування кожної кримінальної справи, незалежно від її категорії (інформація про слідчі дії, тактика проведення слідчих дій, заходи безпеки, які застосовуються щодо учасників розслідування);
- відомості, які відносяться до ТДР, залежать від слідчого, дізнавача і прокурора (наприклад, відомості про результати окремих слідчих дій).

3. *Залежно від тривалості дії режиму таємниці:*

- відомості постійної дії: про заходи безпеки, що застосовані до учасників організованих злочинних груп, які погодилися співпрацювати з органами розслідування в обмін на зміну їм «установчих» даних і місце проживання ...;
- відомості тривалої дії: результати проведення слідчих дій, які були проведені без участі обвинуваченого та його захисника, допити очевидців та інших свідків і потерпілого, що можуть становити ТДР і бути недоступними для обвинуваченого та його захисника до закінчення розслідування та ознайомлення з матеріалами кримінальної справи;
- відомості короткострокової дії: про тактику проведення слідчих дій, в яких брав участь обвинувачений (підозрюваний).

4. Залежно від суб'єктів, які можуть бути носіями таємниці слідства:

- відомості, носіями яких можуть бути виключно працівники правоохоронних органів: про планування розслідування, про взаємодію слідчих і оперативних працівників, про заходи безпеки, що застосовуються до окремих учасників розслідування та ін.;

- відомості, носіями яких, крім працівників правоохоронних органів, можуть бути потерпілі, очевидці, інші свідки, адвокати, поняті.

5. ***Залежно від змісту таємниці слідства:***

- відомості про особу, місце проживання та інші ідентифікуючі ознаки учасників розслідування: працівників правоохоронних органів, які брали участь у розслідуванні, працівників органу дізнання, слідчих, прокурорів, експертів і фахівців; про родичів і близьких співробітників правоохоронних органів, які брали участь у розслідуванні; окремих учасників попереднього розслідування (свідків, потерпілих, підозрюваних, обвинувачених та ін.); про родичів та інших близьких учасників кримінального процесу, які не є співробітниками правоохоронних органів;
- відомості про заходи щодо забезпечення безпеки учасників розслідування;
- відомості, які відображатимуть стратегію та тактику розслідування[148].

Однак окремі відомості в даній класифікації можуть належати до різних груп, що ускладнює визначенні захисту ТДР[149].

Також необхідно зазначити, що до складу правового інституту ТДР входять два типи правових норм – ***норми матеріального права*** (матеріальні норми) та ***норми процесуального права*** (процесуальні норми).

В свою чергу сукупність норм матеріального права, що входять до правового інституту ТДР можна розділити на ***загальні***, які регулюють порядок захисту та/або забезпечення доступу до інформації, що може відноситися до ТДР (персональні дані, комерційна таємниця, банківська таємниця) та ***спеціальні***, які

[148] Крылов А. В. К вопросу об определении тайны следствия / А. В. Крылов // Российский следователь. – 2003. – № 9. – С. 32–38.

[149] Ляш А. О. Недопустимість розголошення відомостей досудового розслідування / А. О. Ляш //Часопис Національного університету «острозька академія». Серія «Право». – 2013. – № 1(7). – [Електронний ресурс]. – Режим доступу: http://lj.oa.edu.ua/articles/2013/n1/13laovdr.pdf.

регулюють порядок захисту та/або забезпечення доступу до інформації, що безпосередньо становить ТДР.

До ***загальних матеріальних норм*** правового інституту ТДР відносяться деякі норми Законів України «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис» та ін.

До спеціальних норм матеріального права, що входять до правового інституту ТДР можна віднести деякі норми Законів України «Про судочинство та статус суддів» і «Про доступ до судових рішень».

Специфіка ***процесуальних норм***, що входять до правового інституту ТДР, визначається поширенням їх дії лише процесуальні правовідносини, що виникають в процесі судочинства або досудового розслідування. Такі норми містяться, насамперед, в КПКУ, ЦПКУ, КУпАП та ін.

ТДР (таємницю слідства) складають всі відомості, отримані в процесі здійснення слідчих і оперативно-розшукових дій. Тому вмістом кримінального провадження є інформація певного роду, що формалізована відповідно до вимог кримінального процесуального закону з певним доступом до неї. Так, у кримінальному провадженні може знаходитися інформація, що не підлягає розголошенню ні за яких умов. До неї належать форми, методи та результати оперативно-розшукових заходів, утримання та матеріали оперативно-розшукової справи, інформація яких відноситься до державної таємниці, відповідно до ст. 8 ЗУ «Про державну таємницю». Також, відповідно до ч. 4 ст. 6 ЗУ «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві»[150] і ч. 4 ст. 18 ЗУ «Про державний захист працівників суду і правоохоронних органів»[151] до ІзОД відносяться відомості про заходи безпеки та осіб, взятих під варту.

[150] Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві: Закон України від 23.12.1993 р. № 3782-XII // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 51.

[151] Про державний захист працівників суду і правоохоронних органів: Закон України від 23.12.1993 р. № 3781-XII // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 50.

З усього розглянутого слідують ***правові ознаки ТДР:***

1) ТДР – це вид ІзОД, який регулюється КПКУ та іншими законодавчими актами;

2) ТДР складають всі відомості, отримані в процесі здійснення слідчих і оперативно-розшукових дій, а також інформація, що не підлягає розголошенню (форми, методи та результати оперативно-розшукових заходів, утримання та матеріали оперативно-розшукової справи, інформація яких відноситься до ДТ);

3) розголошення ТДР може негативно вплинути на розкриття злочину і викриття винних.

§6.2. Види таємної інформації в кримінальному провадженні

Щодо *другої складової правового інституту ТДР* (режиму ТДР) необхідно зазначити, що особливість правового регулювання даного виду таємниці полягає в тому, що в юридичній науковій літературі існує дискусія з приводу загальної назви та вмісту ТДР.

Досудове розслідування (дізнання) є однією із стадій кримінального провадження, яке починається з моменту внесення відомостей про кримінальне правопорушення до Єдиного реєстру досудових розслідувань і закінчується закриттям кримінального провадження, або направленням до суду обвинувального акту, клопотанням про застосування примусових заходів медичного або виховного характеру, клопотанням про звільнення особи від кримінальної відповідальності (п. 7 ч. 1 ст. 3 КПКУ).

Тобто разом з ТДР використовується багато інших видів таємної інформації: в процесі кримінального провадження в суді першої інстанції, яке включає підготовче судове провадження, судовий розгляд і ухвалення судового рішення, провадження з перегляду судового рішення в апеляційному або касаційному порядку, Верховним Судом України, а також за ново виявленими обставинами. Тому в науковій літературі крім поняття *«ТДР»* використовується

поняття ***«таємниця слідства і судочинства»***, яка включає в себе ***професійну таємницю суддів***[152].

Основним міжнародно-правовим актом, що встановлює стандарти діяльності судових органів і який закріплює цей вид таємної інформації, є «Основні принципи незалежності судових органів»[153], схвалені ООН. Згідно з п. 15 цих принципів *«судді зобов'язані зберігати професійну таємницю щодо своєї роботи та конфіденційної інформації, отриманої в ході виконання ними своїх обов'язків, за винятком відкритих судових розглядів, і їх не можна змушувати давати показання з таких питань»*.

Згідно зі ст. 12 Кодексу професійної етики судді[154] *«суддя не може робити публічні заяви, коментувати в засобах масової інформації справи, які перебувають у провадженні суду, і піддавати сумніву судові рішення, що набрали законної сили. Суддя не має права розголошувати інформацію, яка стала йому відомою у зв'язку з розглядом справи»*. Також слід зазначити, що нерозголошення даного виду інформації, поширюється не тільки на професійних суддів, а й на народних засідателів і присяжних, які можуть здійснювати правосуддя згідно з нормами ст. 127 Конституції України.

Ст. 7 ЗУ «Про доступ до судових рішень»[155] визначені *відомості, які не можуть бути розголошені в текстах судових рішень, відкритих для загального доступу*, а саме:

- імена (ім'я, по батькові, прізвище) фізичних осіб;
- адреса місць проживання або перебування фізичних осіб, номери телефонів або інших засобів зв'язку, адреси електронної пошти, ідентифікаційні номери (коди);
- реєстраційні номери транспортних засобів;

---

[152] Ємельянов С. Л. Таємниця слідства та судочинства в України / С. Л. Ємельянов // Ученые записки Таврического национального университета им. В. И. Вернадского. – Серия «Юридические науки». – Том 26 (65). – 2013. – № 2-1 (Ч. 2). – С. 311.

[153] Основні принципи незалежності судових органів: Міжнародний документ від 13.12.1985 р. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_201.

[154] Кодекс професійної етики судді, затверджений V З'їздом суддів України 24.10.2002 р. // Вісник Верховного Суду України. – 2002. – № 5. – С. 24-34.

[155] Про доступ до судових рішень: Закон України від 22.12.2005 р. // Відомості Верховної Ради. – 2006 .– № 15.– Ст. 128.

- інша інформація, що дозволяє ідентифікувати фізичну особу.

До зазначених відомостей *не належать*:

- прізвища та ініціали суддів, які прийняли судове рішення;
- імена посадових чи службових осіб, які, виконуючи свої повноваження, беруть участь в цивільному, господарському, адміністративному або кримінальному провадженнях, справах про адміністративні правопорушення (проступки);
- імена сторін у справі, яка розглядалася міжнародною судовою чи іншою міжнародною організацією, на вирішення якої в тексті судового рішення містяться посилання.

Однак поняття *«таємниця слідства і судочинства»* є досить суперечливим, оскільки воно порушує одну з основ судочинства – принципу гласності та відкритості, гарантованого ст. 129 Конституції України та п. 20 ст. 7 КПКУ.

Нормами ст. 27 КПКУ та ст. 11 ЗУ «Про судоустрій і статус суддів»[156] гарантується гласність і відкритість судового провадження та його повне фіксування технічними засобами.

Ніхто не може бути обмежений у праві на отримання в суді усної або письмової інформації про результати розгляду його судової справи. Кожен, хто не є стороною у справі, має право на вільний доступ до судового рішення.

Для забезпечення прозорості діяльності судової влади та створення механізму для реалізації гласності судового процесу в Україні був прийнятий ЗУ «Про доступ до судових рішень». На виконання зазначеного закону з 1.06.2006 р. доступ до судових актів судів загальної юрисдикції здійснюється через Єдиний державний реєстр судових рішень, роботу якого забезпечує Державна судова адміністрація України. Доступ до реєстру здійснюється через офіційний веб-портал судової влади України за адресою: http://reyestr.court.gov.ua.

[156] Про судоустрій і статус суддів: Закон України від 07.07.2010 р. // Відомості Верховної Ради. – 2010 .– № 41–45. – Ст. 529.

Розгляд справ у судах відбувається відкрито, крім випадків, встановлених процесуальним законом. Будь-який присутній в залі судового засідання, може вести стенограму, робити нотатки, використовувати портативні аудіозаписувальні пристрої. Проведення в залі судового засідання фотозйомки, відеозапису, транслювання судового засідання по радіо і телебаченню, а також проведення звукозапису із застосуванням стаціонарної апаратури допускаються на підставі ухвали суду, що приймається з урахуванням думки сторін та можливості проведення таких дій без шкоди для судового розгляду.

Учасники судового провадження та особи, які не брали участі у кримінальному провадженні, але щодо яких суд вирішив питання про їх права, свободи, інтереси чи обов'язки, не можуть бути обмежені у праві на отримання в суді як усної, так і письмової інформації про результати судового розгляду і в праві на ознайомлення з процесуальними рішеннями, а також отримання їх копій.

Ніхто не може бути обмежений у праві на отримання в суді інформації про дату, час і місце судового розгляду та про вжиті в ньому судові рішення, крім випадків, встановлених законом.

Розгляд справи в закритому судовому засіданні допускається за вмотивованим рішенням суду у випадках, передбачених процесуальним законом. Слідчий суддя або суд може прийняти рішення про здійснення кримінального провадження у *закритому судовому засіданні* впродовж усього судового розгляду або його окремої частини лише у наступних випадках:

1) якщо обвинуваченим є неповнолітній;
2) розгляду справи про злочин проти статевої свободи та статевої недоторканості особи;
3) необхідності запобігти розголошенню відомостей про особисте та сімейне життя чи обставин, які принижують гідність особи;
4) якщо здійснення провадження у відкритому судовому засіданні може призвести до розголошення таємниці, що охороняється законом;
5) необхідності забезпечення безпеки осіб, що беруть участь у кримінальному провадженні.

Особисті записи, листи, зміст особистих телефонних розмов, телеграфних та електронних повідомлень можуть бути розглянуті у відкритому судовому засіданні тільки в тому випадку, якщо слідчий суддя або суд не прийме рішення про їх розгляд в закритому судовому засіданні, на підставі зазначеного п. 3.

Судове рішення, ухвалене у відкритому судовому засіданні, проголошується публічно. Для закритого судового засідання, судове рішення проголошується публічно з пропуском закритої інформації, і яка на момент проголошення судового рішення підлягає подальшої захисту від розголошення.

При розгляді справ перебіг судового процесу фіксується технічними засобами в порядку, встановленому процесуальним законом. Офіційним записом судового засідання є лише технічний запис, здійснений судом у порядку, передбаченому п. 4 ст. 107 КПКУ. Фіксування судового засідання за допомогою технічних в є обов'язковим. У разі неприбуття в судове засідання всіх осіб, які беруть участь у провадженні, або в разі, якщо судочинство здійснюється судом за відсутності осіб, фіксування за допомогою технічних засобів кримінального провадження в суді не здійснюється.

Учасники судового провадження мають право отримати копію запису судового засідання, зробленого за допомогою технічних засобів.

Незастосування технічних засобів фіксування кримінального провадження у випадках, якщо воно є обов'язковим, тягне недійсність відповідної процесуальної дії та отриманих в результаті її здійснення результатів, за винятком випадків, якщо сторони не заперечують проти визнання такої дії та результатів її здійснення чинними.

В процесі прийняття судового рішення виникає «***таємниця нарадчої кімнати»*** (ст. 82^1 Закону України «Про судоустрій і статус суддів») або «***таємниця наради суддів»*** (ст. 367 КПКУ). Згідно з нормами цих законодавчих актів при ухваленні судового рішення ніхто не має права перебувати в нарадчій кімнаті, крім складу суду, який розглядає справу. Суд може перервати нараду лише для відпочинку з настанням нічного часу. Під час перерви судді не можуть

спілкуватися з особами, які брали участь у кримінальному провадженні. Під час перебування в нарадчій кімнаті суддя не має права розглядати інші судові справи. Судді не мають права розголошувати хід обговорення та ухвалення рішення у нарадчій кімнаті. Єдиною інформацією, яка публікується за результатами наради суддів, є рішення, постанова чи вирок суду.

Таємниця нарадчої кімнати є однією з гарантій виконання конституційної вимоги незалежності суддів і підпорядкування їх тільки закону. Таємниця наради дозволяє суддям вільно висловлювати свою думку з будь-якого питання, яке розглядається, відстоювати її, наводити аргументи, голосувати за те рішення, яке суддя вважає правильним і справедливим[157].

Таємниця наради суддів забезпечується також відсутністю протоколу і розголошенням тільки результатів голосування, а не його ходом.

В нарадчій кімнаті судді обговорюють і вирішують питання, перелічені в ст. 368 КПКУ. Ці питання головуючий послідовно ставить на голосування, причому кожне питання в такій формі, щоб на нього можна було дати тільки позитивну або негативну відповідь. Нарада суддів проводиться з кожного питання, при цьому ніхто із суддів не має права утримуватися від голосування при винесенні рішення. Щоб усунути вплив особливого становища головуючого на інших суддів, особливо на народних засідателів, закон зобов'язує його голосувати останнім (ст. 375 КПКУ). Дотримання цього порядку в нарадчій кімнаті не фіксується в будь-якому процесуальному документі і в силу таємниці наради суддів не може бути перевірено при перегляді справи в апеляційному чи касаційному порядку. Ніяких винятків з правила про таємницю наради суддів у КПКУ не передбачено.

Відповідно до ст. 54 Закону України «Про судоустрій і статус суддів» суддя зобов'язаний «*не розголошувати відомості, які становлять таємницю, що охороняється законом, в тому числі і таємницю нарадчої кімнати і закритого судового засідання*».

[157] Бараннік Р. В., Назаренко П. Г. Особливості охорони інформації, що становить таємницю у кримінальному судочинстві / Р. В. Бараннік, П. Г. Назаренко // Адвокат. – № 4 (127). – 2011. – С. 15–18.

Також, в процесі кримінального провадження може розглядатися ***інформація, що складає одну із законодавчо визначених таємниць*** (ст. 162 КПКУ):

В процесі здійснення кримінального судочинства може виникати «***таємниця особи, щодо якої здійснюються заходи безпеки***», передбаченої Законом України «Про забезпечення безпеки осіб, що беруть участь в кримінальному судочинстві»[158].

Зокрема, особи, які беруть участь у кримінальному судочинстві, за наявності реальної загрози їх життю, здоров'ю, житлу чи майну мають право на забезпечення безпеки. Відомості про заходи безпеки та осіб, взятих під захист, є ***ІзОД.***

Також в КПКУ введено поняття «***таємниця спілкування»*** (п. 7 ст. 7). Згідно зі ст. 14 даного Кодексу та ст. 31 Конституції України «таємниця спілкування» – правове положення, відповідно до якого, в ході кримінального провадження кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Втручання в приватне спілкування захисника, священнослужителя з підозрюваним, обвинуваченим, засудженим, виправданим – заборонено.

Втручання в таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених КПКУ, з метою виявлення та запобігання тяжкому чи особливо тяжкого злочину, встановлення його обставин, особи, яка вчинила злочин, якщо іншим способом неможливо досягти цієї мети. Інформація, отримана в результаті втручання у спілкування, не може бути використана інакше як для вирішення завдань кримінального судочинства.

Нормами ст. 258 КПКУ гарантується невтручання в приватне спілкування. Зокрема, ніхто не може зазнавати втручання у приватне спілкування без ухвали слідчого судді. Прокурор, слідчий за погодженням з прокурором зобов'язаний звернутися до слідчого судді з клопотанням про дозвіл на втручання в приватне спілкування в порядку, передбаченому ст. 246, 248, 249 КПКУ, якщо будь-яка слідча

[158] Про забезпечення безпеки осіб, які беруть участь в кримінальному судочинстві: Закон України від 23.12.1993 р. // Відомості Верховної Ради України. – 1993. – № 11.– Ст. 51.

дія передбачає таке втручання. Ч. 4 ст. 258 КПКУ передбачено, що втручанням в приватне спілкування є отримання доступу до змісту спілкування за умови, що учасники спілкування мають достатні підстави вважати спілкування приватним.

Різновидом втручання в приватне спілкування є:

1) аудіо-, відеоконтроль особи;
2) арешт, огляд і виїмка кореспонденції;
3) зняття інформації з транспортних телекомунікаційних мереж;
4) зняття інформації з електронних інформаційних систем.

В разі втручання в таємницю спілкування існує загроза порушення конституційних прав особи, оскільки відсутній контроль над припиненням подальшого втручання в приватне спілкування в кримінальному провадженні – фактичні дані про злочин або особу вже отримані, а термін дії постанови слідчого судді ще не закінчився. В такому випадку, прокурор повинен прийняти процесуальне рішення у вигляді постанови про припинення негласної слідчої дії і повідомити про це слідчому судді письмово.

Існують рішення Європейського суду, які встановлюють стандарти розгляду клопотань про надання дозволу на втручання в приватне спілкування.

Наприклад, у справі «Людвіг Людí проти Швейцарії» Суд зазначає, що, починаючи попереднє розслідування відносно заявника 15 березня 1984 р., суддя-слідчий Лауфенського районного суду видав наказ про прослуховування його телефонних розмов. Немає сумніву в тому, що телефонне прослуховування було втручанням у приватне життя і кореспонденцію пана Людí. Таке втручання не є порушенням Конвенції, якщо воно відповідає вимогам п. 2 ст. 8. Підставою для цього заходу були ст. 171b і ст. 171c Бернського Кримінально-процесуального кодексу, які застосовуються навіть на попередньому етапі розслідування, якщо є вагома підстава вважати, що готується вчинення кримінального правопорушення. Крім того, воно було призначене для «запобігання злочину» і Суд взагалі не сумнівається в його необхідності в демократичному суспільстві.

У справі «Ван Вондел проти Нідерландів» заявник скаржився на порушення його права на недоторканність приватного життя, оскільки ряд його (телефонних) розмов з паном Р. був записаний останнім, які Департамент внутрішніх розслідувань Національної поліції надав пану Р., також дав вказівки по суті розмови, яку слід вести з заявником. У рішенні Суд не погодився з тим, що надання такої допомоги з боку органів влади не регулюється нормами, спрямованими на забезпечення правових гарантій проти довільних дій. Суд дійшов висновку, що оспорюване втручання було здійснено не «відповідно до закону», а заявник був позбавлений мінімальному ступені захисту, на яку він мав право відповідно до принципу верховенства права в демократичному суспільстві.

Отже, на практиці при прийнятті рішення про надання дозволу на втручання в приватне спілкування необхідно дотримуватися міжнародних стандартів, встановлені рішеннями Європейського суду з прав людини[159].

Відповідно до чинного законодавства кримінальне провадження складається з кількох частин, сукупність яких становить систему стадій кримінального процесу, в яких відбувається обіг інформації, що становить ТДР і розглянуті вище таємниці. На підставі цього можна окремо виділити види таємної інформації в кримінальному провадженні *(рис. 6.1)*[160].Таким чином, зараз обсяг інформації, доступ до якої обмежено у процесі досудового розслідування та судочинства чинним законодавством, значно ширше, ніж поняття *таємниця досудового розслідування*, *таємниця слідства*, *таємниця нарадчої кімнати*, *таємниця осіб, щодо яких здійснюються міри безпеки*, *таємниця спілкування* тощо.

[159] Стефанів Н. Дотримання прав особи при наданні дозволу на втручання в приватне спілкування. Практика Європейського суду з прав людини / Н. Стефанів // Слово Національної школи суддів. – № 1 (2). – 2013. – С. 32–38.

[160] Ємельянов С. Л. Таємниця слідства та судочинства в України / С. Л. Ємельянов // Ученые записки Таврического национального университета им. В. И. Вернадского. – Серия «Юридические науки». – Том 26 (65). – 2013. – № 2-1 (Ч. 2). – С. 312.

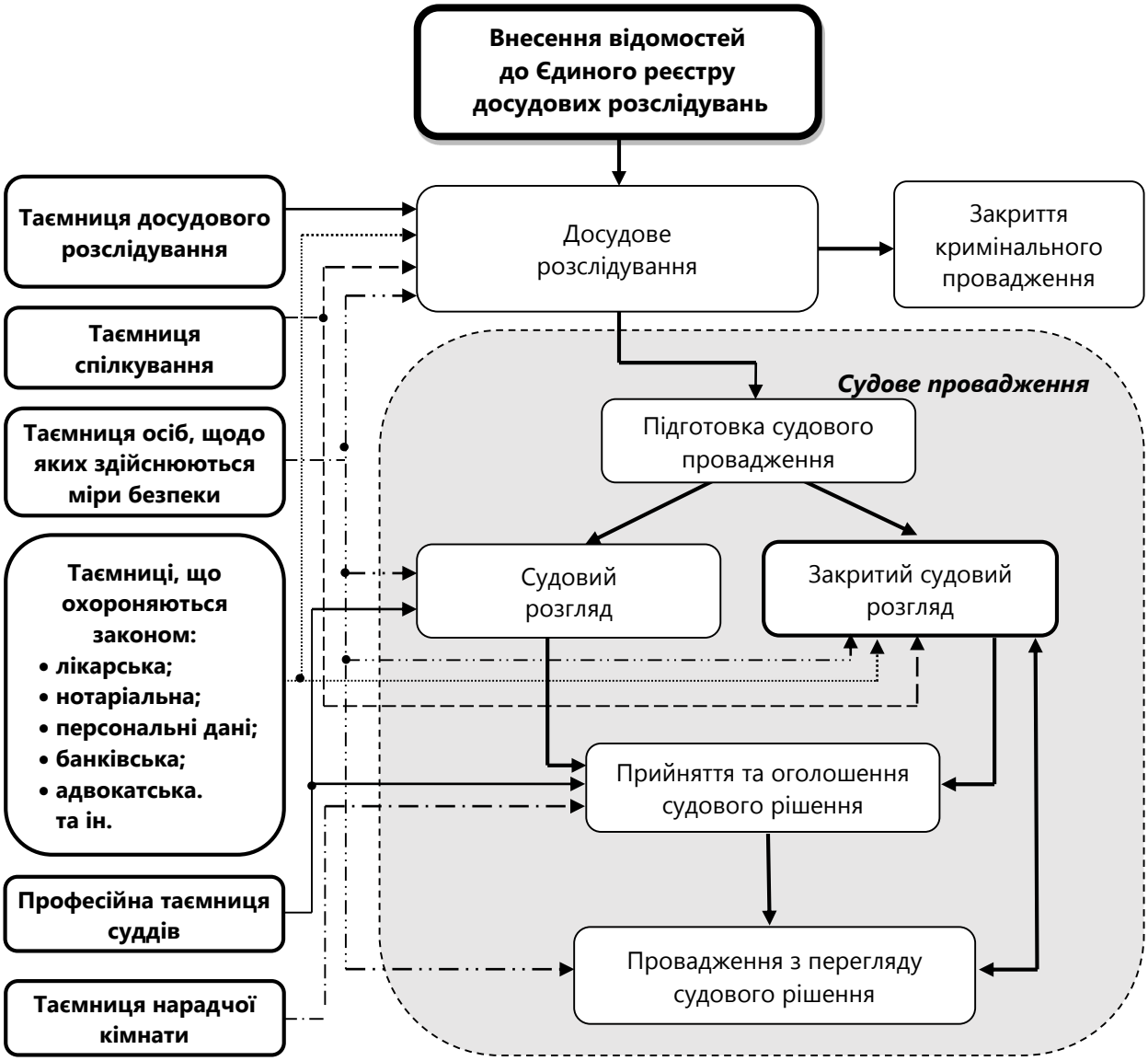

Рис. 6.1. Види таємної інформації в кримінальному судочинстві

§6.3. Засоби з охорони та захисту таємниці досудового розслідування

Згідно із законодавством України ТДР полягає у забороні розголошення даних досудового розслідування або дізнання без дозволу прокурора, слідчого або особи, яка провадила дізнання чи досудове розслідування, особою, попередженою у встановленому законом порядку про обов'язок не розголошувати такі дані.

Заборона на розголошення відомостей досудового розслідування випливає з особливостей завдань кримінального провадження. Зокрема, необхідність встановлення та розшуку осіб, які вчинили кримінальне правопорушення, запобігання знищення доказів винними особами або їх спільниками, іншими зацікавленими

в результатах досудового розслідування особами з метою перешкоджання проведення розслідування, здатності вплинути на хід розслідування, нанести шкоду в об'єктивності встановлення обставин кримінальної правопорушення. Існування цієї заборони також обумовлено тим, що передчасне розголошення даних слідства третім особам у приватній бесіді, публічному виступі, в ЗМІ може скомпрометувати учасників провадження, негативно вплинути на розкриття злочину, викриття винних, оскільки інформованість окремих зацікавлених осіб або організованих злочинних угрупувань про направлення розслідування і про конкретні слідчі та інші процесуальні дії, дозволить їм активно протидіяти зусиллям слідчого або оперативників[161].

