Державний вищий навчальний заклад
«Запорізький національний університет»
Міністерства освіти і науки України

О. В. Синєокий

ВИСОКОТЕХНОЛОГІЧНЕ ІНФОРМАЦІЙНЕ ПРАВО УКРАЇНИ

Навчальний посібник

Харків
«Право»
2010

УДК 35.078.3:343.451:044(477)(075.8)
ББК 67.9 (4 УКР)
С 38

Рекомендовано до друку вченою радою
Запорізького національного університету
(протоколи засідань № 10 від 26.06.2008 р. та № 5 від 25.12.2009 р.)

Рецензенти:

Т. О. Коломоєць, завідувачка кафедри адміністративного та господарського права Запорізького національного університету, доктор юридичних наук, професор, заслужений юрист України;

В. В. Погосов, завідувач кафедри мікро- та наноелектроніки Запорізького національного технічного університету, доктор фізико-математичних наук, професор;

В. О. Голубєв, професор кафедри спеціальної техніки, інформатики та інформаційних технологій Донецького юридичного інституту Луганського державного університету внутрішніх справ, кандидат юридичних наук, доцент;

Г. В. Мазулін, начальник відділу спеціальних видів досліджень Науково-дослідного експертно-криміналістичного центру при ГУ МВС України в Запорізькій області, полковник міліції, кандидат фармацевтичних наук

Синєокий О. В.

С 38 Високотехнологічне інформаційне право України : навч. посібник для студ. юрид. та неюрид. спец. / О. В. Синєокий ; Запоріз. нац. ун-т, юрид. ф-т. — Х. : Право, 2010. — 360 с.

ISBN 978-966-458-194-0

У виданні охарактеризовано організаційно-правові основи політики концептуального розвитку нанотехнологій та модернізації систем передавання інформації у сфері боротьби зі злочинністю. Розкрито основи правового регулювання волоконно-оптичних технологій, що використовуються в інформаційно-телекомунікаційних системах.

Уперше у вітчизняній літературі окрему увагу приділено системному дослідженню організаційно-правових особливостей інформаційних технологій, наноіндустрії та нових обчислювальних електронних систем інтелектуального обробления інформації у галузі протидії злочинності. Визначено інноваційні перспективи застосування високих технологій щодо стримування інформаційної злочинності.

Розраховано для поглибленого вивчення навчальних дисциплін «Інформаційне право», «Правове регулювання інформаційної безпеки» та інших відповідних спецкурсів, що вивчаються студентами юридичних та неюридичних спеціальностей вищих навчальних закладів. Запропонований матеріал не дублює раніше опубліковані праці, тому ця робота може стати корисною для науковців та практичних фахівців із захисту інформації.

УДК 35.078.3:343.451:044(477)(075.8)
ББК 67.9 (4 УКР)

ISBN 978-966-458-194-0

Перелік умовних скорочень

- АРМ — автоматизоване робоче місце
- ВОГЗ — волоконно-оптична головка зчитування
- ВОЛЗ — волоконно-оптичні лінії зв'язку
- ВРУ — Верховна Рада України
- ГАІС — галузева автоматизована інформаційна система
- Гц — герц, одиниця виміру частоти періодичних процесів
- ГПУ — Генеральний прокурор України (Генеральна прокуратура України)
- ГУ — Головне управління
- Дб — децибел, логарифмічна одиниця рівнів, загасань та посилень
- ДІТ — Департамент інформаційних технологій
- ДНК — дезоксирібонуклеінова кислота, що забезпечує зберігання, передавання від покоління до покоління та реалізацію генетичної програми розвитку і функціонування живих організмів
- ДСТСЗІ — Департамент спеціальних телекомунікаційних систем та захисту інформації
- ЄІТС — єдина інформаційно-телекомунікаційна система
- ЕОМ — електронно-обчислювальні машини
- ЕС — експертна система
- ЗМІ — засоби масової інформації
- ІКТ — інформаційно-комунікаційні технології
- ін. — інший (інші)
- ІПС — інформаційна підсистема
- КК — Кримінальний кодекс
- ККД — коефіцієнт корисної дії
- км — кілометр
- КМУ — Кабінет Міністрів України
- КПК — Кримінально-процесуальний кодекс
- м — метр
- м. — місто
- Мбіт — мегабайт (мегабит), одиниця виміру кількості інформації 10^6
- МВС — Міністерство внутрішніх справ
- МЗСОГ — міждержавні змішані слідчо-оперативні групи
- МЕОМ — мала електронна обчислювальна машина
- мкм — мікрометр, одна тисячна частина міліметру

▪ млрд — мільярд

▪ МФТІ (ДУ) — Московський фізико-технічний інститут (Державний університет)

▪ НАН — Національна академія наук (України)

▪ НАСА (NASA — англ. *National Aeronautics and Space Administration*) — Національне агентство США з аеронавтики та дослідження космічного простору

▪ НВК — науково-виробнича компанія

▪ НВЧ — надвисока частина

▪ НДЕКЦ — Науково-дослідний експертно-криміналістичний центр

▪ нм — нанометр

▪ нс — наносекунда

▪ ОВС — органи внутрішніх справ

▪ ОЕКК — оптико-електронний кабінет криміналістики

▪ ОК — оптичний комутатор

▪ п. — пункт

▪ ПК — персональний комп'ютер

▪ РАН — Російська академія наук

▪ р. (рр.) — рік, роки

▪ РФ — Російська Федерація

▪ с. — секунда

▪ СБУ — Служба безпеки України

▪ ст. — стаття, століття

▪ СНД — Співдружність Незалежних Держав

▪ СОГ — слідчо-оперативна група (слідчо-оперативні групи)

▪ СППР — система підтримки прийняття рішень

▪ СУБД — система управління базами даних

▪ США — Сполучені Штати Америки

▪ Тбіт — терабайт 10^{12}, одиниця виміру інформації

▪ УРСР — Українська Радянська Соціалістична республіка

▪ ч. — частина

▪ CD-ROM (англ. *Compact Disc Read Only Memory* — компакт-диск тільки з можливістю читання) — оптичний носій інформації у вигляді диска з отвором у центрі, інформація з якого зчитується за допомогою лазера

▪ DVD (англ. *Digital Versatile Disc* — цифровий багатоцільовий диск) — носій інформації, який виконаний у вигляді диску, ззовні схожий з компакт-диском, однак має можливість зберігати більший обсяг інформації за ра-

хунок використання лазера з меншою довжиною хвилі, ніж для звичайних компакт-дисків

▪ HTTP (англ. *HyperText Transfer Protocol* — «протокол передачі гіпертексту») – протокол прикладного рівня передачі даних, який використовується в Інтернеті для отримання інформації з веб-сайтів, основним об'єктом маніпуляції чого є послідовність символів у запиті клієнта, що ідентифікує абстрактний або фізичний ресурс.

▪ UA — міжнародна абревіатура (походить від англ. *Ukraine*, що означає ISO-код України)

Концептуалізація політики розвитку високих технологій передавання інформації у сфері боротьби зі злочинністю

Ми тонемо в інформації та задихаємося від браку знань.
(Джон Нейзбітт)

Нанотехнологія — це дійсно портал до нового світу.
(Ріта Колвел)

Вступ

XXI століття. Планета Земля перебуває на порозі грандіозних подій. Інформаційна революція детермінована передусім якісно новим проривом у високотехнологічних галузях економіки та соціальної сфери.

Економічна, політична, інформаційна незалежність відповідає інтересам будь-якої держави, оскільки вона забезпечує свободу і розвиток особистості, суспільства і держави, забезпечує їх життєздатність.

Інтенсивний розвиток новітніх технологій у сфері комунікацій, глобальні інтеграційні процеси, становлення інформаційного суспільства викликають пильну увагу до можливостей впливу на індивідуальну і масову свідомість, актуалізують проблему правового регулювання суспільних відносин у галузі інформаційної політики.

Система інформаційного права як науки перебуває у стадії формування та розвитку. Практика правозастосування, законодавчі ініціативи значно відстають за часом від правової реальності, тому актуальними розробками сьогодні є дослідження у галузі «правова діяльність — інфотехнології». Особливо це стосується «високих», «нових» або «критичних» технологій.

Утім до цього часу ще не знайдено цілісну формулу високотехнологічного інформаційного права.

Високотехнологічні правовідносини є соціальними відносинами найвищого (критичного) рівня, які виникають у сфері технологій нового покоління, а звідси мають особливий правовий зміст, оскільки регулюють правила поведінки у сфері розроблення та застосування високих технологій.

Разом із тим, потрібно визнати, що юридична наука та практика на крок відстають від технологічного розвитку. Утім чи готові правознавці ґрунтов-

но спрогнозувати наслідки стрімкого інформаційно-технологічного прориву й створити наперед правовий фундамент?

На перетинанні законів юридичних із законами фізичними виникає ще маловідома соціотехнологічна субстанція. Безумовно зрозуміло, що будь-якими нормативно-правовими актами неможливо змінити рух елементарних часток.

Утім, з одного боку, на соціально-економічні процеси за допомогою законів потрібно впливати та змінювати їх відповідно до вимог часу. В умовах високотехнологічного суспільства настає час щодо виокремлення так званих «гарячих» норм (тобто щоденного, постійного, поточного застосування), поряд з якими існуватимуть вибіркові, альтернативні та «кріогенні» норми. Останнім терміном зазвичай визначають технології та засоби діяльності в умовах низьких температур. Для запуску в дію таких правових норм на державному рівні мають бути розроблені та створені спеціальні пускові механізми. У першу чергу це стосується особливих правових режимів у інноваційних центрах, про що далі ще піде мова. До того ж не винятком постають і фізико-хімічні, медико-біологічні та інформаційно-технологічні процеси.

З іншого боку потрібно формувати дієву правову основу щодо фахового впровадження нових технологічних рішень в окремі види інформаційної діяльності.

І третє. Що спільного може бути між цифровими правами людини, інформаційною злочинністю та нанотехнологіями? Для відповіді на ці, а також інші нестандартні запитання ми спробували дещо відійти від шаблонних підходів та ув'язати, на перший погляд, несумісні процеси, передусім відштовхуючись від основної тези, що без системних механізмів, які б на сучасному етапі соціотехнологічного розвитку суспільства забезпечували правове регулювання інноваційних процесів, існує загроза поштовху необоротної ланцюгової реакції, негативні наслідки чого можуть призвести до непередбачуваних подій, зокрема від техногенних катастроф до розповсюдження нових злочинних технологій, і врешті-решт, до інформаційного хаосу та колапсу. Звідси випливає, що технологічні досягнення мають широко використовуватись в юридичній практиці, запроваджуючи розвиток цифрової юриспруденції.

Узагальнення основних різноаспектних факторів з цього приводу надає підстави щодо важливого застереження – подібний юридичний експеримент має відбуватися в рамках інформаційного права як нової галузі права, що найбільш активно розвивається, і відривається від «формально-наукових» стереотипів.

Результатом за авторською гіпотезою стало знайдення спільного стрижня – фактично закладено початок формування юридичної моделі майбутнього, структурні компоненти якої складатимуться з нової логіки взаємовпливу права й високих технологій. У зв'язку з цим сьогодні потрібно розробити нестандартні юридичні рішення на нові виклики, що виникають та виникатимуть далі у зв'язку з розвитком нових технологій опрацювання інформації.

Розробити на десятиріччя наперед юридичні механізми та створити для цього соціально-економічні й технологічні умови, покликана політика інноваційної безпеки, в структурі якої важливе місце відведено політиці розвитку високих технологій передавання інформації у сфері боротьби зі злочинністю.

У зв'язку з цим у рамках висловленого припущення докладно розглянуто гіпотезу, згідно з якою високотехнологічне інформаційне право є окремою підгалуззю (науковою теорією), що формується у рамках науки інформаційного права.

Досягнення науки інформаційного права має стати важливим чинником, здатним вплинути на вдосконалення політики у сфері боротьби зі злочинністю, на основі прискорення науково-технологічної модернізації інформаційно-телекомунікаційної системи органів, які ведуть боротьбу зі злочинністю в сучасних умовах. Актуальність використання нових інформаційних технологій у сфері правоохоронної діяльності визначається не лише потребою наукового узагальнення цієї проблематики, але й невизначеностями в напрямках реформування системи органів, які ведуть боротьбу зі злочинністю.

Україна має власну історію розвитку базових засад інформаційного простору, створення інформаційно-телекомунікаційних технологій і загальнодержавних інформаційно-аналітичних систем різного рівня та призначення, в якій мають місце яскраві сторінки, коли після Великої Вітчизняної війни зруйнована Україна у складі Радянського Союзу в рекордний строк створила ядерні, космічні, комп'ютерні технології і зберегла в них лідерство, навіть незважаючи на катаклізми останніх десятиліть. Тому потрібно вкрай об'єктивно оцінювати радянське минуле України, особливо другої половини XX ст. У період 1950–1980 років УРСР, а особливо її південно-східний регіон, досягла значного науково-технічного розвитку, на декілька порядків випереджаючи інші республіки у складі Радянського Союзу.

Широко в світі відома українська школа кібернетики. На початку 90-х років минулого століття в УРСР було сформовано концепції та програми

інформатизації. Вже у 1980–1990 роках учені (перш за все фізики-ядерники) для вирішення складних математичних завдань намагалися комбінувати декілька різних робочих станцій, використовуючи вільні обчислювальні ресурси для скорочення часу оброблення. Разом із цим потрібно відзначити, що розпад СРСР обумовив глибоку системну технологічну, наукову, освітню, а звідси й інтелектуальну кризу, наслідки чого ми, на жаль, відчуваємо й дотепер, у тому числі у сфері розвитку і впровадження сучасних технологій.

Тенденції повільного відродження науково-технічного потенціалу України з'явилися на початку XXI ст. Утім соціально-політичні події кінця 2004 — початку 2005 рр. загальмували повернення України до клубу світових лідерів в інформаційно-технологічній сфері. Проте інтелектуальний потенціал України невичерпний і сьогодні щонайменше тисячі молодих учених і фахівців готові довести, що вони варті своїх дідів, які за два тижні створювали якісно нові танки, винаходили унікальні технології електрозварювання, розраховували ланцюгову реакцію. Тим більше, що розвиток нанотехнологій, протягом 5–10 років дає змогу одержати нові матеріали, які у сотні разів міцніші й у десятки разів важать менше, ніж найкращі сорти сталі.

Україна — батьківщина першого в континентальній Європі комп'ютера МЕОМ в змозі створити комп'ютери потужніші і компактніші, ніж існуючі. Чекають ноу-хау науковців проблеми авіакосмічної галузі, екології, енергетики, національної безпеки, боротьби з міжнародним тероризмом, освіти, медицини.

У цьому зв'язку як перспективний вектор політики подальшого розвитку інформатизації правоохоронних органів можна визначити новий напрям науково-практичних досліджень — формування вітчизняної наукової школи високопродуктивних систем передавання інформації у сфері боротьби зі злочинністю, потенціал чого розкривається в рамках синергетичної парадигми та інноваційних можливостей. Хоча, як зазначається в літературі, системно-інформаційний підхід не заперечує системного підходу як універсального напряму методології спеціально-наукового пізнання і соціальної практики, а значно розширює можливості використання змістовно гнучких принципів системного підходу, які не підлягають будь-якій жорсткій концептуалізації [124, с. 22–25].

Сьогодні одним із показників рівня розвитку країни є рівень інформатизації, що ґрунтується на системах зв'язку і передання інформації.

Розроблення скляних волоконних світловодів з низьким рівнем затухання світла слушно вважається одним із найбільш яскравих досягнень науки і

техніки XX ст. Завдяки використанню волоконних світловодів замість атмосфери було створено оптичні системи зв'язку з надвисокою швидкістю передавання інформації. З другого боку, дисперсія і нелінійність скла, з якого виготовлено волоконні світловоди, складають фізичну основу механізму передавання інформації на значні відстані. Для того щоб перебороти ці труднощі, потрібно провести фундаментальні дослідження з метою розроблення правової регламентації волоконно-оптичних інформаційних систем.

Волоконна оптика в цей час одержала широкий розвиток і застосовується в різних галузях науки і виробництва (зв'язок, радіоелектроніка, енергетика, термоядерний синтез, медицина, космос, машинобудування, літаючі об'єкти, обчислювальні комплекси). Вже зараз волоконно-оптичні технології суттєво впливають на розвиток людського суспільства, визначають ефективність таких важливих державних сфер, як діяльність органів, що ведуть боротьбу зі злочинністю. Інакше кажучи, високі технології передавання інформації стають однією з науково-технологічних галузей, які справляють найбільший вплив на розвиток людського суспільства.

Нанонаука та нанотехнології є двома новітніми галузями науки, що на сучасному етапі інформаційного розвитку суспільства застосовуються в різних соціальних сферах. Існує безліч думок відносно того, куди рухаються нанотехнології [140], утім експерти єдині в одному: не має значення, хто ви, чим займаєтесь, але дана наука та її технології швидко втрутяться до вашого життя, тому що фактично ми знаходимося на порозі інноваційного етапу постіндустріальної революції.

Наноскопічні наука і техніка скоріше за все стануть причиною наступного стратегічного технологічного прориву. Тому тільки синхронний розвиток техніки та науки постає неодмінною умовою руху людської цивілізації за обраним шляхом високих технологій в інформаційній сфері. І хоча цей шлях іноді піддається критиці, на сьогодні альтернатив йому не існує.

На цей час українська наноіндустрія відчуває гостру нестачу висококласних фахівців як для розвитку нанонауки, так і для просування її результатів на ринок. А без розв'язання проблеми організаційно-правової регуляції нових технологій держава може виявитися серед аутсайдерів світового ринку, в тому числі у наногалузі.

Зараз збереглися необхідна науково-дослідницька і виробнича інфраструктура та відповідний кадровий потенціал науковців, що вже мають досвід у проведенні міждисциплінарних досліджень, який може поповнюватися талановитою молоддю з числа випускників вищих навчальних закладів.

На цей час нанотехнологія вже є міждисциплінарною наукою. Можливо, що об'єднання зусиль учених та інженерів недостатньо, а тому до них доведеться підключити юристів та політиків. Звідси майже беззаперечно випливає, що для плідного обговорення проблем правового регулювання нанотехнологічних інновацій юристи повинні знати, що це таке.

При цьому багато системних питань доведеться вирішувати не тільки висококваліфікованим спеціалістам з вищою технічною або економічною освітою, а й фаховим юристам. Тому Вашій увазі представлено перше дослідження, де без порушення загального контексту праці докладно висвітлено організаційно-правові аспекти розвитку нанотехнологій.

Нанотехнологія — це революційна технологія, яка й визначить профіль XXI ст. Звідси для успішного подолання відставання України у сфері розвитку нанотехнологій необхідно модернізувати цикл фундаментальних і прикладних досліджень та підготувати підприємства до виготовлення наноматеріалів.

Саме тому потрібно з використанням теоретичного потенціалу нанонауки розвивати антикримінальний сектор нанотехнологій, у тому числі у сфері розвитку заходів протидії інтелектуальній злочинності, та забезпечити ефективний рівень міждержавного співробітництва у цій галузі.

Звідси наукове розроблення національної програми розвитку високих технологій постає пріоритетною державною програмою розвитку, оскільки являє собою інтелектуальний прорив у сфері боротьби зі злочинністю.

Пропоноване видання ґрунтується на використанні енциклопедичного підходу до викладення матеріалу та за архітектонікою складається з двох частин. Так, у першій частині, матеріал якої подається за унікальною структурною побудовою, змістовно викладено проблеми концептуалізації політики розвитку оптоволоконних систем передавання інформації та нанотехнологій у сфері боротьби зі злочинністю. Зокрема, розкрито організаційно-правові аспекти впровадження волоконно-оптичних ліній зв'язку в інформаційно-телекомунікаційні системи органів прокуратури та внутрішніх справ України, стратегії розвитку високотехнологічної інформатизації правоохоронних органів тощо. Особливу увагу присвячено національним програмам розвитку нанотехнологій, проблемам модернізації та освоєння нових технологічних коридорів передавання інформації у сфері боротьби зі злочинністю.

Після кожного розділу визначаються основні підсумки та пропонуються контрольні запитання. Крім цього, з метою покращення сприйняття найважливіші питання подано схематично (22 схеми), а головні підсумкові

співвідношення умовно визначено виведеними за допомогою законів логіки формулами (20 формул).

Друга частина за функціональним призначенням є довідково-контрольною, де в систематизованому вигляді розміщено тести з спецкурсу, питання для самоперевірки, індивідуальні завдання та термінологічний словник. Слід зауважити, що цей вокабулярій неможна назвати вичерпним, оскільки дефініції, які містяться в ньому, завдяки систематизації різних науково-енциклопедичних джерел є збірними, з елементами авторського тлумачення та подаються до тих значень слів, у яких застосовані у цьому виданні.

При підготовці роботи використано практичний та науково-педагогічний досвід автора, а також частково окремі положення, викладені у навчальних виданнях та наукових публікаціях щодо розглядуваної тематики і суміжних проблем [183–210]. Під час висвітлення другорядних питань, які виникали у контексті предмета основного дослідження, ми намагалися бути лаконічними та ґрунтовно зазначити посилання на основні та додаткові літературні джерела, якщо у читачів виникне бажання глибше ознайомиться з певними фаховими питаннями, що їх зацікавили. Тому структуру посібника завершує список використаної та рекомендованої літератури, який складається з 256 різноманітних джерел.

Розділ 1

Інформаційна політика. Право. Високі технології

У цьому розділі ...

• ***Державна політика розвитку високих технологій передавання інформації.***

Поняття та види інформації ◄► Інформатизація ◄► Інформаційне суспільство ◄► Інформаційна діяльність ◄► Сутність інформаційної політики ◄► Національна програма інформатизації ◄► Політика інформатизації правоохоронних органів ◄► Мета національної інформаційної політики.

• ***Високотехнологічне інформаційне право в системі права України: об'єкти, суб'єкти, методологія.***

Теорія правової інформатики ◄► Право та правовідносини ◄► Інформаційне право ◄► Поняття та види високих технологій ◄► Право високих технологій ◄► Методи та методологія. Синергетика права ◄► Основні принципи, об'єкти і суб'єкти ◄► Проект Інформаційного кодексу України.

• ***Кримінально-правова політика у сфері високих інформаційних технологій.***

Поняття кримінально-правової політики ◄► Інформаційні правопорушення і злочини у сфері високих технологій ◄► Злочинність у сфері високих технологій ◄► Кримінальне право і право високих технологій ◄► Комп'ютерні злочини ◄► Правові проблеми інсайдерської інформації.

1.1. Державна політика розвитку високих технологій передавання інформації

o ***Поняття та види інформації***

Інформація є одним із найбільш загальних понять науки, що означає діякі відомості, сукупність певних даних та/або знань. У праві під інформацією пропонується вважати документовані або публічно оголошені відомості про події та явища, що відбуваються в суспіль-

стві, державі та навколишньому природному середовищі. Під терміном «законодавство» прийнято розуміти сукупність законів та інших нормативно-правових актів, що забезпечують правове регулювання суспільних відносин на всій території держави.

Найбільш повну характеристику поняття «інформація» подано у визначеннях, закріплених у багатьох законодавчих та підзаконних нормативно-правових актах [66; 67; 70; 128; 164; 169; 225; 226; 227]. Так, під інформацією у ст. 1 Закону України «Про інформацію» розуміються документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі [67].

Закон України «Про захист економічної конкуренції» визначає інформацію як відомості в будь-якій формі і вигляді, збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, рисунки, 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.

Інформація є об'єктом права власності громадян, організацій (юридичних осіб) і держави. Інформація може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження. Власник інформації щодо об'єктів своєї власності має право здійснювати будь-які законні дії. У статті 6 Закону України «Про науково-технічну інформацію» також визначено, що науково-технічна інформація є об'єктом права власності.

Узагалі дослідники виділяють такі основні властивості інформації: а) нематеріальність; б) інваріантність відносно носіїв — та сама інформація може бути записана різними знаковими системами, що можуть використовувати різні фізичні носії для запису; в) розмноження — інформація, на відміну від речовини та енергії має здатність до поширення; г) здатність бути реалізованою — має тенденції матеріалізації, тобто може бути використаною, стати товаром та послугою на ринку [152, с. 249–252].

Потоки різних видів соціально-економічної інформації, що використовуються в органах виконавчої влади, класифікуються за: періодичністю виникнення і передавання (п'ятирічна, річна, піврічна тощо); ступенем взаємозв'язку (характеризується кількістю всіх видів інформації, що надходить до органів виконавчої влади, взаємозалежних

з даним конкретним видом повідомлень, зведень); ступенем сталості (розглядається тривалий проміжок часу, протягом якого інформація зберігає своє значення); структурою (основна — уся офіційна, допоміжна — уся неофіційна і кількісна); методами утворення (формування інформації на основі аналізу діяльності суб'єктів і об'єктів управлінського впливу, в перебігу дослідження всіх масивів інформації, що надходить з даного питання, аналізу стану справ у різних сферах громадського життя); закріпленням та втіленням в матеріальні форми (візуальна, документальна, звукова) та за багатьма іншими ознаками [116].

Проблеми інформації досліджуються у різних наукових галузях, але на сьогодні не існує єдиного нормативного визначення поняття «інформація», яке б цілком відповідало вимогам часу.

У загальному вигляді соціальну інформацію визначають як сукупність знань, відомостей, даних та повідомлень, які формуються й відтворюються в суспільстві, а також використовуються індивідами, групами, організаціями, різними соціальними інститутами з метою регулювання соціальної взаємодії, суспільних відносин і процесів. Утім із позиції інформаційного підходу до соціальної інформації варто відносити інформаційні моделі в соціальних системах різного обсягу та складності.

Якість інформації – це ступінь її відповідності потребам споживачів. Властивості інформації є відносними показниками, оскільки залежать від інформаційної потреби. Визначають такі основні властивості, що характеризують якість інформації, як: об'єктивність, повнота, достовірність, адекватність, доступність, актуальність, емоційність.

Узагалі дослідниками виділяються такі основні властивості інформації: а) нематеріальність; б) інваріантність по відношенню до носіїв – та сама інформація може бути записана різними знаковими системами, ці знакові системи можуть використовувати різні фізичні носії для запису; в) розмноження – інформація, на відміну від речовини та енергії має здатність до розповсюдження; г) здатність бути реалізованою – має тенденції матеріалізації, тобто може бути використаною, стати товаром та послугою на ринку [152, с. 249–252].

Усього нараховується велика кількість різних видів інформації, більшості з яких притаманні визначальні особливості.

Інформацію можна розділи на види за декількома ознаками.

Інформація, за умовами (режимом) захисту (охорони) при збиранні, одержанні, зберіганні, використанні та поширенні інформації, поділяється на публічну інформацію та конфіденційну інформацію.

Особиста інформація – це інформація про особу (в тому числі дитину), її особисте життя. Особиста інформація фактично є приватною таємницею та належить до конфіденційної інформації.

Службова інформація – це інформація про фінансову діяльність, господарську діяльність (яка не пов'язана з секретами виробництва, введенням новацій та ноу-хау, розробкою стратегії розвитку, веденням переговорів, розробкою та впровадженням нових технологій) та внутрівідомчу службову діяльність установи, її посадових, службових осіб та кореспонденцію (доповідні записки, листування між підрозділами тощо), які пов'язані з процесом прийняття рішень та передують їх прийняттю.

Офіційна інформація – це інформація про офіційну діяльність установи, її посадових, службових осіб та офіційні документи. Офіційна інформація може бути віднесена до публічної інформації та конфіденційної інформації. Крім того, публічна інформація визначається як інформація, що вільно збирається, отримується, зберігається, використовується та поширюється.

З метою систематизації, пропонуємо загальний спектр усіх видів та рівнів інформації систематизувати у 14 спеціальних інформаційних груп:

Таблиця

№	Групи	Види інформації
1	2	3
1	*За призначенням*	Універсальна, вища, масова, народна, національна, федеральна, суспільна, соціальна, енциклопедична, довідкова, спеціальна, особиста, галузева, міжгалузева, наукова, науково-технічна, технологічна, теоретична, практична, методична, пошукова, конструкторська, дослідницька, історична, філософська, міжнародна, політична, парламентська, урядова, виборча, партійна, муніципальна, ліберальна, консервативна, демократична, ідеологічна, революційна, військова, цивільна, економічна, комерційна, розрахункова, господарська, торговельна, підприємницька, ринкова, лізингова, податкова, юридична, інвестиційна, медична, фармацевтична, лікарська, санітарно-гігієнічна, демографічна, музична, педагогічна, культурна, церковна, релігійна, ритуальна, поштова, геодезична, географічна, топографічна, корабельна, транспортна, археологічна, архітектурна, спортивна, екологічна, гуманітарна, інженерна, космічна, святкова, комічна, місцева, територіальна, кваліфікаційна, колоніальна, екзаменаційна, туристична, антикризова та ін.

Продовження табл.

1	2	3
2	*За режимом користування*	Загального розповсюдження, статусна, індивідуальна, особиста, взаємна, офіційна, публічна, державна, статистична, колективна, групова, корпоративна, фахова, ділова, службова, неслужбова, архівна, бібліографічна, документальна, банківська, фінансова, інвестиційна, страхова, фондова, трейдерська, журналістська, літературна, публіцистична, видавнича, поліграфічна, редакційна, рекламна, кінематографічна, музейна, патентна, інсайдерська, енергетична, елітна, презентаційна, аматорська, навчальна, курсова, тестова, залікова, виховна, молодіжна, статева та ін.
3	*За режимом доступу*	Загальнодоступна, професійна, особлива, авторська, анонімна, іменна, фамільна, конфіденційна, секретна, закрита, прихована, зовнішня, внутрішня, відкрита, режимна, заборонена, таємна, агентурна, конспіративна, законспірована, зашифрована, криптографічна, з обмеженим доступом про особу, приватна, партнерська та ін.
4	*За рівнем якості та достовірності*	Понятійна, термінологічна, кількісна, якісна, низькоякісна, неякісна, нова, застаріла, достовірна, недостовірна, сертифікована, корисна, фіктивна, дезінформація, компрометуюча, тенденційна, ґрунтовна, необґрунтована, перекручена, контрафактна, чорнова, механічна, уточнена та ін.
5	*За рівнем системності*	Генеральна, тактична, стратегічна, фактична, системна, концептуальна, інтеграційна, несистемна, безсистемна, вибіркова, випадкова, систематизована, унікальна, модернізаційна, координаційна, узагальнена, підсумкова, типізована, родова, категорійна, аналітична, статутна, реферативна, функціональна, ключова, організаційна, регламентна, основна, окрема, допоміжна, дорадча, визначальна, другорядна, різнорівнева, неповна, полемістична, асиметрична, альтернативна, недосконала, латентна, реформована, факультативна, кореспондуюча, контрольна, вирішальна, дзеркальна, діагностична, адаптована, додаткова, бонус-інформація, експромт-інформація та ін.
6	*За рівнем технологічності*	Комп'ютерна, програмна, електронна, цифрова, аналогова, оптична, мультимедійна, томографічна, кібернетична, високотехнологічна, інноваційна, проектна, віртуальна, інтерактивна, Інтернет-інформація, постіндустріальна, голографічна, мобільна, аудіоінформація, відеоінформація, фотографічна та ін.

Закінчення табл.

1	2	3
7	*За структурою та обсягом*	Стандартна, єдина, фізична, матеріальна, атомна, молекулярна, хімічна, нульова, наноінформація, мікроінформація ... мегаінформація, гігаінформація, тераінформація, множинна, регіональна, локальна, фіксована, суперінформація, метаінформація, моноінформація та ін.
8	*За походженням та природою впливу*	Цивілізаційна, первинна, вихідна, відправна, інтелектуальна, психологічна, суб'єктивна, об'єктивна, конструктивна, креативна, категорична, свідома, несвідома, безсвідома, підсвідома, правдива, помилкова, сумлінна, сумнівна, перманентна, необхідна, критична, резонансна, рекомендована, контактна, адитивна, асоціативна, агресивна, позитивна, негативна, нейтральна, обов'язкова, консультативна, ситуаційна, пріоритетна, марна, безглузда, паразитична, порочна, зворотна, діалогічна, націоналістична, вікова, расова, PR-інформація та ін.
9	*За формою представлення*	Текстова, числова, графічна, звукова, візуальна, лінійна, циклічна, схематична, модульна, кольорова та ін.
10	*За засобами передачі*	Усна, письмова, вербальна, невербальна, сигнальна, телевізійна, телеграфна, телеметрична, квантова, математична, аеронавігаційна, генетична, багатоканальна та ін.
11	*За юридичним характером*	Правова, нормативна, законодавча, підзаконна, відомча, міжвідомча, процесуальна, дисциплінарна, правозахисна, захисна, правоохоронна, криміналістична, кримінологічна, віктомологічна, оперативно-розшукова, контртерористична, судова, прокурорська, наглядова, позовна, апеляційна, касаційна, слідча, експертна, нотаріальна, адвокатська, пенологічна, адміністративна, конституційна, митна, виконавча, контрольно-ревізійна та ін.
12	*За рівнем загрози*	Венчурна, ризикована, підозріла, проблемна, протиправна, кримінальна, злочинна, надзвичайна, загрозлива, небезпечна, трагічна, віктимна, віктимізаційна, терористична, запобіжна, корупційна, рейдерська та ін.
13	*За фінансовим рівнем*	Оплатна, безкоштовна, кредитна, авансова, бюджетна, валова, витратна, валютна, іпотечна, комісійна та ін.
14	*За терміном*	Прем'єрна, поточна, першочергова, щорічна, квартальна, щомісячна, тижнева, щоденна, чергова, проміжна, кінцева, експрес-інформація, дострокова, майбутня та ін.

Отже, завдяки подібному структуруванню ми нарахували існування понад 350 особливих видів інформації. Разом із тим, аналіз різноманітних джерел надає підстави про ствердження щодо існування трьох основних видів інформації: особистої, службової та офіційної. Ми з цим спрощенням не зовсім згодні, оскільки таке групування ґрунтується виключно на єдиній ознаці – режимі використання інформації. Тому безумовно, наш варіант ще не є остаточною конструкцією, оскільки при запропонованому підході потрібно зауважити, що певні із цих рівнів інформації можуть повністю або частково перекривати один одного чи доповнювати окремі кількісно-якісні показники.

Так, лікарська, фармацевтична та санітарно-гігієнічна є складовими медичної інформації (з однієї групи). Разом із тим, наприклад, агентурна інформація є складовою як таємної, так і оперативно-розшукової інформації (з різних груп). Або службова інформація являється службовою таємницею та належить до конфіденційної інформації. Врешті-решт сьогодні вже потрібно передбачити у майбутньому утворення більш складних інформаційних конструкцій, що можуть складатися з великої кількості ланок і, навіть, утворювати замкнутий колоподібний ланцюг.

Останнє можна розуміти як *інформаційний цикл* – будь-яку багаторазову інформаційну послідовність, що організована за допомогою умовних виходів, переходів, завершення та продовження інформаційних груп.

Таким чином, пропонується визначати інформацію як відомості, що передаються усним, письмовим, електронним, оптичним або іншим способом, зокрема за допомогою умовних символів, сигналів, алгоритмів, спеціальних технологій та технічних засобів.

о ***Інформатизація***

У порядку постановки проблеми та у зв'язку з її науковими та практичними завданнями слід зазначити, що ключовим чинником прояву інформаційного суспільства є інформатизація.

Інформація є явищем багатоаспектним і універсальним. Разом із тим щодо співвідношення таких понять, як «інформація», «інформатизація» та «інформаційне забезпечення», два останні у свою чергу постають похідними. При цьому «інформатизація» означає динамічний процес, а «інформаційне забезпечення» — вищий інформатизаційний рівень усіх соціальних процесів, що може бути представлено формулою (схема 1.1):

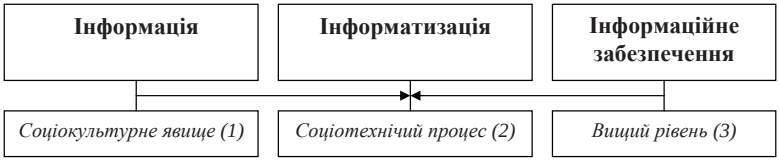


Схема 1.1

Створення та функціонування інформаційних систем тісно пов'язані з розвитком інформаційних технологій — основних складових компонентів інформаційної системи [79].

Всеосяжність інформатизації як соціотехнологічного процесу означає, що науковий зміст системної інформатизації постає як множина взаємопов'язаних організаційних, правових, науково-технічних та інших процесів, спрямованих на формування умов для задоволення потреб громадян і суспільства, реалізації їх прав, обов'язків через створення, застосування та розвиток комп'ютерних інформаційних систем, мереж, інформаційних ресурсів і технологій.

Таким чином, інтегруючою метою для сукупності процесів, що входять до змісту поняття «інформатизація суспільства», є створення умов для активного і плідного використання у діяльності фізичних і юридичних осіб, суспільства і держави накопичених та систематизованих за допомогою інформаційних і телекомунікаційних технологій наукових знань для досягнення високого рівня добробуту людей в усіх сферах життєдіяльності.

Отже, інформатизація одночасно є політикою і процесами, спрямованими на побудову та розвиток телекомунікаційної інфраструктури, яка об'єднує територіально розподілені інформаційні ресурси.

о ***Інформаційне суспільство***

Поняття «інформаційне суспільство» почало використовуватись у другій половині XX ст. Відзначають, що «інформаційне суспільство» виражає ідею нової фази в історичному розвитку передових країн, тобто не прихід «постіндустріального» суспільства, а створення нового соціального зразка, що є результатом «другої індустріальної революції», яка в основному ґрунтується на мікроелектронній технології.

Однією із основних ознак сучасної глобальної цивілізації і культури є формування інформаційного суспільства — суспільства, в

якому діяльність людей, їх соціальне формування забезпечуються через застосування здобутків інформатики, послуг з використанням комп'ютерних інформаційних технологій, у тому числі технологій електронної телекомунікації [67–69].

Метою інформатизації суспільства є такий суспільний устрій, за якого будь-яка предметна діяльність людей здійснюється за допомогою інформаційних технологій і сучасних технологій зв'язку.

У сучасному суспільстві, де основним технічним засобом технології перероблення інформації є комп'ютер, відбувся суттєвий вплив як на концепцію побудови і використання технологічних процесів, так і на якість результативної інформації.

Держава зобов'язана постійно дбати про своєчасне створення, належне функціонування і розвиток інформаційних систем, мереж, банків і баз даних у всіх напрямах інформаційної діяльності [41]. Держава гарантує свободу інформаційної діяльності в цих напрямах усім громадянам та юридичним особам у межах їх прав і свобод, функцій і повноважень.

На цей час в Україні сформовано певні правові засади побудови інформаційного суспільства: прийнято низку нормативно-правових актів, які регулюють суспільні відносини щодо створення інформаційних електронних ресурсів, захисту прав інтелектуальної власності на ці ресурси, впровадження електронного документообігу, захисту інформації.

Входження України до транснаціонального інформаційного суспільства є свідченням усвідомлення на державному рівні одного із шляхів інтеграції до міжнародних структур. Ці шляхи набули узагальненої умовної назви — дорога до глобальної кіберцивілізації. Сутність формування останньої полягає у приєднанні локальних (регіональних) суспільств, держав до сучасної світової комп'ютерної інформаційної культури.

З метою підвищення ефективності розвитку інформаційного суспільства необхідно створити цілісну систему законодавства, гармонізовану з нормами міжнародного права з питань розвитку інформаційного суспільства, зокрема здійснити кодифікацію інформаційного законодавства.

Останнім часом з'явилося поняття «постіндустріальне суспільство», основними ознаками якого виступають: 1) переорієнтація

економіки від товаровиробництва до сервісу і домінування наукоємких галузей промисловості; 2) принципово новий спосіб організації технологічної сфери, детермінований створенням інтелектуальних технологій; 3) радикальне зміщення акцентів у соціальній структурі суспільства; 4) модернізація і переструктурування інституційної сфери, зовнішньоформальною стороною якої виступає її комп'ютерізація, а внутрішньозмістовною — імперативна орієнтація на модернізаційні пріоритети інтелектуалізму і відповідне профілювання [168].

Таким чином, пріоритетним завданням постіндустріального суспільства є принципово новий спосіб організації технологічної сфери, детермінований створенням високоінтелектуальних технологій, тобто нового соціального зразка, що є результатом «другої індустріальної революції», яка в основному ґрунтується на суперкомп'ютерних, оптоволоконних, нано- і мікроелектронних технологіях. До інформаційних сфер належать засоби масової інформації, телекомунікації та зв'язку, глобальні комп'ютерні мережі, індустрія різних інформаційних послуг [25].

Отже, якщо врахувати викладені об'єктивні передумови переходу світової спільноти до інформаційного суспільства, то використання у повсякденній діяльності людей інформаційно-телекомунікаційних технологій є необхідним атрибутом життя прогресивного суспільства.

Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки затверджено 9 січня 2007 р. [169]. Зазначеним документом визначаються завдання, цілі та напрями розвитку інформаційного суспільства в Україні та національна політика розвитку інформаційного суспільства в Україні. Крім того, позначені організаційно-правові основи розвитку інформаційного суспільства в Україні включають: інституційне, організаційне та ресурсне забезпечення; відповідні об'єднання громадян; механізми інтеграції України у світовий інформаційний простір та механізми реалізації Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки.

Таким чином, визначимо головні складові поняття «інформаційне суспільство»: 1) модернізація інформаційної економіки на інноваційну модель; 2) індустрія інформаційних послуг; 3) сучасні інтелектуальні інформаційні технології та прогресивні технології волоконно-

оптичного зв'язку; 4) значний потенціал науки; 5) розвиток нанотехнології; 6) комп'ютерізація суспільно-політичних, економічних та інших процесів; 7) інформаційне та матеріально-технічне забезпечення різноманітних послуг.

о ***Інформаційна діяльність***

Узагалі діяльність визначається як специфічна людська форма ставлення до навколишнього світу, що за змістом становить його доцільну зміну в інтересах людей, умову існування суспільства (доцільність — це відповідність явища чи процесу певному становищу, матеріальна або ідеальна модель якого виступає метою діяльності).

Потрібно визначити, що будь-яка діяльність щодо збирання, зберігання, використання і поширення інформації, спрямована на задоволення інформаційних потреб різноманітних суб'єктів, визнається інформаційною.

Закон України «Про інформацію» регламентує правові основи інформаційної діяльності (статті 12–16). Він також визначає, що зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності є одним з головних напрямів державної інформаційної політики.

Окремі законодавчі і підзаконні нормативно-правові акти визначають специфічні види інформаційної діяльності. Зокрема, Закон України «Про науково-технічну інформацію» передбачає, що аналітично-синтетичне оброблення науково-технічної інформації — це процес оброблення інформації за методом аналізу і синтезу змісту документів з метою одержання необхідних відомостей, а також шляхом їх класифікації, оцінювання, зіставлення та узагальнення.

Основними напрямами інформаційної діяльності є: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Як пояснювальний принцип категорія «інформаційна діяльність» використовується при вивченні інформаційних процесів. Однак така «інформатизована» діяльність є тільки засобом досягнення (проміжним результатом) головної мети — продуктивного виробництва, оброблення і використання наукових знань (інформаційних ресурсів як раціональної форми їх зберігання) з метою подолання матеріально-енергетичної та екологічної кризи і забезпечення подальшого розвитку суспільства в усіх сферах життєдіяльності.

Отже, інформаційна діяльність є сукупністю дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

o ***Сутність інформаційної політики***

Як вище ми мали можливість усвідомити, інформаційна політика привертає увагу багатьох дослідників, оскільки є однією з найважливіших сфер державної діяльності. Вона виступає як невід'ємний вимір і відбиток соціального життя. В основі формування різних галузей законодавства і розвитку правової системи держави, правових форм і напрямів її діяльності лежить політика, що відображує принципи, стратегію, основні напрями і форми досягнення соціальних цілей, які ставлять перед собою суспільство, політичні і владні структури, що його представляють.

Держава здійснює зовнішню і внутрішню політику.

Термін «політика», як і більшість інших термінів соціального і політичного дискурсу, використовується для позначення певних понять. Буквально термін «політика» (від грец. politike) — державна діяльність; державні, суспільні справи, з якими пов'язані засади політичної культури. Тому дефініція «політика» так і не має однозначного тлумачення [158, с. 64–65], і це пов'язане з тим, що мета політики і способи її досягнення не залишалися незмінними, як, утім, не залишався незмінним і зміст самого поняття «політика». По-перше, політика розуміється як сфера соціального життя, пов'язана з діяльністю держави, управлінням суспільними справами і використанням публічної влади. У контексті нашого дослідження політика являє собою сукупність інформаційних видів діяльності у сфері боротьби зі злочинністю, інформаційно-телекомунікаційних відносин і технологічних подій, до яких в певній мірі може бути застосовано прикметник «політичний». По-друге, даний термін застосовується для позначення стратегії, політичного курсу, певної лінії діяльності. У цьому значенні він уживається в словосполученнях типу «інноваційна політика», «технологічна політика», «інформаційна політика», у тому числі стосовно ситуацій, не пов'язаних прямо з діяльністю державних та інших публічних інститутів і організацій. Нарешті, по-третє, термін «політика» використовується у тих випадках, коли мовець прагне підкреслити хитрість, обережність, обачність певного суб'єкта або

використання їм маніпуляції, обману та інших подібного роду прийомів і способів діяльності заради досягнення корисної мети. При вживанні в цьому значенні він звичайно втрачає об'єктивність і здобуває позитивні або (частіше) негативні асоціації. Якщо у своєму останньому значенні термін «політика» звичайно використовується тільки у повсякденній мові, то перші два поняття є ключовими категоріями політичної науки.

Напрям системних дій, основними складовими яких виступають регуляторні заходи, бюджетні пріоритети, закони та інші нормативно-правові акти стосовно певного питання чи комплексу питать, що здійснюється державною владою, становить структурний зміст поняття «*державна політика*».