Дані досудового розслідування можна оголосити лише з дозволу слідчого або прокурора та тільки в тому обсязі, в якому вони представляють можливим. У необхідних випадках слідчий попереджає всіх учасників досудового розслідування (свідків, потерпілого, захисника, експерта, спеціаліста, перекладача, понятих та інших осіб, присутніх при проведенні досудового розслідування) про обов'язок не розголошувати без його дозволу даних досудового розслідування.

Необґрунтоване оприлюднення даних досудового розслідування серйозно ускладнює провадження по кримінальній справі, спричиняє порушення прав і законних інтересів громадян, ускладнення здійснення правосуддя, може спричинити втрату доказів, порушити права та інтереси учасників процесу тощо. Відомості, які має слідство і дізнання, об'єктивно представляють інтерес для сторони, яка надає протидію розслідуванню.

Основними способами необґрунтованого (злочинного) оприлюднення відомостей, що входять до ТДР є:

1) отримання інформації через корумпованих працівників правоохоронних органів;
2) безпосереднє спостереження і аналіз дій працівників правоохоронних органів;

[161] Уголовный процессуальный кодекс Украины: Научно-практический комментарий / Отв. ред. С. В. Кивалов, С. Н. Мищенко, В. Ю. Захарченко. – Х.: Одиссей, 2013. – С. 472.

3) аналіз виступів працівників правоохоронних органів в засобах масової інформації, а також журналістів, які проводять «журналістське розслідування»;
4) встановлення прослуховуючої апаратури і апаратури прихованої відео-та фотозйомки;
5) знімання інформації з технічних каналів зв'язку;
6) проникнення в комп'ютерні мережі правоохоронних органів;
7) отримання інформації через спеціально впроваджених в ряди працівників правоохоронних органів суб'єктів;
8) провокації працівників правоохоронних органів на необережне розголошення слідчої таємниці;
9) отримання інформації від родичів та інших близьких працівників правоохоронних органів, яким ТДР була розголошена цими працівниками з необережності;
10) отримання інформації через підозрюваних, обвинувачених, які брали участь у проведенні слідчих дій у справі;
11) отримання інформації через потерпілих і свідків, які беруть участь у розслідуванні;
12) отримання інформації через адвокатів, які захищають підозрюваних і обвинувачуваних;
13) отримання інформації через експертів, фахівців, а також інших учасників кримінального процесу – перекладачів, законних представників.

У чинному законодавстві України представлені кримінально-правові засоби забезпечення неприпустимості розголошення інформації, що становить ТДР та інших видів таємниць.

Зокрема, за розголошення *даних досудового слідства* або *дізнання*, вчинене суддею, прокурором, слідчим, працівником органу дізнання, оперативно-розшукового органу незалежно від того, чи брала ця особа безпосередньо участь у досудовому слідстві чи дізнанні, якщо розголошені дані ганьблять людину, принижують її честь і гідність встановлена кримінальна відповідальність ст. 387 ККУ.

Також, відповідно до ч. 1 ст. 381 ККУ розголошення відомостей про заходи безпеки щодо особи, взятої під захист, службовою особою,

яка прийняла рішення про ці заходи, особою, яка її здійснює, або службовою особою, якій ці рішення стали відомі у зв’язку з її службовим становищем, а так ж особою, взятою під захист, якщо ці дії заподіяли шкоду здоров'ю особи, взятої під захист – карається штрафом від ста до трьохсот неоподатковуваних податком мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеження волі на строк до трьох років.

Відповідальність за розголошення відомостей, що становлять «*таємницю особи, щодо якої здійснюються заходи безпеки*», передбачена ст. 25 ЗУ «Про забезпечення безпеки осіб, що беруть участь в кримінальному судочинстві»:

Частиною 1 передбачена дисциплінарна відповідальність за розголошення відомостей про заходи безпеки особами, які прийняли рішення про ці заходи, або особами, які їх здійснюють. А у випадках, коли розголошення цих відомостей спричинило тяжкі наслідки – передбачена кримінальна відповідальність.

Частиною 2 вказаної статті передбачена адміністративна відповідальність передбачена за розголошення таких відомостей особою, взятою під захист. А в разі, якщо це призвело або могло призвести до тяжких наслідків, – кримінальну відповідальність.

За розголошення охоронюваної законом таємниці, у тому числі *таємниці нарадчої кімнати* або *таємниці* , яка стала відома судді під час розгляду справи в *закритому судовому засіданні* згідно зі ст. 83 ЗУ «Про судоустрій і статус суддів» передбачено дисциплінарну відповідальність судді.

Відсутність в законодавстві чіткого поняття ТДР та відомостей, які її складають, дає підставу деяким учасникам досудового розслідування зневажливо ставитися до збереження розглянутих видів таємниць. Це вимагає розробки та прийняття окремого нормативно-правового акту щодо правового регулювання обігу таємної інформації в процесі досудового розслідування та судочинства.

Висновки

ТДР є різновидом професійної таємниці і покликана забезпечити успішне розкриття злочинів і викриття обвинуваченого.

ТДР відноситься до ІзОД.

ТДР становлять відомості, отримані в процесі здійснення слідчих і оперативно-розшукових дій, а також інформація, що не підлягає розголошенню (форми, методи і результати оперативно-розшукових заходів, утримання та матеріали оперативно-розшукової справи, інформація яких відноситься до державної таємниці). Їх розголошення може негативно вплинути на розкриття злочину і викриття винних.

Крім ТДР, в процесі досудового розслідування використовуються ще різновиди таємниць, такі, як: професійна таємниця суддів, таємниця нарадчої кімнати, таємниця спілкування, таємниця осіб, щодо яких здійснюються міри безпеки та ін.

Відсутність в законодавстві України чіткого визначення ТДР і відомостей, що відносяться до неї, створюють неналежний правовий захист даного виду таємниці.

7 ПРОФЕСІЙНА ТАЄМНИЦЯ ТА ІНШІ ВИДИ ТАЄМНИЦЬ, ПЕРЕДБАЧЕНІ ЗАКОНОДАВСТВОМ УКРАЇНИ

§7.1. Поняття, ознаки та види професійної таємниці

У сучасному законодавстві України чіткого визначення ***професійної таємниці*** (ПТ) немає. На сьогоднішній день єдиним законом, в якому згадується ПТ, є ЗУ «Про доступ до публічної інформації». В ст. 8 ПТ відноситься до таємної інформації: *«Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю».*

Згідно зі ст. 21 ЗУ «Про інформацію» таємна інформація відноситься до ІзОД, тобто ПТ є ІзОД і повинна мати власний ***правовий інститут,*** розглянутий раніше.

Щодо *першої складової правового інституту* ***(загальної частини****) ПТ* зазначимо те, що не тільки в чинному законодавстві, але й в юридичній науці немає єдиного розуміння щодо поняття, правової природи та змісту ПТ, її співвідношення з іншими видами таємниць, зокрема службової (СТ).

У юридичній енциклопедії ПТ визначається як узагальнена назва відомостей (переважно з обмеженим доступом), якими володіє особа у зв'язку із здійсненням ним професійної діяльності та розголошення яких заборонено[162].

ПТ умовно розподіляють на два види[163]:

- ПТ в чистому вигляді, обумовлена самим родом діяльності (комерційна, службова та ін.);
- ПТ складовою частиною якої є довірена особиста таємниця.

ПТ – інформація, що захищається законом, яка довірена або

[162] Юридична енциклопедія: в 6 т. / Редкол.: Ю70 Ю. С. Шемшученко (голова редкол.) та ін. – К.: «Укр. енцикл.», 1998. – [Електронний ресурс]. – Режим доступу: http://cyclop.com.ua/content/view/1277/58/1/14/#26849.

[163] Смолякова И. В. Тайна и уголовно-процессуальный закон / И. В. Смолякова. – М.: Луч, 1997. – С. 85.

стала відомою особі (держателю) виключно в силу виконання ним своїх професійних обов'язків, не пов'язаних з державною або муніципальною службою, поширення якої може завдати шкоди правам і законним інтересам іншої особи (довірителя), яка довірила ці відомості , і яка не є державною або комерційною таємницею[164].

До основних ***суб'єктів правовідносин*** в області ПТ відносяться довірителі (власники), утримувачі і користувачі ПТ.

Довіритель – фізична особа (незалежно від громадянства), що довірила відомості іншій особі, а також його правонаступники (у тому числі спадкоємці).

Утримувач – фізична або юридична особа, якій виключно в силу його професійної діяльності (професійних обов'язків) були довірені або стали відомі відомості, що становлять ПТ.

Користувач – особа, якій відомості, що становлять ПТ, стали відомі на законних підставах у зв'язку з виконанням ним своїх службових обов'язків у випадках і порядку, встановлених законом.

Поширеною ознакою ПТ є і те, що вона може належати особі, яка у зв'язку зі своїм професійним статусом отримала доступ до конфіденційних відомостей і не перебуває на державній або муніципальній службі. В цьому випадку інформація буде мати характер СТ.

Однак, ПТ і СТ суттєво відрізняються за суб'єктним і об'єктним складом, умовами виникнення та режимами правового захисту. Держателем ПТ є особа, яка не перебуває на державній або муніципальній службі, якій певна інформація надана клієнтом – довірителем таємниці. І навпаки, СТ – це конфіденційна інформація, яка стала відома в державних органах та органах місцевого самоврядування тільки на законних підставах і при виконанні їх представниками службових обов'язків. На відміну від ПТ, яку становить тільки «чужа» інформація, СТ крім таємниці довірителя може містити службову інформацію, що є власністю держави[165].

---

[164] Информационное право / под ред. И. Л. Бачило, В. Н. Лопатин, М. А. Федотов, Б. Н. Топорина. – СПб.: Питер, 2001. – С. 535–539.

[165] Ємельянов С. Л. Стан та розвиток професійної таємниці в Україні / С. Л. Ємельянов // Право і безпека. – 2011. – № 5 (2). – С. 1–7.

Але варто враховувати й те, що на практиці трапляються випадки, коли певна ПТ (на законних підставах) надається органам державної влади, і коли одна і та ж інформація захищається одночасно і ПТ, і СТ.

Тому, не заперечуючи теоретичної самостійності ПТ і СТ, необхідно констатувати їх тісний взаємозв'язок в практичному аспекті збереження інформації, що є предметом ПТ. Розмежування цих таємниць є умовним, що не дозволяє сформувати комплексний підхід до вирішення практичних проблем розкриття та розслідування розголошення ПТ[166].

Встановлення правового режиму ПТ є правомірним тільки у випадках, коли отримання доступу до інформації, що відноситься до ПТ, обумовлено специфікою професії і є невід'ємним її елементом.

Заборона на поширення довіреної інформації не має абсолютного характеру, оскільки нормативно-правовими актами передбачено цілий ряд випадків, які зобов'язують носіїв відповідної інформації надати її в розпорядження уповноважених органів (наприклад, правоохоронних) та їх посадовим особам[167].

Таким чином, можна виділити ***правові ознаки ПТ:***

1) довірена добровільно довірителем або стала відома особі у силу виконання ним своїх професійних обов'язків;
2) особа, якій довірено інформацію, не перебуває на державній або муніципальній службі (інакше інформація буде вважатися СТ);
3) заборона на поширення довіреної або інформації, що стала відомою, яка може завдати шкоди правам і законним інтересам довірителя, встановлений чинним законодавством;
4) інформація не відноситься до відомостей, що становлять державну або комерційну таємницю [168].

[166] Резнікова Г. І. Професійна таємниця: поняття, ознаки та види / Г. І. Резнікова // Трибуна докторанта, аспіранта і здобувача. – 2013. – Вип. 26. – С. 280–292.

[167] Рожнов А. А. Уголовно-правовая охрана профессиональной тайны : автореф.дис... канд. юрид. наук: 12.00.08 / А. А. Рожнов; Казан. гос. ун-т. – Казань, 2002. – С. 17.

[168] Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. – Барнаул, АлтГТУ, 2011. – С. 121.

Щодо *другої складової правового інституту ПТ (**режиму ПТ**)* відзначимо, що особливості правового регулювання ПТ полягають в тому, що відповідні правила поведінки своїм виникненням зобов'язані не загальнолюдським моральним нормам, а нормам корпоративної моралі або професійної етики.[169]

Ці норми виникли в процесі здійснення того чи іншого виду професійної діяльності, і для людини, що не відноситься до даної професії, можуть бути не прийнятними.

До ПТ відноситься інформація, з якою мають справу представники так званих «саморегульованих» професій та інші особи, яким ці відомості були довірені у зв'язку з їх професійним становищем. До ПТ слід віднести наступні таємниці: ***лікарську***, ***нотаріальну***, ***адвокатську***, ***аудиторську***, ***журналістську***, ***інсайдерську***, ***страхування***, ***сповіді***, ***усиновлення***, ***авторства***, ***голосування***, ***зв'язку (листування)***.

Деякі вчені до різновиду ПТ включають також і БТ. Але як було розглянуто раніше, БТ має свій правовий інститут з чітко визначеним колом відомостей, що становлять її, механізмом її збереження та розкриття, а також нормами цивільно-правової та кримінально-правового захисту. Це підтверджує і ст. 8 ЗУ «Про доступ до публічної інформації», де ПТ і БТ відділені.

Обов'язок не розголошувати довірену їм інформацію належить до професійних обов'язків та є складовою частиною внутрішніх правил певної професії. Важливим у цьому відношенні є питання довіри – особа, яка потребує певної професійної допомоги, погоджується надати про себе інформацію, очікуючи збереження її у таємниці. Надана нею інформація може бути розголошена лише за його згодою. При цьому така інформація надається при реалізації (захисту) особою своїх прав і свобод (наприклад, право на здоров'я, на правову допомогу, на свободу віросповідання). Тому розголошення довіреної інформації спричинить обмеження прав особам, які не зможуть вільно користуватися послугами відповідних професій, без впевненості в захищеності переданої інформації.

[169] Кормич Б.А. Інформаційне право. Підручник / Б.А. Кормич. – Харків:БУРУН і К, 2011. – С. 207.

Обов'язок зберігати інформацію виникає у представника професії, яким її було довірено; обов'язок не порушувати цю таємницю виникає і в інших осіб, зокрема, державних органів, які повинні поважати і не порушувати ПТ[170].

Щодо *третьої складової правового інституту ПТ – **санкцій***, зазначимо таке, що правовий режим ПТ, як виду ІзОД, полягає в законодавчій забороні доступу до цих відомостей третіх осіб та встановленні санкцій за їх розголошення.

Для здійснення її правового захисту необхідно прийняти спеціальний закон, в якому доцільно закріпити загальне визначення ПТ як інформації, довіреної представникам певних професій фізичними або юридичними особами з метою здійснення (захисту) своїх прав і законних інтересів; правові ознаки та критерії, за якими інформація буде ставитися до ПТ; перелік відомостей, які не можуть становити ПТ на підставі обмежень до публічної інформації, а також інформації, яка не може становити державну та комерційну таємницю; виділення в рамках кримінального законодавства загальної норми, яка передбачає підставу відповідальності за порушення ПТ, а саме – за незаконний збір, використання та поширення відомостей, що становлять ПТ, яке завдало значної шкоди правам та інтересам фізичної або юридичної особи; привести вичерпний перелік випадків і законодавчих підстав для отримання інформації, що становить ПТ, державними органами, органами місцевого самоврядування та їх посадовими особами; визначити обов'язок збереження ПТ та її захист в режимі СТ, адміністративну та дисциплінарну відповідальність користувачів ПТ з числа державних органів та органів місцевого самоврядування та їх посадових осіб за розголошення ПТ або використання її у власних інтересах або в інтересах третіх осіб тощо.

Таким чином, ПТ є самостійним видом ІзОД і повинна мати свій власний правовий інститут. Але сьогодні в нашій країні створені тільки певні елементи правового інституту ПТ. Окремі види інформації, складові ПТ, регулюються правовими нормами різних галузей

[170] Науково-практичний коментар до Закону України «Про доступ до публічної інформації» / Під заг. ред.. Д. Котляр. – К., 2012. – С. 146.

законодавства. Ці норми не завжди взаємоузгоджені, їх кількість має тенденцію до збільшення, оскільки зростає кількість напрямів і видів професійної діяльності. Тому побудувати комплексну концептуальну модель ПТ неможливо.

§7.2. Інші види таємниць, передбачені законодавством України

Крім розглянутих раніше видів таємниць (державна, банківська, комерційна, професійна) в чинному законодавстві України в тому чи іншому обсязі згадується більше 30 видів таємниць.

Проаналізуємо детальніше деякі з видів ПТ, визначимо їх зміст і правові ознаки, норми, що визначають їх статус, системи захисту тощо.

Лікарська таємниця

Лікарська таємниця – це інформація, що містить факти звернення за медичною допомогою, результати обстеження особи, про стан здоров'я, діагноз захворювання й інші відомості в медичних документах громадян[171].

За законодавством України до лікарської таємниці належать такі відомості:

- про хворобу, медичне обстеження, огляд та їх результати, інтимну та сімейну сторони життя громадянина (ст. 40 ЗУ «Основи законодавства України про охорону здоров'я»)[172];
- відомості про реципієнтів, а також про осіб, які заявили про свою згоду або незгоду стати донорами у разі смерті (ст. 17 ЗУ «Про трансплантацію органів та інших анатомічних матеріалів людини»[173]);
- про результати тестування особи з метою виявлення ВІЛ, про наявність або відсутність у особи ВІЛ-інфекції (ст. 13 ЗУ «Про протидію поширенню хвороби, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з

[171] Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. – Барнаул, АлтГТУ, 2011. – С. 122.

[172] Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 р. // Відомості Верховної Ради. – 1993. – № 4. – Ст. 19.

[173] Про трансплантацію органів та інших анатомічних матеріалів людині: Закон України від 16.07.1999 р. // Відомості Верховної Ради. – 1999. – № 41. – Ст. 377.

ВІЛ»)[174];

- про зараження особи інфекційним захворюванням, що передається статевим шляхом, проведенні медичного огляду і обстеження з цього приводу, відомості інтимного характеру, отримані у зв'язку з виконанням професійних обов'язків посадовими особами та медичними працівниками установами охорони здоров'я (ст. 26 ЗУ «Про захист населення від інфекційних захворювань»)[175];
- про перенесені та наявні в особи, яка виявила бажання здати кров та (або) її компоненти, захворювання, а також про вживання нею наркотичних речовин та властиві їй інші форми ризикованої поведінки, які можуть сприяти зараженню донора інфекційними хворобами, що передаються через кров, і за наявності яких виконання донорських функцій може бути обмежене (ст. 14 ЗУ «Про донорство крові та її компонентах»)[176];
- відомості про наявність у особи психічного розладу, про факти звернення за психіатричною допомогою та лікування у психіатричному закладі або перебування в психоневрологічних закладах для соціального захисту або спеціального навчання, а також інші відомості про стан психічного здоров'я особи, її приватне життя (ст. 6 ЗУ «Про психіатричну допомогу»)[177].

На підставі аналізу нормативно-правової бази можна стверджувати, що *об'єктом лікарської таємниці* є інформація про:

- факти звернення за медичною допомогою;
- стан здоров'я пацієнта;
- діагнозі та хвороби;
- медичний огляд та його результати;
- методи лікування;

---

[174] Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ: Закон України від 12.12.1991 р. // Відомості Верховної Ради. – 1992. – № 11. – Ст. 152.

[175] Про захист населення від інфекційних хвороб: Закон України від 06.04.2000 р. // Відомості Верховної Ради. – 2000. – № 29. – Ст. 228.

[176] Про донорство крові та її компонентів: Закон України від 23.06.1995 р. // Відомості Верховної Ради. – 1995. – № 23. – Ст. 183.

[177] Про психіатричну допомогу: Закон України від 09.06.2000 р. // Відомості Верховної Ради. – 2000. – № 19. – Ст. 143.

- інтимну та сімейну сторони життя;
- інші відомості, отримані при медичному обстеженні.

Суб'єктами збереження лікарської таємниці є медичні працівники та інші особи, яким у зв'язку з виконанням своїх професійних чи службових обов'язків стало відомо про об'єкти лікарської таємниці (лікарі, провізори, санітари, нянечки, студенти медичних вузів і коледжів, немедичний персонал мед установ та ін.). Вони не можуть бути допитані як свідки відповідно до п. 2 ч. 4 ст. 65 КПКУ[178].

Зазначені особи не мають права розголошувати такі відомості, крім передбачених законами випадків[179].

Варто також зазначити, що, попри хибне уявлення, що склалося в свідомості багатьох людей, ***не мають права*** отримувати інформацію, що становить лікарську таємницю без відповідної згоди пацієнта:

- чоловік або дружина пацієнта;
- батько або мати (по досягненні пацієнтом повноліття – 18 років);
- представники, адвокати (якщо відсутні чіткі документальні повноваження).

Також, обов'язок по збереженню лікарської таємниці та невикористання її на шкоду людині передбачено в *Клятві лікаря («Клятва Гіппократа»)*[180].

Лікарську таємницю (інформацію про пацієнта) необхідно відрізняти від *медичної таємниці* (інформації для пацієнта).

За нормами, що регулюють лікарську таємницю, лікар зобов’язаний надавати медичну інформацію пацієнтові (ст. 39 ЗУ «Основи законодавства України про охорону здоров'я»): пояснити пацієнту в доступній формі інформацію про стан його здоров'я, мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, зокрема наявності ризику для життя й

[178] Кримінальний процесуальний кодекс України від 13.04.2012 р. // Відомості Верховної Ради. – 2013. – № 9-13. – Ст. 88.
[179] Бабич О. Лікарська таємниця / О. Бабич // Управління закладом охорони здоров’я. – 2012. – № 4. – С. 11-16.
[180] Про Клятву лікаря: Указ Президента України від 15.06.1992 р. № 349 // Збірник указів Президента України. – 1992. – № 2.

здоров'я. Пацієнт має право ознайомитися з історією своєї хвороби та іншими документами, що можуть служити для подальшого лікування.

В особливих випадках, коли повна інформація може завдати шкоди здоров'ю пацієнта, лікар може її обмежити. В цьому випадку він інформує членів сім'ї або законного представника пацієнта, враховуючи особисті інтереси хворого. Так само лікар діє, якщо пацієнт знаходиться в несвідомому стані.

Ця норма практично є *єдиним випадком*, *коли людина може бути обмежена в отриманні персональної інформації про себе*.

Згідно зі ст. 145 ККУ за «*умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки, – карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років»*.

Також, «*розголошення службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником, відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, небезпечної для життя людини, або захворювання на синдром набутого імунодефіциту (СНІДу) і його результатів, що стали їм відомі у зв'язку з виконанням службових або професійних обов'язків – карається штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого»* (ст. 132 ККУ).

Нотаріальна таємниця

Нотаріальна таємниця – «*сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов'язки тощо*».[181]

Предметом нотаріальної таємниці є не тільки інформація, яка стала відома нотаріусу у процесі нотаріальної діяльності, а й відомості, які нотаріус отримав з інших джерел при виконанні своїх професійних обов'язків, а також процесуальна діяльність самого нотаріуса, спрямована на досягнення певного правового результату[182].

Нотаріус та особи, визначені у ст. 1 ЗУ «Про нотаріат», а також стажист нотаріуса зобов'язані зберігати нотаріальну таємницю, навіть якщо їх діяльність обмежується наданням правової допомоги чи ознайомленням з документами, а також, якщо нотаріальну дію, або дію, прирівняну до нотаріальної, не вчинили.

Обов'язок дотримання нотаріальної таємниці поширюється також на осіб, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків чи іншої роботи, осіб, залучених для вчинення нотаріальних дій у якості свідків, та на інших осіб, яким стали відомі відомості, що становлять предмет даної таємниці.

Порядок надання відомостей, що становлять нотаріальну таємницю, визначений ст. 8 ЗУ «Про нотаріат»:

- довідки про вчинені нотаріальні дії та копії документів, що зберігаються у нотаріуса, видаються нотаріусом виключно фізичним та юридичним особам, за дорученням яких або щодо яких вчинялись нотаріальні дії. У разі смерті особи чи визнанні її померлою, такі довідки видаються спадкоємцям померлого. У разі визнання особи безвісти зниклою, опікун, призначений для охорони майна полеглого, має право отримувати довідки про вчинені нотаріальні дії,

[181] Про нотаріат: Закон України від 2.09.1993 р. // Відомості Верховної Ради. – 1993. – № 39. – Ст. 383.

[182] Панталієнко Я. П. Нотаріальна таємниця – одне з загальних правил вчинення нотаріальних дій / Я. П. Панталієнко // Радник: Український юридичний портал. – [Електронний ресурс]. – Режим доступу: http://radnuk.info/statti/230-tsuv-pravo/3585-2010-01-29-17-38-54.html.

якщо це необхідно для збереження майна, над яким встановлено опіку;

- довідки про вчинені нотаріальні дії та інші документи надаються нотаріусом протягом десяти робочих днів на обґрунтовану письмову вимогу суду, прокуратури, органів, що здійснюють оперативно-розшукову діяльність, органів досудового слідства у зв'язку з кримінальним провадженням, цивільними, господарськими, адміністративними справами, справами про адміністративні правопорушення, що знаходяться в виробництв цих органів, з обов'язковим зазначенням номера справи та, додатково, гербової печатки відповідного органу;
- довідки про суму нотаріально посвідчених договорів, які необхідні виключно для встановлення дотримання законодавства з питань оподаткування, надаються нотаріусом протягом 10 робочих днів на обґрунтовану письмову вимогу органів доходів і зборів.

Довідки про наявність складеного заповіту та витяги із спадкового реєстру за виключенням заповідача видаються тільки після смерті заповідача.

Нотаріус не вправі давати показання як свідок щодо відомостей, що становлять нотаріальну таємницю, крім випадків, коли цього вимагають особи, за дорученням яких або щодо яких вчинялися нотаріальні дії.

Будь-яке втручання в діяльність нотаріуса, зокрема з метою перешкоджання виконанню ним своїх обов'язків або спонукання до вчинення ним неправомірних дій, у тому числі вимоги від нього, його стажиста, інших працівників, які перебувають у трудових відносинах з нотаріусом, відомостей, що становлять нотаріальну таємницю, до забороняється й тягне за собою відповідальність відповідно до законодавства (ст. 8-1 ЗУ «Про нотаріат»).

Однак сьогодні відсутній закон, який би чітко регулював питання відповідальності за розголошення нотаріальної таємниці. Питання відповідальності винних осіб за розголошення нотаріальної таємниці можна розглядати, керуючись загальними нормами українського законодавства. У відповідності зі ст. 1166 ЦКУ «*майнову шкоду,*

заподіяну неправомірними рішеннями, діями чи бездіяльністю особистим немайновим правам фізичної або юридичної особи, відшкодовується в повному обсязі особою, яка заподіяла шкоду». Нотаріусу під час нотаріального процесу за участю перекладача необхідно роз'яснювати відповідальність перекладача на підставі цієї статті. Що ж до стажиста і помічника, то при укладанні з ними трудового договору необхідно закріплювати цю норму.

Адвокатська таємниця

Адвокатська таємниця – «*будь-яка інформація, що стала відомою адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у трудових відносинах з адвокатом, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених Законом підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, змісту рад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи і відомості, отримані адвокатом при здійсненні адвокатської діяльності*».[183]

Суб'єктами, на яких поширюється обов'язок збереження інформації, що становить адвокатську таємницю, є адвокат, його помічник, стажер та особи, що знаходяться в трудових відносинах з адвокатом, адвокатським бюро, адвокатським об'єднанням, а також на особу, щодо якої припинено або призупинено право на зайняття адвокатською діяльністю. Їм забороняється розголошувати відомості, що становлять предмет адвокатської таємниці, і використовувати їх у своїх інтересах або в інтересах третіх осіб.