Формуючись під впливом різних чинників, політика накладає своєрідний відбиток на інформаційне життя людей. Його необхідно враховувати в інформаційно-правовій діяльності, навіть якщо такий відбиток заслуговує на наше глибоке презирство і зневагу. Звертає на себе увагу той факт, що центральною категорією інформаційної політики виступає держава [55, с. 165].

Сьогодні навряд чи можна назвати державу, вилучену із загального інформаційно-комунікативного простору і незалежну від загальних інформаційних потоків. Життєдіяльність суспільного організму нині цілком визначається рівнем розвитку, якістю функціонування та безпекою інформаційного середовища [223, с. 68].

Державна інформаційна політика — це сукупність основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації. Інформаційна політика виникає у зв'язку з необхідністю реалізації таких інтересів груп, які визначають їх суспільне становище і не піддаються задоволенню без втручання третьої сили, котрою стала держава як специфічний суспільний інститут. Міжнародно-правові стандарти прав людини і громадянина на свободу слова і право на інформацію закріплені в законодавстві багатьох країн світу. Поряд з цим передбачаються випадки обмеження доступу до інформації, визначаються правові режими окремих видів інформації з обмеженим доступом. Не є винятком і вітчизняне законодавство.

Право України містить низку норм, які регулюють відносини щодо забезпечення прав власників певних категорій інформації на об-

меження доступу до неї. Інформаційна політика України характеризується демонополізацією інформаційного сектору, впровадження нових мультимедійних засобів зв'язку в усі сфери державного управління. Звідси тенденції розвитку законодавства України зумовлюють інтерес до сфери інформаційних відносин, зокрема до прав суб'єктів-учасників таких відносин.

Отже, державна інформаційна політика є складовою частиною внутрішньої та зовнішньої політики країни, що полягає у регулюванні інформаційних потоків та інформаційної діяльності структур усіх форм власності і підпорядкованості, а також організацій інформаційного профілю.

о ***Національна програма інформатизації***

Перехід України до інформаційного суспільства вимагає вдосконалення механізмів регулювання правовідносин, що виникають між громадянами, юридичними особами приватного права та державою.

З метою задоволення цих потреб органи державної влади та органи місцевого і регіонального самоврядування створюють інформаційні служби, системи, мережі, бази і банки даних [106]. Порядок їх створення, структура, права та обов'язки визначаються КМУ або іншими органами державної влади, а також органами місцевого і регіонального самоврядування. Водночас склалися такі передумови, які потребують прискореного розвитку інформаційного суспільства в Україні. Насамперед це пов'язано із соціально-економічною нерівністю, яка виникає між розвинутими країнами і країнами, що розвиваються, внаслідок суттєвої різниці в темпах зростання обсягів та номенклатури товарів і послуг, які виробляються та надаються за допомогою ІКТ.

Разом із тим ступінь розбудови інформаційного суспільства в Україні порівняно зі світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України, оскільки: 1) відсутня координація зусиль державного і приватного секторів економіки з метою ефективного використання наявних ресурсів; 2) ефективність використання фінансових, матеріальних, кадрових ресурсів, спрямованих на інформатизацію, впровадження ІКТ у соціально-економічну сферу, зокрема в сільське господарство, є низькою; 3) наявне відставання у впровадженні технологій електронного бізнесу, електронних бірж та аукціонів, електронних депозитаріїв, використанні безготівкових роз-

рахунків за товари і послуги тощо; 4) рівень інформатизації окремих галузей економіки, деяких регіонів держави є низьким; 5) розвиток нормативно-правової бази інформаційної сфери недостатній; 6) створення інфраструктури для надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг з використанням мережі Інтернет відбувається повільно; 7) рівень комп'ютерної та інформаційної грамотності населення є недостатнім, впровадження нових методів навчання із застосуванням сучасних ІКТ — повільним; 8) рівень інформаційної представленості України в Інтернет-просторі є низьким, а присутність україномовних інформаційних ресурсів — недостатньою; 9) рівень державної підтримки виробництва засобів інформатизації, програмних засобів та впровадження ІКТ є недостатнім, що не забезпечує всіх потреб економіки і суспільного життя; 10) спостерігаються нерівномірність забезпечення можливості доступу населення до комп'ютерних і телекомунікаційних засобів, поглиблення «інформаційної нерівності» між окремими регіонами, галузями економіки та різними верствами населення; 11) не вирішуються у повному обсязі питання захисту авторських прав на комп'ютерні програми, відсутні системні державні рішення, спрямовані на створення національних інноваційних структур (центрів, технополісів і технопарків) з розроблення конкурентоспроможного програмного забезпечення [121].

Головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян і суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [97].

На сучасному етапі реалізації Програми передбачається сприяння створенню і освоєнню виробів обчислювальної техніки та електроніки, сучасних приладів і обладнання, конкурентоспроможних на світовому ринку, створенню замкнутого технологічного циклу вітчизняного виробництва сучасних компакт-дисків і перспективних DVD-дисків для забезпечення запису, збереження і розповсюдження аудіо- і відеоінформації та комп'ютерних баз даних великої ємності, створенню діючих зразків високоефективних ЕОМ різних класів, інтелектуальних робочих станцій, нейрокомп'ютерів, масових засобів інформатизації, таймерних

комп'ютерних систем, систем комп'ютерного управління технологічними процесами, створенню вітчизняної елементної бази, налагодженню серійного виробництва електронних карток і впровадженню інформаційних систем з їх використанням.

Інформатизація наукової діяльності сприятиме підвищенню ефективності наукових досліджень, створенню потужної системи науково-технічної інформації та її використанню на всіх етапах наукової діяльності за умови активізації всіх її форм. Повинні бути створені умови для широкої комп'ютеризації та математизації природничих і гуманітарних наук, входження у світову інформаційну мережу баз даних та знань, формування в майбутньому «об'єднаного» чи «колективного» інтелекту.

У міжнародному співробітництві з проблем інформатизації головним є активна участь України у реалізації міжнародних проектів, спрямованих на формування умов для входження до глобальних інформаційних систем, захист при виконанні цих проектів національних інтересів і реалізація стратегічних цілей української зовнішньої політики [212].

Необхідно організувати та постійно вдосконалювати взаємозв'язок національних телекомунікаційних систем із комп'ютерними мережами інших країн та глобальною мережею Інтернет, забезпечити доступ до міжнародних інформаційних масивів та баз даних і геоінформаційних систем [121].

В Україні поступово нарощується система нормативно-правових актів, спрямованих на регулювання такого засобу доступу громадян до інформації, як Інтернет. Це, зокрема, Указ Президента України від 31 липня 2000 р. № 928 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні», постанови Кабінету Міністрів України від 4 січня 2002 р. № 3 «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади», від 11 лютого 2004 р. № 150 «Про офіційне оприлюднення регуляторних актів, прийнятих місцевими органами виконавчої влади, територіальними органами центральних органів виконавчої влади та їх посадовими особами, і внесення змін до Порядку оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади»,

Порядок інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади, затверджений Наказом Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України від 25 листопада 2002 р. № 327/225, Порядок функціонування веб-сайтів органів виконавчої влади, затверджений Наказом Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв'язку та інформатизації України від 25 листопада 2002 р. № 327/225, розпорядження Голови Верховної Ради України від 24 травня 2001 р. № 462 «Про затвердження Положення про Веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет» та інші нормативно-правові акти [45–46; 67–72; 128–129; 163–167; 173–174].

Указ Президента України від 31 липня 2000 р. № 928/2000 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» окреслює основні напрями використання Інтернету, зокрема: 1) створення у найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу громадян, навчальних закладів, наукових та інших установ і організацій усіх форм власності, органів державної влади та органів місцевого самоврядування, суб'єктів підприємницької діяльності до мережі Інтернет; 2) розширення і вдосконалення подання у мережі Інтернет об'єктивної політичної, економічної, правової, екологічної, науково-технічної, культурної та іншої інформації про Україну, зокрема тієї, що формується в органах державної влади та органах місцевого самоврядування, навчальних закладах, наукових установах та організаціях, архівах, а також бібліотеках, музеях, інших закладах культури, розширення можливостей для доступу в установленому порядку до інших національних інформаційних ресурсів, постійне вдосконалення способів подання такої інформації; 3) забезпечення конституційних прав людини і громадянина на вільне збирання, зберігання, використання та поширення інформації, свободу думки і слова, вільне вираження своїх поглядів і переконань; 4) забезпечення державної підтримки розвитку інфраструктури надання інформаційних послуг через мережу Інтернет; створення умов для розвитку

підприємницької діяльності та конкуренції у галузі використання каналів електронного зв'язку, створення можливостей для задоволення на пільгових умовах потреб у зазначених послугах навчальних закладів, наукових установ та організацій, громадських організацій, а також бібліотек, музеїв, інших закладів культури, закладів охорони здоров'я, з врахуванням розташованих у сільській місцевості; 5) розвиток та впровадження сучасних комп'ютерних інформаційних технологій у системі державного управління, фінансовій сфері, підприємницькій діяльності, освіті, наданні медичної та правової допомоги та інших сферах; 6) вирішення завдань щодо гарантування інформаційної безпеки держави, недопущення поширення інформації, розповсюдження якої заборонено відповідно до законодавства; 7) вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інтелектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів усіх форм власності, умисне поширення комп'ютерних вірусів [225].

Важливим нормативно-правовим актом є Порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи «Електронний Уряд», затверджений Наказом Державного комітету зв'язку та інформатизації України від 15 серпня 2003 р. № 149, який визначає процедуру надання органами виконавчої влади інформаційних та інших послуг громадянам і юридичним особам з використанням електронної інформаційної системи «Електронний Уряд». Інформаційні послуги, що мають надаватися з використанням електронної інформаційної системи «Електронний Уряд», визначено в Переліку інформаційних та інших послуг електронної інформаційної системи «Електронний Уряд». Можливість надання органом виконавчої влади певної послуги визначається готовністю цього органу влади надавати відповідну державну (адміністративну) послугу в електронній формі та потребою громадян і юридичних осіб у цій послузі [35].

Управління використанням Інтернет охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь всі зацікавлені сторони і відповідні міжурядові та міжнародні організації. У зв'язку із цим залишаються неврегульованими такі питання: а) по-

літичні повноваження щодо пов'язаних з Інтернетом питань державної політики міжнародного рівня, які мають права і обов'язки стосовно Інтернету; б) приватний сектор відіграє і повинен продовжувати відігравати важливу роль у розвитку Інтернету в технічній та економічній сферах; в) громадянське суспільство також відіграє важливу роль у питаннях, пов'язаних з Інтернетом, особливо на рівні громад, і має продовжувати відігравати таку роль; г) міжурядові організації відіграють і повинні продовжувати відігравати роль, що сприяє координації пов'язаних з Інтернетом питань державної політики; ґ) міжнародні організації повинні відігравати важливу роль у розробленні технічних стандартів і відповідної політики щодо Інтернету.

Таким чином, разом із позитивними досягненнями широке використання мережі Інтернет призвело до появи низки соціальних, організаційних, юридичних та інших проблем, які терміново потребують розв'язання.

о ***Політика інформатизації правоохоронних органів***

Головним інструментом реалізації державної політики у сфері інформатизації правоохоронних органів є формування правових засад розвитку зазначеного системного процесу. На даний час інформатизація правоохоронних органів здійснюється шляхом створення та експлуатації кожним органом власних інформаційних систем та підсистем. Крім цього, існують спеціалізовані міжвідомчі інформаційно-телекомунікаційні системи, які забезпечують збирання, накопичення інформації та обмін нею лише між окремими підрозділами правоохоронних органів, переважно на рівні взаємодії їх центральних апаратів.

Звідси основними причинами низького рівня інформаційної взаємодії і координації у правоохоронній сфері є міжвідомчі та організаційно-правові неузгодженості, що у цілому знижує ефективність політики інформатизації правоохоронних органів. У зв'язку з цим у сучасних умовах інформатизація правоохоронних органів набуває особливої актуальності, оскільки є системним процесом, що має забезпечити високотехнологічний прорив у цьому напряму.

Правовою основою інформатизації правоохоронних органів є Указ Президента України від 31 січня 2006 р. № 80/2006 «Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань

боротьби зі злочинністю» та розпорядження КМУ від 15 березня 2006 р. № 146-р «Про утворення міжвідомчої координаційної групи із створення і функціонування Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби із злочинністю».

9 квітня 2009 р. КМУ затвердив Державну програму інформаційно-телекомунікаційного забезпечення правоохоронних органів, де окремо визначено актуальність потреби удосконалення методів боротьби зі злочинністю, зокрема за рахунок підвищення ефективності інформаційно-телекомунікаційного забезпечення правоохоронних органів [45; 227].

Метою цієї Програми є забезпечення створення умов для поліпшення координації організаційних, профілактичних, оперативно-розшукових заходів, а також підвищення ефективності інформаційно-аналітичного забезпечення правоохоронної діяльності за рахунок удосконалення інформаційної взаємодії шляхом використання сучасних захищених інформаційно-телекомунікаційних систем і проведення стандартизованих (уніфікованих) процедур обміну інформацією. Таким чином, основним функціональним завданням політики інформатизації правоохоронних органів на сьогодні слід визначити створення Єдиної інтегрованої міжвідомчої комп'ютерної інформаційно-телекомунікаційної системи правоохоронних органів.

Отже, системна інформатизація правоохоронних органів дасть змогу підвищити її практичну віддачу та прискорити високотехнологічну інтеграцію.

o ***Мета національної інформаційної політики***

Поряд із позитивними здобутками потрібно визнати певні прорахунки державної політики у сфері розвитку високих інформаційних технологій. Так, розуміючи, що інформаційна діяльність — це головна продукуюча діяльність в умовах інформаційного суспільства, слід визначити, що Google як найбільша пошукова Інтернет-система світу станом на 2009 р. містить 366 600 000 посилань англійською мовою. Натомість російською мовою — 366 000, а українською взагалі — 36 000 посилань.

Визначимо три основні проблеми державної політики розвитку високих технологій у сфері інформатизації: 1) розроблення і просування універсальних принципів та норм з метою розв'язання висо-

котехнологічних проблем інформаційної галузі, збереження і примноження інтелектуальних надбань цивілізації; 2) сприяння становленню високотехнологічного інформаційного суспільства шляхом забезпечення доступу та широкого використання глобальних інформаційних ресурсів; 3) інноваційні пошуки в галузі інформації, комунікацій та розвитку нових інформаційних технологій.

Отже, метою національної інформаційної політики України є створення передумов для побудови в державі розвиненого інформаційного суспільства як органічного сегменту глобального інформаційного співтовариства, забезпечення пріоритетного розвитку інформаційних ресурсів та інфраструктури, впровадження новітніх інформаційних технологій, захисту національних інформаційних цінностей, забезпечення конституційних прав на свободу слова та вільний доступ до інформації.

На підставі наукового аналізу наведено основи державної політики розвитку високих інформаційних технологій та визначено її стратегічні цілі, що надає підстави для виведення логічної мережі (схема 1.2).

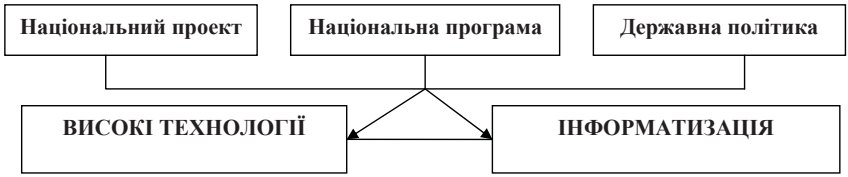


Схема 1.2

Таким чином, основні поняття, винесені до назви розділу 1, складають умовну мережу «ІНФОРМАЦІЙНА ПОЛІТИКА (1) — ПРАВО (2) — ВИСОКІ ТЕХНОЛОГІЇ (3)», яка може тлумачитися як «ЦІЛІ-ЗАВДАННЯ (1) — ЗАСОБИ ДОСЯГНЕННЯ (2) — РЕЗУЛЬТАТ (3)». З цього випливає, що інформаційна політика визначає стратегічні цілі-завдання, оптимальним регулятором процесу досягнення яких виступають право в цілому та його окремі галузеві інститути. Звідси ми бачимо, що результатом як кінцевою крапкою цілей-завдань постають високі технології. При цьому їх сукупність у свою чергу також є новим соціотехнічним процесом інформаційного змісту.

Отже, підсумуємо, що політика розвитку високих інформаційних технологій — це система певних суспільних відносин і взаємодії соціальних груп, спрямованих на реалізацію своїх інформаційних потреб. При цьому все ж таки вирішальним є економічний інтерес, що визначає необхідність правового регулювання суспільних відносин у галузі інформаційної індустрії.

1.2. Високотехнологічне інформаційне право в системі права України: об'єкти, суб'єкти, методологія

o ***Теорія правової інформатики***

Інформатика (нім. *informatik*, франц. *informatique*, англ. *computer science* — компьютерная наука — у США, англ. *computing science* — обчислювальна наука — у Великій Британії) — це наука про способи одержання, накопичення, зберігання, перетворення та передавання інформації, а також її використання в обчислювальних машинах та обчислювальних мережах [254].

Визначення інформації як правової категорії, її правового статусу, значення в правотворчості та правовому регулюванні, зокрема при прийнятті управлінських рішень, — це ті питання, які розглядали в своїх наукових дослідженнях І. В. Арістова, О. М. Бандурка, К. І. Беляков, Н. Г. Бєляєва, А. Б. Венгеров, В. І. Іванов, Д. А. Керімов, В. К. Колпаков, А. М. Куліш, Б. Г. Литвак, В. М. Плішкін, Ю. А. Тихомиров та ін.

Особливо слід підкреслити внесок у розроблення проблеми інформаційного забезпечення державного управління таких провідних учених, як В. Б. Авер'янов, Г. В. Атамчук, В. Г. Афанасьєв, О. М. Бандурка, І. Л. Бачило, Д. Белл, А. І. Берг, Ю. П. Битяк, М. С. Вертузаєв, Є. Галантер, В. М. Глушков, П. Джонстон, Ф. Є. Емері, В. В. Зуй, Р. А. Калюжний, М. Кастеллс, Ю. М. Козлов, А. П. Коренєв, В. Д. Малков, В. Г. Машликін, Дж. Міллер, В. А. Мінаєв, В. С. Михалевич, А. М. Омаров, В. Ф. Опришко, Г. І. Петров, Н. С. Полєвой, Г. Х. Попов, К. Прибрам, Р. Сассерінд, Е. П. Семенюк, І. В. Сергієнко, Д. Н. Узнадзе, А. Д. Урсул, М. Я. Швець, Г. В. Щьокін, В. В. Цвєтков, Л. П. Юзьков та ін.

Серед вітчизняних дослідників — фундаторів української школи правової інформатики у комплексі з інформаційним правом та інформаційною безпекою можна відзначити таких, як доктори наук — І. Арістова, Р. Калюжний. П. Мельник. Н. Мироненко, А. Музика, Н. Нижник, В. Попович, Л. Савченко, С. Ріпна, В. Шамрай, В. Шкарупа; кандидати наук — Д. Азаров, П. Біленчук, В. Брижко, К. Бєляков, В. Павловський, В. Голубєв, М. Гуцалюк, Ю. Жаріков, О. Крупчан, А. Марущак, І. Рогатюк, Г. Середа, О. Шинальський, Ю. Ящуринський та ін.

Наведемо визначення правової інформатики як прикладної науки, що вивчає проблеми збирання, реєстрації, зберігання, сприйняття, оброблення та використання правової інформації (нормативної, довідкової, криміналістичної, статистичної тощо) [256].

Дослідження щодо застосування здобутків інформатики в юридичній діяльності в Україні свідчать, що в нашій країні окреслилися ознаки активного формування у правничій науці вітчизняної наукової школи — правової інформатики — комплексних досліджень на межі правознавства і прикладної інформатики [237]. Як складові особливої частини правової інформатики або на рівні спеціальних комплексних міжгалузевих інститутів зазначені дослідники активно формують: криміналістичну, кримінологічну, оперативно-розшукову, фінансово-правову, податкову, адміністративно-правову інформатики.

Таким чином, слід визначити, що правова інформація — це сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо [122]. Дещо забігаючи наперед, потрібно зазначити нетотожність співвідношення правової інформатики (1) з інформаційним правом (2). До предмета правової інформатики належать питання інформаційного забезпечення *(Iz)* правових процесів *(Ld)*. Разом із тим предметом інформаційного права виступають, навпаки, питання правового забезпечення та регулювання *(Lz)* інформаційної діяльності, відносин та процесів *(Id)*, що можна представити формулою

$$1 = \frac{Iz}{Ld} \neq \frac{Lz}{Id} = 2 \ . \qquad (1.1)$$

Таким чином, теоретичні основи правової інформатики складаються із двох основних компонентів: інформатики та права, про що докладніше говоритиметься далі.

о ***Право та правовідносини***

У повсякденному житті під правом розуміють загальнообов'язкові правила поведінки, встановлені та санкціоновані державою у вигляді законів, указів тощо. У найбільш доступному визначенні право є системою регуляції суспільних відносин, мета якої — встановлення режиму правопорядку.

За більш розширеним тлумаченням право слід розуміти як засновану на уявленні про справедливість міру свободи і рівності, що відображує потреби суспільного розвитку, яка у своїй основі склалася в процесі повторюваних суспільних відносин і визнається та охороняється державою.

Таким чином, право є закономірним результатом внутрішнього розвитку регулятивної системи, відповіддю на потребу суспільства в регулюванні економічних, політичних, соціальних відносин. У суб'єктивному розумінні право є видом та мірою дозволеної чи приписаної поведінки суб'єкта суспільних відносин.

Одна з найважливіших властивостей права — його здатність виступати в ролі регулятора суспільних відносин. Саме в цьому полягає соціальне призначення права. Правове регулювання відбувається внаслідок впливу норм права на свідомість людей, а через неї — на їх поведінку. Її одноманітність і повторюваність, відповідність вимогам права становлять зміст правового регулювання [63]. Отже, право — це система норм (правил) поведінки, що встановлюються або санкціонуються державою (компетентними державними органами, іншими суб'єктами, наділеними такими повноваженнями, або населенням у результаті референдуму), гарантуються нею, містяться в нормативно-правових актах і регулюють найважливіші сфери суспільних відносин.

Соціальні норми покликані забезпечити врегулювання відносин, що існують між людьми в суспільстві. Термін «норма» — багатозначний, його розглядають як правило поведінки, встановлену міру, кількість тощо. Нормування суспільних відносин при зміні соціальних умов завжди потребує встановлення певної міри можливої поведінки людей. При визначенні системи інформаційного права ми виходимо

з того, що первинним осередком права є норма права. Норми права, які регулюють одні й ті самі відносини, називаються інститутом права. Інститути права залежно від своєї значущості розташовані у прийнятому в юриспруденції порядку й утворюють систематику певного правового явища. Основною формою стандартизації норм суспільних інформаційних відносин є законодавство.

Ґрунтуючись на тому, що правовідносинами називають суспільні відносини, змістом яких є суб'єктивні права та юридичні обов'язки осіб, що охороняються державою, право у сфері інформаційних відносин слід розуміти як вид поінформованості суб'єктів та міру інформатизації суспільства, що відображує інформаційні потреби суспільного розвитку, яка у своїй основі склалася в процесі повторюваних суспільних відносин і визнається та охороняється державою.

Оскільки інформаційні відносини виникають у різних сферах суспільного життя і є у тій чи іншій мірі предметом регулювання багатьох галузей права, то першим критерієм для класифікації права на інформацію є зв'язок останнього із предметом правового регулювання різних галузей права.

За цим критерієм виділяємо права на інформацію, пов'язані із предметом правового регулювання конституційного (право на інформацію про діяльність органів державної влади), цивільного (право власності на інформацію), сімейного (право на інформацію про стан здоров'я заручених), господарського (право суб'єкта господарювання на одержання інформації про результати перевірок його діяльності), фінансового (право на інформацію про державний бюджет) та інших галузей права.

о ***Інформаційне право***

Поняття інформаційного права з'явилося відносно нещодавно — на межі 80–90-х років XX ст. [39]. Хоча це не є вичерпним доказом того, что позначуваного ним явища не існувало раніше. Утім, такий подхід є цілком справедливим в природничих науках, але може виявитися невірним в соціальних.

Інтеграція наукових знань — це процес «зв'язування» окремих диференційованих ідей, методів, частин та функцій взаємодіючих наук у єдине ціле. Синтезовані у будь-якій предметній галузі пізнання, вони разом утворюють уже нову галузь знань, нову науку. Особливо гостро це відчувається у формуванні суспільних відносин ново-

го типу — інформаційних процесів, обумовлених високотехнологічною революцією. У правовій сфері саме це може стати основними передумовами високотехнологічного інформаційного прориву, тобто принципово нового розв'язання проблем нетрадиційним шляхом.

Інформаційне право предметно охоплює правову регуляцію достатньо широкого спектру суспільних відносин в інформаційному просторі, а саме: правові засади діяльності друкованих засобів масової інформації (преси) та правовий статус інформаційних агенцій, бібліотечну та архівну діяльність, телебачення, радіомовлення і кінематографію, законодавство у сфері видавничої справи, правове регулювання державної статистики та організаційно-правові основи рекламної діяльності тощо [233].

Інформаційне право є галузевою юридичною наукою, що динамічно розвивається [19]. Виникають нові правові терміни, набувають додаткового значення фундаментальні юридичні поняття [217, с. 3].

Так, поряд із визначенням терміна «інформаційне право» сучасні юридичні енциклопедії містять визначення терміна «комп'ютерне право» як комплексної галузі права, яка регулює суспільні відносини у сфері інформатики, створення і використання електронно-обчислювальних машин, засобів і продуктів електронного програмування.

Уживаються також такі термінологічні конструкції, як «інформаційно-комп'ютерне право», «електронне право», «кібернетичне право» та «правова кібернетика» [102, с. 13].

Таким чином, інформаційне право постійно розвивається та вдосконалюється, оскільки воно є сукупністю правових норм, що регулюють соціальні відносини, які так чи інакше взаємодіють або пов'язані з інформацією.

о ***Поняття та види високих технологій***

Науково-технічна революція — це крок до формування глобальної високотехнологічної цивілізації. Ми бачимо, що багато явищ соціального життя все більшою мірою відображуються в так званому «віртуальному світі» — у тих інформаційних сферах, носіями яких виступають як засоби масової інформації, так і глобальні комп'ютерні телекомунікаційні мережі та системи.

Сьогодні інформаційна сфера неможлива без застосування автоматизованих інформаційних систем та банків даних, програмного забезпечення операційних систем, прикладного та сервісного про-

грамного забезпечення, інших інформаційних технологій, що засновані на використанні засобів обчислювальної техніки і зв'язку. Подальше вдосконалення середовища накопичення інформації на різних носіях, глобальне охоплення населення засобами зв'язку, що дозволяють передавати інформацію в будь-яку точку планети, автоматизоване оброблення інформації заздалегідь розробленими алгоритмами — це три технічні досягнення, на яких базуються сучасні інформаційні технології і які можуть бути використані для проведення оперативно-технічних заходів. Таким чином, нові інформаційні технології деякі автори пропонують визначати як цілісну систему операцій стосовно збирання, зберігання, оброблення та передавання інформації, що здійснюється з використанням комп'ютерної техніки та телекомунікаційних каналів зв'язку.

Разом із тим технологія як об'єкт правового регулювання і один з ключових термінів інформаційного законодавства залишається фактично невизначеною. У найбільш загальному випадку під поняттям «технологія» розуміють сукупність взаємопов'язаних способів оброблення матеріалів, виготовлення виробів та процесів, що супроводжують ці види робіт. Власне сам процес становить певну сукупність дій, спрямованих на досягнення поставленої мети. Він повинен визначатися вибраною людиною стратегією і реалізовуватися за допомогою сукупності різних засобів та методів.

Поняття нових інформаційних технологій визначається як сукупність методів та засобів реалізації інформаційних процесів у різних галузях людської діяльності. Інакше кажучи, вони є засобами реалізації інформаційної діяльності людини. Засобами реалізації цієї діяльності є електронно-обчислювальна техніка, цифрові засоби телекомунікації, волоконно-оптичні системи зв'язку та передавання інформації, інформаційні нанотехнології, суперкомп'ютерні та Гріт-технології, розвиток яких постійно стимулюється прогресом інформаційних відносин.

П. І. Орлов, порівнюючи проблеми інформації та інформатизації, акцентує увагу на тому, що нові інформаційні технології засновані на впровадженні обчислювальної техніки, засобів зв'язку, систем телекомунікації. Таким чином, на його думку, нові інформаційні технології визначаються як цілісна система операцій щодо збирання, збері-

гання, оброблення та передавання інформації, що здійснюється з використанням комп'ютерної техніки та телекомунікаційних каналів зв'язку [144, с. 8, 29].

Отже, класифікаційною ознакою, яка відносить інформацію до сфери нових технологій, є електронне оброблення інформації (з метою її збереження, передавання, копіювання, перероблення, знищення, кодування тощо) та використання мереж зв'язку, в більшості своїй глобальних.

Реалізація функцій інформаційної системи неможлива без знання зорієнтованої на неї інформаційної технології. Остання може існувати й поза сферою інформаційної системи.

Термін «технологія» походить від базового терміна «техніка», який означає загальну назву різноманітних пристроїв, механізмів та приладів, не існуючих в природі, а виготовлених людиною. Універсальної класифікації технічних засобів ще не створено. Тенденція зростання ролі науки в житті сучасного суспільства сьогодні зумовлює використання високотехнологічних рекомендації в правоохоронній практиці. При цьому наголошується на проблемах, що лежать на стиках різних галузей знань, оскільки тільки їх тісна взаємодія нині забезпечує пріоритети на всіх напрямах науки та техніки [117, с. 139].

Тому з погляду політики розвитку існують підстави стосовно окремого визначення найбільш міцного зв'язку техніки з наукою, що може бути визначено так:

$$\sum T + L = Tl\,, \tag{1.2}$$

де T — техніка *(technika)*; L — наука *(logos)*; Tl — технологія *(technology)*.

Відповідно до визначення поняття «технологія» інформаційна технологія — це процес, що використовує сукупність засобів і методів збирання, оброблення і передавання даних (первинної інформації) для одержання інформації нової якості про стан об'єкта, процесу або явища (інформаційного продукту).

Інформаційна технологія є більш ємним поняттям, що відображує сучасне уявлення про процеси перетворення інформації в інформа-

ційному суспільстві. Метою нових технологій у галузі передавання інформації є отримання інформації для аналізу і прийняття на його основі рішення на виконання будь-якої дії.

У майстерному сполученні двох інформаційних технологій — управлінської та комп'ютерної — запорука успішної роботи інформаційної системи.

Кожна наука має свій предмет. Інформаційні правовідносини, що складаються у сфері високих технологій, на цей час ще не є завершеними, оскільки вони охоплюють лише основи високотехнологічної теорії інформаційного права. Тим більше, що подолання інформаційно-технологічного відставання у сфері боротьби зі злочинністю вимагає здійснення ланцюгової реакції «мета — теорія — практика — суспільний результат». Тож, ми наблизилися до розуміння базової формули, де високотехнологічна теорія є окремою підгалуззю інформаційного права. На ці питання відповіді може дати ґрунтовна побудова нової високотехнологічної теорії інформаційного права, де одним із основних елементів постає правовий зміст поняття «висока технологія».

Потрібно оцінити порівняльно-правове співвідношення термінів «висока технологія» і «нова технологія». Крім цих, зустрічаються похідні від зазначених термінів: «високоінтелектуальна технологія», «інноваційна технологія», «передова технологія», «критична технологія» тощо.

Термін «висока технологія» (*high-tech*) є більш ємним, ніж термін «критична технологія», а за часом створення може включати нові технології, розроблені останніми роками XXI ст. Високі технології — це технології, які стануть визначальними у постіндустріальному суспільстві [54, с. 646]. Під інтелектуальними технологіями розуміють високі наукоємні технології, що відтворюють елементи інтелекту людини [41, с. 29]. Складні за розробленням вони досить прості в експлуатації, навіть для непрофесійного користувача.

До високих технологій можна віднести оптоволоконні, інтегрально-волоконні, лазерні, комп'ютерні, цифрові, космічні, нанотехнології та деякі інші, але з обов'язковою ознакою їх створення протягом останніх 30–40 років, тобто з початку 60-х років XX ст. до сьогодні. Слід визнати, що до цього часу в законодавстві відсутнє визначення такого поняття, як «високі технології» та похідних і суміжних термінів.

Звідси постає проблема відсутності нормативно-правового регулювання суспільних відносин, що виникають у цій галузі. «Нова технологія» і «новітня технологія» також є двома різними термінами. При цьому новітні технології в інформаційній сфері випереджають нові приблизно на п'ять років. Отже, високі технології, з одного боку, є вищими, ніж «звичайні», а з другого — ще можуть поступово зростати, але не бути піковими, на відміну від критичних, які є якісним ривком після досягнення певної критичної межі. Звідси термін «критичні технології» за рівнем є вищим, ніж термін «високі технології». Адже критичний рівень завжди є фактично піковим або максимальним, після чого технологічні властивості мають структурно перейти вже на інший уніфікований рівень. З метою систематизації понять пропонуємо для єдиного позначення сукупності таких технологій вживати єдиний термін «прогресивні технології», або «прогтехнології» (*prog-tech*).

З метою розвитку Основ політики РФ в галузі розвитку науки і технологій на період до 2010 р. розроблено Правила формування, коректування і реалізації пріоритетних напрямів розвитку науки, технології та техніки в РФ і переліку критичних технологій. 25 серпня 2009 р. цей перелік критичних технологій, що підпадають під чинність закону про порядок здійснення іноземних інвестицій у стратегічні галузі, було затверджено [136].

До переліку включено 35 технологій, що мають важливе соціально-економічне значення або важливе значення для оборони країни і безпеки держави. У списку критичних технологій — клітинні технології, нанотехнології, технології біоінженерії, водневої енергетики, нових і поновлюваних джерел енергії. До переліку включено також технології оброблення, зберігання, передавання і захисту інформації, створення інтелектуальних систем навігації, оброблення композиційних, керамічних матеріалів, кристалічних матеріалів, полімерів і еластомірів. Крім цього, визначено галузі, що мають стратегічне значення для забезпечення оборони країни і безпеки держави. Так, до стратегічних галузей віднесено 42 види діяльності [146].

Систематизовані за термінологічними ознаками поняття з цього приводу схематично наведено нижче (схема 1.3).

Перша група	*Друга група*	*Третя група*
Критичні технології	Екстремальні технології	Високі технології
Електронні технології	Прогресивні технології	Нові технології
Ефективні технології	Максимальні технології	Новітні технології
Передові технології	Революційні технології	Супертехнології
Креативні технології	Модернізаційні технології	Метатехнології
Цифрові технології	Високопродуктивні технології	Інноваційні технології

Схема 1.3

Звідси стає беззаперечним, що сьогодні проблеми розроблення правового забезпечення нових інформаційних технологій, у тому числі щодо організації роботи правоохоронних органів, мають не тільки теоретичне, а й суто практичне значення.

Утім, зрозуміло, що від того, який правовий зміст вкладається у поняття високих інформаційних технологій, залежатиме розгляд питань про механізм їх виявлення, принципи, класифікацію, нормативне регулювання, практичні рекомендації щодо вдосконалення взаємодії і координації.

о ***Право високих технологій***

Більшість дослідників відзначають, що високотехнологічний прорив призвів до значних соціальних змін у суспільстві, найважливішим з яких є поява нового виду правовідносин — у сфері високих технологій.

Високотехнологічні правовідносини — це правила поведінки у сфері розроблення та застосування високих технологій, що регулюють інформаційні взаємовідносини, є проявом їх волі та забезпечуються прогресивними (інноваційними) заходами соціально-інформаційного впливу. Ці правила поведінки встановлюють напрями і кордони дій суб'єктів інформаційних відносин, створюються з урахуванням соціотехнологічного досвіду та інформаційних інтересів людей.

Правову основу інформаційної діяльності у сфері високих технологій становить інформаційне законодавство, під яким розуміють множину нормативно-правових актів, прийнятих Верховною Радою України у формі законів та постанов нормативного змісту, що регулюють нові соціотехнологічні відносини, що складаються у цій галузі.

У цілому джерелами високотехнологічного інформаційного права є Конституція України, інші законодавчі і підзаконні нормативні правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з питань правового регулювання суспільних відносин у сферах інформації та високих технологій.

Звідси бачимо, що право високих технологій можна розуміти як в об'єктивному, так і в суб'єктивному змісті. Так, право високих технологій в об'єктивному змісті — це суспільні відносини у сфері високих технологій, які втілюються у нормах, урегульованих на публічно-правовому та приватноправовому рівнях. Право високих технологій у суб'єктивному змісті — це множина прав і обов'язків конкретних учасників суспільних відносин, що виникають у сфері розроблення, виробництва та використання високих технологій як об'єкта соціотехнологічних відносин.

Таким чином, високотехнологічне інформаційне право є сукупністю правових норм, які регулюють інноваційні розроблення в інформаційній сфері, що забезпечує нормативно-правове регулювання процесу високотехнологічного розвитку інформаційного суспільства.

Високотехнологічне інформаційне право як наука — це система наукових знань про право високих технологій як підгалузь інформаційного права, його предмет, методи, принципи правового регулювання інформаційних відносин у сфері високих технологій, історію розвитку суспільних відносин в інформаційній сфері та порівняльно-правовий аналіз норм високотехнологічного права зарубіжних країн.

У цілому право високих технологій як підгалузь інформаційного права ще перебуває на початковому етапі свого формування. Отже, пропонуємо далі розглядати високотехнологічне інформаційне право як систему правового регулювання інформаційних відносин у сфері високих технологій.

o ***Методи та методологія. Синергетика права***

Науковий метод — це сукупність основних способів дослідження феноменів, систематизації, коректування нових і отриманих раніше знань для вирішення завдань у рамках будь-якої науки.

Методологія інформаційного права також перебуває у стадії розвитку. Об'єктивно вона поєднує методологічні засади права, інформатики, тектології (теорії організації соціальних систем), соціальної кібернетики та інших гуманітарних і технічних наук [148, с. 60].

Методи інформаційного права визначаються залежно від контексту змісту категорії. Провідним методом інформаційного права вважається метод комплексного застосування методів конституційного, адміністративного, цивільного, трудового та кримінального права [148, с. 57].

Останнім часом учені все більше приділяють увагу одному з найбільш інтегральних спрямувань методології вивчення соціального буття — соціальній синергетиці [126]. Для розуміння міждисциплінарної природи об'єктів високотехнологічного інформаційного права потрібно з'ясувати сутність поняття «синергетика права».

Синергетика — це відносно молодий міждисциплінарний науковий напрямок. Синергетика вивчає загальні закономірності самоорганізації, становлення структур, які утворюються в складних, відкритих системах у процесі перманентного потокового обміну речовиною, енергією та інформацією з навколишнім середовищем у нерівноважних умовах. Важливим для синергетики є виявлення просторово-часової структури організації, умов її виникнення і розвитку. Об'єктами дослідження синергетики виступають найрізніші системи — від атома до людини.

Слово «синергетика» (від грец. συν — спільно і грец. εργος — діючий) і означає «спільна дія», підкреслюючи узгодженість поведінки часток, що відображується в функціонуванні системи як цілого. Тобто, пропонуються базові моделі, нові поняття і методи, які можуть бути застосовані в даній ситуації, стати основою побудови нової нелінійної пізнавальної парадигми, а можуть залишитися знахідками в різних дисциплінах. Основними завданнями синергетики є вивчення природних явищ і процесів на основі принципів самоорганизації систем, що складаються з підсистем. Таким чином, синергетика — це наука, яка займається вивченням процесів самоорганізації і виникнення, підтримки, стабільності та розпаду структур будь-якої природи [9].

Зі світоглядної точки зору синергетику іноді позиціонують як «глобальний еволюціонізм», або «універсальну теорію еволюції», що дає єдину основу для опису механізмів виникнення будь-яких новацій подібно тому, як інколи кібернетика визначалася як «універсальна теорія управління», однаково придатна для опису будь-яких операцій регулювання і оптимізації: у природі, техніці, суспільстві і под. Час показав, що загальний кібернетичний підхід виправдав далеко не всі надії, що покладалися на нього.

Аналогічно й тлумачення масштабного застосування методів синергетики зазнає критики [81].

Зрозуміло, у соціальній і медійной системах з позицій управлінської діяльності нелінійність ґрунтується на багатоваріантності, а отже, інформаційно більш насичена. Інформаційна множина створює можливість вибору, адекватного цільовим настановам діяча. Чутливість нелінійного мислення до інформаційних мікровпливів являє собою «режим із загостренням», здатний породити з будь-якої мікрофлуктуації макроструктуру.

Суб'єкт, що зафіксував і осмислив певну інформацію, потенційно здатний згідно зі своїми індивідуальними якостями, умотивованістю розпушувати структуру в локальній зоні і за допомогою резонансного порушення призвести систему до точки біфуркації. Структура відповідно до принципу динамічної організованості (впорядкованості з потенційною можливістю дії) відкрита для діяча, тобто готова до зміни конфігурації [113].

На рівні сучасної інформаційної системи в цілому нестійкість пов'язана з інформаційно-комунікативною революцією, що створює нову технологічну базу цивілізації. Конвергенція засобів обчислювальної техніки із засобами інформаційної комунікації породжує ефект соціально-технологічної інтегрованості системи [89]. Телекомунікаційна революція замінює єдинолінійність комунікаційного акту багатофункціональним, діалоговим зв'язком, здійснює «стиск» простору і часу, породжуючи нові ступені волі для індивіда і соціуму (і нові проблеми).

Інформаційний синергізм, або синергетичний ефект, — це ефект взаємозв'язку і взаємодії, підвищення результативності за рахунок використання взаємозв'язку і взаємопосилення соціотехнологічного впливу інформаційної діяльності.

На відміну від системного підходу, де основна увага акцентується на зв'язках частин у цілому, синергетика досліджує причини властивостей системи. У системному підході аналіз ведеться, як правило, на якісному рівні. Синергетика займається дослідженням систем, що складаються з великого числа частин, компонентів або підсистем, інакше кажучи, деталей, складним чином взаємодіючих між собою. Можна втрутитися в потрібний момент у перебіг подій і змінити його. Отже, майбутнє також, виявляється, має не єдиний варіант. А відповідь синергетики полягає в тому, що в безлічі випадків відбувається самоорганізація, пов'язана з виділенням так званих параметрів порядку [250].

Таким чином, синергетика є науковою дисципліною, що розглядає закономірності процесів системної інтеграції і самоорганізації в різних системах. Більш того, як бачимо, синергетика покликана відігравати роль свого роду метанауки, що помічає та вивчає загальний характер тих закономірностей і залежностей, які окремі науки вважали «своїми». Тому синергетика виникає не на стиці наук, у більшменш широкій чи вузькій прикордонній галузі і досліджує системи, що мають загальний («інтернаціональний») характер стосовно окремих наук.

Підхід — це комплекс механізмів пізнання або практики, що характеризує конкуруючі між собою стратегії і програми в науці, політиці, філософії або організації життя та діяльності людей. Синергетика завжди розглядалась як міждисциплінарний підхід, тому що принципи, що управляють процесами самоорганізації, представляються узгодженими безвідносно природи систем і для їх опису повинен бути придатний загальний математичний апарат.

Звідси синергетичний підхід у теорії права являє собою систему міждисциплінарних прийомів, що характеризуються низкою ознак, заснованих на ідеях спільної дії елементів теорії права, які визначають системність взаємозалежних і взаємозумовлених підходів у вивченні права, що ґрунтуються на принципах самоорганізації.

Стосовно науки інформаційного права синергетичний підхід включає систему прийомів, способів пізнання інформаційних явищ, процесів і станів науково-правової діяльності, спрямованих на розкриття казусних явищ як у самій правовій науці, так і в юридичній

практиці, на виведення законів, принципів протікання інформаційних процесів та їх саморегулювання.

Ось тому синергетичний ефект виявляється в теорії права і теорії правового регулювання тоді, коли в результаті погодженої, спільної дії елементів даних систем виникає нова якість, що не може бути досягнуто на рівні окремих їх елементів.

Слід зазначити, що існує зв'язок високотехнологічної теорії інформаційного права з іншими юридичними науками — адміністративним, конституційним, цивільним, фінансовим, інвестиційним правом тощо. За спрямованістю цієї роботи перш за все зазначимо дисципліни кримінально-правового циклу: кримінальне право, кримінальний процес, кримінологію, криміналістику, судову експертизу та окремі підгалузеві інститути. Далі про кожний з них чекає докладний аналіз системних зв'язків.

Важливим аспектом теорії інформаційного права є проблематика його підсистем, що схематично показано нижче (схема 1.4).

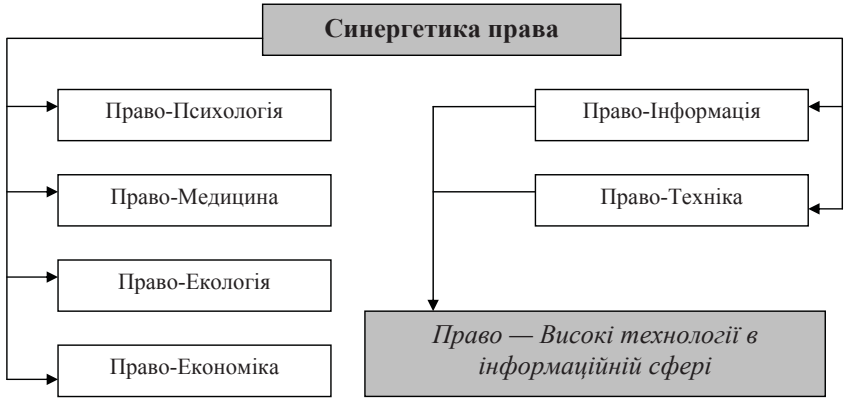


Схема 1.4

Таким чином, стає зрозумілим, чому методологічна основа високотехнологічного інформаційного права щодо з'ясування нових соціотехнологічних явищ базується на теорії цивілізаційного підходу.