У разі пред'явлення клієнтом вимог до адвоката у зв'язку з адвокатською діяльністю адвокат звільняється від обов'язку збереження адвокатської таємниці в межах, необхідних для захисту його прав та інтересів (ч. 4 ст. 22 ЗУ «Про адвокатуру та адвокатську діяльність»).

[183] Про адвокатуру та адвокатську діяльність: Закон України від 05.07.2012 р. // Відомості Верховної Ради. –2012. – № 27. – Ст. 282.

У такому випадку суд, орган, що здійснює дисциплінарне провадження стосовно адвоката, інші органи чи посадові особи, які розглядають вимоги клієнта до адвоката або яким стало відомо про пред'явлення таких вимог, зобов'язані вжити заходів для запобігання доступу сторонніх осіб до адвокатської таємниці та її розголошення.

Особи, винні в доступі сторонніх осіб до адвокатської таємниці або її розголошенні, несуть відповідальність згідно із законом.

Документи, пов'язані з виконанням адвокатом доручення, не підлягають оглядові, розголошенню чи вилученню без його згоди.

Відповідно до норм ст. 10 Правил адвокатської етики[184], «*інформація та документи можуть втратити статус адвокатської таємниці за письмовою заявою клієнта (особи, якій відмовлено в укладення договору про надання правової допомоги) з передбачених Законом України «Про адвокатуру та адвокатську діяльність» підстав. При цьому інформація та документи, отримані від третіх осіб, що містять відомості про них, можуть поширюватися з урахуванням вимог законодавства з питань захисту персональних даних*».

За розголошення адвокатської таємниці дисциплінарна відповідальність адвоката передбачена ст. 33-42 ЗУ «Про адвокатуру та адвокатську діяльність». Крім того, відповідно до ч. 3 ст. 47 КПКУ «*захисник не має права розголошувати відомості, що стали йому відомі у зв'язку з участь у кримінальному провадженні і становлять адвокатську або іншу охоронювану законом таємницю*».

Податкова таємниця

В Україні правового інституту ***податкової таємниці*** на сьогодні не існує, але встановлені окремі норми чинного законодавства, що стосуються правових обмежень на доступ до інформації, отриманої в ході податкової діяльності.

Відповідно до ст. 17.1.9 Податкового кодексу України[185] платник податків має право «*на нерозголошення контролюючим органом*

[184] Правила адвокатської етики. – [Електронний ресурс]. – Режим доступу: http://document.ua/pravila-advokatskoyi-etiki-doc152603.html.

[185] Податковий кодекс України від 02.12.2010 р.// Відомості Верховної Ради. – 2011. – № 13-17. – Ст. 112.

(посадовими особами) відомостей про такого платника без його письмової згоди, та відомостей, що становлять конфіденційну інформацію, державну, комерційну чи банківську таємницю та стали відомими під час виконання посадовими особами службових обов'язків, крім випадків, коли це прямо передбачено законами». Згідно зі ст. 21.1 посадові особи контролюючих органів зобов'язані: не допускати розголошення ІзОД, що збирається, використовується, зберігається при реалізації функцій, покладених на контролюючі органи.

Інформація, що збирається, використовується та формується контролюючими органами у зв'язку з обліком платників податків, вноситься до інформаційних баз даних і використовується з урахуванням обмежень, передбачених для податкової інформації з обмеженим доступом (ст. 63.12 Податкового кодексу України).

Аудиторська таємниця

Так само як і податкова таємниця, аудиторська таємниця не має свого інституту таємниці.

Аудиторська діяльність визначається як підприємницька діяльність з проведення і надання послуг, супутніх аудиту. Аудит – це незалежна перевірка фінансової або бухгалтерської звітності організації.

До ***аудиторської таємниці*** можна віднести «*інформацію, отриману при проведенні аудиту та виконанні інших видів аудиторських послуг*» (п. 4 ст. 19 ЗУ «Про аудиторську діяльність»)[186].

Неналежне зберігання аудиторської таємниці аудиторами і аудиторськими фірмами тягне відповідальність, передбачену ст. 21 ЗУ «Про аудиторську діяльність». Аудитор (аудиторська фірма) несе майнову та іншу цивільно-правову відповідальність відповідно до договору та закону. Але розмір майнової відповідальності аудиторів (аудиторських фірм) не може перевищувати фактично завданих замовнику збитків з їх вини.

[186] Про аудиторську діяльність: Закон України від 22.04.1993 р. // Відомості Верховної Ради. – 1993. – № 23. – Ст. 243.

За неналежне виконання професійних обов'язків до аудитора (аудиторської фірми) можуть бути застосовані Аудиторською палатою України стягнення у вигляді попередження, зупинення дії сертифіката на строк до одного року або анулювання сертифіката, виключення з Реєстру (ст. 22 ЗУ «Про аудиторську діяльність»).

У разі розголошення аудиторської таємниці, організація має право зажадати компенсації для відшкодування понесених збитків.

Журналістська таємниця

Журналістська таємниця або як її ще називають, ***таємниця журналістських джерел***, також прямо в законодавстві не визначена. Але можна вважати, що її становить інформація про особу, що побажала залишитися анонімним джерелом інформації журналіста, яка стала відома журналісту, посадовим особам, журналістському персоналу та службовому персоналу журналістської установи при здійсненні ними своїх професійних обов'язків.

Ще в 1954 р. на Другому Всесвітньому Конгресі Міжнародної федерації журналістів у м. Бордо було прийнято Декларацію принципів поведінки журналіста, п. 6 якої закріплює, що «*журналіст зобов'язаний дотримуватися професійної таємниці і не розголошувати джерело інформації*»[187].

Захист журналістських джерел закріплений в різних міжнародних документах. Наприклад, ст. 10 Європейської конвенції з прав людини гарантує захист журналістських джерел[188]. Для більш точного зазначення з цього питання Радою Європи була прийнята Рекомендація № R(2000)7 «Про право журналістів не розкривати свої джерела інформації». Це право має бути визнане і забезпечене для будь-якої фізичної та юридичної особи, регулярно або професійно задіяної в зборі та публічному поширенні інформації через будь-які

[187] Декларация принципов поведения журналиста Международной Федерации Журналистов. – [Електронний ресурс]. – Режим доступу: http://www.presscouncil.ru/index.php/teoriya-i-praktika/dokumenty/754-deklaratsiya-printsipov-povedeniya-zhurnalista-mezhdunarodnoj-federatsii-zhurnalistov.

[188] Европейская конвенция о защите прав человека и основополагающих свобод. – [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.

засоби масової інформації[189].

У нашій країні відповідно до ч. 3 ст. 25 ЗУ «Про інформацію» журналіст має права не розкривати джерело інформації або інформацію, яка дозволяє встановити джерела інформації, крім випадків, коли його зобов'язали для цього рішенням суду.

Ст. 26 ЗУ «Про друковані засоби масової інформації (пресу) в Україні» наділяє журналіста правом «*на збереження таємниці авторства та джерел інформації, за винятком випадків, коли ці таємниці обнародуються на вимогу суду*». Журналіст зобов'язаний «*задовольняти прохання осіб, які надають інформацію, щодо їх авторства або збереження таємниці авторства*»[190].

З цим перетинається норма ч. 9 ст. 59 ЗУ «Про телебачення і радіомовлення», де вказано, що один з обов'язків телерадіоорганізації – «*зберігання в таємниці, на підставі документального підтвердження, відомостей про особу, яка передала інформацію або інші матеріали за умови нерозголошення її імені*»[191].

Інсайдерська таємниця

Останнім часом в області інформаційної безпеки актуальними стали повідомлення про те, що більшу загрозу ринку цінних паперів представляють угоди вчинені з використанням інсайдерської інформації.

Термін «інсайдерський» в перекладі з англійської означає «внутрішній», тобто *інсайдерська інформація* – це внутрішня інформація компанії. Наслідки використання інсайдерської інформації при здійсненні угод можуть бути наступними:

- використання інформації ставить володаря в переважне становище, що дає йому можливість здійснювати маніпулювання цінами на біржових торгах;
- використання інсайдерської інформації приносить економічну

[189] Рекомендация № R (2000)7 Комитета Министров Совета Европы. – [Електронний ресурс]. – Режим доступу: http://www.coe.kiev.ua/docs/km/r(2000)7.htm.

[190] Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. // Відомості Верховної Ради. – 1993. – № 1. – Ст. 1.

[191] Про телебачення і радіомовлення: Закон України від 21.12.1993 р. // Відомості Верховної Ради. – 1994. – № 10. – Ст. 43.

вигоду її володареві після виконання зобов'язань, що виникли на підставі угод, укладених з використанням такої інформації[192].

Директива 2003/6/ЄС «Про інсайдерську діяльність та ринковому маніпулюванні, зловживаннях на ринку»[193] визначає ***інсайдерську інформацію*** як інформацію, публічно не розкриту, що володіє відомою цінністю, що відноситься до одного або кількох емітентів фінансових інструментів або до одного чи декількох таких інструментів, яка в разі розкриття неодмінно зробить значний вплив на котирування фінансових інструментів або відповідних деривативів.

У нашій країні інсайдерська таємниця регулюється ЗУ «Про цінні папери та фондовий ринок». Згідно зі ст. 44, ***інсайдерська таємниця*** – це «*неоприлюднена інформація про емітента, його цінні папери або правочини щодо них, оприлюднення якої може значно вплинути на вартість цінних паперів*»[194] .

За незаконне використання інсайдерської інформації передбачається кримінальна відповідальність, згідно зі ст. 232-1 ККУ.

Таємниця страхування

Таємниця страхування – *це конфіденційна інформація щодо діяльності фінансового становища страхувальника – клієнта страховика, яка стала відома йому при взаєминах з клієнтом або третіми особами при проведенні діяльності в галузі страхування, розголошення якої може принести матеріальну чи моральну шкоду клієнту* (ст. 40 ЗУ «Про страхування»)[195].

Посадові особи уповноваженого органу у випадку розголошення в будь-якій формі відомостей, що є таємницею страхування, несуть відповідальність, передбачену законом[196].

---

[192] Добровольский В. И. Инсайдерская информация в мировой практике, служебная информация и коммерческая тайна в России // Предпринимательское право. – 2008. – № 4. – С. 11-16.

[193] Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) OJ L 096, 12.04.2003. P/ 0016-0025. – [Електронний ресурс]. – Режим доступу: https://www.esma.europa.eu/system/files/Dir_03_6.pdf.

[194] Про цінні папери та фондовий ринок: Закон України від 23.02.2006 р. // Відомості Верховної Ради. – 2006. – № 31. – Ст. 268.

[195] Про страхування: Закон України від 07.03.1996 р. // Відомості Верховної Ради. – 1996. – № 18. – Ст. 78.

[196] Пасічний В. О. Страхування: Навч. посібник для студентів вищих навчальних закладів **/** В. О. Пасічний, В. В. Жван; Харк. нац. акад. міськ. госп-ва. – Х.: ХНАМГ, 2009. – С. 142-146.

Інформація про юридичних та фізичних осіб, яка містить таємницю страхування, подається страхувальником у наступних випадках:

- на письмовий запит або з письмового дозволу власника такої інформації;
- на письмову вимогу суду або за рішенням суду;
- органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, податкової міліції на їх письмову вимогу відносно операцій страхування конкретної юридичної або фізичної особи за конкретним договором страхування у разі порушення кримінальної справи відносно даної фізичної або юридичної особи;
- центральному органу виконавчої влади з питань фінансового моніторингу відповідно до ЗУ «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму».

Обмеження щодо отриманої інформації, що містить таємницю страхування, не поширюються на службовців Уповноваженого органу, які в межах повноважень, наданих чинним Законом, здійснюють державний нагляд за страховою діяльністю.

Законом передбачено вичерпний перелік випадків, при яких може надаватися інформація, що містить таємницю страхування. Розголошення таємниці страхування спричиняє за собою адміністративну відповідальність відповідно до ст. 164 КУпАП в розмірі від 9 до 18 неоподатковуваних мінімумів доходів громадян, а в окремих випадках (умисне розголошення таємниці страхування) – кримінальну відповідальність згідно зі ст. 232 ККУ: «*умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, вчинене з корисливих чи інших особистих мотивів і таке, що завдало істотної шкоди суб'єкту господарської діяльності*», карається штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з позбавленням 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.

Таємниця сповіді

Таємниця сповіді законодавчо чітко не визначена. Але в ст. 3 ЗУ «Про свободу совісті та релігійні організації» передбачається, що «*ніхто не має права вимагати від священнослужителів відомостей, отриманих ними при сповіді віруючих*»[197].

Ця таємниця поширюється тільки на інформацію, передану священнослужителю під час сповіді, а також особливою роллю і статусом церкви. Надати захист відомостям, які довіряються особою під час сповіді представнику релігійної організації, держава визнає особливість відносин між віруючими і церквою і риси, характерні обряду сповіді. Тим самим, законом надається захист прав особистості на недоторканність особистого і сімейного життя, свободи думки, свободи віросповідання.

Згідно з ч. 2 п. 5 ст. 65 КПКУ священнослужителі не можуть бути допитані як свідки про відомості, одержані ними на сповіді віруючих.

Аналогічна норма міститься й в ст. 51 ЦПКУ, де наданий вичерпний перелік осіб, які не підлягають допиту як свідки, в тому числі і священнослужителі – про відомості, одержані ними на сповіді віруючих.

Таємниця усиновлення

Таємниця усиновлення – це відомості про «*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»* відповідно до ст. ст. 226-228 Сімейного кодексу України[198].

Особи, яким у зв'язку з виконанням службових обов'язків доступна інформація, що містить таємницю усиновлення, а також інші особи, яким стало відомо факт усиновлення, зобов'язані не

[197] Про свободу совісті та релігійні організації: Закон України від 23.04.1991 р. // Відомості Верховної Ради. – 1991. – № 25. – Ст. 283.

[198] Сімейний кодекс України // Офіційний вісник України. – 2002. – № 7.– Ст. 273.

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) – передбачається кримінальна відповідальність відповідно до ст. 168 ККУ.

Таємниця авторства

Таємниця авторства згадується в ст. 26 ЗУ «Про друковані засоби масової інформації (пресу) в Україні», згідно з якою цією таємницею є «конфіденційна інформація про особу (автора), оскільки йдеться про вирішення особи обмежити доступ до інформації про себе».

Автор будь-якого твору має право:

- вимагати визнання свого авторства шляхом зазначення належним чином імені автора на творі і його примірниках і за будь-якого публічного використання твору, якщо це практично можливо;
- забороняти під час публічного використання твору згадування свого імені, якщо він як автор твору бажає залишитись анонімом;
- вибирати псевдонім, зазначати і вимагати зазначення псевдоніма замість справжнього імені автора на творі і його примірниках і під час будь-якого його публічного використання;
- вимагати збереження цілісності твору і протидіяти будь-якому перекрученню, спотворенню чи іншій зміні твору або будь-якому іншому посяганню на твір, що може зашкодити честі і репутації автора[199].

Таємниця голосування

Таємниця голосування при виборах до органів державної влади та органів місцевого самоврядування гарантована ст. 71 Конституції України: «*Вибори до органів державної влади та органів*

[199] Про авторське право та суміжні права: Закон України від 23.12.1994 р. // Відомості Верховної Ради. – 1994. – № 13.– Ст. 64.

місцевого самоврядування є вільними і відбуваються на основі загального, рівного і прямого виборчого права шляхом ***таємного голосування***».

Таємність волевиявлення виборців під час голосування на виборах встановлена спеціальними законами про вибори (референдум). Очевидно, що таємниця голосування, як вид таємної інформації, поширюється на пряме волевиявлення виборців при обранні представницьких органів влади або на державні посади, наділені представницьким мандатом, і ця таємниця не поширюється на таємне голосування, застосовувана при обранні на будь-які інші посади (наприклад, голосування за керівників колегіальних органів влади).

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, – карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від одного до трьох років з позбавленням права обіймати певні посади чи займатися певного діяльністю на строк до трьох років (ст. 159 ККУ передбачена кримінальна відповідальність).

<u>Таємниця зв'язку (листування)</u>

Ст. 9 ЗУ «Про телекомунікації» передбачає «*захист* ***таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій***. *Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом. Оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічних та організаційних заходів щодо захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами»*[200].

[200] Про телекомунікації: Закон України від 18.11.2003 р. // Відомості Верховної Ради.– 2004.– № 12. – Ст. 155.

Також й в ст. 1, 3, 8 ЗУ «Про поштовий зв'язок»[201] йде мова про «***таємниці інформації у сфері надання послуг поштового зв'язку***». Це дає підстави говорити про існування ***таємниці зв'язку*** як різновиду професійної таємниці в Україні.

Це підтверджує і ст. 163 ККУ, яка передбачає кримінальну відповідальність за «*порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер*».

Висновки

У сучасному законодавстві чіткого визначення ПТ не існує.

До ПТ відноситься інформація, з якою мають справу представники так званих «саморегульованих» професій та інші особи, яким ці відомості були довірені у зв'язку з їх професійним становищем. До ПТ слід віднести наступні таємниці: лікарську, нотаріальну, адвокатську, аудиторську, журналістську, інсайдерську, страхування, сповіді, усиновлення, авторства, голосування, зв'язку (листування).

Правові інститути зазначених ПТ знаходяться в стадії формування та вимагають подальших наукових досліджень і вдосконалення нормативно-правової бази щодо підтримки всіх їх складових: загальної частини, режиму секретності (конфіденційності) і санкцій.

[201] Про поштовий зв'язок: Закон України від 4.10.2001 р. // Відомості Верховної Ради. – 2002. – № 6. – Ст. 39.

8 ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

§8.1. Поняття, ознаки та законодавче визначення персональних даних

На сучасному етапі демократичних перетворень Україна визнає людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю.

Передумовою нормативної регламентації поняття «персональні дані» (ПД) в законодавстві України стали міжнародні документи, які узагальнюють юридичне визначення поняття «ПД».

Згідно зі ст. 2 (а) Директиви 95/46/ЄС Європейського парламенту та Ради Європейського Союзу «Про захист осіб у зв'язку з обробкою персональних даних та про вільний обіг цих даних»[202]: *«ПД означають будь-яку інформацію, пов'язану з ідентифікованою фізичною особою («суб'єктом даних»); ідентифікованою особою є особа, яка може бути ідентифікована прямо або побічно, зокрема, за допомогою посилання на ідентифікаційний номер або на один або декілька чинників, специфічних для її фізичної, психологічної, ментальної, економічної, культурної або соціальної ідентичності».*

В ст. 2 Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних»[203] під ПД розуміють *«будь-яку інформацію, що стосується конкретно визначеної особи або особи, яка може бути конкретно визначено (суб'єкт даних)».*

В Україні вперше норми, що стосуються ПД, були введені Конституцією України. Ст. 32 визнає, що *«ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених*

[202] Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных. – [Електронний ресурс]. – Режим доступу: http://www.datepersonale.md/file/Directiva_95_46_ru.pdf.

[203] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. – [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/MU81311.html.

Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, встановлених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»[204].

Також, відповідно до ст. 10 ЗУ «Про звернення громадян»[205] *«не допускається розголошення одержаних із звернень відомостей про особисте життя громадян без їх згоди чи відомостей, що становлять державну або іншу таємницю, що охороняється законом, та іншої інформації, якщо це ущемляє права і законні інтереси громадян»*.

Конфіденційна інформація про особу, визначена Конституцією України, є одним з найважливіших елементів конституційно-правового статусу людини і громадянина, і становить особливий вид ІзОД.

Правовий інститут ПД в Україні можна представити у вигляді трьох складових.

Щодо ***загальної частини*** – *першої складової правового інституту* ПД, в ст. 11 ЗУ «Про інформацію» закріплено, що інформація про фізичну особу (персональні дані) – це *«відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована»*. Аналогічне визначення ПД закріплено й в ст. 2 ЗУ «Про захист персональних даних»[206].

Отже, ПД – це будь-які відомості, що відносяться до фізичної особи, на підставі яких ця особа може бути ідентифікована.

В ч. 2 ст. 11 ЗУ «Про інформацію» перераховані відомості, що відносяться до конфіденційної інформації про фізичну особу, зокрема, *«дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження»*.

Звідси видно, що законодавець не наводить вичерпного переліку відомостей, які можуть становити ПД фізичної особи.

---

[204] Конституція України. // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.

[205] Про звернення громадян: Закон України від 02.10.1996 р. // Відомості Верховної Ради. – 1996. – № 47. – Ст. 256.

[206] Про захист персональних даних: Закон України від 01.06.2010 р. // Відомості Верховної Ради. – 2010. – № 34. – Ст. 481.

На визначення вмісту інформації, що становить ПД, спрямовані й інші нормативно-правові акти, зокрема, органів судової влади. Аналіз їх матеріалів судової практики дає підстави віднести до ПД фізичної особи такі дані:

- інтимні сторони життя;
- захворювання;
- непорядні вчинки;
- злочинну діяльність;
- відомості, які ганьблять потерпілого і його близьких;
- майнове становище та ін.[207]

Також при визначенні ПД законодавець не в повному обсязі врахував ряд положень розглянутих вище міжнародних нормативно-правових актів, згідно з якими ПД можна розділити на дві групи:

- *дані загального вмісту* – прізвище, ім'я, по батькові, дата і місце народження, освіта та ін.;
- *дані приватного змісту* – расове походження, політичні, релігійні та інші віросповідання, а також здоров'я або приватне життя[208].

При класифікації ПД слід приділити особливу увагу також біометричним (антропометричним) даним, даним про фізіологічні особливості людини, на основі яких можна його ідентифікувати (зріст, вага, колір волосся, група крові, голос, почерк, відбитки пальців, результати аналізу ДНК, цифровий образ особи, сітківка ока тощо). Саме біометрична ідентифікація може дати абсолютно точну картину ідентифікації громадянина за допомогою унікальних біологічних параметрів. Не існує двох людей з однаковими біометричними ознаками[209].

---

[207] Марущак А. І. Інформаційне право: Доступ до інформації: Навчальний посібник. – К.: КНТ, 2007. – С. 27-28.

[208] Основи інформаційного права України: навч. посіб. / В. С. Цимбалюк, В. Д. Гавловський, В. М. Брижко та ін.; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. 2-ге вид., переробл. і допов.– К.: Знання, 2009. – С. 282–365.

[209] Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. – [Електронний ресурс]. – Режим доступу: http://www.vestnik-pravo.mgu.od.ua/archive/juspradenc6-3-1/23.pdf.

Потреба в надійній ідентифікації, досягнутий рівень біометрики, а також прагнення України до спрощення візового режиму з державами Європейського Союзу привели до прийняття Закону України «Про Єдиний державний демографічний реєстр і документах, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[210].

Перелік біометричних даних особистості в ЗУ «Про захист персональних даних» відсутній, але дії по них, як правило, мають спеціальне правове регулювання, зокрема, такі дані мають особливий статус у сфері оперативно-процесуальної діяльності.

Сьогодні в нашій країні діє більше двох десятків законодавчих актів, що регулюють суспільні відносини, пов'язані з відомостями, що містять ПД. Серед них: Конституція України, Закони України «Про інформацію», «Про нотаріат», «Про телекомунікації», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про міліцію», «Про банки і банківську діяльність», «Основи законодавства про охорону здоров'я» та ін.

В 2010 р. Указом Президента України № 1085/2010 «Про оптимізацію системи центральних органів виконавчої влади»[211] створена Державна служба з питань захисту ПД як центрального органу влади України, діяльність якого спрямовується і координується Кабінетом Міністрів України. У 2011 р. Указом Президента України № 390 затверджено Положення про Державну службу України з питань захисту ПД[212].

В ЗУ «Про захист персональних даних» наведено вичерпний список *суб'єктів* інформаційних відносин, пов'язаних з ПД:

- суб'єкт ПД – це фізична особа, ПД якого обробляються;

[210] Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. // Відомості Верховної Ради. – 2013. – № 51. – Ст. 761.

[211] Про оптимізацію системи центральних органів виконавчої влади: Указ Президента України від 09.12.2010 р. № 1085/2010 // Офіційний вісник України. – 2010. – № 94. – С. 15. – Ст. 3334.

[212] Про Положення про Державну службу України з питань захисту персональних даних: Указ Президента України від 06.04.2011 р. № 390/2011 // Офіційний вісник України. – 2011. – № 28. – С. 36. – Ст. 1160.

- володілець ПД – фізична або юридична особа, яка визначає мету обробки ПД, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;
- розпорядник ПД – фізична або юридична особа, якій володільцем ПД або законом надано право обробляти ПД від імені володільця;
- третя особа – будь-яке особа, за винятком суб'єкта ПД, володільця або розпорядника ПД і Уповноваженого Верховної Ради України по правам людини, якій володільцем або розпорядником ПД здійснює передачу ПД;
- Уповноважений Верховної Ради з прав людини.

Володільцем чи розпорядником ПД можуть бути підприємства, установи і організації всіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють ПД відповідно до закону.

Розпорядником ПД, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить сфері управління цього органу.

Володілець ПД може доручати обробку ПД розпоряднику, відповідно до договору, складеною в письмовій формі. Розпорядник може обробляти ПД тільки з метою і в обсязі, зазначених у договорі.

Уповноважений Верховної Ради з прав людини (омбудсмен) є посадовою особою, статус якого визначається Конституцією України (ст. 101), Законами України «Про Уповноваженого Верховної Радою з прав людини»[213] та «Про державну службу»[214], а також іншими законами України.

Уповноважений здійснює свою діяльність незалежно від інших державних органів та посадових осіб. Діяльність Уповноваженого доповнює існуючі засоби захисту конституційних прав і свобод

[213] Про Уповноваженого Верховної Ради України з прав людини: Закон України від 23.12.1997 р. // Відомості Верховної Ради. – 1998. – № 20. – Ст. 99.
[214] Про державну службу: Закон України від 162.1993 р. // Відомості Верховної Ради. – 1993 – № 52. – Ст. 490.

людини і громадянина, не відміняє їх і не тягне перегляду компетенції державних органів, що забезпечують захист і відновлення порушених прав і свобод.

Повноваження Уповноваженого не можуть бути припинені чи обмежені у разі закінчення строку повноважень Верховної Ради України або її розпуску (саморозпуску), введення воєнного чи надзвичайного стану в Україні або в окремих її місцевостях. Місцезнаходженням Уповноваженого є столиця України – місто Київ. Для звернення до Уповноваженого можна використовувати й офіційний веб-сайт (http://ombudsman.gov.ua).

Ст. 55 Конституції України проголошено право будь-якого громадянина, звертатися до Уповноваженого з прав людини за захистом своїх прав.

Сфера компетенції українського омбудсмена є досить широкою. Оскільки в законі немає ні єдиного винятку щодо поширення юрисдикції Уповноваженого на конкретних посадових осіб, предметом його контролю є діяльність усіх посадових та службових осіб органів державної влади та органів місцевого самоврядування. Підпадає під юрисдикцію Уповноваженого і діяльність суддів. Але оскільки суди у своїй діяльності є незалежними і під час здійснення своїх функцій не можуть піддаватися ніякому впливу. У своїй діяльності вони підкоряються лише закону. Тому контрольні функції Уповноваженого щодо діяльності суддів стосуються не суті судових рішень, а пов'язані, зокрема, з порушенням термінів розгляду справ в судах, недотриманням процесуальних норм. Сфера компетенції Уповноваженого поширюється також на інших осіб, які в тому чи іншому обсязі виконують державно-владні функції[215].