У високотехнологічному інформаційному праві використовується вся сукупність способів регулюючого впливу на інформаційні право-

відносини, що виникають у сфері високих технологій, тобто як диспозитивне регулювання (свобода вибору, рівність сторін, децентралізація, координація), так і імперативне регулювання (централізоване здійснення владних повноважень, сувора субординація). Залучення різних методів у систему високотехнологічного інформаційного права не означає їх довільного зіткнення або конкуренції. Дискусії з питань значущості тих чи інших методів для високотехнологічного інформаційного права можна нівелювати, тільки виробивши самостійну правову систему для розв'язання проблем, що виникають в інформаційних відносинах з приводу розроблення та використання високих технологій.

Відповідно до цього нижче на схемі показано основні методи високотехнологічного інформаційного права, які використовувалися в роботі, що дало змогу запровадити методологічно уніфікований системно-інформаційний підхід на всіх рівнях управлінської системи до збирання та опрацювання інформації і визначення її релевантності (цінності) (схема 1.5).

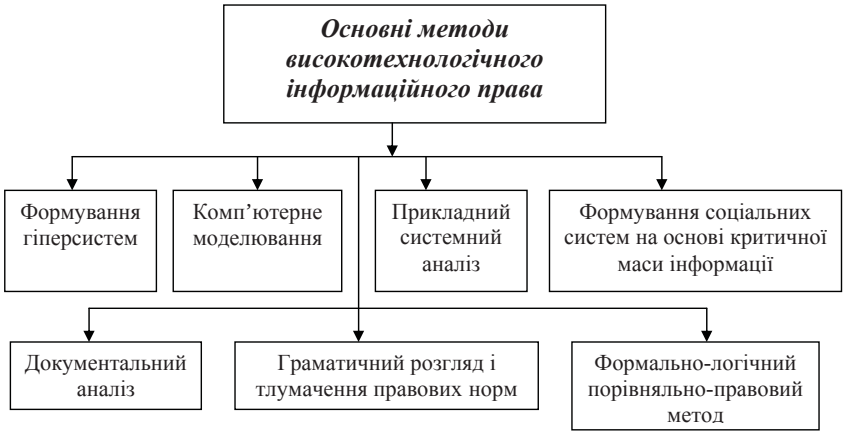


Схема 1.5

Метою розвитку високих технологій в інформаційній сфері є підвищення ефективності системи за рахунок одержання синергетичного ефекту. Синергетика в теорії інформаційного права виступає в ролі методу, реалізуючи свої ідеї в дослідженні її елементів. При цьому

синергетика не може й не повинна диктувати умови в доктрині і концептуальному розвитку високотехнологічного інформаційного права.

Таким чином, спробуємо описати науковий синергетичний зміст правової регуляції високотехнологічної інформатизації:

$$I = \frac{I \overset{2}{\longleftrightarrow} HT}{L} \Rightarrow T+ \uparrow , \tag{1.3}$$

де I — інформація; $I2$ — інформатизація; HT — високі технології; L — правова регуляція; $T+$ — технологічний прорив.

Отже, правова регуляція високих технологій є новою категорією, зміст якої можна визначити за допомогою теорії синергетичного підходу. З позицій такого підходу зазначений новий феномен може розглядатися як динамічна система інформаційних взаємодій суб'єкта з техносвітом, у процесі чого відбуваються створення особливої правової конструкції, втілення її в об'єкті правового регулювання, здійснення і перетворення інформаційних правовідносин суб'єктів у сфері високотехнологічної діяльності.

o ***Основні принципи, об'єкти і суб'єкти***

Основними принципами інформаційних правовідносин є: гарантування права на інформацію; гарантування рівних умов суб'єктам інформаційних відносин; гарантування інформаційної безпеки суб'єктів інформаційних відносин; відкритість, загальнодоступність інформації та свобода її обміну; істинність, вірогідність інформації; повнота, вичерпність інформації; законність збирання, одержання, зберігання, використання та поширення інформації; свобода думки і слова, вільного вираження своїх поглядів і переконань; гарантування правового захисту принципів інформаційних відносин.

З цього визначимо основні принципи інформаційного права: принцип вірогідності, принцип доступності, принцип захищеності, принцип збалансованості, принцип мінімаксу, принцип оперативності, принцип повноти, принцип прозорості, принцип регулярності, принцип рівноправності та деякі інші галузеві принципи.

Об'єкт і предмет науки та навчальної дисципліни «Інформаційне право» визначаються відповідно до сутності інформаційного законодавства.

Об'єктом інформаційного права є суспільні інформаційні відносини. Провідний предмет (об'єкт) суспільних відносин — це інформація (відомості, дані, знання, таємниця тощо).

Безпосередніми предметами є конкретні види та форми інформації щодо конкретних інформаційних відносин, інформаційної діяльності та ін. Зокрема, безпосереднім предметом в нашій роботі є політика розвитку високих технологій передавання інформації у сфері боротьби зі злочинністю.

З цього приводу далі визначимо об'єкти і суб'єктів високотехнологічного інформаційного права. В цілому відомо, що об'єкт — це те, на що спрямована та чи інша діяльність (або те, що створено цією діяльністю). Об'єкт у праві — це суспільні відносини, закріплені чинними правовими нормами. Об'єкт права — це конкретні майнові і немайнові блага та інтереси, з приводу яких відносини регламентовано законом.

Об'єкт правового регулювання, як правило, являє собою умовне виділення визначеного відокремленого кола суспільних відносин, що мають єдину якість. Це дозволяє узагальнити норми права, які регулюють сферу суспільних відносин, а також нормативну спільність як галузь права.

Доктринально визнаються багатооб'єктність юридичних норм стосовно застосування законодавства в правовій кваліфікації суспільних інформаційних відносин, що складаються у високотехнологічних галузях економіки, природна єдність усіх умовно визначених галузей права, які у єдності утворюють систему першого порядку — право України.

Об'єктами інформаційних відносин вважають документовану або публічно оголошену інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах. Об'єктами інформаційної діяльності частіше за все називають інженерно-технічні споруди (приміщення) з визначеною контрольованою зоною, де здійснюється діяльність, пов'язана з інформацією.

Таким чином, визначимо, що об'єктом інформаційного права є суспільні відносини, пов'язані зі створенням, формуванням, зберіганням, обробленням, поширенням, використанням інформаційних продуктів, управлінням процесом формування та використання

інформаційного продукту та надання інформаційних послуг, розвитком та застосуванням нових технологій роботи інформації та її передавання в системах і мережах комунікацій, посиленням безпеки в інформаційній сфері, а також з юридичною відповідальністю суб'єктів права в цих відносинах.

Предметом самостійного правового регулювання можуть бути суспільні відносини у сфері високотехнологічної інформації, що включать питання застосування високих технологій під час отримання та використання інформації, правового захисту, права власності як на технології, так власне і на інформацію, боротьби з інформаційною злочинністю, а також договірні відносини у сфері інформатики.

За наслідками аналізу правового регулювання високотехнологічних інформаційних відносин в Україні та міжнародній практиці є сенс визначити, що основним об'єктом регулювання високотехнологічного інформаційного права є особливі суспільні інформаційні відносини, які формуються під впливом використання високих технологій. Основним предметом цих суспільних відносин, як і власне інформаційних відносин, залишається інформація (відомості, дані, знання, технології, тайна тощо).

Підсумуємо, що *об'єктами високотехнологічного інформаційного права* є передові технології усіх видів та найменувань: нові, високі, інформаційні, критичні та ін.; інформаційно-телекомунікаційні системи та підсистеми; системні інформаційні інновації та окремі інноваційні проекти в інформаційно-телекомунікаційній галузі; процес наукового дослідження, розроблення та організація впровадження високотехнологічних інновацій у виробництво та споживча аудиторія високих технологій у сфері інформаційних послуг.

Суб'єкт права — це фізична або юридична особа, держава, державне чи муніципальне утворення, що володіє за законом спроможністю мати та здійснювати безпосередньо або через представника суб'єктивні права і юридичні обов'язки (тобто правосуб'єктністю).

Суб'єкти права є необхідним елементом правовідносин у всіх галузях права, однак у кожній з них становище суб'єктів має певну специфіку.

Суб'єктами інформаційних правовідносин пропонують вважати фізичних осіб (громадян України, іноземців та осіб без громадянства),

юридичних осіб приватного права та юридичних осіб публічного права, які є правоздатними, наділені законодавством України інформаційними правами і обов'язками, а також державу Україна та іноземні держави [217, с. 152]. У цьому контексті важливим елементом виступає інформаційна дієздатність, тобто визначена інформаційним законодавством юридична можливість суб'єкта інформаційних правовідносин здійснювати свої інформаційні права і обов'язки, реалізуючи які він здатний бути активним учасником інформаційних відносин [217, с. 69]

Отже, суб'єкти інформаційного права — це учасники інформаційних відносин, які володіють інформаційними правами і обов'язками, організаційно здійснюючі їх на нормативно-правовій основі, передбачених законом випадках несуть відповідну правову відповідальність. Такими учасниками є громадяни, юридичні особи або держава, які набувають передбачених законом прав і обов'язків у процесі інформаційної діяльності. Основними учасниками цих відносин виступають автори, споживачі, поширювачі, зберігачі (охоронці) інформації.

Інформаційна правосуб'єктність — це здатність суб'єкта інформаційних правовідносин мати інформаційні права та набувати своїми діями суб'єктивні інформаційні права і обов'язки, які складають зміст інформаційних правовідносин [217, с. 72]. Адже відомо, що правовий статус — це встановлений нормами права стан його суб'єктів, сукупність їх прав і обов'язків.

Ураховуючи це, визначимо учасників високотехнологічних інформаційних правовідносин, що володіють інформаційною правосуб'єктністю: громадяни України, іноземні громадяни, особи без громадянства, юридичні особи усіх форм власності, господарські товариства, державні установи та підприємства (корпорації), науково-дослідні та професійно-освітні заклади, органи влади і управління та їх посадові особи, засоби масової інформації та їх штатні працівники, інші інформаційно-телекомунікаційні засоби. Тобто, зазначені учасники є *суб'єктами високотехнологічного інформаційного права України*.

о ***Проект Інформаційного кодексу України***

Проблеми інформаційного суспільства, що виникають у контексті недосконалого правового регулювання інформаційних та інформаційно-інфраструктурних відносин, потребують нормативного

вирішення. Зокрема, потрібно визначити загальні засади регулювання суспільних відносин в інформаційному просторі.

Сьогодні необхідність обговорення проблем кодифікації інформаційного законодавства України зумовлена сукупністю значної кількості неузгоджених правових норм у сфері інформаційних відносин, яка досягла у своїй кількості критичного стану. Зважаючи на відсутність системності у підходах до кодифікації інформаційного законодавства, однією з важливих проблем учасники «круглого столу» назвали підготовку і прийняття Інформаційного кодексу України, який би відповідав рівню розвитку інформаційних відносин та адекватно врегульовував питання функціонування інформаційної сфери.

Звідси бачимо, що коли в Україні сформується блок з більшості законів у сфері інформатизації, в найближчій перспективі це стане основою Інформаційного кодексу України. Тому в цьому кодексі всі закони стосовно інформації та інформаційної діяльності мають бути зведені в один. Існують проекти Інформаційного кодексу України.

Так, О.А. Баранов пропонує за архітектонікою, типовою для національної юридичної доктрини, розділити цей акт кодифікації на Загальну (книга перша) та Особливу (книга друга) частини. При цьому книгу першу традиційно слід почати із загальних положень, де доцільно відобразити основи інформаційного законодавства, гарантії і захист прав та інтересів в інформаційній сфері, об'єкти і суб'єктів інформаційного законодавства, функції держави та її органів в інформаційній сфері, інформацію, основні положення про інформаційну інфраструктуру.

У книгу ж другу пропонується внести такі окремі частини: інформаційні відносини, загальні положення обігу та створення інформації, питання щодо поширення, використання, зберігання та знищення (утилізації) інформації. Завершити кодекс обґрунтовується розділом, де слід визначити правовий режим інформації: відкрита інформація, інформація з обмеженим доступом, інформація обмеженого використання, право власності на інформацію [18, с. 214–268].

Висловлюючись з цього приводу, зазначимо, що подібна конструкція є застарілою і недосконалою, оскільки вона вже не відповідає сучасним вимогам. Ми ж, у свою чергу, вважаємо за зручніше укладати кодекс із трьох основних частин: Загальної (основні інститути інфор-

маційного права), Особливої (правове регулювання окремих інформаційних галузей та інформаційно-інфраструктурних відносин) та Спеціальної (правові засади високих технологій та захисту інформації).

4 червня 2009 р. в Інституті законодавства Верховної Ради України відбувся «круглий стіл» на тему «Проблеми кодифікації інформаційного законодавства України». Метою обговорення його учасників було вирішення питань: національної політики розвитку інформаційного суспільства в Україні; сучасного стану кодифікації інформаційного законодавства; наукового забезпечення кодифікації інформаційного законодавства; пріоритетів законодавчого забезпечення інформаційних відносин в Україні.

Учасники «круглого столу» узагальнили свої думки щодо наукового забезпечення кодифікації інформаційного законодавства України, окреслили перспективні напрями його розвитку та висловили сподівання щодо подальшої співпраці з Інститутом законодавства Верховної Ради України з метою забезпечення правової системи України якісними нормативно-правовими актами [252].

Інформаційний кодекс України має об'єднати, гармонізувати та розвивати норми і принципи суспільних відносин, що визначені в законодавстві України; враховувати ратифіковані Україною міжнародні договори; легалізувати позитивні звичаї у сфері інформаційних відносин та норми суспільної моралі, загальнолюдські цінності, визначені в Статуті ООН, Декларації прав людини, Європейській конвенції про захист прав людини та основоположних свобод та інших загальноприйнятих міждержавних нормативних актах, які сьогодні виступають у ролі стандартів, що визначають цивілізованість світового співтовариства у цілому.

Отже, нині проект інформаційного кодексу формується як єдина довідково-правова система стосовно систематизації інформаційного законодавства, що містить нормативно-правові документи, матеріали судової практики, довідкові та консультаційні матеріали щодо питань застосування норм інформаційного права.

Таким чином, високотехнологічне інформаційне право охоплює пізнання нормативно-правових основ інформаційних правовідносин, що виникають у сфері високих технологій. Ґрунтуючись на аналізі викладеного, є сенс резюмувати, що високотехнологічне право —

основний нормативний регулятор інформаційних відносин найвищого (критичного) рівня, які виникають у сфері технологій нового покоління, де під останньою слід розуміти сукупність критичних технологій усіх видів.

1.3. Кримінально-правова політика у сфері високих інформаційних технологій

Поняття кримінально-правової політики

Складовою правової реформи в Україні є здійснення юридичної політики, під якою в теорії права розуміють ті принципи і цілі, які держава втілює в життя при створенні і застосуванні права, його норм у діяльності юридичних установ, формуванні та розвитку правосвідомості населення.

Юридична відповідальність є важливим елементом правового регулювання суспільних відносин у сфері обігу інформації з обмеженим доступом, сутність якого полягає в цілеспрямованому впливі на поведінку індивідів за допомогою юридичних засобів з метою впорядкування зазначених суспільних відносин, надання їм системності і стабільності, уникнення різких загострень соціальних конфліктів, утілення принципів соціальної справедливості тощо.

Виходячи із загального визначення юридичної політики, можна дати визначення і політики у сфері боротьби зі злочинністю: політика у сфері боротьби зі злочинністю визначає цілі, принципи, стратегію, напрями діяльності органів, які проводять дізнання, досудове слідство і оперативно-розшукову діяльність, її основні форми і методи.

Формування системи соціальної політики у сфері боротьби зі злочинністю передбачає пошук механізмів оптимального розподілу соціально-правової відповідальності поміж її основними суб'єктами. Звідси завдання державної політики в галузі розвитку нових інформаційних технологій полягають у тому, аби створити умови для виявлення цих внутрішньо диференційованих інтересів, оцінювання і акумуляції їх в єдиний спільний інтерес.

В юридичній і спеціальній літературі проблемам інформаційної безпеки та боротьби зі злочинами у сфері інформаційних технологій приділяється певна увага з боку таких учених, як: П. Д. Біленчук, М. С. Вертузаєв, Б. В. Вехов, О. Г. Волеводз, В. О. Голубєв, О. Ф. Долженков, В. В. Крилов, М. В. Салтевський, І. В. Сервецький та ін.

Політика у сфері боротьби зі злочинністю як антикримінальна діяльність держави реалізується в різних організаційно-правових формах. Кримінально-правова політика є однією з основних складових державної політики у сфері боротьби зі злочинністю [105, с. 673].

Кримінальний закон складається із сукупності систематизованих і окремих законодавчих актів, які визначають загальні принципи відповідальності. За допомогою юридичної відповідальності встановлюються механізми охорони і захисту суспільних відносин від неправомірних посягань шляхом покарання діянь, які порушують умови нормального розвитку суспільства, суперечать інтересам держави, суспільства і окремих індивідів.

Високі технології передавання інформації у сфері боротьби зі злочинністю структурно мають втілюватися в таких видах, що схематично показані нижче (схема 1.6).

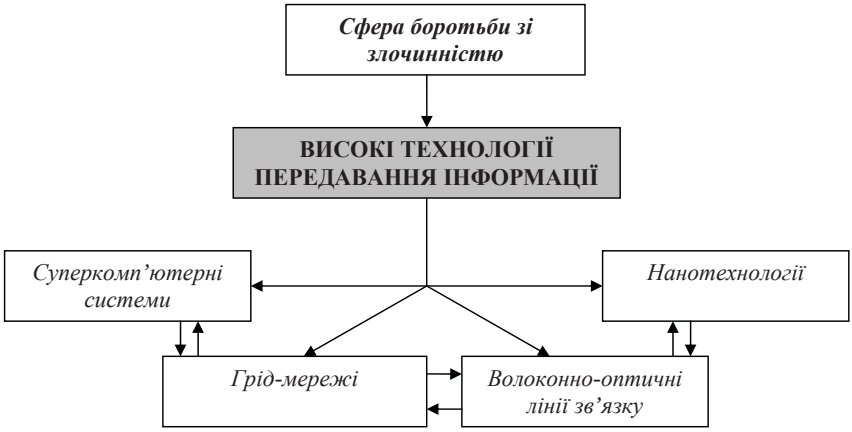


Схема 1.6

Таким чином, з одного боку, складовою частиною державної політики є інформаційна політика, а з другого — складовою частиною юридичної політики, здійснюваної в Україні, є політика у сфері боротьби зі злочинністю, яка формується законодавчою гілкою влади. Поряд з терміном «політика у сфері боротьби зі злочинністю» можливе застосування терміна «антикримінальна політика».

о ***Інформаційні правопорушення і злочини у сфері високих технологій***

Логічно визнати правову категорію правопорушень у сфері суспільних інформаційних відносин як «правопорушення, що вчиняються з використанням інформаційних технологій». Ми згодні з тим, що таке позначення є не дуже зручним для вживання у побутовій мові, тому можливе позначення «інформаційні правопорушення», тим більш, що об'єктом цієї категорії правопорушень є інформація та тісно пов'язані з нею технології її оброблення — інформаційні технології.

Предметом таких дій є інформація (інформаційні ресурси) та інформаційні технології, об'єктом — соціальні відносини щодо правового захисту майнових або суспільних інтересів держави, юридичних і фізичних осіб, а також їх прав і свобод в інформаційній сфері [22].

Отже, інформаційні правопорушення (правопорушення, що вчиняються з використанням інформаційних технологій) — це сукупність передбачених чинним законодавством суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну і повну інформацію.

Таким чином, нормативні визначення злочинів у сфері високих технологій, а звідси — й високотехнологічної злочинності відсутні. Утім, подібні терміни мають багатоаспектне застосування, що призвело, з одного боку, до розширення їх тлумачення, а з другого — до невиправданого звуження цієї сфери виключно до комп'ютерних злочинів.

о ***Злочинність у сфері високих технологій***

Відомо, що злочинність як негативне соціально-правове явище становить певну систему взаємопов'язаних елементів [105, с. 75].

Злочинність існує в суспільстві відносно самостійно, однак зі своїми закономірностями, кількісними та якісними характеристиками, що не притаманні її окремим елементам, і потребує специфічних державних і соціальних заходів контролю. Отже, злочинність — це системна сукупність злочинів.

Сучасний стан злочинності свідчить про те, що вона перетворилася на специфічну антисуспільну систему, яка досягла високого технологічного рівня.

Вид злочинності, який складається з категорії правопорушень, що вчиняються з використанням інформаційних технологій, сьогодні іменують по різному — «комп'ютерна злочинність», «кіберзлочинність» [224], «злочинність у сфері високих технологій», «е-злочини» та ін. І дійсно, адже з'явилися такі нові форми Інтернет-злочинності, як кадінг, атаки в мережі, Інтернет-шахрайство, кібертероризм тощо. Відповідно пов'язану із нею сукупність дій позначають як «комп'ютерні злочини», «кіберзлочини», «злочини у сфері високих технологій».

Інформаційна злочинність стає одним з найнебезпечніших соціально-правових феноменів сучасного світу. Комп'ютерна злочинність виступає складовою інформаційної злочинності і розуміється як сукупність комп'ютерних злочинів, де комп'ютерна інформація є предметом злочинних посягань, а також злочинів, які вчиняються за допомогою комп'ютерних засобів [105, с. 673].

Нині спеціальні дослідження проводяться щодо прогнозування розвитку комп'ютерної злочинності; планування заходів із запобігання та протидії комп'ютерній злочинності з конкретним визначенням цілей та завдань такої діяльності на найближчі роки [7, с. 26; 26, с. 320].

Поряд із цим високий динамізм розвитку інформаційних технологій, їх складність та безмежна сфера використання зумовлюють недостатню науково-теоретичну розробленість інформаційно-правової проблематики, чинної законодавчої бази та призводить до складностей у практичній діяльності правоохоронних органів.

Високотехнологічна злочинність — це системна сукупність двох груп злочинів: у сфері високих технологій та вчинених з використанням високих технологій. Високотехнологічна злочинність заподіює особливо загрозливі негативні для суспільства та людей наслідки, чого раніше з об'єктивних причин не було.

Звідси слід визнати, що людство ще залишається фактично не готовим до стрімкого оновлення злочинності і тому сьогодні вкрай необхідна модернізація існуючих державних, соціальних і технологічних заходів контролю.

У різних країнах ці питання вирішуються по-різному. Зокрема, у МВС України створено підрозділ по боротьбі зі злочинами у сфері високих технологій, єдиним напрямом якого є протидія злочинним проявам у сфері комп'ютерних технологій.

o ***Кримінальне право і право високих технологій***

Поняття кримінального права визначають як сукупність соціальних відносин, які дозволяють і забезпечують особі суспільну можливість жити, володіти та забороняти решті членів суспільства шкодити і руйнувати ці можливості. Звідси саме існування кримінального права як особливого регулятора суспільних відносин обумовлене необхідністю підтримувати соціальний порядок в інформаційному суспільстві, попереджаючи будь-які відхилення від встановлених правил поведінки.

З метою кращого розуміння проблеми співвідношення кримінального права з правом високих технологій потрібно відштовхуватися від змісту та обсягу терміна «високі технології».