В області захисту ПД Уповноважений має досить широке коло повноважень, визначене ст. 23 ЗУ «Про захист персональних даних».

Отже, основні функції омбудсмена полягають у здійсненні контролю над діяльністю виконавчих та інших органів державної

[215] Карпачева Н. И. Состояние соблюдения и защиты прав и свобод человека в Украине: Первый ежегодный доклад Уполномоченного Верховной Рады Украины по правам человека / Перевод с украинского. – Харьков: Консум, 2002. – С. 29–38.

влади на дії тих чи інших органів або посадових осіб, що призвели до порушення прав і свобод людини та громадянина. Законодавчо Уповноваженому надано достатньо ефективні засоби впливу на порушників законодавства про захист ПД, контролю діяльності суб'єктів, що здійснюють їх обробку, а також захисту прав суб'єктів відповідної інформації.

Особисті немайнові права на ПД, які належать кожній фізичній особі, є невід'ємними і непорушними. *Суб'єкт ПД має право:*

1) знати джерела збору, місцезнаходження своїх ПД, мета їх обробки, місцезнаходження або місце проживання (перебування) володільця або розпорядника ПД або дати відповідальне доручення для отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
2) отримувати інформацію про умови надання доступу до ПД, зокрема, інформацію про третіх осіб, яким передаються його ПД;
3) на доступ до своїх ПД;
4) отримувати не пізніше як за тридцять календарних днів з дня отримання запиту, крім випадків, передбачених законодавством, відповідь на те, обробляються чи його ПД, а також отримувати вміст таких ПД;
5) пред'являти вмотивовану вимогу щодо зміни або знищення своїх ПД будь-яким володільцем і розпорядником, якщо ці дані обробляються незаконно чи є недостовірними;
6) пред'являти вмотивовану вимогу володільцю ПД із забороною проти обробки своїх ПД;
7) на захист своїх ПД 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 ;
8) звертатися із скаргами на обробку своїх ПД до Уповноваженого, або до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист ПД;
10) вносити застереження стосовно обмеження права на обробку своїх ПД;
11) відкликати згоду на обробку ПД;
12) знати механізм автоматичної обробки ПД;
13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Також законодавчо встановлені і *об'єкти захисту,* щодо персоніфікованої інформації та випадки її обмеження:

1) об'єктами захисту є ПД.
2) ПД можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією ПД, які стосуються особи, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень.
3) ПД, зазначені в декларації про майно, доходи, витрати та зобов'язання фінансового характеру, оформленої за формою і в порядку, встановленим ЗУ «Про засади запобігання та протидії корупції», не належать до ІзОД, крім відомостей, визначених ЗУ «Про засади запобігання та протидії корупції».

Не відноситься до ІзОД інформація про отримання в будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених ст. 6 ЗУ «Про доступ до публічної інформації» (публічна ІзОД).

Законом може бути заборонено віднесення інших відомостей, що є ПД, до ІзОД.

§8.2. Обробка персональних даних

Відповідно до *другої складової правового інституту ПД* (режиму ПД) визначимо наступне.

Головний зміст і призначення будь-якої інформаційної діяльності полягає в задоволенні політичних, економічних, фінансових, технологічних, культурних, інформаційних та інших потреб людини,

суспільства і держави, в результаті здійснення певних дій. Дії з ПД припускають обробку даних в процесі їх збирання, реєстрації, накопичення, збереження і поширення.

Обробка даних – *це будь-яка дія або сукупність дії, таких як збір, реєстрація, накопичення, збереження, адаптація, зміна, відновлення, використання та поширення (реалізація, передача), знеособлення, знищення ПД, у тому числі з використанням інформаційних (автоматичних) систем* (ст. 2 ЗУ «Про захист персональних даних»).

Основні дії з ПД можна представити у вигляді схеми *(рис. 8.1*).[216]

Кожна з дій несе змістовне і правове навантаження.

Збір ПД передбачає дії підбору та впорядкування відомостей про фізичну особу (ст. 12).

Реєстрація ПД – це фіксування ідентифікаційних реквізитів про фізичну особу з метою обліку та систематизації ПД.

Накопичення ПД передбачає дії об'єднання та систематизації відомостей про фізичну особу або групі фізичних осіб, або внесення цих даних до бази ПД (п. 1 ст. 13).

Переробка ПД – внесення змін і доповнень (модифікація) до даних.

Поширення ПД передбачає дії передачі відомостей про фізичну особу за згодою суб'єкта ПД (п. 1 ст. 14).

Доступ до ПД передбачає наявність у фізичних осіб права знати, які відомості, і з якою метою, ким збираються, реєструються, накопичуються, зберігаються і поширюються. Людина не може бути обмежена у праві доступу до своїх ПД.

Порядок доступу до ПД третіх осіб визначається умовами згоди суб'єкта ПД, наданих володільцю ПД на обробку цих даних, або відповідно до вимог закону. Порядок доступу третіх осіб до ПД, які знаходяться у володінні розпорядника публічної інформації, визначається ЗУ «Про доступ до публічної інформації».

---

[216] Інформаційне право та правова інформатика у сфері захисту персональних даних / Авт. кол-в: В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець: Монографія; За ред. доктора економічних наук, професора, члена-кореспондента Академії правових наук України М. Швеця. – К.: НДЦПІ АПрН України, 2006. – С. 100–107.

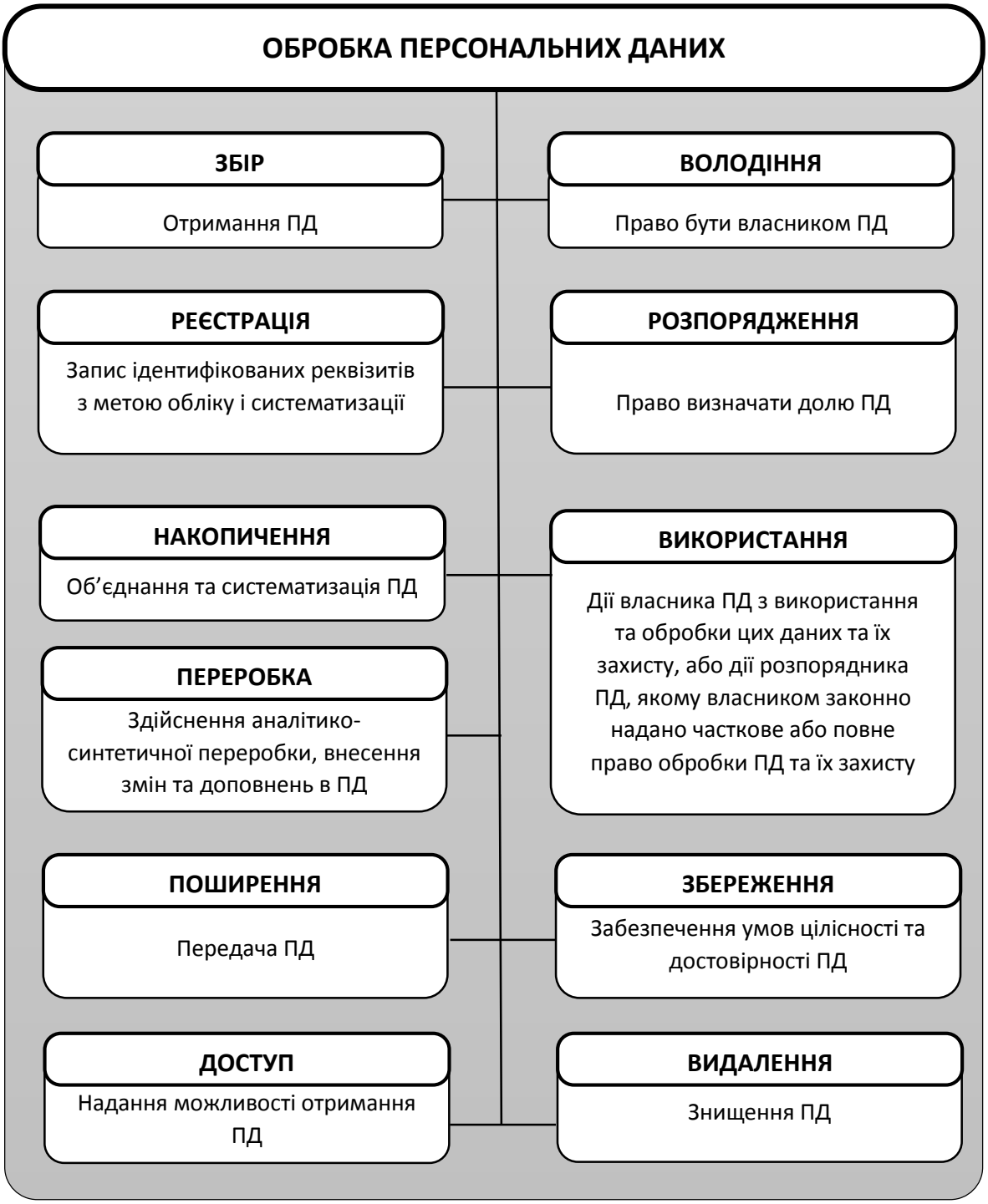

Рис. 8.1. Обробка персональних даних

Доступ до ПД третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог закону або не може їх забезпечити.

Суб'єкт відносин, пов'язаних з ПД, подає запит щодо доступу до ПД володільцю цих даних.

У запиті зазначаються:

- прізвище, ім'я та по батькові, місце проживання (місце

знаходження) і реквізити документа, що посвідчує фізичну особу, яка подає запит;

- найменування, місцезнаходження юридичної особи, яка подає запит, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи;
- прізвище, ім'я та по батькові, а також інші відомості, що дозволяють ідентифікувати фізичну особу, про якого запитується;
- відомості про базу ПД, щодо якої подається запит, відомості про володільця чи розпорядника ПД;
- перелік запитуваних ПД;
- мета чи правові підстави для запиту.

Термін вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження. Протягом цього терміну володілець ПД доводить до відома особи, яка подає запит, що запит буде задоволено, або що відповідні ПД не підлягають наданню, із зазначенням підстави, визначеного у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом. Суб'єкт ПД має право на отримання будь-яких відомостей про себе у будь-якого суб'єкта відносин, крім випадків, встановлених законом.

Володіння ПД передбачає право використання та право на захист ПД.

Розпорядження ПД передбачає право визначати використання ПД.

Використання ПД містить в собі право на здійснення дій з ПД і право на захист своїх ПД, а також право на надання третій особі часткового або повного використання відомостей, що становлять ПД.

Збереження ПД передбачає створення умов належної цілісності та достовірності відомостей про особу.

Видалення або ***знищення*** ПД передбачено у випадках (ст. 15):

1) закінчився строк збереження даних, визначених згодою суб'єкта ПД на обробку цих даних або законом;

2) припинені правовідносини між суб'єктом ПД і володільцем або розпорядником, якщо інше не передбачено законом;
3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;
4) набрання законної сили рішенням суду з видалення або знищення ПД.

Законодавчо передбачено загальні та спеціальні вимоги до обробки ПД.

Згідно зі ст. 6 ЗУ «Про захист персональних даних» обробка ПД здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, який відповідає певним цілям такої обробки.

Обробка ПД здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта цих даних, або у випадках, передбачених законами України, та у порядку, встановленому законодавством.

Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Якщо обробка ПД необхідна для захисту життєво важливих інтересів суб'єкта ПД, обробляти дані без його згоди можна до часу, коли отримання згоди стане можливим.

ПД обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, в яких вони збиралися або подальшому оброблялися.

Згідно зі ст. 7 забороняється обробка ПД про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

На основі розглянутого можна виділити ***основні права володільця*** ПД. Володілець має право знати:

- хто і де обробляє його ПД;
- кому передаються його ПД;

- де зберігаються його ПД;
- як реалізувати право на доступ до своїх ПД;
- механізм обробка його ПД (у разі їх автоматичної обробки).

Крім того, до основних прав володільця відноситься і право вимагати знищення або виправлення ПД, якщо вони обробляються незаконно чи є недостовірними.

З цими правами пов'язані вісім основних принципів обробки ПД, сформульованих у Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (ст. 5-8):

1) *принцип законності*: ПД повинні оброблятися сумлінно і законно, причому тільки при наявності підстав і з дотриманням вимог;
2) *принцип конкретності цілей*: ПД повинні виходити з конкретними законними цілями і не оброблятися способами, несумісні з цими цілями;
3) *принцип пропорційності*: ПД повинні бути адекватними, чи не надлишковими і відповідати цілям обробки;
4) *принцип якості даних*: ПД повинні бути точними та своєчасно оновлюватися;
5) *принцип обмеження терміну обробки*: ПД не повинні зберігатися довше, ніж це необхідно;
6) *принцип прозорості та опозиції*: ПД повинні оброблятися з дотриманням прав фізичної особи, включаючи право на доступ до даних і зауважень щодо їх обробки;
7) *принцип захисту даних*: ПД повинні оброблятися з дотриманням технічних вимог щодо захисту даних;
8) *принцип обмеження передачі іноземним суб'єктам*: ПД повинні не передаватися за межі країни без відповідного захисту.

Цих норм і принципів цілком вдавалося дотримуватися в «доцифрову» епоху, коли інформаційні обміни відбувалися безпосередньо у фізичному середовищі, з пристроїв і мереж, які можна було відносно легко ідентифікувати і відстежити (наприклад, телефон або радіо). Але технологічний прогрес і глобалізація значною

мірою змінили те, як збираються ПД, як до них здійснюється доступ і яким чином вони використовуються (обробляються). Практично у всіх країнах найбільш проблемною сферою захисту ПД є сьогодні ІКТ та Інтернет, в якому традиційні нормативно-правові механізми та підходи до захисту ПД стають неефективними[217].

§8.3. Захист конфіденційної інформації в мережі Інтернет та соціальних мережах

Питання, що стосуються захисту ПД в мережі Інтернет та соціальних мережах, на сьогоднішній день є актуальними. Це пов'язано з невисоким рівнем грамотності населення в питаннях безпеки власних ПД.

При роботі в мережі Інтернет користувач отримує масу корисної і не дуже інформації. Однак при цьому нерідко відомості про користувача і про його інформаційних потребах надходять до осіб, про існування яких він навіть не здогадується. Це відбувається через те, що в мережі Інтернет на базі існуючих протоколів і стандартів при інформаційному обміні здійснюється збір інформації про користувача та про використовуване ним програмному забезпеченні, комп'ютерних даних і комп'ютерах.

Отримувані дані про користувача можуть однозначно його ідентифікувати (наприклад, містити вказані ним ім'я та прізвище, дату народження, місце проживання та ін.), а можуть й ідентифікувати апаратно-програмне забезпечення, за допомогою якого здійснюється доступ в мережу Інтернет.

Також при роботі в мережі Інтернет за допомогою клієнтського програмного забезпечення, призначеного для доступу до веб-сайтів, можливий збір відомостей про встановлене програмне забезпечення і режими роботи комп'ютера. Крім того, за ip-адресою можна визначити інформацію про місцезнаходження комп’ютера або обладнання Інтернет-провайдера (постачальника послуги доступу до мережі

[217] Гнатюк С. Л. Особливості захисту персональних даних в сучасному кіберпространстві: правові та техніко-технологічні аспекти: Аналітична доповідь. — [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2013_table/1010_dopov.pdf.

Інтернет). Все це створює реальні можливості для порушення інформаційних прав осіб, які отримують інформацію в мережі Інтернет.

Існує два підходи до вирішення даної проблеми: технічний та організаційно-правовий.

Технічний підхід полягає у створенні та розповсюдженні численних програмних і апаратних рішень в сфері інформаційної безпеки для комп'ютерних систем користувача і провайдера, а також у створенні спеціалізованих Інтернет-сервісів.

Організаційно-правовий підхід для захисту користувачів у мережі Інтернет, у тому числі і захист ПД, неможливо забезпечити і застосувати в рамках одного окремо взятого національного законодавства. Мережа Інтернет – транскордонна та має ознаками екстериторіального і загального доступу. У зв'язку з цим виникає велика кількість проблем, пов'язаних з юрисдикцією, контролем, обмеженням, захистом прав та інтересів громадян.

Ще в 1999 р. була розроблена Рекомендація №R(99)5 Комітету Міністрів держав-членів Ради Європи «Про захист недоторканності приватного життя в Інтернеті»[218], яка містить основні принципи щодо захисту особистості щодо збору та обробки ПД:

- при роботі в мережі Інтернет користувачі повинні використовувати всі доступні засоби для захисту своїх даних і ліній зв'язку (наприклад, доступні засоби шифрування для конфіденційної електронної пошти або коди доступу до свого комп'ютера);
- при реєстрації на сайтах необхідно використовувати мінімум особистих даних;
- найкращий спосіб забезпечення безпеки особистості – це анонімний доступ і анонімне використання послуг, анонімні засоби здійснення платежів;
- надавати тільки ті дані, які необхідні для виконання певних дій, про які Ви проінформовані;

[218] Рекомендация № R (99) 5 Комитета Министров государствам-членам Совета Европы по защите неприкосновенности частной жизни в Интернете. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_357

- адреса електронної пошти є інформацією персонального характеру, тому необхідно уточнювати про його використання;
- з обережністю ставиться до сайтів, на яких просять інформацію особистого характеру більшу, ніж це потрібно для доступу;
- постачальник послуг Інтернет несе відповідальність за правильне використання ПД та ін.

Однак сьогодні при використанні мережі Інтернет відбувається масове порушення чинного законодавства у сфері захисту ПД. Причому часто витіки ПД з Інтернет-ресурсів пов'язані не з діями віртуальних зловмисників, а зі слабким рівнем захисту інформації. Причиною потрапляння ПД користувача мережі Інтернет в «треті руки» можуть бути дії співробітників Інтернет-компаній, що обробляють ці дані. У той же час, користувачі також зобов'язані самі піклується про захист своєї інформації, в тому числі уважно читати умови ліцензійних і користувальницьких угод.

Так звані «дрібні крадіжки» ПД в мережі відбуваються постійно, – найпоширеніші – злом паролів для входу в соціальну мережу або електронну пошту, для того щоб розіслати спам по всім доступним контактам. Але крім цього, інформація про людину та її діях в мережі не тільки записується, а й передається «третім особам», причому без втручання користувача. Наприклад, портал Mail.ru в умовах користувацької угоди повідомляє, що компанія «вправі, за першою вимогою відповідно до уповноваженого правоохоронного та іншого уповноваженого державного органу, але відповідно до чинного законодавства, передавати такому державному органу наявну інформацію про користувача». Тобто якщо власника поштової скриньки запідозрять в екстремізмі або інші правопорушення, то за відповідним запитом вся інформація про нього буде передана в правоохоронні органи для проведення розслідування. Те ж саме декларує і компанія «Яндекс» у своїй політиці конфіденційності, в окремому розділі, який стосується умов обробки інформації користувача та передачі її третім особам. Там же, до речі, уточняється, що для користувача дані можуть бути передані третім особам в рамках продажу бізнесу. Примітне, що Mail.ru залишає за собою право

використання матеріалів в якості реклами, які користувач зробив загальнодоступними. Також популярна система електронної пошти Gmail «читає» переписку своїх користувачів – веде аналіз текстів листів за допомогою спеціальних автоматизованих систем, що визначають звідти ключові слова і використовують ці дані для тематики рекламних показів[219].

Без електронної пошти сьогодні неможливо уявити роботу будь-якого офісу підприємства, організації, органу влади або місцевого самоврядування. Але й тут виникає проблема захисту конфіденційної інформації. У підписах електронних листів містяться відомості про їх кореспондентів – прізвища, імена, по батькові, назви посад, номера телефонів, адреси електронної пошти, це як мінімум. Виникає питання: «Як застосовувати в даному випадку ЗУ «Про захист персональних даних»?. Відповіді на нього немає ні в нормативно-правових актах, ні в методичних рекомендаціях.

Ще один аспект використання ПД в мережі Інтернет – електронна комерція. Здійснюючи покупки в Інтернет-магазинах, покупець надає свої ПД (прізвище, ім'я, номер телефону, домашню адресу для доставки та ін.). І тут виникає ряд питань: Як власник магазину може довести згоду на обробку ПД покупця? Пославшись на те, що той сам заповнив необхідні поля при покупці товару й тим самим висловив непряму згоду на їх обробку? А якщо це ПД не покупця, а іншої людини, які покупець вважав за потрібне використовувати при оформленні замовлення, а ця третя особа не тільки не давало згоди, а й знати не знає про використання його ПД? Чому відповідальність за це повинен нести магазин? Цілком може бути, що відомості, зазначені при замовленні, взагалі не є чиїмись ПД, а вигадані.

При покупці авіаквитків, пасажир цілком може вказати не тільки свої ПД, але відомості про інших осіб, для яких купуються квитки. Дотримуючись вимог закону, перевізник повинен підтвердити згоди на обробку ПД всіх пасажирів, які купили квитки через Інтернет. А в

[219] Благовещенский А. Читайте мелкий шрифт – [Електронний ресурс]. – Режим доступу: http://www.rg.ru/2011/05/05/internet.html.

разі, якщо дані представлялися не самим пасажиром, а третьою особою, негайно повідомити такого пасажира про початок опрацювання відомостей про нього, вказавши в повідомленні обов'язкові реквізити, передбачені законом. На практиці такого порядку майже не дотримуються. Але в даному випадку до авіакомпанії можна пред'явити претензії, а до її посадових осіб – застосувати санкції.

Інтернет-рекрутинг теж викликає безліч питань про захист ПД, розміщених на сайтах пошуку роботи. Використання Інтернет-сайтів для пошуку роботи чи кандидатів на заміщення вакантних посад стало сьогодні дуже поширеним. Для цього треба зайти на сайт, авторизуватись і заповнити форму з резюме, тобто вказати свої ПД. Тут знову ж виникає проблема, власники сайт повинні представити згоду суб'єкта на обробку його ПД, а інакше робота цих сайтів стає поза законом[220].

Соціальні мережі зайняли важливе місце в житті практично кожного користувача Інтернет. Мети їх використання різні – спілкування, вчинення правочинів, розповсюдження реклами, розміщення інформації та ін. Не дивлячись на позитивну сторону розширення соціальних мереж, існують і певні недоліки: поки одні отримують користь від спілкування в соціальній мережі, інші використовують їх для різного роду шахрайства, пропаганди насильства та екстремізму, вчинення злочинів. Практично кожна соціальна мережа виступає оператором ПД, який обробляє персональну інформацію користувачів даної мережі.

Користувачі соціальних мереж, добровільно розміщуючи інформацію, що містить ПД (прізвище, ім'я, стать, дату народження, освіту, номера телефону) розміщуючи фотографії, що дозволяють зробити ідентифікацію суб'єкта, не замислюються про шкоду, яка може бути їм заподіяна. ПД, завантажені в соціальну мережу, поширюються в мережі Інтернет, і їх практично неможливо видалити.

[220] Емельянинков М. Как защищать персональные данные в Интернет. – [Електронний ресурс]. – Режим доступу: http://old.infosec.ru/presscentre/publication/PD_protection_internet.

Розглядаючи розміщення персональної інформації в соціальній мережі, можна говорити про двоїстий характер її доступності. З одного боку, інформація користувача соціальної мережі схована від третіх осіб і є недоступною для пошукових систем, а з іншого боку – відкрита. Відкритість персональної інформації дозволяє сформувати досьє на кожного зареєстрованого користувача соціальної мережі, не порушуючи при цьому положень законодавства. Ще одним недоліком розміщення персональної інформації в соціальних мережах є вільний перегляд третіми особами відкритих даних і можливість їх копіювання. На розсуд користувача доступ до даних, що становить персональний характер, може обмежуватися, якщо ця можливість передбачається оператором соціальної мережі[221].

Сучасному суспільству, яке активно користується послугами соціальних мереж, повинно бути відоме таке поняття, як фішинг – Інтернет-шахрайство з метою крадіжки ПД. Існують різні форми витоку інформації, наслідками яких є загроза зміни, копіювання, блокування, поширення, знищення ПД та інші несанкціоновані дії, які можуть завдати непоправної шкоди, як суб'єкту ПД, так і репутації організації-роботодавця та ін. Хоча адміністратори сайтів й використовують технології для забезпечення захисту від вірусів та іншого шкідливого програмного забезпечення, ці методи захисту не зможуть убезпечити від пасивного збору інформації про користувачів. В цілях власної безпеки користувачі соціальних мереж в першу чергу повинні самостійно контролювати питання безпеки їх ПД у відкритих ресурсах. Для запобігання фішинг-атак використовувати програми-файрволи, міжмережеві екрани і антивірусне програмне забезпечення.

Дослідження проблеми безпеки користувачів соціальних мереж на прикладі популярної мережі vk.com, показало, що дана соціальна мережа не несе відповідальності за збереження, поширення ПД і їх безпечне використання, що зазначено в користувача угоді. І відповідно, дія ЗУ «Про захист персональних даних» на неї не поширюється.

[221] Комкова К. С. Безоапсность персональной информации в социальных сетях: правовой аспект / К. С. Комкова // Вестник южного научного центра. – Т. 9. – № 3. – 2013. – С. 71-75.

Для захисту своїх ПД в соціальних мережах необхідно дотримуватися таких правил. При роботі в соціальних мережах необхідно ознайомиться з політикою конфіденційності, і налаштувати параметри для захисту своїх даних. Також в політиці конфіденційності можна дізнатися рівень безпеки: яку інформацію, і яким чином збирає сайт, хто має доступ до цієї інформації, які заходи щодо забезпечення інформації реалізовані, як довго зберігається інформація, і як можна зв'язатися з адміністрацією сайту у випадку порушення конфіденційності. Якщо при реєстрації в соціальній мережі запитують занадто багато ПД, можливо, краще від неї відмовитися. Також треба пам'ятати про те, що вся інформація, розміщена в соціальних мережах, залишається в мережі, тому публікувати можна тільки такі повідомлення та фотографії, які не можуть скомпрометувати людину[222].

У 2012 р. Всеукраїнською громадською організацією «Українська асоціація захисту ПД» було ініційовано та проведено перше дослідження в рамках громадського моніторингу відкритості та прозорості обробки ПД в Інтернеті. Результати дослідження показали, що тільки третина веб-ресурсів національного сегменту Інтернет надають суспільству і користувачам мінімальні відомості про розпорядників ПД – найменування юридичної або ім'я фізичної особи, яке і є, за законом, відповідальним за обробку ПД відвідувачів і за дотримання їх прав на невтручання в приватне життя. Так само, приблизно третина веб-ресурсів повідомляють відвідувачам про їхні права.

Автори моніторингу також констатують, що більша частина національних веб-ресурсів (більше трьох чвертей), не забезпечують відкритості та прозорості обробки ПД, ігнорують вимоги ратифікованої Україною Конвенції «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», положень ЗУ «Про захист персональних даних», рекомендацій Комітету міністрів Ради

[222] Защита конфиденциальности в социальных сетях: Электронное руководство TrendLabs по жизни в цифровом мире. – [Електронний ресурс]. – Режим доступу: http://www.trendmicro.com.ru/media/br/eguide-how-to-protect-your-privacy-on-social-media-ru.pdf.

Європи державам-членам Ради Європи «Про захист недоторканності приватного життя в Інтернеті».

Щоб якось виправити існуюче становище, в 2012 р. вищевказаної Українською асоціацією було прийнято Декларацію «Про забезпечення недоторканності приватного життя в Інтернет»[223], мета якої полягає в:

- формуванні та забезпеченні реалізації умов для зменшення ризиків, пов'язаних з не інформованістю операторів телекомунікацій, провайдерів доступу Інтернет, провайдерів сервісів Інтернет та інших, про загрози втручання в приватне життя, про вимоги міжнародних стандартів та національного законодавства, рекомендаціях міжнародних організацій та практиці щодо захисту ПД;
- виявленні, зниженні та попередженні ризиків, пов'язаних з можливим небезпечним і потенційно небезпечним контентом, а також щодо дій осіб, що використовують можливості мережі Інтернет в протиправних і аморальних цілях (з метою шантажу, переслідувань, спокуси, сексуальної експлуатації та іншими протиправними діями);
- залученні органів державної влади, цивільної та бізнес-громадськості до проблем захисту ПД в Інтернеті, як першочергового завдання у формуванні безпечної Інтернет-середовища, визначення основних напрямів і створення відповідних умов для її вирішення.

Сьогодні до цієї Декларації приєднався ряд провідних українських національних телекомунікаційних компаній, таких як: Київстар, МТС Україна та ін.

На підставі вище розглянутого необхідно відзначити, про недостатнє законодавче регулювання відносин у сфері забезпечення конституційних прав і свобод громадян в інформаційному середовищі. Розвиток українського законодавства в мережі Інтернет сьогодні є першочерговим завданням.

[223] За забезпечення недоторканості приватного життя в Інтернет: Декларація. – [Електронний ресурс]. – Режим доступу: http://uapdp.org/images/Declaration.pdf.

§8.4. Організаційно-правові методи захисту персональних даних

Володільці, розпорядники ПД та треті особи зобов'язані забезпечити захист цих даних від випадкових втрат або знищення, від незаконної обробки, у тому числі незаконного знищення або доступу до персональних даних.

В органах державної влади, органах місцевого самоврядування, а також у володільця чи розпорядника ПД, які здійснюють обробку цих даних, що підлягають повідомленню відповідно до закону, створюється (визначається) структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом ПД при їх обробці. Інформація про зазначений структурний підрозділ або про відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

Структурний підрозділ або відповідальна особа, організує роботу, пов'язану із захистом ПД при їх обробці:

- інформує та консультує володільця чи розпорядника ПД з питань дотримання законодавства про захист ПД;
- взаємодіє з Уповноваженим та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист ПД.

Фізичні особи – підприємці, в тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист ПД, якими вони володіють, згідно з вимогами закону.

Щодо *третій складової* правового інституту ПД визначимо, що чинним законодавством встановлена цивільна і кримінальна відповідальність за порушення встановлених вимог щодо захисту ПД.

Ст. 28 ЗУ «Про захист персональних даних» передбачає відповідальність встановлену законом, але в самому законі немає чіткої конкретизації відповідальності.

У 2011 р. був прийнятий ЗУ «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за

порушення законодавства про захист персональних даних»[224], який доповнює КУпАП та ККУ.

Згідно зі ст. 188[39] КУпАП:

Неповідомлення або несвоєчасне повідомлення суб'єкта ПД про його права, у зв'язку з включенням його ПД в базу ПД, мету збору цих даних та осіб, яким ці дані передаються, – тягнуть за собою накладення штрафу на громадян від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб'єктів підприємницької діяльності – від трьохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян.

Неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту ПД про зміну відомостей, що подаються для державної реєстрації бази ПД, – тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб'єктів підприємницької діяльності – від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню, – тягне за собою накладення штрафу на громадян від трьохсот до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб'єктів підприємницької діяльності – від чотирьохсот до семисот неоподатковуваних мінімумів доходів громадян.

Ухилення від державної реєстрації бази ПД – тягне за собою накладення штрафу на громадян від трьохсот до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб'єктів підприємницької діяльності – від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян.

[224] Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних: Закон України від 02.06.2011 р. № 3454-VI // Відомості Верховної Ради. – 2011. – № 50. – Ст. 549.

Недодержання встановленого законодавством про захист ПД порядку захисту ПД в базі ПД, що призвело до незаконного доступу до них, – тягне за собою накладення штрафу від трьохсот до тисячі неоподатковуваних мінімумів доходів громадян.

Згідно зі ст. 188^{40} невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту ПД щодо усунення порушень законодавства про захист ПД – тягне за собою накладення штрафу на посадових осіб, громадян-суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян.

Згідно зі ст. 182 ККУ незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, – караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, – караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк.

Істотною шкодою у цій статті, якщо вона полягає у заподіянні матеріальних збитків, вважається шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Також ст. 163 ККУ встановлює кримінальну відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер.

Згідно з ЦКУ (ст. 22, 23, 277, 1166, 1167) фізична особа може звернутися до суду за захистом своїх прав, порушених у зв'язку з розголошенням ПД, має право на спростування недостовірної інформації та на відшкодування майнової та моральної шкоди.

Висновки

ПД – це будь-які відомості, що відносяться до фізичної особи, на підставі яких ця особа може бути ідентифікована.

ПД є ІзОД і має свій правовий інститут.

Прийняття ЗУ «Про захист персональних даних» було одним з кроків наближення правової системи України до європейських стандартів.

Існує необхідність зміни існуючого та створення нового законодавства в галузі захисту ПД в мережі Інтернет.

9 МІЖНАРОДНИЙ ДОСВІД У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ ТА В БОРОТЬБІ ІЗ КОМП'ЮТЕРНОЮ ЗЛОЧИННІСТЮ

§9.1. Міжнародний досвід в боротьбі з загрозами інформаційній безпеці

Розробка і вдосконалення законодавчої бази ІБ будь-якої держави є необхідним заходом, що забезпечує потребу в захисті інформації при розвитку соціально-економічних, політичних та військових напрямків сфер його життя.

Першими правовими актами в галузі захисту інформації були закони про захист ДТ. До цих пір у всіх розвинених країнах шпигунство і зраду відносять до найбільш тяжких злочинів.

В даний час на міжнародному рівні інформація вважається найціннішим ресурсом життєзабезпечення суспільства та має широке соціальне значення.

Аналіз міжнародного досвіду правового забезпечення ІБ показує, що основними напрямками у вирішенні цієї проблеми в світовому співтоваристві є: захист прав особистості в інформаційній сфері, захист державних інтересів, захист підприємницької та фінансової діяльності, захист інформації від комп'ютерних злочинів[225].

Захист прав особистості в інформаційній сфері визначається Загальною декларацією прав людини та Конвенцією Ради Європи з прав людини. Ст. 19 Загальної декларації прав людини (1948 р.) говорить: *«Кожна людина має права на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими способами і незалежно*

[225] Сёмкин С.Н, Сёмкин А. Н. Основы правового обеспечения защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2008. – С. 44

від державних кордонів»[226]. Ст. 10 Конвенції «Про захист прав людини і основних свобод» (1950 р.) гарантує *«запобігання розголошенню інформації, одержаної конфіденційно»*[227]. Незважаючи на те, що ці міжнародні документи були прийняті ще до появи та активного використання ІКТ, вони є актуальними і в наш час.

Згідно з доповіддю Генеральної Асамблеї ООН А/55/40 міжнародна ІБ сьогодні визначається як *«стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі»*[228].

У міжнародно-правовому регулюванні світових процесів інформаційної безпеки важливим кроком явилося прийняття резолюції Генеральної Асамблеї ООН 54/90 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки». В даному документі сформульовано питання про доцільність розробки міжнародних принципів, спрямованих на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем і сприяючих боротьбі з тероризмом і криміналом. Світове співтовариство визнало міжнародну безпеку як глобальну проблему, яка вимагає негайного вирішення[229].

В напрямку міжнародної ІБ було прийнято чимало документів, що дозволяє зробити висновок про формування міжнародного інформаційного законодавства.

У багатьох країнах крім міжнародних документів в галузі захисту ІБ існує ряд державних нормативно-правових актів, що регулюють відносини у даній сфері.

---

[226] Всеобщая декларация прав человека. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_015.

[227] Конвенция «О Защите прав человека и основных свобод». – [Електронний ресурс]. – Режим доступу: http://www.hand-help.ru/documents/evrop_konv.html.

[228] Report of the Human Rights Committee. – [Електронний ресурс]. – Режим доступу: http://www.un.org/documents/ga/docs/55/a5540vol2.pdf.

[229] Аверченков В. И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – Брянск: БГТУ, 2007. – С. 122–126.

Правове регулювання інформаційної безпеки в США

Головним документом правового регулювання інформаційної безпеки США є «Закон про інформаційну безпеку», в якому передбачено реалізацію мінімально достатніх дій по забезпеченню безпеки в федеральних комп'ютерних системах, без обмеження всього спектру можливих дій. Згідно з цим законом за випуск стандартів та настанов, спрямованих на захист від знищення і несанкціонованого доступу до інформації, а також від крадіжок і підробок, що виконуються за допомогою комп'ютерів, відповідає Національний інститут стандартів і технологій.

В США за останні 20 років були спрощені експортні обмеження на криптозасоби, сформована інфраструктура з відкритими ключами, розроблено велику кількість стандартів (наприклад, стандарт ЕЦП – FIPS 186-2). Все це дозволило створити загальнонаціональну інфраструктуру електронної аутентифікації.

Програма безпеки інформаційних систем США включає в себе:

- періодичну оцінку ризиків з розглядом внутрішніх і зовнішніх загроз цілісності, конфіденційності та доступності систем, а також даних, асоційованих з критично важливими операціями і ресурсами;
- правила та процедури, що дозволяють, спираючись на проведений аналіз ризиків, економічно виправданим чином зменшити ризики до прийнятного рівня;
- навчання персоналу з метою інформування про існуючі ризики та про обов'язки, виконання яких необхідне для їх (ризиків) нейтралізації;
- періодичну перевірку та переоцінку ефективності правил і процедур;
- дії при внесенні суттєвих змін в систему;
- процедури виявлення порушень інформаційної безпеки і реагування на них; ці процедури повинні допомогти зменшити ризики, уникнути великих втрат, організувати взаємодію з правоохоронними органами.

Крім цього, в законодавстві США є в достатній кількості і положення обмежувальної спрямованості, і директиви, що захищають інтереси таких відомств, як Міністерство оборони, ФБР, ЦРУ[230].

Системи захисту інформації в Китайській народній республіці

У сучасному світі Китай є однією з країн Азіатсько-Тихоокеанського регіону, що найбільш активно розвивається, і є лідером в питаннях інформаційного протиборства і по наявності сучасного захисту національних інформаційних ресурсів.

Законодавство у сфері ІКТ в Китаї почало розвиватися паралельно з розвитком сучасних інформаційних систем.

У 1994 р. Держрадою країни опубліковані положення «Про охорону комп'ютерних та інформаційних систем». Законотворчий процес в області регулювання Інтернету почався в 1995 р., коли був прийнятий ряд заходів, що запобігають незаконну онлайнову діяльність в Інтернеті. У положенні «Про охорону безпеки міжнародної мережі комп'ютерних та інформаційних систем», опублікованому Міністерством державної безпеки КНР, описуються категорії інформації, розробка, збільшення, пошук і розповсюдження якої забороняються, а також кваліфіковані види діяльності, які відносяться до посягання на безпеку комп'ютерних та інформаційних систем. Прийняте в 2001 р. положення «Про охорону комп'ютерних програм» є першим нормативним актом в галузі охорони безпеки комп'ютерних систем Китаю. У 2003 р. був прийнятий Закон «Про авторські права», в якому комп'ютерні програмні продукти вперше прирівняні до категорії охоронюваних авторськими правами.

Постанова «Про охорону комп'ютерних мереж», прийнята в Китаї у 2004 р., встановлює кримінальну відповідальність за такі види комп'ютерних злочинів:

[230] Аверченков В. И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – Брянск: БГТУ, 2007. – С. 54–59.

1) Мережева атака і пошкодження комп'ютерної системи. До даного типу правопорушень в Китаї віднесені наступні:

- хакерська атака з метою перехоплення, знищення, зміни і підробки інформації, що зберігається в комп'ютері, порушення нормального функціонування комп'ютерної системи та мереж;
- розробка та поширення комп'ютерних вірусів;
- розкрадання інформації, що зберігається в комп'ютері.

2) Мережеве шахрайство.
3) Розкрадання грошових коштів з фінансових установ шляхом несанкціонованого доступу до комп'ютерних систем.
4) Азартні ігри в онлайновому середовищі і реклама послуг сексуального характеру в Інтернеті.
5) Посягання на авторські та суміжні права, злочини проти інтелектуальної власності.
6) Розкрадання інформації, що становить державну таємницю, проникнення в інформаційні системи державних служб.
7) Розповсюдження порнографічної продукції, інформаційних продуктів, що викликають прояви расизму і розпалювання міжнаціональної ворожнечі, іншої інформації, що загрожує державній безпеці.
8) Посягання на приватне життя громадянина. До даного типу правопорушень в Китаї відносять:

- підробка, поширення інформації, що ущемляє честь і гідність громадянина;
- відвертий наклеп, брехня, поширення інформації від чужого імені;
- розголошення інформації про особисте життя людини без будь-якого на те дозволу.

Для посилення контролю над мережею Інтернет та визначення її виконавчого апарату в Китаї додається багато зусиль. В країні орган громадської безпеки (міліція), несе відповідальність за забезпечення інформаційного захисту. Закон Китаю «Про міліцію» та інші відповідні законодавчі та нормативні акти покладають на

міліцію країни наступні функції контролю над інформаційною безпекою в Інтернеті:

- визначення категорій ступенів безпеки інформаційної системи і реальних методів їх захисту;
- доведення цих відомостей до користувачів Інтернету;
- розслідування справ, пов'язаних з несанкціонованим використанням комп'ютерної інформації;
- розробка систем попередження поширення комп'ютерних вірусів та іншої небезпечної інформації;
- розробка реальних методів державного регулювання продажу мережевих продуктів, інформаційних систем;
- контроль діяльності щодо забезпечення інформаційної безпеки в Інтернеті;
- відстеження правопорушень в Інтернеті.

В даний час китайський виконавчий апарат безпеки мережі Інтернет досить успішно проводить роботу з контролю інформаційного обміну та припинення незаконної діяльності в китайському сегменті мережі Інтернет[231].

Політика Європейського Союзу у сфері інформаційної безпеки

Починаючи з 1990-х років у розвитку інформаційного суспільства в Європейському Союзі, піднімалися питання про виникаючі ризики і загрози в області інформаційної безпеки. Для вирішення проблем інформаційної безпеки було прийнято комплекс нормативно-правових актів у складі системи правового регулювання телекомунікацій та захисту інформації[232].

Так, у 2001 р. Європейською комісією були видані повідомлення «Мережева та інформаційна безпека: пропозиції для

[231] Аверченков В. И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. – Брянск: БГТУ, 2007. – С. 110–117.

[232] Смирнов А. А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Монография. – М.: ЮНИТИ-ДАНА, 2011. – С. 110.

підходу європейській політиці»[233], в яких проводився аналіз ситуації та основних тенденцій у сфері забезпечення інформаційної безпеки, і пропонувалися рішення для її забезпечення на просторі ЄС. В даному повідомленні були введені поняття *«мережева та інформаційна безпека»*, які визначалися як: *«здатність мережі або інформаційної системи протистояти на заданому рівні надійності випадковим загрозам або умисним шкідливим діям, які піддають ризику доступність, автентичність, цілісність і конфіденційність збережених або переданих з ними служб, доступ до яких здійснюється за допомогою таких мереж або систем»*.

Пропонований Комісією підхід для європейської політики щодо забезпечення мережевої та інформаційної безпеки ґрунтується на наступних складових:

- забезпечення прикладного характеру правових норм на основі загального розуміння основних питань безпеки і спеціальних заходів з її забезпечення;
- необхідність постійного вдосконалення правового регулювання з урахуванням технічного прогресу і нових загроз, що ним породжуються;
- потреба в доповненні ринкових механізмів політичними мірами;
- формування європейського внутрішнього ринку інформаційно-комунікаційних послуг.

Співвідношення основних сфер політики ЄС в інформаційній сфері являє собою: діяльність в галузі мережевої та інформаційної безпеки, боротьбу з кіберзлочинністю, захист інформації та діяльність у сфері телекомунікацій *(рис. 9.1)*.

[233] Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions «Network and Information Security: Proposal for A European Policy Approach». Brussels, 6.6.2001. COM (2001)298 final. – [Електронний ресурс]. – Режим доступу: http://www.etsi.org/WebSite/document/aboutETSI/EC_Communications/COM_298.pdf.

Рис. 9.1. Співвідношення основних сфер політики ЄС в інформаційній сфері

Усі сфери політики перетинаються між собою, тобто мають як загальні питання, так і свій зміст стосовно кожної з них і припускають триступеневий підхід, що охоплює:

1) спеціальні заходи щодо забезпечення системи інформаційної безпеки;
2) правове регулювання електронних комунікацій, включаючи питання захисту інформації та приватного життя;
3) боротьбу з кіберзлочинністю.

В рамках першого напряму були прийняті Рішення 2002/С43/02 від 28.01.2002 р. «Про загальні підходи і спеціальні заходи в сфері мережевої та інформаційної безпеки»[234] і Рішення 2003/С48/01 від

[234] Council resolution 2002/C 43/02 of 28 January 2002 on a common approach and specific actions in the area of network and information security.

18.02.2003 р. «Про європейський підхід щодо культури мережевої та інформаційної безпеки»[235].

В рамках другого напрямку в 2002 р. була прийнята Директива 2002/58/ЕС «Про приватне життя та електронні комунікації»[236], яка встановила гарантії захисту ПД і недоторканності приватного життя в електронних комунікаціях. Також право на захист ПД включено Хартією Європейського Союзу про основні права 2007 р. [237]

Для розвитку європейської політики в сфері системи інформаційної безпеки в 2006 р. була прийнята «Стратегія безпеки інформаційного суспільства: діалог, партнерство і розширення можливостей»[238], яка містить огляд сучасного стану загроз безпеці інформаційного суспільства та визначає додаткові заходи щодо забезпечення системи інформаційної безпеки. В Стратегії зазначається, що, незважаючи на активні зусилля на міжнародному, європейському та національному рівні, виникають все нові виклики безпеці, включаючи атаки на інформаційні системи з корисливими цілями, поширення шкідливого програмного забезпечення. Комісія акцентує увагу на зростанні використання мобільних пристроїв (включаючи 3G мобільні телефони , портативні відеоігри та ін.), і мережевих мобільних послуг, що в перспективі здатне зробити їх головною мішенню комп'ютерних атак. Будь-які нові форми платформ для комунікації та інформаційних систем неминуче створюють нові можливості для шкідливих атак.

Однією з фундаментальних цілей ЄС є надання його громадянам простору свободи, безпеки та законності без внутрішніх кордонів. В рамках політики ЄС в даній сфері здійснюється діяльність інститутів ЄС і держав-учасників ЄС з боротьби зі злочинністю, одним з нових видів

---

[235] Council resolution 2003/C 48/01 of 18 February 2003 on a European approach towards a culture of network and information security.

[236] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications.

[237] Хартия Европейского Союза об основных правах (2007/C303/01) // Европейский Союз: Основополагающие акты в редакции Лиссабонского договора с комментариями / отв. ред. С. Ю. Кашкин. – М.: ИНФРА-М, 2010. – С. 554-570.

[238] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. A strategy for a Secure Information Society – «Dialogue, partnership and empowerment». Brussels, 31.5.2006. COM(2006) 251 final.

якої є кіберзлочинність, яка охоплює нові злочини, характерні для Інтернет-середовища, такі як напади на інформаційні системи або фішинг (підробка сайтів банку для запрошування паролів, що забезпечують доступ до банківських рахунків жертв). Крім того, все більше традиційних злочинів, таких як шахрайство та поширення нелегального контенту (матеріали сексуального насильства над дитиною або такі, що підбурюють до насильства в Інтернеті) все частіше здійснюються з використанням комп'ютерів в якості засобів вчинення злочину.

З урахуванням розвитку кіберзлочинності Європейська Комісія розробила політику по боротьбі з нею, пропозиції якої були сформульовані в Повідомленні 2007 р. «На шляху до спільної політики в боротьбі з кіберзлочинністю»[239]. Основне призначення Повідомлення – розвиток співробітництва між правоохоронними органами, державно-приватного партнерства та міжнародного співробітництва. У даних Повідомлень пропонується реалізація комплексу заходів для боротьби з кіберзлочинністю, включаючи запуск оперативного співробітництва між національними правоохоронними органами; збільшення фінансової підтримки ініціатив з підготовки національних правоохоронних органів з розслідування кіберзлочинів; підтримку досліджень у сфері боротьби з кіберзлочинністю; прийняття з боку приватного сектора заходів з підвищення обізнаності про небезпеки кіберзлочинності; реалізація заходів щодо запобігання та протидії, скоординованим і великомасштабним атакам на інформаційну інфраструктуру.

В останні роки в ЄС діють кілька інноваційних проектів у сфері протидії кіберзлочинності. У червні 2010 р. було прийнято рішення про заснування Спеціальної групи з кіберзлочинності в ЄС (European Union Cybercrime Task Force), до якої увійшли представники від Європолу, Євроюсту та Європейської Комісії, покликаної сприяти транскордонній боротьбі з кіберзлочинністю.

[239] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 «Towards a general policy on the fight against cybercrime». Brussels, 22.5.2007. COM(2007) 267 final.

Під егідою Європолу в 2010 р. розпочато реалізацію дослідницького проекту з аналізу організованої злочинності, що використовує можливості Інтернету iOCTA (Strategic analysis of Internet Facilitated Organised Crime), мета якого полягає в оцінці існуючих і перспективних тенденцій розвитку кіберзлочинності та інформуванні про оперативну роботу і політиці ЄС в даній сфері. Дослідження iOCTA засновані на аналізі оперативної інформації від правоохоронних установ ЄС і матеріалів з відкритих джерел.

Пріоритетом до 2020 р. в основних стратегічних документах ЄС названа безпека в кіберпросторі.

Аналіз розглянутого дозволяє зробити висновок про те, що створена в ЄС система інформаційної безпеки забезпечує здатність адекватного реагування на основні типи загроз.

§9.2. Сутність поняття «комп'ютерна злочинність» і її характерні риси

Термін «***комп'ютерний злочин***» вперше з'явився в американській пресі на початку 60-х років минулого століття, коли були виявлені перші випадки злочинів, скоєних з використанням комп'ютерів. Пізніше цей термін став використовуватися і в правоохоронних органах багатьох країн світу. З розвитком ІКТ також з'явилися й інші терміни: інформаційні злочини, злочини у сфері високих технологій, кіберзлочини та ін.[240]

Вперше склад комп'ютерного злочину був сформульований в 1979 р. на Конференції американської асоціації адвокатів в м. Далласі (США), де фігурували такі визначення[241]:

- використання або спроба використання комп'ютера, обчислювальної системи або мережі комп'ютерів з метою отримання грошей, власності або послуги, прикриваючись

[240] Використання інформаційних технологій в судах: Навчальний посібник / Ємельянов С. Л., Логінова Н. І., Тодощак О. В., Якутко В. Ф. – Одеса: Фенікс, 2014. – С. 64–93.

[241] Емельянов С. Л. Некоторые аспекты компьютерной преступности и борьбы с нею / С. Емельянов, И. Гловюк, Е. Емельянова // Бизнес и безопасность. – 2006. – № 3. – С. 143–145.

фальшивими приводами, обіцянками або видаючи себе за іншу особу;

- умисна несанкціонована дія, зміни, що мають ціллю спотворення, знищення або крадіжку комп'ютера, обчислювальної системи, мережі комп'ютерів або систему математичного забезпечення, програм або інформації, що міститься в них;
- умисне несанкціоноване порушення зв'язку між комп'ютерами, обчислювальними системами або мережами комп'ютерів.

У 1986 р. в м. Парижі групою експертів Організації економічного співробітництва та розвитку (ОЕСР) було запропоновано конкретну кримінальну визначення комп'ютерного злочину, під яким розумілася «*будь-яка незаконна, неетична або недозволена поведінка, що зачіпає автоматизовану обробку і (або) передачу даних»*.

Поряд з цим визначенням в практичне використання був введений термін «кіберзлочинність», що охоплює будь-який злочин, яке може *«вчинятися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі чи проти інформації в комп'ютерній системі або мережі. В принципі, воно охоплює будь-яке злочин, який може бути скоєно в електронному середовищі»*[242].

Отже, загальноприйнятого визначення комп'ютерної злочинності не існує. Ці злочини тісно пов'язані з ІКТ. Вони часто містять в собі цілий ряд незаконних дій, вчинених за допомогою системи обробки даних або проти неї. Термін охоплює комп'ютер, допоміжне обладнання, програмне забезпечення, засоби зв'язку та телекомунікацій, інформаційні мережі та бази даних, комп'ютерну інформацію тощо.

[242] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002. – С. 86.

Зараз під терміном ***«комп'ютерна злочинність»*** розуміють всі злочинні дії, при яких електронна обробка інформації була б знаряддям їх вчинення або їх об'єктом.

Комп'ютерна злочинність має ряд *характерних рис*, а саме[243]:

- її рівень (розмах) тісно пов'язаний з економічним рівнем розвитку суспільства у різних державах і регіонах;
- міжнародний (транскордонний) характер;
- труднощі у визначенні «місцезнаходження» злочину;
- слабкі зв'язки між ланками в системі доказів;
- неможливість спостерігати і фіксувати докази візуально;
- широке використання злочинцями засобів шифрування;
- висока латентність;
- заподіяння високих економічних збитків та ін.

§9.3. Використання міжнародно-правового досвіду протидії комп'ютерній злочинності

Міжнародне співробітництво правоохоронних та судових органів розвинених країн є одним з основних аспектів боротьби з комп'ютерною злочинністю.

З метою уніфікації кримінального законодавства Європейський Комітет з проблем злочинності Ради Європи в 1989 р. підготував спеціальні Рекомендації №R(89)9, в яких були визначені загальні характеристики комп'ютерних злочинів[244]. Ці рекомендації складаються з двох списків (*рис. 9.2*):

- ***мінімальний***: обов'язковий список правопорушень, який необхідно включити в національні кримінальні законодавства;
- ***необов'язковий*** (вибірковий або факультативний) список правопорушень.

[243] Біленчук П. Д. Комп'ютерна злочинність [навчальний посібник] / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – Київ: Атіка, 2002. – С. 66.

[244] Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – С. 128–132.

Рис. 9.2. Рекомендація № R(89)9 Ради Європи

У перелік правопорушень, рекомендованих для обов'язкового включення у внутрішні національні законодавства всіх країн Ради Європи (*мінімальний список*) було внесені 8 складів злочинів, пов'язаних з *використанням комп'ютерних технологій*:

1) ***Комп'ютерне шахрайство.*** Введення, зміна, вилучення, видалення або пошкодження комп'ютерних даних або програм, або інше втручання в процес обробки даних, яке впливає на результат обробки даних таким чином, що це веде до економічних збитків або втрати власності іншої людини, з метою отримання незаконним шляхом економічного прибутку для себе чи іншої особи.
2) ***Комп'ютерна підробка.*** Введення, зміна, вилучення, видалення або пошкодження комп'ютерних даних або програм, або інше втручання в процес обробки даних, що здійснюється таким способом або за таких умов, при яких вони класифікувалися б національним законодавством як

фальсифікація, досконалий проти традиційного об'єкта такого правопорушення.