Як уже зазначалося, високі технології — це найбільш прогресивні та наукомісткі технології промисловості, перехід до використання яких на сучасному етапі розвитку економіки є найважливішою ланкою науково-технічної революції. Більш того, перелік високих технологій не обмежується виключно комп'ютерними, а є суттєво розширеним. Звідси буде логічним правове уточнення обсягу поняття «високі технології».

У свою чергу право високих технологій регулює соціальні відносини, які виникають під час розроблення та впровадження високих технологій, тобто не обмежується правовою регуляцією соціальних відносин, що виникають виключно в інформаційній сфері.

Під високотехнологічним правом, або правом високих технологій, пропонується розуміти нормативно закріплені основні принципи дослідження, виробництва, організації та функціонування будь-яких передових технологій. Тобто, обсяг високотехнологічного інформаційного права не тотожний обсягу права високих технологій, оскільки останнє є правовим регулятором більш високого рівня. З цього стає зрозумілим співвідношення зазначених правових галузей як частини та цілого.

Прикладів злочинів, що вчиняються із застосуванням високих технологій, безліч: банківські системи безготівкових розрахунків [219], пластикові платіжні засоби [245], мобільний телефонний зв'язок [29], комп'ютерна злочинність [20; 243; 244] тощо. М. Стрельбицький, М. Вертузаєв, О. Юрченко та деякі інші дослідники як на шпальтах спеціальних видань, так і у відкритих засобах масової інформації, зазначали про це [220].

Звідси пропонуємо розділяти термін *«злочини у сфері високих технологій»* (*С* —) з терміном *«злочини, вчинені з використанням високих технологій»* (*С* +), яким може бути охоплено суттєво більший спектр злочинів, що дає підстави для такої юридичної комбінації:

$$C - \xleftarrow{1} \frac{A}{HT} \xrightarrow{2} C + \diagup 1 + 2 \ldots , \qquad (1.4)$$

де *А* — загальна множина злочинів; *НТ* — сфера високих технологій; 1+2 ... — інші види злочинів.

До першої групи злочинів можуть бути включені: порушення авторського права і суміжних прав (ст. 176 КК, розділ V), злочини проти безпеки виробництва (статті 271–275 КК, розділ X), пошкодження об'єктів магістральних нафто-, газо- та нафтопродуктопроводів (ст. 292 КК, розділ XI), порушення порядку здійснення міжнародних передач товарів, що підлягають державному експортному контролю (ст. 333 КК, розділ XIV), злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361–363[1] КК, розділ XIV), розробка, виробництво, придбання, зберігання, збут, транспортування зброї масового знищення (ст. 440 КК, розділ XX).

Друга група злочинів може включати значно більш широкий спектр кримінально караних діянь від злочинів проти громадської безпеки (наприклад, міжнародний нанотероризм, до розгляду чого ми ще повернемося) (розділ IX КК) до злочинів проти громадського порядку та моральності (наприклад, ввезення, виготовлення, збут і розповсюдження порнографічних предметів) (розділ XII КК), способи вчиненя яких ґрунтуються на високих технологіях.

Співвідношення злочинності двох видів — інформаційної та комп'ютерної, а також двох видів злочинів — у сфері високих технологій та вчинених з використанням високих технологій показано нижче (схема 1.7).

Схема 1.7

o ***Комп'ютерні злочини***

Сучасне інформаційне суспільство характеризується високим динамізмом розвитку інформаційних технологій, їх складністю та безмежною сферою використання. Це зумовлює недостатню науково-теоретичну розробленість чинної законодавчої бази щодо встановлення і притягнення до відповідальності за «комп'ютерні злочини», призводить до труднощів у практичній діяльності правоохоронних та судових органів.

Злочин — це передбачене КК України (ч. 1 ст. 11) суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом злочину [104]. З цього визначення випливають ознаки злочинів усіх видів: суспільна небезпечність, протиправність, винність, караність і наявність суб'єкта.

Стисло охарактеризуємо злочини, що посягають на відносини у сфері оброблення інформації в ЕОМ, автоматизованих системах,

комп'ютерних мережах і мережах електрозв'язку, права власності фізичних та юридичних осіб на інформацію і доступу до неї.

З огляду на зміст кримінально-правової характеристики злочинів у сфері інформаційних комп'ютерних технологій комп'ютер та його програмне забезпечення можуть бути як предметом злочину, так і засобом, за допомогою якого реалізовується задум злочинця [25, с. 5]. Повідомлення електрозв'язку, які розповсюджуються без попередньої згоди адресатів, серед користувачів інформаційних послуг отримали назву «спам» (spam), у зв'язку із чим останнім часом в юридичній літературі вже з'явилися наукові публікації з цього приводу.

Внесені законодавцем зміни до КК та КПК України від 23 грудня 2004 р. розширили можливість регулювати злочини у сфері високих технологій і уникнули прогалин та неточностей, які були допущені у першій редакції розділу XVI КК України [127, с. 16].

Суб'єктами відносин, пов'язаних з обробленням інформації в ЕОМ, автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, є: 1) власники інформації чи уповноважені ними особи; 2) власники технічних засобів автоматизованого оброблення чи уповноважені ними особи; 3) користувачі інформації; 4) користувачі технічних засобів автоматизованого оброблення.

Родовим об'єктом злочинів, передбачених розділом XVI Особливої частини КК України, є врегульовані законом суспільні відносини забезпечення безпеки автоматизованого оброблення інформації [104].

Додатковими обов'язковими об'єктами цих злочинів є відносини власності на інформацію, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, а також право користувачів на доступ до зазначеної інформації та користування нею.

Предметом комп'ютерних злочинів є: 1) інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами зв'язку; 2) технічні засоби автоматизованого оброблення та захисту інформації (елементи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку).

Інформація матеріалізується в носіях інформації, якими можуть бути фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах. Носіями інформації в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку виступають тверді фізичні об'єкти (жорсткі диски, дискети, компакт-диски та ін.), сигнали (у каналах зв'язку), поля (оперативна пам'ять ЕОМ та її периферійних пристроїв). Носії інформації можуть бути вилучені з володіння законного власника або пошкоджені чи знищені. Інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах, зберігається на носіях такої інформації у формі даних [25, с. 6].

Об'єктивна сторона злочинів у сфері використання ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку полягає в: 1) несанкціонованому втручанні в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 2) створенні з метою використання, розповсюдження або збуту, а також розповсюдженні або збуті шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; 3) несанкціонованому збуті або розповсюдженні інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства; 4) несанкціонованих діях з інформацією, яка оброблюється у ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку; 5) порушенні правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; 6) умисному масовому розповсюдженні повідомлень електрозв'язку, вчиненому без попередньої згоди адресатів [88].

Характерною особливістю розглядуваних посягань є те, що всі вони вчиняються шляхом активних дій. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизо-

ваних систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, може вчинятися шляхом бездіяльності.

Суб'єктом злочинів, передбачених статтями 361–363 [1] КК України, може бути фізична осудна особа, яка досягла 16-річного віку. Суб'єкт окремих злочинів — спеціальний. Ним може бути: 1) особа, яка не має права доступу до певної інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, або до технічних засобів її автоматизованого оброблення (ст. 361 КК); 2) особа, яка має право доступу до інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, у зв'язку із займаною посадою або спеціальними повноваженнями (ст. 362 КК); 3) неслужбова особа, яка належить до персоналу автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, тобто працівників, які перебувають у трудових відносинах з власником технічних засобів (уповноваженою ним особою чи розпорядником) та призначені для здійснення функцій управління і обслуговування ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363 КК).

Суб'єктом злочину, передбаченого ст. 363 КК України, може бути також будь-яка інша особа, яка відповідно до своїх трудових, службових обов'язків або на основі відповідної угоди з власником ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку виконує роботу, пов'язану з їх експлуатацією і зобов'язана при її виконанні дотримуватися встановлених правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також порядку та правил захисту інформації, яка в них оброблюється.

Суб'єктивна сторона злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку характеризується прямим умислом і, як правило, корисливим мотивом. Лише діяння, передбачене ст. 363 КК України, може вчинятися як умисно, так і через необережність.

Ознаками кваліфікованих видів злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж

і мереж електрозв'язку є вчинення таких діянь: 1) повторно; 2) за попередньою змовою групою осіб; 3) із заподіянням значної шкоди [25, с. 10–12].

Поняття значної шкоди є оцінною ознакою і потребує вирішення у кожному конкретному випадку з урахуванням усіх обставин справи та розміру матеріальних збитків. Значною шкодою у статтях 361–363[1] КК України, якщо вона полягає у заподіянні матеріальних збитків, уважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

У сфері використання ЕОМ у чинному КК України передбачено шість складів злочинів [104], що може бути схематично представлено таким чином (схема 1.8).

о ***Правові проблеми інсайдерської інформації***

На завершення викладення матеріалу розділу 1 стисло розглянемо особливості *інсайдерської інформації* (англ. *insider information*).

Власне термін «інсайдер» використовується у зв'язку із секретною, прихованою або закритою інформацією або знаннями. Адже загальнодоступною інформацією є інформація, що не потребує окремих привілеїв відносно доступу до неї. Звідси інсайдер — це член окремої групи осіб, які мають доступ до інформації, не доступної широкій публіці. Наголосимо, що «інсайдер» є нейтральним терміном, який залежно від контексту може мати як позитивний, так і негативний зміст.

У сучасному інформаційному світі поняття інсайдерських даних розповсюджено як джерело послідовного управління [254].

У широкому змісті інсайдерську інформацію визначимо як будь-яку важливу інформацію, що відома обмеженій кількості близьких до її джерел суб'єктів, зокрема відносно впровадження нових технологій, дострокове розкриття якої може викликати негативні наслідки.

З цього приводу виникає питання: чи надає підстави несанкціоноване передавання інсайдерської інформації щодо притягнення до юридичної відповідальності, адже в інформаційному законодавстві України таке поняття до цього часу відсутнє? Тому пропонуємо підготувати проект закону щодо внесення змін до КК України, що передбачають кримінальну відповідальність за використання інсайдерської інформації та маніпулювання цінами на фінансовому ринку.

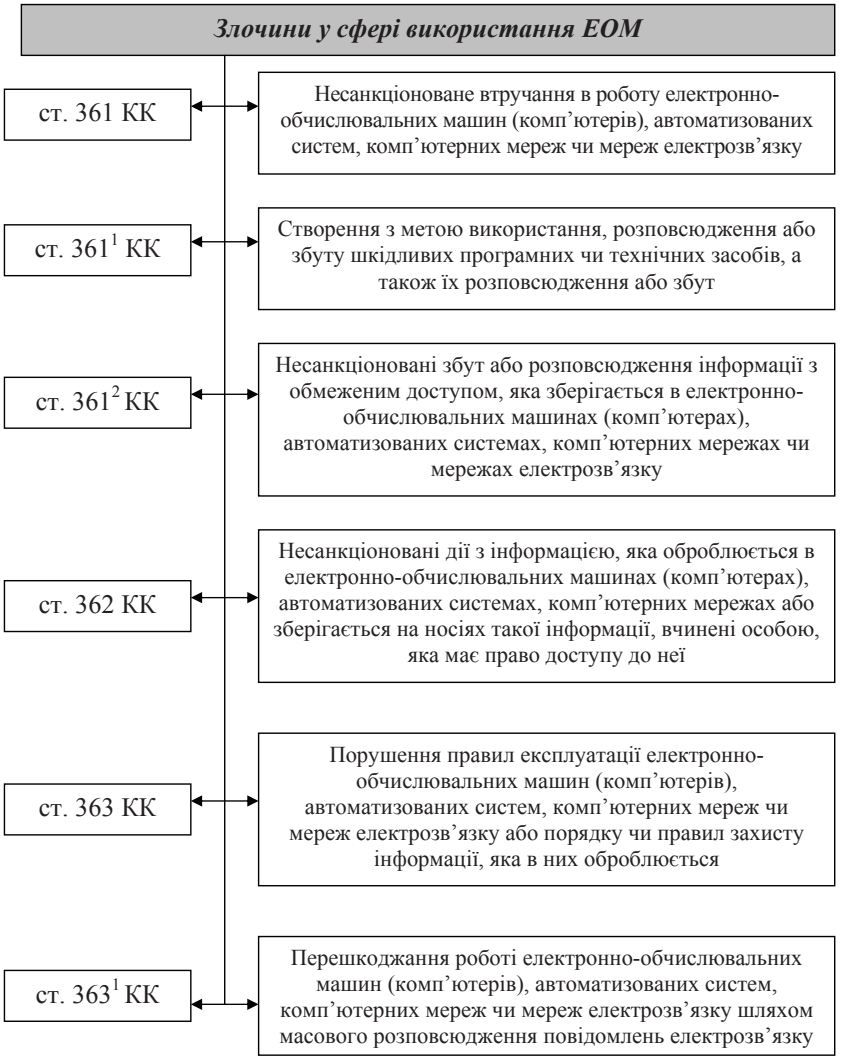


Схема 1.8

Таким чином, правові аспекти протидії використанню інсайдерської інформації остаточно не вирішено, а заходи відповідальності, що дотепер безсистемно використовуються у різному

ступені, не сприяють припиненню протиправної діяльності інсайдерів.

Викладене надає нам підстави щодо виведення складного співвідношення категорій *«правове забезпечення»* та *«високотехнологічне забезпечення»* у такий спосіб:

$$\frac{A}{B} \Leftrightarrow \frac{C}{D}, \tag{1.5}$$

де правове забезпечення інформаційного діяльності (A) виступає основним чинником інформаційної надійності, захищаючи інформаційну безпеку правовими засобами (B). Поряд із цим, високотехнологічне забезпечення правової діяльності (C) є компонентом процесу інформатизації, а звідси підвищує інформаційний рівень (D).

Нарешті, спробуємо вивести формулу змістовного співвідношення основних категорій:

$$\frac{X}{Y} \leq \frac{W}{Z}, \tag{1.6}$$

де інформаційне право (X) співвідноситься з правом високих технологій (Y) як менша частина правовідносин, що формуються у високотехнологічній сфері (W), основним регулятором яких виступає високотехнологічне інформаційне право (Z).

З цього можна припустити, що правове регулювання високих технологій входить до предмета інформаційного права, але разом із тим високотехнологічні інформаційні правовідносини є більш складними, а тому додатково потребують удосконалення особливостей механізму правової регуляції. Таким чином, правове регулювання високих технологій є предметом високотехнологічного інформаційного права.

Основні положення, що викладені у розділі 1 стосовно правового регулювання процесів розроблення, впровадження та використання нових технологій, у тому числі в інформаційній сфері, пропонується використати під час розроблення проекту Закону України «Про високі (прогресивні) технології».

Резюме. *Дослідження механізму державного регулювання високотехнологічних інформаційних правовідносин дає змогу визначити такі основні результати: 1) поняття інформація та високі технології постають як правові категорії; 2) розкрито статус інформаційних правовідносин, що виникають у високотехнологічній сфері; 3) з'ясовано місце високотехнологічної теорії інформаційного права в системі права України; 4) визначено об'єкти та суб'єктів високотехнологічного інформаційного права; 5) з'ясовано мету національної інформаційної політики; 6) висвітлено основні засади та принципи кримінально-правової політики у сфері високих інформаційних технологій; 7) визначено поняття злочинів та охарактеризовані їх окремі види у сфері високих технологій.*

Ключові слова*: інформація; інформатизація; інформаційна діяльність; високі технології; інформаційні технології; національна програма; державна політика; інформаційне право; право високих технологій; злочинність у сфері високих технологій.*

Контрольні запитання

1. Високотехнологічне інформаційне право як наука та навчальна дисципліна.
2. Місце високотехнологічного інформаційного права в системі права України.
3. Предмет та система високотехнологічного інформаційного права.
4. Функції та джерела високотехнологічного інформаційного права.
5. Поняття та основні напрями інформаційної діяльності.
6. Відмінність між поняттями «загальнодоступна інформація», «службова інформація» та «інсайдерська інформація».
7. Загальні засади здійснення інформаційної політики держави та шляхи формування транснаціонального інформаційного суспільства.
8. Характеристика понять «інформаційне суспільство» та «постіндустріальне суспільство».
9. Стратегії та основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки.
10. Державна програма інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою зі злочинністю.

11. Правовий зміст категорій «інформація», «інформатизація», «технологія», «інформаційна технологія» та «інформаційна система».
12. Поняття та види високих (прогресивних) технологій.
13. Співвідношення термінів «висока технологія» та «критична технологія» в інформаційній сфері.
14. Особливості формування правовідносин у сфері високих технологій.
15. Інформаційний кодекс України як кодифікаційний акт у галузі правового регулювання високих та інформаційних технологій.
16. Співвідношення кримінального права та права високих технологій.
17. Поняття та види злочинів у сфері високих технологій.
18. Структура та основні кількісно-якісні показники злочинності у сфері високих технологій.
19. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
20. Перспективи розвитку правових засад високих технологій в інформаційній галузі.

Розділ 2

Основи оптоволоконних телекомунікацій

У цьому розділі ...

- ***Телекомунікаційна мережа та види електронних інформаційних ресурсів.***

Сфера телекомунікацій ◄► Класифікація телекомунікацій ◄► Поняття та види телекомунікаційних послуг ◄► Суб'єкти ринку телекомунікаційних послуг ◄► Інформаційні ресурси та інформаційні продукти ◄► Інформаційні системи та процеси ◄► Компоненти інформаційної системи ◄► Нові інформаційні технології.

- ***Оптоволоконна система передавання інформації: історія і сучасність.***

Ретроспектива проблеми ◄► Оптичне волокно ◄► Оптоелектроніка і нановолокна ◄► Типи волоконно-оптичних кабелів ◄► Види волоконно-оптичних комунікацій.

- ***Організаційно-правові аспекти оптоволоконних телекомунікацій.***

Волоконна оптика і криміналістика ◄► Волоконно-оптичні лінії зв'язку і телекомунікаційна мережа правоохоронних органів ◄► Методи інформаційної безпеки та системи захисту інформації ◄► Інформаційна надійність оптоволоконних телекомунікацій.

2.1. Телекомунікаційна мережа та види електронних інформаційних ресурсів

о *Сфера телекомунікацій*

До телекомунікаційних систем належать: телеграф, телефон (у тому числі радіотелефон), радіо, супутниковий зв'язок, телекс, телебачення (у тому числі кабельне), комп'ютерні мережі тощо. У сфері передавання інформації для позначення телекомунікаційних засобів найчастіше використовуються такі терміни: «система», «мережа», «лінія», «магістраль», «коридор» та деякі інші.

З метою вирішення питання щодо співвідношення понять «телекомунікаційна мережа» і «телекомунікаційна система» потрібно визначити, що зазначені поняття можуть бути використані як тотожні, так і як частина та ціле. Зокрема, телекомунікаційна мережа може бути як повноцінною системою, так і підсистемою системи більш високого рівня; телекомунікаційна система завжди складається з однієї або декількох телекомунікаційних мереж.

Масова комунікація (англ. — *mass communications*) — це діяльність щодо трансляції, перенесення у практичну (масову) свідомість духовно-практичних цінностей у формі оцінок тих або інших соціальних груп суспільно значущих подій. Сьогодні термін «телекомунікації» означає здатність передавати текст, голос, зображення і навіть нематеріальні активи (грошові перекази) через мережі разом із функціональною інформацією, призначеною для управління комп'ютерними системами. Телекомунікаційні технології є одним з найбільш важливих чинників, які впливають на формування інформаційного суспільства.

Отже, масові комунікації здійснюються за допомогою технічних засобів і приймають вигляд публічного процесу виробництва інформації, її передавання засобами преси, радіо, телебачення та міжособистісного спілкування.

Сфера телекомунікацій — складова частина галузі зв'язку України. Телекомунікації є невід'ємною частиною виробничої та соціальної інфраструктур України і призначені для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах.

Закон України «Про телекомунікації» встановлює правову основу інформаційної та іншої діяльності у сфері телекомунікацій, а також визначає повноваження держави щодо управління та регулювання зазначеної діяльності, права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами.

Згідно з п. 38 ч. 1 ст. 1 Закону України від 24 червня 2004 р. «Про телекомунікації» термін «телекомунікації» означає передавання, випромінювання та (або) приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах [69]. Тобто,

телекомунікації — це процес дистанційного передавання даних на засадах інформаційних технологій.

о ***Класифікація телекомунікацій***

Розрізняють такі телекомунікації: а) *відомчі* — телекомунікації, які використовуються фізичними або юридичними особами для задоволення власних потреб; б) *загального користування* — телекомунікації, які використовуються для надання телекомунікаційних послуг усім користувачам; в) *подвійного використання* — відомчі або спеціальні телекомунікації, які, крім виконання своїх основних функцій, забезпечують надання телекомунікаційних послуг іншим користувачам; г) *спеціального призначення* — телекомунікації, які забезпечують передавання і приймання інформації з обмеженим доступом для потреб органів державної влади.

У техниці під зв'язком розуміється передавання інформації (сигналів) на відстань. *Передача даних* — це передавання інформації у вигляді даних з використанням телекомунікаційних мереж. Це поняття охоплює повний інформаційний цикл, де термін *«прийняття інформації»* є складовою позитивною частиною загального процесу передавання інформації. Закінчення такого циклу може також бути негативним у разі *«відмови від інформації»*. Крім цього, зустрічається третій нейтральний варіант — *«переадресація інформації»*. Схематично процес передавання інформації у сфері боротьби зі злочинністю може бути зображено таким чином (схема 2.1).

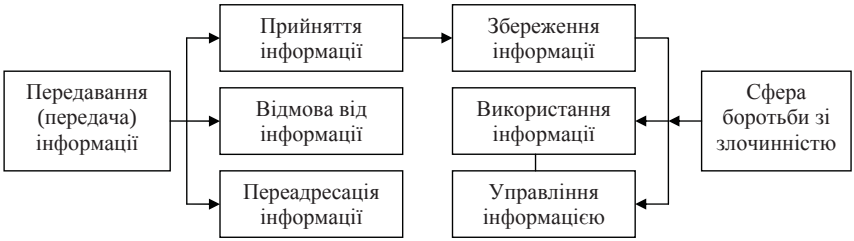


Схема 2.1

Держава гарантує універсальне обслуговування, тобто забезпечення універсального доступу споживачів до телекомунікаційних мереж загального користування та надання загальнодоступних теле-

комунікаційних послуг нормованої якості за регульованими державою тарифами.

Таким чином, телекомунікаційне передавання інформації — це новий крок у мультимедійних технологіях зв'язку. Висока якість зв'язку і повне екранне відеозображення, широкі можливості для роботи над різними проектами, оперативним обміном даними, документами тощо роблять телекомунікаційне передавання інформації потужним інструментом з широким спектром використання.

о ***Поняття та види телекомунікаційних послуг***

Основним об'єктом відносин у сфері телекомунікацій є телекомунікаційна послуга (послуга), тобто продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій.

Телекомунікаційні мережі — це комплекс технічних засобів телекомунікацій та споруд, призначених для обміну інформацією між комп'ютерними системами [145].