3) ***Викривлення комп'ютерної інформації або комп'ютерних програм***. Протиправне видалення, заподіяння шкоди, погіршення якості або придушення комп'ютерних даних чи програм.
4) ***Комп'ютерний саботаж.*** Введення, зміна, видалення комп'ютерних даних або програм, або створення перешкод комп'ютерним системам з наміром перешкоджати роботі комп'ютера або телекомунікаційної системі.
5) ***Несанкціонований доступ.*** Неправомірний доступ до комп'ютерної системи або мережі шляхом обходу захисних механізмів.
6) ***Несанкціонований перехоплення.*** Неправомірний перехоплення повідомлень, що чиниться з допомогою технічних засобів, які входять в комп'ютерну систему або мережу, виходять з комп'ютерної системи або мережі, або передаються в рамках комп'ютерної системи або мережі.
7) ***Несанкціоноване копіювання захищеної авторським правом комп'ютерної програми***. Неправомірне відтворення, розповсюдження або передача в спільне використання комп'ютерної програми, охороняється законом.
8) ***Несанкціоноване копіювання мікросхем.*** Незаконне відтворення мікросхеми або вироби на напівпровідниках, охоронюваних законом, або неправомірне комерційне використання або імпорт з цією метою мікросхем або виробів на напівпровідниках, виготовлених з використанням цієї мікросхеми.

Інші 4 склади злочинів склали необов'язковий список, так як щодо них не було досягнуто загальної згоди:

1) ***Зміна комп'ютерної інформації або комп'ютерних програм***. Неправомірне зміна комп'ютерної інформації або комп'ютерних програм.

2) ***Комп'ютерне шпигунство***. Протиправне придбання недозволеними методами або використання торговельної або комерційної таємниці, з метою нанесення економічної шкоди особі, яка має доступ до цієї таємниці, або отримання незаконної економічного прибутку для себе або третьої особи.
3) ***Протизаконне використання комп'ютера.*** Використання комп'ютера без відповідного дозволу:

- вчинене з ризиком нанесення збитку особі, якій дано право використовувати систему, або заподіяння шкоди самій системі або її роботі;
- вчинене з метою заподіяння шкоди особі, якій надано право використовувати систему або заподіяння шкоди самій системі або її роботі;
- нанесення збитку особі, якій надано право використовувати системою або заподіяння шкоди самій системі або її роботі.

4) ***Несанкціоноване використання захищеної авторським правом комп'ютерної програми.*** Використання без відповідного дозволу комп'ютерних програм, які захищені законом, і були скопійовані без дозволу з метою отримання протизаконного економічного прибутку для себе та інших осіб, або заподіяння шкоди власнику програми.

Поява таких списків завершила багаторічну роботу різних правових систем та інститутів по боротьбі з комп'ютерною злочинністю і створила об'єктивні передумови для міжнародного співробітництва в цій галузі. Однак, в силу рекомендаційного характеру цього документа, не по всіх напрямах була досягнута домовленість, що на практиці призводило до появи нових проблем у боротьбі з цими злочинами.

Наступним кроком у розвитку міжнародного співробітництва в боротьбі з комп'ютерними злочинами з'явилася розробка на початку

90-х років минулого століття робочою групою Інтерполу *кодифікатора комп'ютерних злочинів*[245]:

QA – втручання в роботу або перехоплення інформації в комп'ютерній системі:

QAH – незаконний (несанкціонований) доступ до комп'ютерної системи;

QAI – перехоплення інформації, циркулюючої в комп'ютерній мережі;

QAT – крадіжка часу за надані платні послуги (наприклад, ухилення від сплати за інформаційні послуги телефонного або комп'ютерного зв'язку в Інтернет або переведення їх на іншого користувача подібних послуг);

QAZ – інші випадки несанкціонованого доступу або перехоплення інформації.

Дані діяння, що класифікуються як комп'ютерні злочини, є попередніми і, як правило, необхідними для здійснення інших протиправних діянь, що розглядаються далі.

QD – заміна (модифікація) або спотворення інформації в автоматизованій (комп'ютерній) системі:

QDL – «логічна бомба»;

QDT – «троянський кінь»;

QDV – «комп'ютерні програми-віруси»;

QDW – «комп'ютерні програми-черв'яки»;

QDZ – інші випадки спотворення інформації в автоматизованих системах.

Розглянемо більш докладно дані програми.

«*Логічна бомба*» – програма, що запускається при певних тимчасових або інформаційних умовах для здійснення несанкціонованого доступу до інформації.

«*Троянський кінь*» – спеціальна підпрограма, яка маскується в тексті вільно розповсюджуваних програм і виконує дії, відмінні від

[245] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М., 2002. – С. 127–129.

зазначених у специфікації для загальної програми.

«*Комп'ютерна програма-вірус*» – невелика програма, здатна мимовільно створювати свої копії і модифікувати (заражати) інші програми, файли. Часто містить «логічні бомби» і «трояни». Може супроводжуватися різними аудіо-та відео ефектами та ін.

«*Комп'ютерні програми-черв'яки*» – програма, впроваджувана в систему, часто зловмисно, і що перериває хід обробки інформації в системі. На відміну від вірусів черв'як не спотворює файли даних і програми. Зазвичай черв'як виконується, залишаючись невиявленим, і потім самознищується.

QF – комп'ютерне шахрайство:

QFC – шахрайство з банкоматами;

QFF – комп'ютерна підробка (підробка інформації в автоматизованих системах);

QFG – шахрайство з комп'ютерними ігровими автоматами;

QFM – шахрайство за рахунок неправильного вводу / виводу або маніпуляції програмами;

QFP – шахрайство з платіжними електронними засобами;

QFT – телефонне шахрайство;

QFZ – інші випадки комп'ютерного шахрайства.

QR – несанкціоноване копіювання програмних продуктів:

QRG – несанкціоноване тиражування комп'ютерної гри;

QRS – несанкціоноване тиражування комп'ютерного програмного забезпечення (комп'ютерних програм);

QRT – несанкціоноване тиражування напівпровідникової продукції (топологій, топографій, інтегральних мікросхем);

QRZ – інші випадки несанкціонованого копіювання комп'ютерної інформації.

QS – комп'ютерний саботаж:

QSH – саботаж з допомогою технічного забезпечення комп'ютерної системи;

QSS – саботаж з допомогою програмного забезпечення комп'ютерної системи;

QSZ – інші види комп'ютерного саботажу.

QZ – злочини, пов'язані з комп'ютерами і комп'ютерними технологіями:

QZB – незаконне використання дошки електронних оголошень (BBS);

QZE – крадіжка комерційної таємниці;

QZS – збір, збереження або поширення матеріалів, які є об'єктом судового розгляду або переслідування;

QZZ – інші випадки вчинення КП.

З цього переліку можна судити про те, що до злочинів у сфері комп'ютерної інформації ставиться дуже широкий спектр діяльності. Але, не всі ці діяння були прийняті в національному законодавстві України.

У 2001 р. було розроблено Конвенцію Ради Європи «*Про кіберзлочинність*»[246], що є на сьогодні базовим міжнародним нормативно-правовим актом у сфері боротьби з комп'ютерною злочинністю, який підписала і ратифікувала[247] (із застереженнями та заявами), і Україна.

Аналіз норм цієї Конвенції показує, що вони спрямовані на регулювання трьох основних блоків питань:

- наближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації;
- наближення національних кримінально-процесуальних заходів, направлених на забезпечення збору доказів при розслідуванні таких злочинів;
- можливі форми міжнародного співробітництва у кримінально-процесуальної діяльності.

[246] Конвенція про кіберзлочинність // Офіційний вісник України від 10.09.2007 р. – № 65. – Ст. 2535.

[247] Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. // Відомості Верховної Ради. – 2006. – № 5–6. – Ст. 71.

Конвенція є комплексним документом, що містить норми різних галузей права: кримінального, кримінально-процесуального, авторського, цивільного, інформаційного.

Основною ідеєю цього документа є включення в національне законодавство країн-учасників норми про кримінальну відповідальність за злочини у сфері комп'ютерної інформації. В ній також не дається визначення поняттю ***«злочини у сфері комп'ютерної інформації»***. Воно замінено терміном «***кіберзлочини***», який розкривається за допомогою наступного переліку:

- дії, спрямовані проти комп'ютерної інформації (як предмета злочинного посягання) і використання її як унікальне знаряддя вчинення злочину;
- дії, предметом посягання яких є інші блага, охоронювані законом, а інформація, комп'ютери та інше, є тільки одним з елементів об'єктивної сторони злочину, виступаючи як предмет, знаряддя його вчинення, складової частини способу його вчинення або приховування.

Об'єктом кіберзлочинів, відповідно до Конвенції, є широкий спектр суспільних відносин, що виникають при вчиненні інформаційних процесів з приводу виробництва, збору, обробки, накопичення, збереження, пошуку, розповсюдження та споживання комп'ютерної інформації, а також в інших областях, де використовуються комп'ютери, комп'ютерні системи та мережі. Серед них, враховуючи підвищене громадянське значення, виділяються правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності та доступності комп'ютерних даних і систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського та суміжних прав.

§9.4. Загальна характеристика комп'ютерних злочинців

Особистість злочинця досліджується різними науками, в тому числі *кримінологією* і *криміналістикою*. Кримінологічні дослідження обмежуються, головним чином, тими особливостями людини, які необхідні для кримінальної профілактики, запобігання та попередження

злочинів. Криміналістика вивчає в першу чергу «професійні» якості злочинців, які проявляються, переважно в певних способах, методах, прийомах здійснення злочинів[248].

Загальновідомо, що на місці злочину залишаються сліди, що визначають характерний «почерк» злочинця. Результати злочинної діяльності містять образні сліди людини. Виявлення на місці злочину речових доказів дає можливість отримати відомості про деякі соціально-психологічних ознаках злочинця. Також сліди злочину свідчать про кримінальний досвід злочинця, професію, його соціальне становище, стать, вік, особливості відносин з потерпілим та ін.

Криміналістичні дані про особу злочинця базуються на ***двох специфічних групах інформації.***

Перша група включає дані про особу невідомого злочинця по залишених ним слідах, як на місці злочину, так і в пам'яті свідків, в інших джерелах з метою встановлення напрямів його пошуку і затримання. Ця інформація дає уявлення про загальні ознаки певної групи людей, до яких може відноситися і злочинець.

Друга група об'єднує інформацію, отриману при вивченні особистості вже затриманого підозрюваного або обвинуваченого з метою вичерпної криміналістичної оцінки особи − суб'єкта злочину. З цією метою збираються відомості не тільки про ціннісні орієнтири, особливості соціальних поглядів, але і про його зв'язки, поведінку до, під час і після вчинення злочину. Це може допомогти знайти зі злочинцем психологічний контакт, отримати правдиві показання або вибрати ефективні способи впливу на нього.

Вважається, що ця інформація з урахуванням різних відомостей, що відображаються в інших елементах ***криміналістичної характеристики***, може бути покладена в основу ***типізації злочинців.*** Формування банку типових моделей злочинців, вивчення спільних рис таких людей, дозволяє оптимізувати процес виявлення кола осіб, серед яких доцільний пошук злочинців, що й обумовлює актуальність розгляду цього питання, щодо комп'ютерних злочинців.

[248] Біленчук П. Д. Комп'ютерна злочинність [навчальний посібник] / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – Київ: Атіка, 2002. – С. 121.

Характеризуючи комп'ютерного злочинця, необхідно відзначити, що до сфери комп'ютерних злочинів, входить дуже широке коло осіб. В коло цих осіб входять як висококласні фахівці, що мають спеціальну освіту (математики, програмісти, інженери-електронники та ін.), так і дилетанти. Як відомо правопорушники мають різний соціальний статус і рівень освіти.

Вітчизняні та зарубіжні дослідження дають можливість сформувати абстрактні портрети правопорушників, тобто ***відповідний профіль соціального типу злочинця*.**

В якості однієї з базових ознак, при дослідженні комп'ютерної злочинності розглядають мету і сферу (вид) протизаконної діяльності.

Зараз по цілі та сфері протизаконної діяльності виділяють наступні групи суб'єктів[249] *(рис. 9.3)*.

Рис. 9.3. Різноманіття комп'ютерних злочинців за сферою протизаконної діяльності

Серед фахівців відсутнє єдине тлумачення терміну ***«хакер».*** Спочатку під ***хакером*** (hacker) розумівся високопрофесійний програміст, здатний розробляти і модернізувати комп'ютерні програми, не маючи детальних специфікацій та документації до них. Таке трактування було панівною на рубежі 70-80-х років минулого сторіччя, коли саме зародився і розвинувся світовий хакерський рух. Пізніше, зі зростанням масштабів комп'ютерної злочинності і перетворення їх на самостійний вид злочинності, цей термін набув кримінальний відтінок і став означати комп'ютерного зломщика, здатного незаконним

[249] Емельянов С. Л. О некоторых аспектах криминалистической характеристики современных компьютерных преступников / С. Л. Емельянов. – [Електронний ресурс]. – Режим доступу: http://inter.criminology.org.ua/?p=855/.

способом отримати доступ в комп'ютерні інформаційні системи або мережі.

Однак більшість вчених небезпідставно вважають, що для останньої зазначеної категорії суб'єктів протиправної діяльності більш доцільне використання терміну «***кракер***» (cracker).

Головна відмінність між зазначеними категоріями полягає, не у віці або в рівні майстерності (новачок, професіонал, суперпрофесіонал), а в характері впливу на інформацію і в цільової установці. Суб'єкти обох зазначених категорій шукають і аналізують уразливості («дірки», «люки» та ін.) в апаратно-програмному забезпеченні та здійснюють злом комп'ютерних систем і мереж. Хакери, наприклад, часто мають дослідницькі мети, не роблять шкідливого впливу на інформацію і повідомляють про результати своїх атак. Навпаки, кракери здійснюють злом комп'ютерних систем з метою отримання несанкціонованого доступу до чужої інформації, характер впливу на яку набагато більш небезпечний залежно від їх мотивів *(рис. 9.4)*.

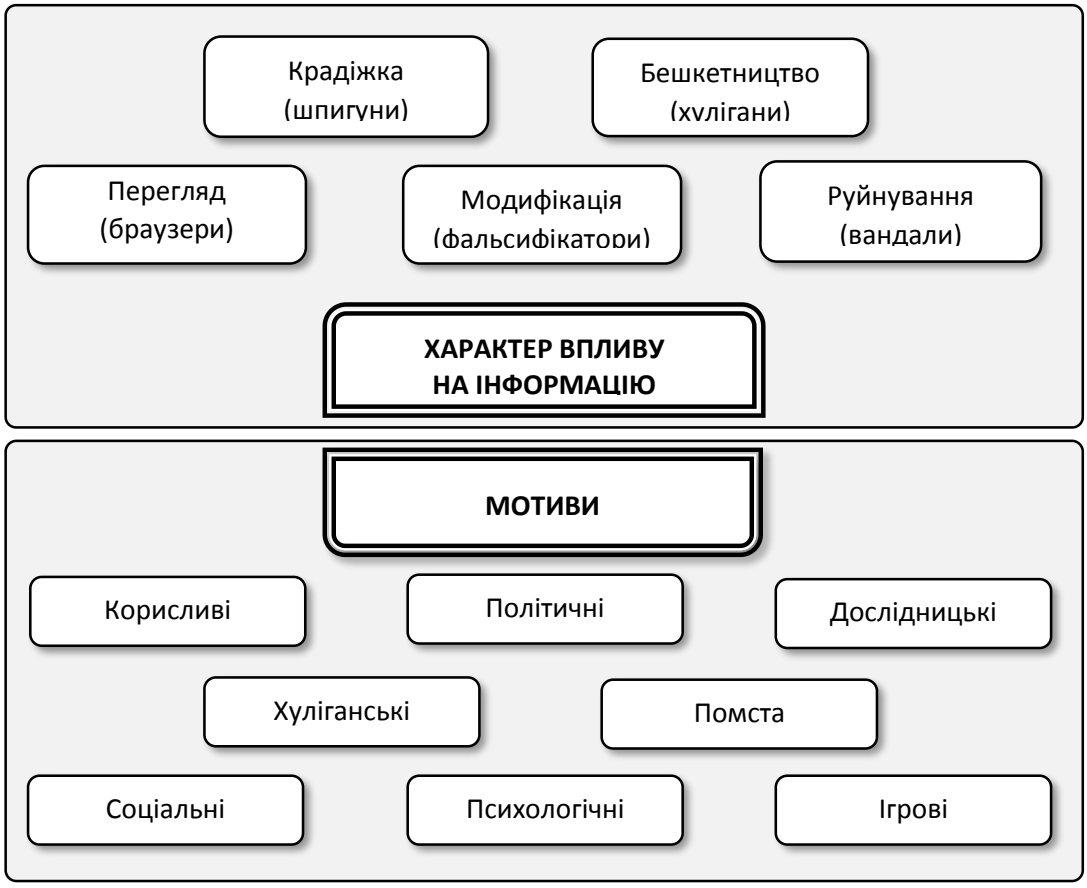

Рис. 9.4. Характер впливу на інформацію та мотивація комп'ютерних злочинців

Статистичні співвідношення різного роду мотивів при вчиненні комп'ютерних злочинів за експертними оцінками[250] складають:

- корисливі мотиви − 60 ... 70%;
- політичні мотиви (тероризм, шпигунство, дисидентство та ін.) − 15 ... 20%;
- дослідницький інтерес (допитливість) − 5 ... 7%;
- хуліганські спонукання і бешкетництво − 8 ... 10%;
- помста − 4%.

Інші мотиви скоєння комп'ютерних злочинів є відносно новими і менш вивченими.

Розглянемо докладно класифікації комп'ютерних злочинців.

Кодувальники (coders) здійснюють злом програмних продуктів, усуваючи або обходячи в них програмні механізми захисту. «Трасує» (розкладають) тексти програм, використовуючи для цього комп'ютерні мови високого рівня, в тому числі, на машинних кодах. «Роздягнені» програми передають (продають) потім, наприклад, комп'ютерним піратам або колекціонерам. Типовий «крек» − обхід необхідності введення реєстраційного або серійного номера ліцензійної програми при її інсталяції на ПК.

Комп'ютерні пірати (wares dudes) спеціалізуються на незаконному (без згоди правовласника) копіюванні ліцензійних програмних продуктів та їх розповсюдженні з метою отримання матеріальної вигоди. Наносять багатомільйонної шкоди розробникам програмних продуктів і проявляються в різних формах: «чорного» і «білого» копіювання, завантаження жорстких дисків ПК при їх продажу, перекачуванні через Інтернет тощо.

Слід зазначити, що в 2007 р., завдяки успіхам, перш за все, в нормотворчій, правозастосовній та профілактичній діяльності державних структур з України знято статус пріоритетної країни-порушника авторських прав (рівень піратства менше 90%)[251].

---

[250] Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – С. 165.

[251] Ємельянов С. Л. Проблема боротьби із комп'ютерним піратством в Україні та шляхи її вирішення / С. Л. Ємельянов // Актуальні проблеми права інтелектуальної власності: Матеріали II Всеукраїнської

Колекціонери (codes kids) колекціонують, використовують і обмінюються захищеними комп'ютерними програмними продуктами, що мають коди доступу, паролі та інші вбудовані програмні засоби захисту, а також кодами телефонного виклику і номерами телефонних компаній, що мають вихід до комп'ютерних мереж загального користування, наприклад Інтернет.

Кардери (card) – спеціалізуються на махінаціях з пластиковими картками, оплачуючи свої витрати з чужих кредитних карт. Типова процедура кардинг полягає в копіюванні інформації, що міститься на магнітній смузі кредитної картки (дамп) і виробництві фальшивої картки – «фантома» з нанесенням на неї скопійованого дампа або отриманням індивідуального PIN-коду від власника реальної карти, наприклад, методами соціальної інженерії.

Кіберкруки (cybercrooks) – спеціалізуються на несанкціоноване проникнення в комп'ютерні системи та мережі (КСС) фінансово-банківських установ і закриті КСС державних силових структур та органів. Використовують КСС для викрадення коштів, отримання цінної фінансової інформації. Популярним товаром є кредитна інформація, інформаційні бази даних правоохоронних органів та інших державних і комерційних структур.

Фішинг (phishing – з англ.: рибна ловля) – відносно новий вид мережевого шахрайства. Його метою є заволодіння шляхом обману персональними даними клієнтів онлайнових аукціонів, Інтернет – магазинів, сервісів грошових переказів та іншої конфіденційної інформації. Постійно вдосконалюються шахраями різні «виверти» спрямовані, в основному, на занадто довірливих або неуважних користувачів, самі (добровільно) розлучаються з конфіденційною інформацією, коли їх просять повторити введення пароля, повідомити номер рахунку та пароль для реєстрації покупки або грошового переказу, зареєструватися на хибному сайті-двійнику Інтернет-магазину та ін., причому бурхливий розвиток Інтернет, мережевий комерції і банкінгу обумовлюють перетворення фішингу в один з

науково-практичної конференції (11 червня 2011 р., м. Одеса) / уклад. Р. Є. Еннан, Г. О. Ульянова. – Національний університет «Одеська юридична академія». – Одеса, 2011. – С. 37-39

найпоширеніших видів комп'ютерного шахрайства. Сьогодні вже можна виділити три популярних види фішингу: поштову, онлайновий і комбінований (фарминг)[252]. В останньому випадку змінюється адреса DNS (Domain Name System) таким чином, щоб користувач взаємодіяв з фальшивим сервером-постачальником послуг (товарів).

Спамери (spam, spiced ham – з англ. – «шинка зі спеціями») займаються масовим (більше 5-ти адресатам) розсилкою непрошених (часто анонімних) повідомлень засобами електронних комунікацій, в першу чергу – по електронній пошті або мобільного зв'язку.

Вірусописаки (Virus Writers, вірмейкерів) здійснюють протиправне пошкодження КСС з метою порушення її функціонування за допомогою програмних (комп'ютерних або мережевих) вірусів.

Порнографи використовують можливості Інтернет для платного розповсюдження матеріалів порнографічного характеру, які вченими називаються «кокаїном для нового покоління». Більше 75% всієї дитячої порнографії поширюється в Інтернет, де, за деякими оцінками, налічується майже 40 тисяч порно сайтів. Моніторинг українських Інтернет-сайтів показав, що на них міститься приблизно 20% забороненої порно продукції, в тому числі і дитяча порнографія.

Кіберсквотинг (cybersquatting) – захоплення доменних імен з метою наживи. Доменні імена найчастіше називають «нерухомістю» онлайнового століття. Добре підібране ім'я може саме по собі забезпечувати досить сильний потік відвідувачів, а значить, і потенційних клієнтів: вдала назва інтуїтивно знаходиться і легко запам'ятовується. Усвідомлення цінності доменів постійно зростає, а слідом росте й їхня ціна.

Фрікери (phreak = phone+break) спеціалізуються на використанні телефонних систем, зломі цифрових АТС телефонних компаній, несанкціонованому отриманні кодів доступу до платних послуг ISDN, крадіжці і підробці телефонних карток тощо, з метою

[252] Сабадаш В. Компьютерная преступность-фишинг, как самый распространенный вид мошенничества / В. Сабадаш. – [Електронний ресурс]. – Режим доступу: http://www.crime-research.ru/articles/sabadash_0602/.

уникнути сплати за надані послуги в сфері ІКТ. У своїй діяльності використовують не тільки програмне забезпечення, але і спеціальну апаратуру, що генерує імпульсні або тональні сигнали виклику телефонних систем. Фрікінг є одним з найстаріших видів протиправної діяльності в сфері високих технологій.

З правової точки зору, відносити хакерів, кракерів, фрікерів, кардерів та інших суб'єктів вище розглянутих категорій до комп'ютерних злочинцям може тільки суд.

Висновки

У зв'язку з розвитком процесів інформатизації та комп'ютеризації суспільства захист інформації є міжнародною проблемою, яка потребує спільного вирішення.

Основними сферами політики ЄС в галузі захисту інформації є: діяльність в галузі мережевої та інформаційної безпеки, боротьбу з кіберзлочинністю, захист інформації та діяльність у сфері телекомунікацій.

Найважливішим міжнародно-правовим актом у сфері боротьби з комп’ютерної злочинністю є Конвенція про кіберзлочинність, яка є комплексним документом, що містить норми різних галузей права: кримінального, кримінально-процесуального, авторського, цивільного, інформаційного. Основною ідеєю цього документа є включення в національне законодавство країн-учасників норм про кримінальну відповідальність за злочини у сфері комп'ютерної інформації.

ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

ТЕМА 1.
Поняття інформації та її захист як складова інформаційної безпеки. Правовий захист інформації

Практичне заняття № 1

1. Поняття «інформація» та підходи до його визначення. Класифікація та властивості інформації.
2. Законодавство України про інформацію. Нормативно-правові акти у сфері захисту інформації.
3. Інформаційна безпека як інтегральна проблема. Концептуальна модель інформаційної безпеки.
4. Інформація як об’єкт захисту. Місцезнаходження інформації. Носії інформації та канали передачі даних. Інформаційні системи та мережі.
5. Основні загрози інформації та їх класифікація.
6. Комп’ютерна злочинність як комплексна загроза інформації.
7. Поняття та сутність правового захисту інформації та його нормативно-правове забезпечення.
8. Системи захисту інформації (СЗІ). Мета та засади побудови типової СЗІ, її структура.
9. Аналіз та управління ризиками.
10. Електронний цифровий підпис (ЕЦП) як програмно-технічний та правовий засіб захисту інформації.

ТЕМА 2.
Види інформації за порядком доступу. Публічна інформація

Практичне заняття № 2

1. Види інформації за законодавством України, законодавчі засади поділу інформації на відкриту та ІзОД.
2. Законодавче визначення публічної інформації. Принцип прозорості та відкритості в діяльності суб'єктів владних повноважень.
3. Порядок доступу до публічної інформації та його законодавче регулювання.
4. Суб'єкти відносин у сфері доступу до публічної інформації.
5. Реалізація права на доступ до публічної інформації. Інформаційний запит.
6. Відповідальність за порушення законодавства про доступ до публічної інформації.

ТЕМА 3.
Інформація з обмеженим доступом та її види

Практичне заняття № 3

1. Інформація з обмеженим доступом (ІзОД) за українським законодавством. Види ІзОД.
2. Законні підстави (вимоги) за якими може бути здійснено обмеження доступу до інформації.
3. Інформація що належить до ІзОД. Інформація що не може бути обмеженою та відомості, що не належать до ІзОД.
4. Поняття конфіденційної інформації, її правові ознаки, відомості що відносяться до конфіденційної інформації.
5. Поняття таємної інформації, її правові ознаки, види таємниць.
6. Службова інформація – поняття та відомості що до неї відносяться.

ТЕМА 4.
Інститут державної таємниці

Практичне заняття № 4

1. Поняття та законодавче визначення державної таємниці (ДТ). Правові ознаки ДТ.
2. Правовий інститут ДТ, його складові. Законодавство України про ДТ.
3. Інформація, що відноситься до ДТ. Інформація, що не відноситься до ДТ.
4. Основні організаційно-правові заходи щодо охорони ДТ.
5. Державні органи в сфері ДТ. Режимно-секретні органи, їх правовий статус та основні завдання.
6. Державний експерт з питань таємниць та його правовий статус.
7. Допуск та доступ до ДТ.
8. Відповідальність за порушення законодавства про державну таємницю.

ТЕМА 5.
Інститути банківської та комерційної таємниць

Практичне заняття № 5

1. Інститут банківської таємниці (БТ) та його склад.
2. Законодавство України про БТ. Інформація, що містить БТ.
3. Співвідношення банківської таємниці із комерційною таємницею.
4. Заходи з охорони та захисту БТ.
5. Відповідальність за розголошення БТ – дисциплінарна, цивільно-правова, кримінальна.
6. Поняття комерційної таємниці (КТ). Правовий інститут КТ та його структура.

7. Промислове (конкурентне) шпигунство як загроза комерційної таємниці.
8. Відомості, що відносяться до КТ та інформація, що не входить до КТ.
9. Заходи із охорони та захисту КТ та їх законодавче регулювання. Система загроз та ризиків.
10. Роль КТ в господарській діяльності.
11. Відповідальність за розголошення КТ, наслідки розголошення КТ.

ТЕМА 6.
Таємниця досудового розслідування

Практичне заняття № 6

1. Поняття таємниці досудового розслідування (ТДР), його законодавче визначення.
2. Правовий інститут ТДР, його особливості. Процесуальні та матеріальні норми права у правовому інституті ТДР.
3. Межі застосування ТДР та поширення її дії на судовий розгляд.
4. Таємниця нарадчої кімнати. Закрите судове засідання.
5. Співвідношення дії ТДР у судовому розгляді із принципом публічності та принципом гласності та відкритості судового провадження та його повного фіксування технічними засобами.
6. Загрози ТДР, заходи з охорони і захисту ТДР.
7. Недосконалість законодавства щодо ТДР, пропозиції з його покращення.

ТЕМА 7.

Професійна таємниця та інші види таємниць, передбачені законодавством України

Практичне заняття № 7

1. Професійна таємниця (ПТ) – поняття, ознаки, законодавче визначення.
2. Правовий інститут ПТ, проблема недосконалості правового інституту ПТ.
3. Інформація, що входить до ПТ за законодавством України.
4. Інформація, що за своєю природою та властивостями може входити до ПТ.
5. Заходи із захисту й охорони ПТ.

Практичне заняття № 8

1. Інші види таємниць, передбачені законодавством, їх поняття, ознаки, норми, які визначають їх правовий статус.
2. Аналіз професійних таємниць за концептуальною моделлю інформаційної безпеки:
   2.1. Лікарська таємниця.
   2.2. Нотаріальна таємниця.
   2.3. Податкова таємниця.
   2.4. Адвокатська таємниця.
   2.5. Журналістська таємниця.
   2.6. Таємниця сповіді.
   2.7. Таємниця голосування.
   2.8. Таємниця зв’язку (листування)

ЛАБОРАТОРНІ РОБОТИ

№1 *Використання шифрування та електронного цифрового підпису для захисту текстового документа*

Мета:

навчитися використовувати спеціальне ПЗ для створення електронного цифрового підпису.

Опис завдання:

- *Створити текстовий документ з умовно «таємною» інформацією;*
- *використовуючи утиліту PGP, створити асиметричну пару ключів;*
- *зашифрувати текстовий документ, додати до нього електронний підпис;*
- *розшифрувати раніше зашифрований текстовий документ, перевірити його цифровий підпис.*

№2 *Складання електронного інформаційного запиту шляхом заповнення інтерактивної форми*

Мета:

навчитися заповнювати інтерактивні форми для подання електронного інформаційного запиту.

Опис завдання:

- *ознайомитися із вимогами до запиту на доступ до публічної інформації;*
- *заповнити інтерактивну навчальну форму для подання електронного інформаційного запиту від імені фізичної особи;*
- *заповнити інтерактивну навчальну форму для подання електронного інформаційного запиту від імені юридичної особи.*

№3 Робота зі службами та інструментами захисту облікових записів користувачів в ОС Windows

Мета:

навчитися використовувати засоби Панелі керування ОС Windows для налаштування захисту облікового запису користувача комп'ютера.

Опис завдання:

- *ознайомитися з можливостями Панелі керування, служб «Облікові записи» та «Безпека сім'ї»;*
- *захистити обліковий запис користувача паролем, створити підказку для пароля;*
- *налаштувати особливі умови доступу до комп'ютера для облікового запису дитини;*
- *вимкнути режим запиту пароля при вході в систему, не видаляючи пароль облікового запису.*

№4 Використання методу комп'ютерної стеганографії для захисту інформації

Мета:

навчитися приховувати текстові повідомлення в графічних файлах

Опис завдання:

- *ознайомитися з можливостями утиліти Fox Secret;*
- *використовуючи утиліту Fox Secret приховати текстове повідомлення (документ) у зображенні;*
- *відкрити прихований у зображенні текстовий файл за допомогою утиліти Fox Secret.*

№5 Парольний захист файлів користувача

Мета:

навчитися захищати паролем найуживаніші файли (текстові документи, електронні таблиці, архіви)

Опис завдання:

- *використовуючи сервісні можливості програми MS Word, захистити паролем текстовий документ;*
- *використовуючи сервісні можливості програми MS Excel, захистити паролем електронну таблицю;*
- *засобами програми-архіватора WinRAR створити захищений паролем архівний файл.*

№6 Налаштування параметрів приватності в мережі Інтернет та соціальних мережах

Мета:

поглибити знання правил безпечного користування мережею Інтернет

Опис завдання:

- *стандартними засобами Інтернет-браузера очистити історію переглядів Інтернет-сторінок та історію завантажень файлів;*
- *відвідати web-сторінки у режимі анонімного перегляду Інтернет-браузера;*
- *ознайомитися із параметрами приватності профілів користувача у популярних соціальних мережах.*

ТЕМИ ДОДАТКОВИХ ІНФОРМАЦІЙНИХ ПОВІДОМЛЕНЬ

1. Комп’ютерна злочинність як комплексна загроза інформації.
2. Електронний цифровий підпис (ЕЦП) як програмно-технічний та правовий засіб захисту інформації.
3. Промислове шпигунство як загроза безпеці комерційної таємниці.
4. Концептуальна модель захисту таємниці досудового розслідування.
5. Концептуальна модель захисту лікарської таємниці.
6. Концептуальна модель захисту нотаріальної таємниці.
7. Концептуальна модель захисту адвокатської таємниці.
8. Концептуальна модель захисту податкової таємниці.
9. Концептуальна модель захисту журналістської таємниці.
10. Концептуальна модель захисту таємниці сповіді.
11. Концептуальна модель захисту таємниці голосування.
12. Концептуальна модель захисту таємниці зв’язку (листування).
13. Концептуальна модель захисту аудиторської таємниці.
14. Концептуальна модель захисту інсайдерської таємниці.
15. Концептуальна модель захисту таємниці усиновлення.
16. Концептуальна модель захисту таємниці страхування.
17. Концептуальна модель захисту таємниці авторства.
18. Концептуальна модель захисту службової таємниці.

ТЕМИ РЕФЕРАТІВ

1. Історія становлення та розвитку інституту персональних даних.
2. Визначення поняття персональних даних – доктринальний та нормативно-правовий підходи.
3. Персональні дані як складова права на приватність.
4. Міжнародне законодавство та стандарти в сфері захисту персональних даних.
5. Українське законодавство про захист персональних даних.
6. Суб'єкти відносин, пов'язаних із захистом персональних даних.
7. Персональні дані як об’єкт захисту.
8. Суб’єкт персональних даних та його права.
9. Правове регулювання використання персональних даних.
10. Вимоги до обробки персональних даних.
11. Співвідношення понять «використання», «обробка», «збирання» «накопичення та зберігання» персональних даних.
12. Порядок видалення або знищення персональних даних.
13. Порядок доступу до персональних даних.
14. Відповідальність за порушення законодавства про захист персональних даних.
15. Повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних.
16. Судова практика у справах щодо захисту персональних даних.
17. Захист персональних даних в соціальних мережах.
18. Конфіденційність інформації в мережі Інтернет.

ЗАПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Поняття «інформація» та підходи до його визначення. Властивості інформації.
2. Законодавство України про інформацію. Нормативно-правові акти у сфері захисту інформації.
3. Інформаційна безпека як інтегральна проблема. Концептуальна модель інформаційної безпеки.
4. Інформація як об’єкт захисту.
5. Місцезнаходження інформації. Носії інформації та канали передачі даних.
6. Основні загрози інформації та їх класифікація.
7. Комп’ютерна злочинність як комплексна загроза інформації.
8. Поняття та сутність правового захисту інформації та його нормативно-правове забезпечення.
9. Системи захисту інформації (СЗІ). Мета та засади побудови типової СЗІ, її структура.
10. Аналіз та управління ризиками.
11. Електронний цифровий підпис (ЕЦП) як програмно-технічний та правовий засіб захисту інформації.
12. Види інформації за законодавством України, законодавчі засади поділу інформації на відкриту та інформацію з обмеженим доступом.
13. Законодавче визначення публічної інформації. Принцип прозорості та відкритості в діяльності суб’єктів владних повноважень.
14. Порядок доступу до публічної інформації та його законодавче регулювання.
15. Суб’єкти відносин у сфері доступу до публічної інформації.
16. Реалізація права на доступ до публічної інформації. Інформаційний запит.

17. Відповідальність за порушення законодавства про доступ до публічної інформації.

18. Інформація з обмеженим доступом (ІзОД) за українським законодавством. Види ІзОД.

19. Законні підстави (вимоги) за якими може бути здійснено обмеження доступу до інформації.

20. Інформація що належить до ІзОД. Інформація що не може бути обмеженою та відомості, що не належать до ІзОД.

21. Поняття конфіденційної інформації, її правові ознаки, відомості що відносяться до конфіденційної інформації.

22. Поняття таємної інформації, її правові ознаки, види таємниць.

23. Службова інформація – поняття та відомості що до неї відносяться.

24. Поняття та законодавче визначення державної таємниці. Правові ознаки державної таємниці.

25. Правовий інститут державної таємниці, його складові. Законодавство України про державну таємницю.

26. Основні організаційно-правові заходи щодо охорони державної таємниці.

27. Державні органи в сфері державної таємниці. Режимно-секретні органи, їх правовий статус та основні завдання.

28. Державний експерт з питань таємниць та його правовий статус.

29. Допуск та доступ до державної таємниці.

30. Відповідальність за порушення законодавства про державну таємницю.

31. Інститут банківської таємниці та його склад.

32. Законодавство України про банківську таємницю. Інформація, що містить банківську таємницю.

33. Співвідношення банківської таємниці із комерційною таємницею.

34. Заходи з охорони та захисту банківської таємниці.

35. Відповідальність за розголошення банківської таємниці – дисциплінарна, цивільно-правова, кримінальна.

36. Поняття комерційної таємниці. Правовий інститут комерційної таємниці, його структура.

37. Відомості, що відносяться до комерційної таємниці та інформація, що не входить до неї.

38. Промислове (конкурентне) шпигунство як загроза комерційної таємниці.

39. Заходи із охорони та захисту комерційної таємниці та їх законодавче регулювання. Система загроз та ризиків.

40. Роль комерційної таємниці в господарській діяльності.

41. Відповідальність за розголошення комерційної таємниці, наслідки розголошення комерційної таємниці.

42. Поняття таємниці досудового розслідування, його законодавче визначення.

43. Правовий інститут таємниці досудового розслідування, його особливості.

44. Процесуальні та матеріальні норми права у правовому інституті таємниці досудового розслідування.

45. Межі застосування таємниці досудового розслідування та поширення її дії на судовий розгляд.

46. Таємниця нарадчої кімнати. Закрите судове засідання.

47. Співвідношення дії таємниці досудового розслідування у судовому розгляді із принципом публічності та принципом гласності та відкритості судового провадження та його повного фіксування технічними засобами.

48. Загрози таємниці досудового розслідування, заходи з її охорони та захисту.

49. Недосконаліть законодавства про таємницю досудового розслідування, пропозиції з його покращення.

50. Професійна таємниця – поняття, ознаки, законодавче визначення.

51. Правовий інститут професійної таємниці, проблема його недосконалості правового інституту.

52. Інформація, що входить до професійної таємниці за законодавством України.

53. Інформація, що за своєю природою та властивостями може входити до професійної таємниці.

54. Заходи із захисту й охорони ПТ.

55. Лікарська таємниця – поняття та ознаки, інформація, що до неї відноситься.

56. Нотаріальна таємниця – поняття та ознаки, інформація, що до неї відноситься.

57. Податкова таємниця – поняття та ознаки, інформація, що до неї відноситься.

58. Адвокатська таємниця – поняття та ознаки, інформація, що до неї відноситься.

59. Журналістська таємниця – поняття та ознаки, інформація, що до неї відноситься.

60. Таємниця сповіді – поняття та ознаки, інформація, що до неї відноситься.

61. Таємниця голосування – поняття та ознаки, інформація, що до неї відноситься.

62. Таємниця зв’язку (листування) – поняття та ознаки, інформація, що до неї відноситься.

63. Парольний захист файлів користувача як загальнодоступний спосіб захисту інформації.

64. Служби та інструменти захисту облікових записів користувачів ПК та мобільних пристроїв.

65. Параметри приватності та умови безпечного користування інформаційними ресурсами мережі Інтернет.

66. Визначення поняття персональних даних та його законодавче закріплення.

67. Українське законодавство про захист персональних даних.

68. Порядок доступу до персональних даних за ЗУ «Про захист персональних даних».

69. Відповідальність за порушення законодавства про захист персональних даних.

70. Повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних.

71. Персональні дані як складова права на приватність

72. Суб'єкти відносин, пов'язаних із захистом персональних даних.

73. Порядок видалення або знищення персональних даних за ЗУ «Про захист персональних даних».

74. Міжнародне законодавство та стандарти в сфері захисту персональних даних

75. Захист персональних даних в соціальних мережах.

ПІДСУМКОВИЙ ТЕСТ

1. До якого виду інформації відноситься комерційна таємниця?

- відкрита
- інформація з обмеженим доступом
- закрита
- засекречена

2. До якого виду інформації належать персональні дані фізичної особи?

- інформація з обмеженим доступом
- відкрита інформація
- засекречена інформація

3. До якого виду таємниці відноситься інформація про фінансово-економічний стан юридичної особи?

- банківська
- інсайдерська
- комерційна
- професійна

4. Яка інформація може відкрито публікуватися в текстах судових рішень?

- персональні дані фізичної особи
- прізвище та ініціали суддів, які прийняли судове рішення
- реєстраційні номери транспортних засобів
- адреса електронної пошти фізичної особи

5. Яка інформація може належати до службової?

- інформація, зібрана в процесі оперативно-розшукової діяльності
- інформація, що містить державну таємницю
- інформація про фізичну особу

6. Яка інформація не відноситься до державної таємниці?

- інформація про факти порушення прав і свобод громадян
- інформація військово-технічного характеру
- відомості про експорт та імпорт озброєння
- інформація про окремі аспекти негласної правоохоронної діяльності

7. Яка інформація не відноситься до інформації з обмеженим доступом?

- конфіденційна
- таємна
- службова
- відкрита

8. Яка інформація не є банківською таємницею?

- фінансово-економічний стан клієнта
- коди, використовувані банком для захисту інформації
- інформація щодо звітності по окремому банку
- обсяг кредитного портфеля банку

9. Якого виду інформації немає в ЗУ «Про внесення змін до Закону «Про інформацію»?

- правова
- статистична
- соціологічна
- економічна

10. Якого виду інформації за порядку доступу не існує?

- відкрита
- інформація з обмеженим доступом
- закрита

11. Якого режиму секретності державної таємниці не існує?

- таємно
- цілком таємно
- особливої важливості
- для службового користування

12. Яка властивість інформації полягає в її існуванні в незмінному вигляді в певний проміжок часу?

- адекватність
- конфіденційність
- цілісність
- доступність

13. Яка властивість не визначає стан безпеки інформації?

- доступність
- конфіденційність
- цілісність
- актуальність

14. Яка властивість відноситься до юридичних властивостей інформації?

- здатність до тиражування
- селективність
- здатність до трансформації
- невичерпність

15. Яка властивість характеризує якість інформації?

- адекватність
- невичерпність
- системність
- селективність

16. Який вид правового обігу інформації регулюється цивільно-правовими нормами?

- відкритий
- закритий
- обмежений

17. Який вид таємниці не відноситься до професійної?

- інсайдерська
- аудиторська
- нотаріальна
- комерційна

18. Який підхід до поняття «інформація» не дає точного визначення інформації?

- недетермінований
- техноцентричний
- антропоцентричний

20. При якому підході поняття «інформація» інформацію ототожнюють з даними?

- техноцентричний
- недетермінований
- антропоцентричний

21. Розголошення якого виду таємниці може завдати шкоди національній безпеці України?

- державна
- комерційна
- банківська
- таємниці досудового розслідування

22. Різновидом який таємниці є військова таємниця?

- службова
- професійна
- комерційна

23. Вкажіть інформацію, доступ до якої обмежується і розголошення якої може завдати шкоди особі, суспільству і державі?

- секретна
- конфіденційна
- службова

24. Що не входить до складу правового інституту таємниці?

- загальна частина
- режим секретності
- санкції
- закрита частина

25. Яка властивість не відноситься до загальних властивостей інформації?

- системність
- селективність
- невичерпність
- адекватність

БІБЛІОГРАФІЯ

1. Аверченков В. И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин. – Брянск: БГТУ, 2007. – 225 с.
2. Аксенов С. Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти / С. Г. Аксенов // Безопасность бизнеса. – 2008. – № 3.
3. Алексеев С. С. Общие дозволения и общие запреты в советском праве. – М., 1989. – С. 185.
4. Бабич О. Лікарська таємниця / О. Бабич // Управління закладом охорони здоров'я. – 2012. – № 4. – С. 11-16.
5. Банківська енциклопедія / За заг. ред. докт. екон. наук, проф. А. М. Мороза. – К.: Фірма «Ельтон», 1993. – С. 22.
6. Банківське право України: Навч. посібник. Кол. авт.: Жуков А. М., Іоффе А. Ю., Кротюк В. Л., Пасічник В. В., Селіванов А. О. та ін. / За заг. ред. А. О. Селіванова. – К.: Видавничий Дім «Ін Юре», 2000. – 384 с.
7. Бараннік Р. В., Назаренко П. Г. Особливості охорони інформації, що становить таємницю у кримінальному судочинстві / Р. В. Бараннік, П. Г. Назаренко // Адвокат. – № 4 (127). – 2011. – С. 15–18.
8. Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / В. Ю. Баскаков. – К., 2012. – 20 с.
9. Баутов А. Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. – №2. – 2002.
10. Безклубий І. Поняття банківської таємниці / І. Безклубий // Підприємництво, господарство і право. – 2005. – № 4. – С. 16–19.
11. Бєляков К. І. Інформація з обмеженим доступом: проблеми законодавчого регулювання / К. Бєляков // Науковий вісник Національної академії внутрішніх справ України. – 2004. – № 6.– С. 267–277.

12. Біленчук П. Д. Комп'ютерна злочинність [навчальний посібник] / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – Київ: Атіка, 2002. – С. 66.
13. Благовещенский А. Читайте мелкий шрифт – [Електронний ресурс]. – Режим доступу: http://www.rg.ru/2011/05/05/ internet.html.
14. Блінова Г. О. Службова таємниця як вид публічної інформації з обмеженим доступом. – [Електронний ресурс]. – Режим доступу: http://pravoisuspilstvo.org.ua/archive/2013/3_2013/07.pdf.
15. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К.: «МК-Прес», 2005. – С. 39.
16. Бойков А. Д. Предмет и пределы гласности уголовного судопроизводства / А. Д. Бойков // Охрана прав граждан в уголовном судопроизводстве: Сб. науч. тр. – М.: ВНИИ проблем укрепления законности и правопорядка, 1989. – С. 8.
17. Ботвінкін О. Система охорони Державної таємниці в Україні. Історичний аспект / О. Ботвінкін. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 2 (13). – 2006. – С. 83-88.
18. Брединский А. Правовой режим защиты коммерческой тайны в США и Великобритании / А. Брединский. – [Електронний ресурс]. – Режим доступу: http://www.real-voice.info/modules/myarticles/ article.php?storyid =503.
19. Використання інформаційних технологій в судах: Навчальний посібник / Ємельянов С. Л., Логінова Н. І., Тодощак О. В., Якутко В. Ф. – Одеса: Фенікс, 2014. – 157 с.
20. Винер Н. Кибернетика, или Управление и связь в животном и машине. / Пер. с англ. И. В. Соловьева и Г. Н. Поварова; Под ред. Г. Н. Поварова. – 2-е издание. – М.: Наука; Главная редакция изданий для зарубежных стран, 1983. – 344 с.
21. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002. – С. 86.
22. Всеобщая декларация прав человека. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_015.

23. Гавдьо Ю. Банківська таємниця як окремий вид інформації з обмеженим доступом // Юридичний радник. – 2007. – № 4 (18). – С. 9-12.
24. Гаврилов Б. Я. Реализация органами предварительного следствия правовых норм о защите конституционных прав и свобод человека и гражданина. – [Електронний ресурс]. – Режим доступа: http://www.cfin.ru/press/black/2001-1/05_01_gavriloff.shtml.
25. Гаврилов О. А. Курс правовой информатики: Учебник для вузов. – М.: Изд-во НОРМА, 2002. – 432 с.
26. Гвирцман М. В. Правовое регулирование банковской тайны / М. В. Гвирцман // Деньги и кредит. – 1992. – № 6. – С. 57.
27. Гетманцев Д. О. Банківська таємниця: особливості її нормативно-правового регулювання в Україні та в законодавстві зарубіжних країн. Автореф. дис…канд.юр. наук: 12.00.07 / КНУ ім. Т. Шевченка. – К., 2003. – 23 с.
28. Глобализация и информатизация. – [Електронний ресурс]. – Режим доступу: http://www.intuit.ru/studies/courses/505/361/ lecture/ 8595.
29. Гнатюк С. Л. Особливості захисту персональних даних в сучасному кіберпространстві: правові та техніко-технологічні аспекти: Аналітична доповідь. – [Електронний ресурс]. – Режим доступу:http://www.niss.gov.ua/public/File/2013_table/1010_dopov.pdf.
30. Головань С. М. Системи охорони державної таємниці. підручник / С. М. Головань, С. Б. Гордієнко, О. В. Корнейко, А. О. Петров. – Луганськ: вид-во СНУ ім. В. Даля, 2012. – 296 с.
31. Гончар И. Режим коммерческой тайны. Анализ правового статуса института коммерческой тайны в аспекте его реформирования.– [Електронний ресурс].– Режим доступа: http://www.e-news.com.ua/print/124720.html.
32. Господарський кодекс України від 16.01.2003 р. № 436-IV // Відомості Верховної Ради. – 2003. – № 18–22. – Ст. 144.

33. Декларация принципов поведения журналиста Международной Федерации Журналистов. – [Електронний ресурс]. – Режим доступу: http://www.presscouncil.ru/index.php/teoriya-i-praktika/dokumenty/54-deklaratsiya-printsipov-povedeniya-zhurnalista-mezhdunarodnoj-federatsii-zhurnalistov.
34. Державна уніфікована система документації. Основні положення: ДСТУ 3843-99. – [Чинний від 2000-07-01]. – К.: Держстандарт України, 2000. – 8 с. – (Національний стандарт України).
35. Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных. – [Електронний ресурс]. – Режим доступу: http://www.datepersonale.md/file/Directiva _95_46_ru.pdf.
36. Добровольский В. И. Инсайдерская информация в мировой практике, служебная информация и коммерческая тайна в России // Предпринимательское право. – 2008. – № 4. – С. 11-16.
37. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В.В.Домарев.– К.: ООО «ТИД «ДС», 2001. – С. 650.
38. Доронин А. И. Бизнес-разведка / А. И. Доронин. – М.: Ось-89, 2002. – 288 с.
39. Доступ до інформації та електронне урядування / Автори-упорядники М. С. Демкова, М. В. Фігель. – К.: Факт, 2004. –336 с.
40. Доступ до публічної інформації: Навчально-метод. матеріали для тематичного короткотермінового семінару / В. І. Малімон, С. В. Онищук. – Івано-Франківськ: «Місто НВ», 2012. – 88 с.
41. Доступ к публичной информации на Украине тянет на троечку. – [Електронний ресурс]. – Режим доступу: http://svobodainfo.org/ ru/ node/2742.
42. Дробожур Р. Р. Слідова картина як елемент криміналістичної характеристики злочинів у сфері електронної обчислювальної техніки. «Віртуальні сліди» // Сучасні проблеми криміналістики: матеріали міжнародної науково-практичної конференції, присвяченої 100-річчю з дня народження доктора юридичних наук,

професора В. П. Колмакова (27-28 вересня 2013 року, м. Одеса) / упоряд.: В. В. Тіщенко, О. П. Ващук. – Одеса: Юридична література, 2013. – С. 114-118.

43. Европейская конвенция о защите прав человека и основополагающих свобод. – [Електронний ресурс]. – Режим доступа: http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.
44. Емельянинков М. Как защищать персональные данные в Интернет. – [Електронний ресурс]. – Режим доступу: http://old.infosec.ru/presscentre/publication/PD_protection_internet.
45. Емельянов С. Л. Некоторые аспекты компьютерной преступности и борьбы с нею / С. Емельянов, И. Гловюк, Е. Емельянова // Бизнес и безопасность. – 2006. – № 3. – С. 143–145.
46. Емельянов С. Л. О некоторых аспектах криминалистической характеристики современных компьютерных преступников / С. Л. Емельянов. – [Електронний ресурс]. – Режим доступу: http://inter.criminology.org.ua/?p=855/. – Назва з екрану.
47. Ємельянов С. Л. Основи інформаційної безпеки: Навчальний посібник / С. Л. Ємельянов. – Одеса: Фенікс, 2014. –357 с.
48. Ємельянов С. Л. Проблема боротьби із комп'ютерним піратством в Україні та шляхи її вирішення / С. Л. Ємельянов // Актуальні проблеми права інтелектуальної власності: Матеріали II Всеукраїнської науково-практичної конференції (11 червня 2011 р., м. Одеса) / уклад. Р. Є. Еннан, Г. О. Ульянова. – Національний університет «Одеська юридична академія». – Одеса, 2011. – С. 37-39.
49. Ємельянов С. Л. Проблема формування правових інститутів таємниць в Україні / С. Л. Ємельянов // Наукові праці Національного університету «Одеська юридична академія». – 2012. – Т. XII. – С. 130–140.
50. Ємельянов С. Л. Проблемні аспекти організаційно-правового захисту державної таємниці в Україні / С. Л. Ємельянов // Інформаційна безпека. – 2011.– Вип. 1(5). – С. 36–44.
51. Ємельянов С. Л. Стан та розвиток професійної таємниці в Україні / С. Л. Ємельянов // Право і безпека. – 2011. – № 5 (2). – С. 1–7.

52. Ємельянов С. Л. Таємниця слідства та судочинства в України / С. Л. Ємельянов // Ученые записки Таврического национального университета им. В. И. Вернадского. – Серия «Юридические науки». – Том 26 (65). – 2013. – № 2-1 (Ч. 2). – С. 310–316.
53. За забезпечення недоторканості приватного життя в Інтернет: Декларація. – [Електронний ресурс]. – Режим доступу: http://uapdp.org/ images/Declaration.pdf.
54. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов; Алт. гос. техн. ун-т им. И. И. Ползунова. – Барнаул: АлтГТУ, 2011. – 252 с.
55. Защита конфиденциальности в социальных сетях: Электронное руководство TrendLabs по жизни в цифровом мире. – [Електронний ресурс]. – Режим доступу: http://www.trendmicro.com.ru/media/ br/eguide-how-to-protect-your-privacy-on-social-media-ru.pdf.
56. Звід відомостей, що становлять державну таємницю, затв. Наказом Служби безпеки України від 12.08.2005 р. № 440 // Офіційний Вісник України. – 2005. – № 34. – Ст. 2089.
57. Золотар О. О. Обмеження доступу до інформації: інформаційно-правовий аспект. – [Електронний ресурс]. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/iblsd/2012_1/_private/13zooala.pdf.
58. Игнатов С. Д. Следственная тайна и ее пределы / С. Д. Игнатов // Правовая реформа и проблемы ее реализации. – Краснодар, 1989. – С. 257–258.
59. Информационное право / под ред. И. Л. Бачило, В. Н. Лопатин, М.А. Федотов, Б. Н. Топорина. – СПб.: Питер, 2001. – 789 с.
60. Іванова Т. В., Піддубна Л. П. Діловодство в органах державного управління та місцевого самоврядування. Навчальний посібник. – К.: Центр учбової літератури, 2007. – 360 с.
61. Інформатизація управління соціальними системами: Організаційно-правові питання теорії і практики: Навч. посіб. / В. Д. Гавловський, Р. А. Калюжний, В. С. Цимбалюк та ін.: За заг. ред. М. Я. Швеця, Р. А. Калюжного. – К.: МАУП, 2003. – 336 с.