До загальнодоступних телекомунікаційних послуг належать: підключення кінцевого обладнання споживача до телекомунікаційних мереж загального користування (універсальний доступ), послуги фіксованого телефонного зв'язку в межах зони нумерації (місцевий телефонний зв'язок), а також виклик служб екстреної допомоги, послуг довідкових служб і зв'язку за допомогою таксофонів за винятком послуг, що надаються з використанням безпроводового доступу.

Відповідно до Правил надання та отримання телекомунікаційних послуг телекомунікаційні послуги поділяються на загальнодоступні (універсальні) та інші телекомунікаційні послуги. За ознаками надання телекомунікаційні послуги поділяються на основні та додаткові, що нерозривно пов'язані технологічно з наданням певних основних телекомунікаційних послуг. Перелік додаткових послуг визначається технічними можливостями обладнання операторів, провайдерів телекомунікацій.

У місцях з недостатнім рівнем насиченості телекомунікаційних мереж загального користування технічними засобами заяви на надання загальнодоступних телекомунікаційних послуг задовольняються в такій послідовності: 1) органи державної влади та органи місцевого самоврядування, Служба безпеки України, Служба зовнішньої розвід-

ки України та військові установи України; 2) медичні заклади, пожежні частини, організації, що надають інформацію про виникнення стихійних явищ (землетруси, повені, урагани тощо), державні дошкільні виховні та навчальні заклади, державні заклади науки і культури; 3) дипломатичні представництва та консульські установи іноземних держав; 4) громадяни, які відповідно до законодавства України мають право на отримання телекомунікаційних послуг на пільгових умовах; 5) підприємства, установи та організації, громадяни.

Використання ресурсів телекомунікаційних мереж загального користування для потреб телебачення та радіомовлення здійснюється на договірних засадах. Надання телекомунікаційних послуг для потреб телебачення і радіомовлення регулюється законами України «Про телебачення і радіомовлення» та «Про Національну раду України з питань телебачення і радіомовлення». Закон України «Про телекомунікації» визначає, що державне управління у сфері телекомунікацій здійснюють Кабінет Міністрів України, центральний орган виконавчої влади в галузі зв'язку, інші органи виконавчої влади відповідно до закону [69].

Метою стандартизації у сфері телекомунікацій є створення єдиної системи державних і галузевих стандартів та інших нормативних документів, які визначають вимоги до телекомунікаційних мереж, їх технічних засобів та якості телекомунікаційних послуг, а також гармонізація цих вимог з вимогами міжнародних нормативних документів [121].

о ***Суб'єкти ринку телекомунікаційних послуг***

Відповідно до ст. 1 Закону України «Про телекомунікації» суб'єктами ринку телекомунікацій є оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій.

Оператор телекомунікацій — суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж.

Іншим учасником відносин з надання телекомунікаційних послуг є провайдер телекомунікацій. Провайдер (англ. *InternetServiceProvider*, *ISP* — постачальник Інтернет-послуги) — організація, що надає послуги доступу до Інтернету та інші послуги, пов'язані з Інтернетом.

З юридичної точки зору Інтернет-провайдер, або просто провайдер, — це оператор зв'язку, який має ліцензію щодо виділення та надання каналів зв'язку та передавання даних. Серед провайдерів доступу можна виділити первинних (магістральних), що мають, власні магістральні канали зв'язку, та вторинних (міських), що орендують канали зв'язку у власників.

Провайдери надають телекомунікаційні послуги споживачам відповідно до законів України «Про телекомунікації», «Про захист прав споживачів», інших актів законодавства, Правил надання та отримання телекомунікаційних послуг та нормативних документів у сфері телекомунікацій. Законодавство України відносить провайдера телекомунікацій до осіб, що надають телекомунікаційні послуги, іншими словами, провайдер є виконавцем послуг. Провайдер телекомунікацій надає телекомунікаційні послуги на телекомунікаційних мережах оператора телекомунікацій [24, с. 72–76].

Отже, провайдер телекомунікацій — це суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.

o ***Інформаційні ресурси та інформаційні продукти***

У загальному розумінні під терміном «ресурс» або «ресурси» (від англ. *resource* — запаси чи багатство) розуміють засоби, що дозволяють за допомогою певних перетворень дістати бажаного результату.

Інформаційні ресурси — це організована сукупність інформації, інформаційних продуктів та інформаційних технологій, призначених для забезпечення визначених економічних, екологічних, фінансових, інформаційних та інших потреб людини, суспільства і держави.

Національні інформаційні ресурси призначено для забезпечення національних інтересів України, захисту інформаційних прав людини і основних свобод, інтересів суспільства, органів державної влади та органів місцевого самоврядування, юридичних осіб усіх форм власності.

Національні інформаційні ресурси є основою для забезпечення суверенітету та інформаційної безпеки держави, служать вирішенню завдань суб'єктів української економіки, науки, культури та інших сфер діяльності.

Складовими частинами національних інформаційних ресурсів є інформаційні ресурси різної належності та форми власності.

Національні інформаційні ресурси формують з інформаційних продуктів і інформаційних технологій (далі — інформаційний продукт).

Інформаційні продукти включають до складу національних інформаційних ресурсів на підставі експертизи відповідності їх властивостей вимогам задоволення потреб забезпечення національних інтересів України. Принципи і критерії визначення властивостей продуктів і технологій, порядок їх використання, а також порядок проведення експертизи затверджуються Кабінетом Міністрів України.

Згідно ст. 1 Закону України «Про Національну програму інформатизації» інформаційні ресурси — це сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних та ін).

Можна сказати і так: інформаційні ресурси — це сукупність інформаційних продуктів одного або декількох тематичних напрямів, що згруповані за змістом.

Інформаційні ресурси можна визначити й у такий спосіб — це організовані в базах і банках даних інформаційні продукти, що мають ретроспективний характер, необхідні для задоволення інформаційних потреб людини, суспільства і держави.

Інформаційний продукт — це: а) документована інформація, що підготовлена і призначена для задоволення потреб користувача; б) інформаційний продукт — це об'єктивно закріплена на носії інформація, підготовлена для споживання, автоматизованого оброблення та поширення за допомогою мереж передавання даних; в) інформаційний продукт — це результат інформаційної діяльності, процес матеріалізації створюваної продукції.

До складу національних інформаційних ресурсів включають: а) в обов'язковому порядку — інформаційні продукти, створені органами державної влади та органами місцевого самоврядування в порядку здійснення основної діяльності цих органів; б) на умовах державного замовлення — після завершення виконання такого замовлення або відповідного його етапу; в) як похідний результат інших робіт, що виконують із залученням державного бюджету — після завершення виконання таких робіт або їх окремих етапів; г) на основі угоди з власником або виробником — інформаційні продукти, створені за ра-

хунок позабюджетних коштів їх власників або виробників. Включення цих продуктів до складу національних інформаційних ресурсів не призводить до зміни їх власника, якщо інше не передбачено законом або умовами угоди; ґ) на основі відповідних міждержавних або міжнародних угод — міждержавні та міжнародні інформаційні продукти.

Інформаційні продукти, надані в електронному вигляді, розміщують в електронному депозитарії (депозитаріях). Включення інформаційних продуктів до складу національних інформаційних ресурсів фіксується шляхом обов'язкового внесення їх реквізитів до національного електронного реєстру інформаційних ресурсів України. З цього моменту вони вважаються складовими частинами національних інформаційних ресурсів.

Інформаційні продукти вилучають зі складу національних інформаційних ресурсів у тому разі, коли вони перестають відповідати існуючим вимогам щодо якісних характеристик, засобів доступу або коли в них зникає потреба.

Складання переліку інформаційних продуктів, що підлягають вилученню зі складу національних інформаційних ресурсів, здійснюється на підставі експертизи відповідності цих інформаційних продуктів зазначеним вимогам.

Вилучення інформаційних продуктів зі складу національних інформаційних ресурсів фіксується шляхом обов'язкового вилучення їх реквізитів з електронних реєстрів. З цього моменту вони перестають бути складовими частинами національних інформаційних ресурсів.

Електронні інформаційні ресурси — це інформаційні ресурси, розміщені в електронних базах або банках даних, у комп'ютерних системах, системах автоматизованого оброблення і передавання даних. Якщо ці ресурси одержують або передають за допомогою Інтернету, то їх називають веб-ресурсами (від поняття — WWW — «всесвітня павутинна комунікація»).

Веб-ресурси — це інформаційні ресурси у вигляді одного або декількох веб-сайтів. Веб-ресурси можуть бути об'єктами всіх форм власності, договірних відносин відповідно до положень цивільного законодавства і законодавства про інтелектуальну власність [27]. Веб-ресурси можуть використовуватися їх власниками або іншими уповноваженими особами (власниками) з будь-якими цілями, не забороненими законом.

Веб-сайт загального інформаційного змісту не повинен містити персональні дані або інформацію, що становить державну таємницю, та іншу інформацію, що обмежена в поширенні відповідно до закону.

Інформаційні продукти з обмеженим доступом можуть утримуватися на веб-сайті чи іншому інформаційному ресурсі лише за згодою відповідних державних органів чи зацікавлених осіб або їх законних представників.

Власник або власник ресурсу в разі заподіяння йому моральної чи матеріальної шкоди шляхом поширення веб-ресурсом негативної інформації про нього має право на повне відшкодування шкоди. Власник веб-ресурсу або інша уповноважена особа може зареєструвати належний йому інформаційний ресурс як засіб масової інформації. Суб'єкт, що реєструє засіб масової інформації, визнається його засновником і власником. Засіб масової інформації у зв'язку з використанням телекомунікаційних мереж підлягає обов'язковому державному обліку і реєстрації відповідно до порядку, встановленому Кабінетом Міністрів України для друкованих засобів масової інформації.

Інформаційні ресурси можуть бути власністю громадян України, іноземних громадян і осіб без громадянства, органів державної влади та органів місцевого самоврядування, організацій і об'єднань громадян. Право власності на інформаційні ресурси регулюється законодавством України з питань власності, інтелектуальної власності і захисту персональних даних. Крім того, інформаційні ресурси можуть належати до різних форм власності, виступати як товар і бути об'єктами товарних відносин, що регулюються чинним законодавством, за винятком випадків, передбачених законодавством України і відповідними міжнародними договорами України.

Отже, з огляду на наведене пропонуємо визначати інформаційні ресурси як сукупність окремих документів, загальних і спеціалізованих масивів даних в інформаційних системах різного призначення (бібліотеках, архівах, інформаційних фондах, банках даних, інших інформаційних системах) та необхідних технічних засобів для оперативного задоволення інформаційних потреб суб'єктів інформаційних правовідносин.

Підсумовуючи викладене, слід наголосити на тому, що інформаційні ресурси мають свою специфіку: 1) вони не споживані і підда-

ються не фізичному, а моральному зношенню; вони не матеріальні і не залежать від носія інформації; 2) їх використання дозволяє набагато знизити витрати інших видів ресурсів, що веде до значної економії коштів; 3) процес їх створення та використання здійснюється особливим способом — за допомогою комп'ютерної техніки.

о ***Інформаційні системи та процеси***

Для того щоб інформаційне забезпечення діяло, треба створити відповідну інформаційну систему.

Інформаційна система — це взаємопов'язана сукупність засобів, методів і персоналу, що використовуються для зберігання, оброблення та видавання інформації в інтересах досягнення поставленої мети.

Сучасне розуміння інформаційної системи передбачає використання як основного технічного засобу перероблення інформації комп'ютерної техніки. Крім того, технічне втілення інформаційної системи саме по собі нічого не означатиме, якщо не враховано роль людини, для якої призначена вироблена інформація і без якої неможливі її одержання та подання [23, с. 34].

Необхідно також розуміти різницю між комп'ютерами та інформаційними системами. Комп'ютери, оснащені спеціалізованими програмними засобами, є технічною базою та інструментом для інформаційних систем. Виходячи з попередніх міркувань, можна дати сучасне визначення інформаційної системи як системи інформаційного обслуговування, що являє собою організаційно впорядковану сукупність інформаційних ресурсів, технічних засобів і технологій, які реалізують інформаційні процеси в традиційному або автоматизованому режимі для задоволення інформаційних потреб користувачів.

Робота інформаційної системи полягає в обслуговуванні двох зустрічних потоків інформації: введення нової інформації і видавання поточної інформації на запит.

Процес інформаційного пошуку включає послідовність операцій, що спрямовані на збирання, оброблення та надання необхідної інформації. Процеси, що забезпечують роботу інформаційної системи будь-якого призначення, умовно можна представити у вигляді схеми, що складається із блоків: 1) введення інформації із зовнішніх або внутрішніх джерел; 2) оброблення вхідної інформації та подання її у зручному вигляді; 3) виведення інформації для

представлення її у зручному вигляді; 4) зворотний зв'язок — інформацію перероблено людьми даної організації для корекції вхідної інформації (схема 2.2).

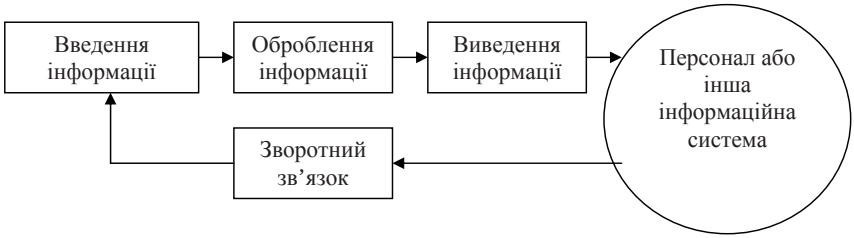


Схема 2.2

У загальному розумінні процес є послідовною зміною станів об'єкта у часі. Відомо, що галузей матеріального права існує набагато більше, ніж процесуальних. Сьогодні ще немає юридичної науки інформаційного процесу у значенні, наприклад, кримінального чи цивільного процесу. Тому інформаційно-правова діяльність у разі відсутності «власного» процесуального права неминуче здійснюється за процедурами одного з існуючих юридичних процесів.

Юридичний процес — це врегульований процесуальними нормами порядок діяльності компетентних державних органів, що полягає у підготуванні, прийнятті та документальному закріпленні юридичних рішень загального або індивідуального характеру. Оскільки юридичний процес фактично є комплексним утворенням, він включає п'ять самостійних процесів: конституційний, кримінальний, цивільний, господарський та адміністративний [110].

Звідси термін «інформаційний процес» можна тлумачити у трьох основних значеннях: 1) *юридичний аспект* — під час виконання інформаційних процесів виникають суспільні відносини, що підлягають правовому регулюванню в інформаційній сфері (точка зору інформаційного права), тобто являє собою правовий механізм вирішення інформаційних питань; 2) *соціотехнологічний аспект* — модернізація процесів програмного забезпечення та технологічного обміну інформацією (точка зору інформатики), тобто фактично являє собою інформатизацію; 3) *комунікативний аспект* — процеси та механізми міжособистісного та міжгрупового спілкування (точка зору соціальної психології).

Отже, інформаційний процес — це процес одержання, створення, збирання, оброблення, накопичення, зберігання, пошуку, поширення та використання інформації. Слід відзначити, що найважливіші особливості юридичного процесу полягають у тому, що він містить як різні правові процедури, так і судові процеси (судочинства). Таким чином, інформаційний процес у правовому аспекті спрямовано на реалізацію норм інформаційного права, при цьому він залишається врегульованим процесуальними нормами інших галузей права.

o ***Компоненти інформаційної системи***

Структуру інформаційної системи складає сукупність окремих її компонентів, які називають підсистемами. Підсистема — це частина системи, виділена за будь-якою ознакою. Загальну структуру інформаційної системи можна розглядати як сукупність підсистем незалежно від сфери застосування. У цьому разі говорять про структурну ознаку класифікації, а підсистеми називають забезпечуючими.

Структура будь-якої інформаційної підсистеми може бути схематично представлена сукупністю забезпечуючих підсистем. Серед останніх звичайно виділяють інформаційне, технічне, математичне, програмне, організаційне та правове забезпечення [23, с. 188].

Інформаційні підсистеми як головні складники інформаційного забезпечення призначені для збирання, накопичення, зберігання, оброблення та передавання інформації певних напрямів правової діяльності й орієнтовані на загальне використання галузевими службами, мають загальновідомчий характер і належать до службових інформаційних підсистем.

Інформаційна мережа створюється за територіальним принципом і має трирівневу структуру: 1) центральна інформаційна мережа; 2) регіональні інформаційні мережі; 3) територіальні інформаційні мережі.

Регіональні інформаційні мережі забезпечують інформаційну взаємодію між галузевими службами, територіальними і центральними інформаційними мережами. Територіальні інформаційні мережі є складниками регіональних мереж і забезпечують інформаційну взаємодію між територіальними підрозділами.

Компоненти інформаційної системи показано нижче у схематичному вигляді (схема 2.3):

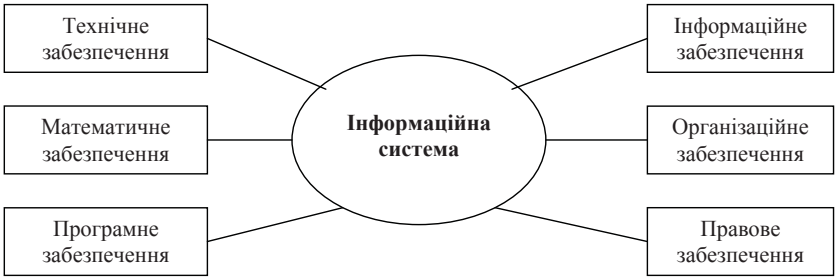


Схема 2.3

Оскільки головне завдання інформаційної системи — обслуговування клієнтів, то її побудовано таким чином, щоб відповідь на будь-яке запитання видавалася швидко і була достатньо повною. Це забезпечується наявністю стандартних процедур пошуку інформації і тим, що дані системи розташовано в певному порядку [23, с. 187].

Універсальний доступ до інформаційної системи має відповідати таким вимогам: 1) забезпечення за вимогою споживача з'єднання його кінцевого обладнання з телекомунікаційними мережами загального користування за регульованими державою тарифами; 2) телекомунікаційні мережі загального користування, до яких підключається кінцеве обладнання споживачів, повинні забезпечувати підтримання голосової телефонії (здійснення і одержання зонових, міжміських, міжнародних дзвінків), факсимільний зв'язок, передавання даних на рівні, достатньому для доступу споживачів до мережі Інтернет; 3) при забезпеченні універсального доступу вартість підключення до телекомунікаційної мережі загального користування не залежить від технології доступу або способу підключення.

Отже, системне співвідношення основних складових компонентів визначимо таким чином:

$$\frac{1(a+b...)}{2(c+d...)} \prec 3 \mapsto 4 \,. \tag{2.1}$$

Це означає, що інформаційні продукти (2) є складовою частиною інформаційних ресурсів (1), а останні, у свою чергу, створюють ін-

формаційні системи (3) для функціонального забезпечення інформаційних процесів (4).

Слід наголосити на тому, що інформаційні системи і технології широко впроваджуються в юридичній діяльності [44], до прикладів чого далі ми ще повернемося.

o ***Нові інформаційні технології***

Інформаційні технології — це цілеспрямовано організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечує продуктивні оброблення даних, пошук та розміщення інформації, доступ до її джерел незалежно від місця розміщення.

Нова інформаційна технологія базується на трьох основних принципах: 1) інтерактивний (діалоговий) режим роботи з комп'ютером; 2) інтегрованість (стикування, взаємозв'язок) з іншими програмними продуктами; 3) гнучкість процесу зміни як даних, так і постановок завдань [23, с. 199].

До поняття нової інформаційної технології включено також комунікаційні технології, які забезпечують передавання інформації різними засобами.

За класами реалізованих технологічних операцій інформаційні технології розглядаються у програмному аспекті і включають: оброблення текстів, електронні таблиці, автоматизовані бази (банки) даних, оброблення графічної та звукової інформації, мультимедійні та інші системи [86].

Програмно-технічна організація обміну з комп'ютером текстовою, графічною, аудіо- та відеоінформацією одержала назву *мультимедіатехнології*. Таку технологію реалізують спеціальні програмні засоби, що мають вбудовану підтримку мультимедіа та дозволяють використовувати її в професійній діяльності, навчально-освітніх, науково-популярних та ігрових галузях.

При застосуванні цієї технології в професійній діяльності відкриваються реальні перспективи використати комп'ютер для озвучування зображень, а також розуміння ним людської мови, ведення комп'ютером діалогу з спеціалістом його рідною мовою. Здатність комп'ютера з голосу сприймати нескладні команди керування програмами, відкривання файлів, виведення інформації на друк та іншими

операціями створює сприятливі умови для взаємодії з ними в процесі професійної діяльності [23, с. 201].

Мобільний зв'язок третього покоління ґрунтується на пакетному передаванні інформації. Слід визначити, що технології мобільного зв'язку 3G (від англ. *third generation* — третє покоління) являють собою набір послуг, які поєднують як високошвидкісний мобільний доступ із послугами Інтернет-мережі, так і технологію радіозв'язку. Цим подібні телекомунікаційні технології забезпечують еволюційний перехід від вузькополосних систем з кодовим розподілом каналів до систем зв'язку третього покоління, по суті створюючи новий інформаційний канал передавання даних. На теперішній час найбільш поширені два стандарти, що дає змогу організовувати відеотелефонний зв'язок, дивитися на мобільному телефоні фільми і телепрограми тощо. Крім того, мережі 3G характеризуються підвищеною екологічною безпекою [255].

Треба зазначити, що терміни «технологія зв'язку» і «сучасна технологія зв'язку» не зовсім чітко передають зміст тієї предметної галузі, яку вони покликані позначати. Тому дослідники пропонують вживати термін «телекомунікаційна технологія» [239, с. 103–108].

Отже, для позначення інформаційно-телекомунікаційних технологій, що мають суттєву специфіку застосування в окремих видах діяльності (наприклад, у правоохоронній та військовій сферах, державному управлінні тощо), доцільно використовувати термін «спеціальні інформаційно-телекомунікаційні технології».

Таким чином, нова інформаційна технологія — це технологія, яка засновується на застосуванні комп'ютерів, активній участі користувачів (непрофесіоналів у галузі програмування) в інформаційному процесі, високому рівні інтерфейсу користувача, широкому застосуванні пакетів прикладних програм загального та проблемного призначення, ефективному постійному доступі користувача до віддалених баз даних та програм завдяки сучасним обчислювальним мережам.

Сучасний розвиток оптичних інформаційних та телекомунікаційних технологій ґрунтується на досягненнях когерентної оптики плівкових та волоконних структур, що потребує окремого висвітлення загальних засад оптоволоконної системи передавання інформації.

2.2. Оптоволоконна система передавання інформації: історія і сучасність

o ***Ретроспектива проблеми***

Явище розповсюдження промінів світла по прозорих циліндрах шляхом повного внутрішнього відбиття відомо здавна. Історію систем передавання даних на значні відстані слід розпочинати з давнини, коли для передавання інформації люди використовували димові сигнали. Відтоді ці системи кардинально змінилися, з'явилися спочатку телеграф, потім — коаксиальний кабель. У своєму розвитку ці системи рано чи пізно досягли фундаментальних обмежень: для електричних систем це явище послаблення сигналу на певній відстані, для НВЧ — носійна частота. Тому тривали пошуки принципово нових систем, і у другій половині XX ст. рішення було знайдено — виявилося, що передавання сигналу за допомогою світла набагато ефективніше.