62. Інформаційне право та правова інформатика у сфері захисту персональних даних / Авт. кол-в: В. Брижко, М. Гуцалюк, В. Цимбалюк, М. Швець: Монографія; За ред. доктора економічних наук, професора, члена-кореспондента Академії правових наук України М. Швеця. – К.: НДЦПІ АПрН України, 2006. – 450 с.
63. Інформаційне право. Тексти лекцій (для студентів денного та заочного відділення спеціальності «Правознавство») / Укладач: Є. А. Таликін. – Луганськ: вид-во СНУ ім. В. Даля, 2013. –155 с.
64. Камалова Г. Г. Анализ понятия и содержания тайны следствия / Г. Г. Камалова // Вестник Удмурского университета. – Серия «Экономика и право». – 2013. – Вып. 1. – С. 156.
65. Карпачева Н. И. Состояние соблюдения и защиты прав и свобод человека в Украине: Первый ежегодный доклад Уполномоченного Верховной Рады Украины по правам человека / Перевод с украинского. – Харьков: Консум, 2002. – 494 с.
66. Ковалева Н. Н. Информационное право России: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К», 2007. – 360 с.
67. Кодекс професійної етики судді, затверджений V З'їздом суддів України 24 жовтня 2002 р. // Вісник Верховного Суду України – 2002. – № 5. – С. 24-34.
68. Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8073-X // Відомості Верховної Ради України. – 1984. – № 51. – Ст. 1122.
69. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М., 2002. – С. 127–129.
70. Комкова К. С. Безопасность персональной информации в социальных сетях: правовой аспект / К. С. Комкова // Вестник южного научного центра. – Т. 9. – № 3. – 2013. – С. 71-75.
71. Конвенция о защите прав человека и основных свобод: ETS N 005 (Рим, 4 ноября 1950 г.). – [Електронний ресурс]. – Режим доступу: http://base.garant.ru/2540800/.
72. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. – [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/1/MU81311.html.

73. Конвенція про кіберзлочинність // Офіційний вісник України від 10.09.2007 р. – № 65. – Ст. 2535.
74. Конституція України // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.
75. Концепція проекту Закону України «Про охорону прав на комерційну таємницю». – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1404-2008-%F0.
76. Концепція реформування законодавства України у сфері суспільних інформаційних відносин (проект). – [Електронний ресурс]. – Режим доступу: http://bezpeka.com/ru/lib/art519.html.
77. Копылов В. А. Информационное право / В. А. Копылов. – М.: Юрист, 2002. – 512 с.
78. Кормич Б. А. Інформаційне право. Підручник. – Харків: БУРУН і К, 2011. –334 с.
79. Кримінальний кодекс України від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131.
80. Кримінальний процесуальний кодекс України від 13.04.2012 р. // Відомості Верховної Ради. – 2013. – № 9-13. – Ст. 88.
81. Кришталюк А. Н. Защита коммерческой тайны: Курс лекций. – [Електронний ресурс].– Режим доступу: http://nauka2020.ru/ Krishtaluk_40213.pdf.
82. Крылов А. В. К вопросу об определении тайны следствия / А. В. Крылов // Российский следователь. – 2003. – № 9. – С. 32–38.
83. Кузьмічов В. С., Лісогор В. Г. Розголошення інформації, що становить таємницю досудового слідства / В. С. Кузьмічов, В. Г. Лісогор // Боротьба з організованою злочинністю й корупцією (теорія і практика): наук.-практ. журнал. – К. : Міжвід. наук.-дослід. центр із проблем боротьби з організованою злочинністю, 2001. – № 4. – С. 176.
84. Кулініч О. О. Інформація з обмеженим доступом як об'єкт цивільних прав: Дис… к.ю.н.: 12.00.03 – Одеса, 2006. –200 с.

85. Лічман Т. В. Класифікація та аналіз загроз безпеці комерційної таємниці підприємства / Т. В. Лічман // Вісник ОНУ ім. І. І. Мечникова. – 2013. – Т. 18. – Вип. 1/1. – С. 230-233.
86. Лукацький А. Класифікація інформації. Анонс нового дослідження. – [Електронний ресурс]. – Режим доступу: http://bis-xpert.ru/sites/default/files/archives/2011/CISCO_for_DLP_ Russia_2011.pdf.
87. Ляш А. О. Недопустимість розголошення відомостей досудового розслідування. – [Електронний ресурс]. – Режим доступу: http://lj.oa.edu.ua/articles/2013/n1/13laovdr.pdf.
88. Марущак А. І. Інформаційне право: Доступ до інформації: Навчальний посібник. – К.: КНТ, 2007. –532 с.
89. Методичні рекомендації щодо практичного впровадження Закону України «Про доступ до публічної інформації» / М. В. Лациба, О. С. Хмара, В. В. Андрусів та ін.; Укр. незалеж. центр політ. дослідж. – К.: Агентство «Україна», 2011. – 144 с.
90. Науково-практичний коментар до Закону України «Про доступ до публічної інформації» / Під заг. ред.. Д. Котляр. – К., 2012. – 335 с.
91. О гражданских и политических правах: Международный пакт от 16.12.1966 г. – [Електронний ресурс]. – Режим доступу: http://zakonbase.ru /content/base/5683.
92. Об исполнении обязанностей и обязательств Украиной: Резолюция 1466 (2005) Парламентской Ассамблеи Совета Европы от 05.10.2005 г. – [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/MU05122.html.
93. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов [и др.]; под ред. А. А. Стрельцова. – М.: Издательский центр «Академия», 2008. – 256 с.
94. Організаційноо-правов засади політики інформаційної безпеки України: Монографія / Б. А. Кормич. – Одеса: Юридична література, 2003. – С. 353–357.

95. Організаційно-правові основи захисту інформації з обмеженим доступом: [навчальний посібник] / А. Б. Стоцький, О. І. Тимошенко, А. М. Гуз та ін., за заг. ред. В. С. Сідака. – К.: Вид–во Європейського університету, 2006. – 232 с.
96. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – С. 128–132.
97. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 р. // Відомості Верховної Ради. – 1993. – № 4. – Ст. 19.
98. Основи інформаційного права України: навч. посіб. / В. С. Цимбалюк, В. Д. Гавловський, В. М. Брижко та ін.; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника. 2-ге вид., переробл. і допов.– К.: Знання, 2009.– С. 282–365.
99. Основні принципи незалежності судових органів: Міжнародний документ від 13.12.1985 р. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_201.
100. Панталієнко Я. П. Нотаріальна таємниця – одне з загальних правил вчинення нотаріальних дій / Я. П. Панталієнко // Радник: Український юридичний портал. – [Електронний ресурс]. – Режим доступу: http://radnuk.info/statti/230-tsuv-pravo/3585-2010-01-29-17-38-54. html.
101. Парламентські слухання з питань розвитку інформаційного суспільства в Україні: Матеріали Парламентських слухань у Верховної Раді України від 21.09.2005 р./ Верховна Рада України; Комітет з питань науки і освіти / М. К. Родіонов (голова редкол., упоряд.), І. Б. Жиляєв (упоряд.). – К.: Парламетн. вид-во, 2006. – 174 с.
102. Парошин А. А. Нормативно-правовые аспекты защиты информации: Учебное пособие /А. А. Парошин. – Владивосток: изд-во Дальневост. федер. ун-та, 2010. – 116 с.
103. Пасічний В. О. Страхування: Навч. посібник для студентів вищих навчальних закладів / В. О. Пасічний, В. В. Жван; Харк. нац. акад. міськ. госп-ва. – Х.: ХНАМГ, 2009. –218 с.

104. Питання забезпечення органами виконавчої влади доступу до публічної інформації: Указ Президента України від 05.05.2011 р. № 547/2011. // Офіційний вісник України. – 2011. – № 35. – С. 14. – Ст. 1433.
105. Податковий кодекс України від 02.12.2010 р. // Відомості Верховної Ради. – 2011. – № 13-17. – Ст. 112.
106. Положення про роботу із засобами обчислювальної техніки і телекомунікаційною мережею Міністерства економіки України: Наказ Міністерства економіки України від 08.06.2010 р. № 630. – [Електронний ресурс]. – Режим доступа: http://www.uapravo.net/akty/administraciya-osnovni/akt8teoz4b.htm.
107. Понарина Н. Н. Глобализация и информационное общество // Общество: политика, экономика, право. – 2012. – № 1. – С. 19–24.
108. Правила адвокатської етики. – [Електронний ресурс]. – Режим доступу: http://document.ua/pravila-advokatskoyi-etiki-doc15.htm.
109. Прескотт Джон Е. Конкурентная разведка: Уроки из окопов. / Джон Е. Прескотт, Стивен Х. Миллер. – М.: Альпина Паблишер, 2003. – 336 с.
110. Про авторське право та суміжні права: Закон України від 23.12.1994 р. // Відомості Верховної Ради. – 1994. – № 13.– Ст. 64.
111. Про адвокатуру та адвокатську діяльність: Закон України від 05.07.2012 р. // Відомості Верховної Ради. –2012. – № 27. – Ст. 282.
112. Про аудиторську діяльність: Закон України від 22.04.1993 р. // Відомості Верховної Ради. – 1993. – № 23. – Ст. 243.
113. Про банки і банківську діяльність: Закон України від 07.12 2000 р. // Відомості Верховної Ради. – 2001.– № 5-6.– Ст. 30.
114. Про бібліотеки і бібліотечну справу: Закон України від 21.05.2009 р. // Офіційний вісник України. – 2009. – № 45. – С. 10. – Ст. 1497.
115. Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16.07.1999 р. // Відомості Верховної Ради. – 1999. – № 40. – Ст. 365.

116. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації»: Закон України від 27.03.2014 р. // Відомості Верховної Ради. – 2014. – № 22. – С. 1950. – Ст. 816.
117. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних: Закон України від 02.06.2011 р. № 3454-VI // Відомості Верховної Ради. – 2011. – № 50. – Ст. 549.
118. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 р. // Офіційний вісник України. – 2011. – № 10. – Ст. 445.
119. Про державний захист працівників суду і правоохоронних органів: Закон України від 23.12.1993 р. № 3781-XII // Відомості Верховної Ради України. – 1994. – № 11. – Ст. 50.
120. Про державні таємниці: проект Закону України. – [Електронний ресурс]. – Режим доступу: http://ssu.gov.ua/sbu/ control/uk/publish/ article;jsessionid=3581DAD591FB53EE22E9011877B4ADC2?art_id= 72055&cat_id=8054/.
121. Про державну службу: Закон України від 16.12.1993 г.// Відомості Верховної Ради України. – 1993. – № 52. – Ст. 490.
122. Про державну таємницю: Закон України від 21.01.1994 р. // Відомості Верховної Ради. – 1994. – № 16.–Ст. 93.
123. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514 // Офіційний вісник України. – 2009. – № 52. – Ст. 1783.
124. Про Доктрину інформаційної безпеки України: проект указу Президента України [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat _id=61025. – 12.06.2014.
125. Про донорство крові та її компонентів: Закон України від 23.06.1995 р. // Відомості Верховної Ради. – 1995. – № 23. – Ст. 183.
126. Про доступ до публічної інформації: Закон України від 13.01.2011 р. // Офіційний вісник України. – 2011. – № 10. – С. 29. – Ст. 446.

127. Про доступ до судових рішень: Закон України від 22.12.2005 р. // Відомості Верховної Ради. – 2006 .– № 15.– Ст. 128.
128. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. // Відомості Верховної Ради. – 1993. – № 1. – Ст. 1.
129. Про електронний цифровий підпис: Закон України від 22.05.2003 р. // Офіційний вісник України. – 2003. – № 25. – С. 111. – Ст. 1175.
130. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. // Офіційний вісник України. – 2003. – № 25. – С. 106. – Ст. 1174.
131. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. // Відомості Верховної Ради. – 2013. – № 51. – Ст. 761.
132. Про забезпечення безпеки осіб, які беруть участь в кримінальному судочинстві: Закон України від 23.12.1993 р. // Відомості Верховної Ради України. – 1993. – № 11.– Ст. 51.
133. Про засади запобігання і протидії корупції: Закон України від 07.04.2011 р. // Відомості Верховної Ради. – 2011.– № 40.– Ст. 404.
134. Про затвердження зобов'язання громадянина України у зв'язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці: Наказ Служби безпеки України від 18.06.2001 р. № 190 // Офіційний вісник України. – 2001. – № 35. – С. 421. – Ст. 1655.
135. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію: затверджено постановою Кабінету Міністрів України від 27.11.1998 р. № 1893 // Офіційний вісник України. – 1998. – № 48. – С. 31.
136. Про затвердження Інструкції про порядок проведення контрольних заходів контрольно-ревізійним сектором Державної судової адміністрації України: Наказ Державної судової адміністрації України від 04.02.2005 р. № 11 // Офіційний Вісник України. – 2005. – № 28. – Ст. 1674.

137. Про затвердження положень з питань державної таємниці та внесення змін до деяких постанов Кабінету Міністрів України: Постанова Кабінету Міністрів України від 29.11.2001 р. № 1601 // Офіційний вісник України. – 2001. – № 49 / № 66. – 2010, ст. 2348/. – С. 56. – Ст. 2190.
138. Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова Національного банка від 14.07.2006 р. // Офіційний вісник України. – 2006. – № 32. – С. 137. – Ст. 2330.
139. Про затвердження форм документів для оформлення громадянам допуску до державної таємниці та порядку їх заповнення: Наказ Служби безпеки України від 04.02.2002 р. № 26 // Офіційний вісник України. – 2002. – № 9. – С. 163. – Ст. 424.
140. Про захист від недобросовісної конкуренції: Закон України від 07.06.1996 р // Відомості Верховної Ради. – 1996. – № 36. – Ст. 164.
141. Про захист економічної конкуренції: Закон України від 11.01.2001 р. // Відомості Верховної Ради. – 2001 .– № 12. – Ст. 64.
142. Про захист населення від інфекційних хвороб: Закон України від 06.04.2000 р. // Відомості Верховної Ради. – 2000. – № 29. – Ст. 228.
143. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI // Відомості Верховної Ради. – 2010. – № 34. – Ст. 481.
144. Про звернення громадян: Закон України від 02.10.1996 р. // Відомості Верховної Ради. – 1996. – № 47. – Ст. 256.
145. Про інвестиційну діяльність: Закон України від 18.09.1991 р. // Відомості Верховної Ради. – 1991.– № 47.– Ст. 646.
146. Про Клятву лікаря: Указ Президента України від 15.06.1992 р. № 349 // Збірник указів Президента України. – 1992. – № 2.
147. Про Концепцію Національної програми інформатизації: Закон України від 4.02.1998 р. // Відомості Верховної Ради. – 1998. – № 27–28. – Ст. 182.
148. Про Національний банк України: Закон України від 20.05.1999 р. // Відомості Верховної Ради.– 1999.– № 29.– Ст. 238.

149. Про Національну програму інформатизації: Закон України від 04.02.1998 р. // Відомості Верховної Ради України. – 1998. – № 27. – Ст. 181.
150. Про нотаріат: Закон України від 2.09.1993 р. // Відомості Верховної Ради. – 1993. – № 39. – Ст. 383.
151. Про оптимізацію системи центральних органів виконавчої влади: Указ Президента України від 09.12.2010 р. № 1085/2010 // Офіційний вісник України. – 2010. – № 94. – С. 15. – Ст. 3334.
152. Про організаційно-правові основи боротьби із організованою злочинністю: Закон України від 30.06.1993 р. // Відомості Верховної Ради. – 1993.– № 35. – Ст. 358.
153. Про основи національної безпеки України: Закон України від 19.06.2003 р. // Відомості Верховної Ради. – 2003. – № 39.– Ст. 351.
154. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9.01.2007 р. // Відомості Верховної Ради. – 2007. – № 12. – Ст.102.
155. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 09.08.1993 р. № 611. – [Електронний ресурс]. – Режим доступа: http://zakon4.rada.gov.ua/ aws/show/611-93-п.
156. Про першочергові заходи щодо забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України: Указ Президента України від 05.05.2011 р. № 548/2011. // Офіційний вісник України. – 2011. – № 35. – С. 15. – Ст. 1434.
157. Про Положення про Державну службу України з питань захисту персональних даних: Указ Президента України від 06.04.2011 р. № 390/2011 // Офіційний вісник України. – 2011. – № 28. – С. 36. – Ст. 1160.
158. Про поштовий зв'язок: Закон України від 4.10.2001 р. // Відомості Верховної Ради. – 2002. – № 6. – Ст. 39.
159. Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ: Закон України від 12.12.1991 р. // Відомості Верховної Ради. – 1992. – № 11. – Ст. 152.

160. Про психіатричну допомогу: Закон України від 09.06.2000 р. // Відомості Верховної Ради. – 2000. – № 19. – Ст. 143.
161. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. // Відомості Верховної Ради. – 2006. – № 5–6. – Ст. 71.
162. Про Рахункову палату: Закон України від 11.07.1996 р. // Відомості Верховної Ради. – 1996.– № 43. – Ст. 212.
163. Про свободу совісті та релігійні організації: Закон України від 23.04.1991 р. // Відомості Верховної Ради. – 1991. – № 25. – Ст. 283.
164. Про сертифіковані товарні склади та прості і подвійні складські свідоцтва: Закон України від 23.12.2004 р.// Відомості Верховної Ради. – 2005.– № 6. – Ст. 136.
165. Про Службу безпеки України: Закон України від 25.03.1992 р. // Відомості Верховної Ради. – 1994. – № 27. – Ст. 382.
166. Про страхування: Закон України від 07.03.1996 р.// Відомості Верховної Ради. – 1996.– № 18. – Ст. 78.
167. Про судоустрій і статус суддів: Закон України від 07.07.2010 р. // Відомості Верховної Ради. – 2010 .– № 41–45. – Ст. 529.
168. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. // Відомості Верховної Ради. – 1994. – № 10. – Ст. 43.
169. Про телекомунікації: Закон України від 18.11.2003 р. // Відомості Верховної Ради. – 2004.– № 12.– Ст. 155.
170. Про трансплантацію органів та інших анатомічних матеріалів людині: Закон України від 16.07.1999 р. // Відомості Верховної Ради. – 1999. – № 41. – Ст. 377.
171. Про Уповноваженого Верховної Ради України з прав людини: Закон України від 23.12.1997 р. // Відомості Верховної Ради. – 1998. – № 20. – Ст. 99.
172. Про утворення Міжгалузевої ради з питань розвитку електронного урядування: Постанова Кабінету Міністрів України від 14.01.2009 р. № 4. – Офіційний вісник України. – 2009. – № 3. – С. 52. – Ст. 77.
173. Про цінні папери та фондовий ринок: Закон України від 23.02.2006 р. // Відомості Верховної Ради. – 2006. – № 31. – Ст. 268.
174. Програма інтеграції України до Європейського Союзу: Указ Президента від 14.09.2000 р. № 1072/2000. – [Електронний ресурс]. –

Режим доступу: http://zakon4.rada.gov.ua/laws/ show/n0001100-00/ card6#Public.

175. Разъяснения Министерства юстиции Украины «Закон Украины «О доступе к публичной информации»: информационный прорыв в Украине». – [Електронний ресурс]. – Режим доступу: http://www.medlaw center.com.ua/ru/105/495.html
176. Резнікова Г. І. Професійна таємниця: поняття, ознаки та види / Г. І. Резнікова // Трибуна докторанта, аспіранта і здобувача. – 2013. – Вип. 26. – С. 280–292.
177. Рекомендация № R (2000)7 Комитета Министров Совета Европы. – [Електронний ресурс]. – Режим доступу: http://www.coe.kiev.ua/ docs/km/r(2000)7.htm.
178. Рекомендация № R (99) 5 Комитета Министров государствам-членам Совета Европы по защите неприкосновенности частной жизни в Интернете. – [Електронний ресурс]. – Режим доступу: http://zakon4.rada. gov.ua/laws/show/994_357.
179. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. – [Електронний ресурс]. – Режим доступу: http://www.vestnik-pravo.mgu.od.ua/ archive/ juspradenc6-3-1/23.pdf.
180. Рішення Конституційного суду України №5-рп/2003 від 05.03.2003 р.(справа про звернення народних депутатів України до Національного банку України // Урядовий кур'єр. – 2003. – № 51.
181. Рожнов А. А. Уголовно-правовая охрана профессиональной тайны : автореф.дис... канд. юрид. наук: 12.00.08 / А. А. Рожнов; Казан. гос. ун-т. – Казань, 2002. – С. 17.
182. Сабадаш В. Компьютерная преступность-фишинг, как самый распространенный вид мошенничества / В. Сабадаш. – [Електронний ресурс]. – Режим доступу: http://www.crime-research.ru/articles/ sabadash_0602/. – Назва з екрану.
183. Сёмкин С.Н, Сёмкин А. Н. Основы правового обеспечения защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2008. – 238 с.

184. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В. С. Сідак, В. Ю. Артемов. – К.: КНТ, 2007. – 160 с.
185. Сімейний кодекс України // Офіційний вісник України. – 2002. – № 7.– Ст. 273.
186. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности / В. Скиба, В. Курбатов. – СПб.: Питер, 2008. – 320 с.
187. Сляднєва В. – Право суб'єкта господарювання на комерційну таємницю та його захист: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.04 «Господарське право» / Г. О. Сляднєва. – Донецьк, 2005. – 19 с.
188. Смирнов А. А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза. Монография. – М.: ЮНИТИ-ДАНА, 2011. – 196 с.
189. Смолькова И. В. Проблемы охраняемой законом тайны в уголовном процессе. – М.: Изд-во «Луч», 1999. – С. 14–17.
190. Смолякова И. В. Тайна и уголовно-процессуальный закон / И. В. Смолякова. – М.: Луч, 1997. – 99 с.
191. Стефанів Н. Дотримання прав особи при наданні дозволу на втручання в приватне спілкування. Практика Європейського суду з прав людини / Н. Стефанів // Слово Національної школи суддів. – № 1 (2). – 2013. – С. 32–38.
192. Стратегія розвитку інформаційного суспільства в Україні: Розпорядження Кабінету міністрів України від 15.05.2013 р. № 386-р // Офіційний вісник України. – 2013. – № 44. – С. 79. – Ст. 1581.
193. Стрельбицька Л. Правові засади захисту банківської та комерційної таємниці // Юридична Україна. – 2005. – № 4. – С. 64-69.
194. Тітомер Є. В. Банківська таємниця як предмет кримінально-правової охорони // Актуальні проблеми держави і права: Збірник наукових праць. – 2008. – Вип. 44. – Одеса: «Юридична література». – С. 311–316.

195. Топалова Л. Господарсько-правові аспекти співвідношення комерційної та банківської таємниці у національному законодавстві // Підприємництво, господарство і право. – 2003. – № 4. – С. 16-20.
196. Угода між Кабінетом Міністрів України та Урядом Королівства Норвегія про захист інформації з обмеженим доступом: Угода ратифіковано Законом України від 30.10.2008 р. № 636-VI // Офіційний вісник України. – 2009. – № 27. – С. 163. – Ст. 916.
197. Угода між Кабінетом Міністрів України та Урядом Литовської Республіки про взаємну охорону інформації з обмеженим доступом: Угода ратифіковано Законом України від 04.06.2004 р. № 1761-IV // Офіційний вісник України. – 2004. – № 33. – С. 192. – Ст. 2239.
198. Уголовный процессуальный кодекс Украины: Научно-практический комментарий / Отв. ред. С. В. Кивалов, С. Н. Мищенко, В. Ю. Захарченко. – Х.: Одиссей, 2013. – 1184 с.
199. Харламова С. О. Проблеми визначення предмета злочинів, пов'язаних з незаконним збиранням, використанням та розголошенням відомостей, що становлять комерційну та банківську таємницю // Юридична Україна. – 2006. – № 10. – С. 86-87.
200. Хартия Европейского Союза об основных правах (2007/C303/01) // Европейский Союз: Основополагающие акты в редакции Лиссабонского договора с комментариями / отв. ред. С. Ю. Кашкин. – М.: ИНФРА-М, 2010. – С. 554-570.
201. Цивільний кодекс України // Відомості Верховної Ради України. – 2003. – № 40-44. – Ст. 356.
202. Чубукова С. Г., Элькин В. Д. Основы правовой информатики (юридические и математические вопросы информатики): Учебное пособие. Изд. 2-е, испр., доп. / Под ред. доктора юридических наук, проф. М. М. Рассолова, проф. В. Д. Элькина. – М.: Юридическая фирма «КОНТРАКТ», 2007. – 287 с.
203. Чугунов А. В. Развитие информационного общества: теории, концепции и программы: Учебное пособие. – СПб.: Ф-т филологии и искусств СПбГУ, 2007. – С. 98 с.
204. Шеннон К. Работы по теории информации и кибернетике: Математическая теория связи. – М., 1963. – 832 с.

205. Юридична енциклопедія. – К.: Українська енциклопедія, 1998. – Т 1. – С. 190.
206. Юридична енциклопедія: в 6 т. / Редкол.: Ю70 Ю. С. Шемшученко (голова редкол.) та ін. – К.: «Укр. енцикл.», 1998. – [Електронний ресурс]. – Режим доступу: http://cyclop.com.ua/content/view/ 1277/58/1/14/#26849.
207. Юсупова Д. Комерційна таємниця як об'єкт трудових відносин: поняття та ознаки / Д. Юсупова // Публічне право. – № 2(10). – 2013. – С. 336-343.
208. Янина Е. В. Актуальные вопросы информационной безопасности: защита коммерческой тайны хозяйствующего субъекта в рамках локального нормативного акта / Е. В. Янина // Актуальные проблемы современной науки. – 2003. – № 2. – С. 109-111.
209. Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions «Network and Information Security: Proposal for A European Policy Approach». Brussels, 6.6.2001. COM (2001)298 final. – [Електронний ресурс]. – Режим доступу: http://www.etsi.org/ WebSite/document/aboutETSI/EC_Communications/ COM_298.pdf.
210. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. A strategy for a Secure Information Society – «Dialogue, partnership and empowerment». Brussels, 31.5.2006. COM(2006) 251 final. – [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/ information_society/doc/com2006251.pdf
211. Council resolution 2002/C 43/02 of 28 January 2002 on a common approach and specific actions in the area of network and information security. – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX:32002G0216(02).
212. Council resolution 2003/C 48/01 of 18 February 2003 on a European approach towards a culture of network and information security. – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003G0228(01).

213. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications. – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.
214. Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) OJ L 096, 12.04.2003. P/ 0016-0025. – [Електронний ресурс]. – Режим доступу: https://www.esma.europa.eu/ystem/files/Dir_03_6.pdf.
215. Report of the Human Rights Committee. – [Електронний ресурс]. – Режим доступу: http://www.un.org/documents/ga/docs/55/ a5540vol2.pdf.

ЛОГІНОВА Наталія Іванівна

ДРОБОЖУР Ростислав Романович

ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЇ

Навчальний посібник