Уперше проходження світла шляхом повних внутрішніх відбиттів було продемонстровано Джоном Тіндалем у Королівському товаристві в Англії в 1870 р., де він використав освітлювану світлом посудину з водою і показав, що коли струмінь води проходив через отвір у стінці посудини, світло розповсюджувалось за шляхом струменя.

Можливість практичного передавання світла по прозорих трубах була доведена В. М. Чиколевим у 1888 р., однак штучно-елементне передавання зображень завдяки світоводам в оптичних та електронноптичних приладах була реалізована лише через 70 років.

Явище, описане Тіндалем, було забуто до 1927 р., коли Байрд в Англії і Ханзел у США розглянули можливість використання скляних волокон без оболонки в телебаченні для передавання і відтворення зображення. Однак їх ідея залишилася нездійсненою. У 1930 р. Ламм у Німеччині на системі із кварцових волокон продемонстрував можливість передавати світло і зображення. Результати його експерименту також не знайшли практичного застосування.

Новий імпульс розвитку волоконна оптика одержала у другій половині XX ст., коли з 1956 р. було впроваджено термін «волоконна оптика».

Лазер (англ. *laser* від *Light Amplification by Stimulated Emission of Radiation* — підсилення світла за допомогою змушеного випромінювання) — устрій, що використовує квантовомеханічний ефект змушеного випромінювання когерентного променя світла. Винахід лазера Мейменом у 1960 р. суттєво вплинув на розвиток сучасної науки і техніки. Лазери здійснили мрію людей і спонукали до інтенсивних досліджень оптичного зв'язку, який на сьогодні став реальністю. Лазери широко поширено в системах оптичного зв'язку та оброблення інформації, в яких сполучаються принципи волоконної та інтегральної оптики [2]. Це ілюструє й той факт, що вже протягом декількох років інтенсивно розроблюються квантові генератори коливань носійної частоти для передавання інформації — найважливіші елементи систем зв'язку.

Бурхливому розвитку наукових досліджень і розробок у галузі оптичного зв'язку сприяли: поява напівпровідникових лазерів, що нині досягли стадії практичного застосування; можливість виробництва волоконних світловодів з наднизькими загасаннями у найбільш оптимальному діапазоні довжин хвиль. У 1966 р. Као і Хокман із STC Laboratory (STL) продемонстрували оптичне волокно зі скла, яке мало загасання в 1000 Дб/км (у той час як загасання в коаксіальному кабелі становило всього 5–10 Дб/км) завдяки домішкам, які в ньому утримувалися.

Існували дві глобальних проблеми при розробленні оптичних систем передавання даних: джерело світла і носій сигналу. Перша розв'язалася з винаходом лазерів у 1960 р., друга — з появою високоякісних ВОЛЗ у 1970 р. Це була розробка Corning Glass Works. Загасання в таких кабелях становило близько 20 Дб/км, що було цілком прийнятним для передавання сигналу в телекомунікаційних системах. У той же час було розроблено досить компактні напівпровідникові GaAs-лазери.

Після інтенсивних досліджень у період з 1975 по 1980 р. з'явилася перша комерційна оптоволоконна система, що оперувала світлом з довжиною хвилі 0,8 мкм і використовувала напівпровідниковий лазер на основі арсеніду галію (GaAs). Продуктивність систем першого покоління складала 45 Мбіт/с, відстань між повторювачами — 10 км.

22 квітня 1977 р. в Лонг-Біч, штат Каліфорнія, компанія General Telephone and Electronics уперше використала оптичний канал для передавання телефонного трафіку на швидкості 6 Мбіт/с.

Друге покоління оптоволоконних систем було розроблено для комерційного використання на початку 80-х років XX ст. Вони оперували світлом з довжиною хвилі 1,3 мкм від InGaAsP-лазерів. Однак обмеженням таких систем були втрати, що виникають в каналі. Але вже у 1987 р. ці системи працювали на швидкості до 1,7 Гбіт/с при відстані між повторювачами 50 км.

На початку 80-х років XX ст. основними сферами застосування ВОЛЗ стали телефонна мережа, кабельне телебачення, внутрішньооб'єктовий зв'язок, обчислювальна техніка, система контролю та управління технологічними процесами та ін. [142].

Перший трансатлантичний телефонний оптоволоконний кабель — ТАТ-8 було уведено в експлуатацію в 1988 р. У його основі лежала оптимізована технологія Desurvire посилення проміння. ТАТ-8 розроблявся як перший підводний оптоволоконний кабель між Сполученими Штатами Америки і Європою [62].

Основним матеріалом волоконно-оптичної лінії зв'язку є оптоволокно. Сьогодні воно використовується як середовище передавання на телекомунікаційних мережах різних рівнів: від міжконтинентальних магістралей до домашніх комп'ютерних мереж.

При оптоволоконній технології передавання даних як середовище використовується кварцовий скляний або пластиковий кабель (*fibre cable*). Кабелі на базі оптичних волокон, які використовуються у волоконно-оптичному зв'язку, дозволяють передавати інформацію на значні відстані з більш високою швидкістю передавання даних, ніж електронними засобами зв'язку.

Таким чином, оптоволоконний зв'язок — це вид зв'язку, що використовує як носій інформаційного сигналу електромагнітне випромінювання оптичного діапазону з використанням волоконно-оптичних кабелів. Завдяки високій носійній частоті і широким можливостям мультиплексування пропускна здатність волоконно-оптичних мереж багаторазово перевищує пропускну здатність усіх інших систем зв'язку і може вимірюватися терабітами в секунду. Мале загасання світла в оптичному волокні сприяє можливості застосування

волоконно-оптического зв'язку на значних відстанях без використання підсилювачів.

о ***Оптичне волокно***

Таким чином, у волоконно-оптичних мережах зв'язку інформація передається за оптичними діелектричними хвилеводами відомим під назвою «оптичне волокно».

Оптичне волокно вважається оптимальним фізичним середовищем для передавання інформації, а також найбільш перспективним середовищем для передавання значних потоків інформації на значні відстані. Підстави для цього випливають з особливостей, притаманних оптичним хвилеводам.

Фактично оптичне волокно є ниткою з оптично прозорого матеріалу (скло, пластик) використовується для перенесення світла усередині себе за допомогою повного внутрішнього відбиття.

Оптичне волокно має круглий перетин і складається із двох частин — серцевини і оболонки. Для забезпечення повного внутрішнього відбиття абсолютний показник переломлення серцевини трохи вище показника переломлення оболонки. Наприклад, якщо показник переломлення оболонки дорівнює 1,474, то показник переломлення серцевини — 1,479.

Промінь світла, спрямований у серцевину, поширюватиметься по ній, випробовуючи багаторазові відбиття від межі серцевина-оболонка. Оптичні волокна, які використуються в телекомунікаційній сфері, мають діаметр 125±1 мікронів. Діаметр серцевини може відрізнятися залежно від типу волокна і національних стандартів.

Основним елементом таких кабелів є оптичне волокно, що буває декількох видів: 1) полімерне оптичне волокно; 2) скловолокно із високоякісного кварцового скла з захисним полімерним покриттям; 3) скловолокно із чистого високоякісного кварцового скла.

Для використання в промислових умовах ринок пропонує волоконно-оптичні кабелі, виконані з полімерного оптичного волокна і скловолокна, а також комбіновані кабелі з мідними жилами.

Оптоволоконний (волоконно-оптичний) кабель — це принципово інший тип кабелю порівняно з електричним або мідним кабелем. Носієм інформації в ньому є світло.

Металева оплітка кабелю звичайно відсутня, оскільки екранування від зовнішніх електромагнітних перешкод тут не потрібно, однак іноді її все ж таки застосовують для механічного захисту від навколишнього

середовища (такий кабель іноді називають броньовим, він може поєднувати під однією оболонкою декілька оптоволоконних кабелів).

Волоконно-оптичний зв'язок вільний від електромагнітних перешкод і недоступний для несанкціонованого використання — перехопити сигнал, переданий по оптичному кабелю, неможливо без його руйнування.

о ***Оптоелектроніка і нановолокна***

Оптоелектроніка являє собою розділ науки і техніки, в якому вивчаються питання генерації, розповсюдження, перетворення та зберігання інформації на основі спільного використання електричних і оптичних методів [236]. Сучасна оптоелектроніка базується на досягненнях низки галузей науки і техніки, серед яких насамперед має бути виділена напівпровідникова і квантова електроніка. У своєму розвитку оптоелектроніка, з одного боку, доповнює сучасну електроніку, а з другого — поступово здобуває все більше самостійне значення.

Елементна база сучасної оптоелектроніки досить різноманітна і містить такі основні групи приладів: 1) оптовипромінювачі: лазери і світловипромінюючі діоди; 2) фотоелектричні приймачі випромінювання (фотоприймачі): фоторезистори, фототранзистори, фототиристори; 3) прилади, що керують випромінюванням для відображення інформації — індикатори, індикаторні панелі; 4) прилади для електричної ізоляції — оптрони; 5) оптичні канали зв'язку та передавання інформації — волоконно-оптичні світловоди.

Основу будь-якої оптоелектронної системи становлять оптовипромінювачі, які підрозділяються на джерела когерентного і некогерентного випромінювання. Пристрої когерентної (лазерної) і некогерентної оптоелектроніки відрізняються один від одного принципом генерації, поширення та реєстрації сигналів [236, с. 3–10].

Таким чином, оптоелектроніка є якісно новим етапом у розвитку електронно-інформаційних технологій, які є розділом науки і техніки, і вивчає як оптичні, так і електронні явища в речовинах, їх взаємозв'язки і перетворення, а також прилади, схеми та системи, створені на основі цих явищ.

Забігаючи уперед, звернемо увагу на те, що нанотехнологія — це застосування нанонауки до технологічних пристроїв, про що йтиметься далі. У цій частині потрібно відзначити, що на основі останніх

міждисциплінарних досягнень виникла нова галузь науки і техніки — наноелектроніка [120].

Зазначений науково-технічний напрямок пов'язаний з дослідженням структур з розмірним квантуванням, створеним штучно у твердому тілі, а також з дослідженням нового класу матеріалів, що являють собою макроскопічні ансамблі металевих наночасток, наночасток напівпровідників або діелектриків, шаруватих наносистем, молекулярних наноплівок, розміри яких коливаються від 1 до 10 нм. У цих наносистемах виявлено низку унікальних сполучень оптичних властивостей [157, с. 13]. Інтенсивні дослідження таких наносистем стимулюються як відкриттям низки принципово нових фундаментальних явищ, так і наявністю широких прикладних можливостей.

У надрах сучасної оптоелектроніки розпочався розвиток інтегральної оптики (нанооптоелектроніки) [120]. Безпосереднім поштовхом до зародження цього напрямку послужили проблеми побудови систем оптичного зв'язку. Дискретні елементи таких систем (лазер, приймач, лінзи, дзеркала тощо) з'єднуються суто зовнішнім чином, інформація оброблюється в електричних каналах. Завданням інтегральної оптики є виключення подвійного перетворення сигналу (оптичного в електричний і навпаки), тобто використання як носія інформації безпосередньо оптичного сигналу. Елементи пристроїв інтегральної оптики повинні виготовлятися на загальній підкладці в єдиному технологічному процесі подібно нано- і мікроелектронним пристроям [2].

Слід відзначити, що пропускна спроможність оптоволокон ще не наблизилася до жодної внутрішньої межі, але вона стримується пропускною спроможністю електроніки з обох кінців проводу. Для додаткового ущільнення інформаційних сигналів нанонаука та нанотехнології активно пропонують ефективні оптоволоконні структури. Так, внутрішнє волокно повинно мати мінімальні втрати щодо розсіювання та може навіть легуватися наноструктурами для відновлення сигналів, що загасають. Подібні перешкоди можуть бути усунені шляхом побудови невеликих (наноскопічних) оптичних пристроїв, що дозволяють маніпулювати світловими сигналами [176, с. 170–171].

Нановолокна традиційно визначаються як циліндричні структури із зовнішнім діаметром менше 1,000 нм і аспектним відношенням (відношенням між довжиною і шириною) більше 50.

Протягом низки років було розроблено декілька типів нановолокон: полімерне, вуглеволокно, керамічне, скляне, металеве та композитне, і вони, як і раніше, залишаються об'єктом інтенсивних досліджень в усьому світі.

У нановолокон є низка діючих і потенційних застосувань для виготовлення широкого діапазону продуктів, включаючи електронні і механічні пристрої, хімічні продукти, датчики та системи керування і контролю, енергетичні пристрої, медичні продукти, продукти біоінжинірингу, автомобільні та авіаційно-космічні компоненти, тепло- і звукоізоляцію, споживчі товари, а також оборонну продукцію і компоненти для забезпечення безпеки.

У 2007 р. нановолокна були запущені в промислове виробництво в США як волокна для створення логотипів, що забезпечують безпеку, компанією ARmark Authentication Technologies, що використала технологію Hills.

Однак виробництво повністю функціонального волокна із нановолокон, вироблених за допомогою більш дешевих технологій, є справою майбутнього. А використання нановолокон як самостійних дійсних фільтраційних матеріалів обмежено деякими чинниками, в основному відсутністю повномасштабних виробничих технологій і високими витратами.

Оптичні нановолокна, виготовлені за допомогою сучасних технологій, мають низку унікальних механічних і оптичних властивостей. Зокрема, вони характеризуються відмінною еластичністю. Такі волокна можуть бути вигнуті в кільця радіусом аж до декількох десятків мікронів (а для звичайних оптичних волокон це, як відомо, проблема). Сучасна технологія дозволяє за допомогою протяження істотно зменшити вихідний діаметр, при цьому зовнішня оболонка матиме діаметр близький до мікрона. Іншим важливим застосуванням нановолокон є їх використання в потужних волоконних лазерах.

Сучасні російські дослідники з МФТІ (ДУ) та Інституту радіотехніки і електроніки РАН В. А. Баган, Ю. К. Чаморовський, С. А. Нікитов та О. Г. Охотніков досліджують два нові ефективні типи оптичних нановолокон, які зможуть в подальшому вдосконалити волоконні лазери: 1) структуроване конусне волокно з діаметром серцевини близько 50 нанометрів, що дозволить концентрувати по-

тужність; 2) багатожильне конусне волокно з наноструктурою, що застосовуватиметься в потужних волоконних лазерах для підвищення їх потужності [15].

Серед безлічі проектів, які в цей час реалізуються в галузі виробництва нановолокна, є проект, що пропонує використовувати лазерне прядіння, розроблювальний дослідниками Університету Віго (Іспанія) і Університету Ратгерс із Нью-Джерсі (США). Вони одержали дуже довге аморфне нановолокно в результаті простого фізичного процесу, для якого не потрібно використання каталізатора, шаблонів або якихнебудь хімічних речовин, а необхідний усього лише матеріалпопередник реакції зі складом потрібного волокна [10]. Цей метод дає змогу не тільки одержати нанорозмірне волокно, а й робити нановолокно безпосередньо із матеріалів, які плавляться при високих температурах, а це неможливо при використанні інших аналогічних технологій, таких як електропрядіння [247].

o ***Типи волоконно-оптичних кабелів***

Оптоволоконний кабель має виняткові характеристики щодо перешкодозахищеності і таємності переданої інформації. Ніякі зовнішні електромагнітні перешкоди в принципі не здатні спотворити світловий сигнал, а сам цей сигнал принципово не породжує зовнішніх електромагнітних випромінювань. Підключитися до цього типу кабелю для несанкціонованого прослуховування мережі практично неможливо, оскільки це вимагає порушення цілісності кабелю. Вартість оптоволоконного кабелю постійно знижується і зараз приблизно дорівнює вартості тонкого коаксіального кабелю.

Поряд із цим оптоволоконний кабель має й деякі недоліки. Головний з них — висока складність монтажу (при установці рознімань необхідна мікронна точність, від точності відколу скловолокна і ступеня його полірування суттєво залежить загасання сигналу). Для установки рознімань застосовують зварювання або склеювання за допомогою спеціального гелю, що має такий самий коефіцієнт переломлення світла, що й скловолокно. У кожному разі для цього потрібні висока кваліфікація персоналу і спеціальні інструменти. Тому найчастіше оптоволоконний кабель продається у вигляді заздалегідь нарізаних шматків різної довжини, на обох кінцях яких уже встановлено рознімання потрібного типу.

Хоча оптоволоконні кабелі й допускають розгалуження сигналів (для цього випускаються спеціальні розгалуджувачі на 2–8 каналів), як правило, їх використовують для передавання даних тільки в одному напрямку, між одним передавачем і одним приймачем. Адже будь-яке розгалуження неминуче послабляє світловий сигнал, і якщо розгалужень буде багато, то світло може просто не досягти кінця мережі.

Оптоволоконний кабель менш міцний, ніж електричний, і менш гнучкий. Чутливий він і до іонізуючих випромінювань, через які знижується прозорість скловолокна, тобто збільшується загасання сигналу. Чутливий він також до різких перепадів температури, у результаті яких скловолокно може тріснути. Нині випускаються оптичні кабелі з радіаційностійкого скла (коштують вони, природно, дорожче).

Оптоволоконні кабелі чутливі також до механічних впливів (удари, ультразвук) — так званий мікрофонний ефект. Для його зменшення використовують м'які звукопоглинаючі оболонки.

Оптоволоконний кабель застосовують тільки в мережах з топологією «зірка» і «кільце». Ніяких проблем узгодження і заземлення в цьому випадку не існує. Кабель забезпечує ідеальну гальванічну розв'язку комп'ютерів мережі. У майбутньому цей тип кабелю, імовірно, витисне електричні кабелі всіх типів або, у будь-якому разі, сильно потіснить їх. Запаси міді на планеті виснажуються, а сировини для виробництва скла цілком достатньо.

Існують два типи оптоволоконних кабелів: 1) багатомодовий кабель, діаметр серцевини якого на порядок більше довжини різних типів світлових хвиль; 2) одномодовий кабель, діаметр серцевини якого 1–10 мкм для розповсюдження одного проміня.

Основні розходження між цими типами пов'язані з різним режимом проходження світлових променів у кабелі.

В одномодовому кабелі практично всі промені проходять той самий шлях, у результаті чого вони досягають приймача одночасно, і форма сигналу практично не спотворюється. Одномодовий кабель передає світло тільки з довжиною хвилі 1,3 мкм. Дисперсія і втрати сигналу при цьому дуже незначні, що дозволяє передавати сигнали на більшу відстань, ніж у разі застосування багатомодового кабелю.

Для одномодового кабелю застосовуються лазерні прийомо-передавачі, що використовують світло винятково з необхідною довжиною хвилі. Такі прийомопередавачі поки ще порівняно коштовні і незанадто довговічні. Одномодовий кабель має переваги завдяки своїм прекрасним характеристикам.

У багатомодовому кабелі траєкторії світлових променів мають помітний розкид, унаслідок чого форма сигналу на прийомному кінці кабелю спотворюється. Центральне волокно має діаметр 62,5 мкм, а діаметр зовнішньої оболонки — 125 мкм (це іноді позначається як 62,5/125). Для передавання може використовуватися звичайний світодіод, що знижує вартість і збільшує строк служби прийомопередавачів порівняно з одномодовим кабелем. Довжина хвилі світла в багатомодовому кабелі дорівнює 0,85 мкм. Припустима довжина кабелю сягає 2–5 км. Нині багатомодовий кабель — основний тип оптоволоконного кабелю, бо він дешевше і доступніше.

Затримка поширення сигналу в оптоволоконному кабелі не сильно відрізняється від затримки в електричних кабелях. Типова величина затримки для найпоширеніших кабелів становить близько 4–5 нс/м.

Існують декілька конструкцій волоконно-оптичного кабелю, які дозволяють застосовувати різні умови прокладки — усередині будинків, у телефонній каналізації, ґрунті. Він також може бути прокладений на опорах залізниць, лініях електропередач, у каналізаційних і водопровідних трубах та іншими способами.

Оптичний комутатор (ОК) — один з найважливіших елементів волоконно-оптичної мережі, без якого неможливо будувати масштабовані архітектури. Як оптичні пристрої, працюючі за принципом додавання каналів, вони дають змогу комутувати окремі хвильові канали. У центральній частині загальноміських мереж вони виконують роль оптичних крос-з'єднувачів, які під'єднують множину вхідних ліній [10]. Динаміка зростання сучасного світового ринку оптичних комутаційних технологій за останнє десятиріччя збільшилася в 10 разів.

Комутатори для крос-з'єднань у волоконно-оптичних мережах поділяють на прозорі та непрозорі. У прозорих комутаторах перетворення оптичного сигналу в електричну форму не відбувається, максимальна кількість портів приблизно 4000. Однак перетворення

оптичного сигналу в електричну форму в непрозорих комутаторах, щільність портів у яких сьогодні до 1024, дозволяє поліпшити керування мережею і забезпечує можливість регенерації сигналів.

Наявні сучасні технології оптичної комутації сигналів, зокрема крос-з'єднувачів, не дозволяють одержувати високі швидкості комутації під час перемикання. До кінця не розв'язані також проблеми структурованості, масштабованості, підвищення продуктивності і надійності таких мереж, що істотно обмежує швидкодію та пропускну здатність оптичного комутатора. Відповідні максимальні розміри операційного поля для паралельного передавання повинні бути узгоджені із комбінаторною складністю операцій оброблення, їх максимальною кількістю, впливом буферизації.

Таким чином, оптичні приймачі виявляють сигнали, передані по волоконно-оптичному кабелю, разом із синхросигналами перетворюють його в електричні сигнали, які потім підсилюють і далі відновлюють їх форму. Оптичний передавач у волоконно-оптичній системі перетворює електричну послідовність інформації на оптичний потік.

Уже існують розробки та дослідні впровадження інформаційних оптоволоконних мереж зв'язку в електронні банківські системи [133]. Згідно з останніми дослідженнями для систем управління вже розроблено спеціальні типи оптичних волокон нового покоління [230].

Уже розроблена та використовується у волоконно-оптичному трансформаторі струму технологія виготовлення оптичних наноструктурних волокон [5, с. 102]. Оптичне нановолокно виготовляється витяжкою з високоякісних кварцових заготівок зі спеціально виготовленими паралельними циліндричними повітряними каналами.

о ***Види волоконно-оптичних комунікацій***

Магістральна мережа зв'язку — це транспортна телекомунікаційна інфраструктура для надання послуг зв'язку, що, як правило, вибудовується на ВОЛЗ із використанням високошвидкісного канального обладнання зв'язку.

Оптоволоконні мережі безумовно є одними із найбільш перспективних напрямків у сфері передавання інформації — кабель волоконно-оптичної комунікації є кращим рішенням для надання суб'єктам телекомунікаційних послуг доступу в Інтернет.

Вартість використання оптоволоконної технології зменшується, що робить цю послугу конкурентоспроможною порівняно із традиційними послугами. Розроблення систем волнового мультиплексирования дозволило в кілька разів збільшити щільність передавання даних по одному волокну й до 2003 р. при застосуванні технології спектрального щільнення було досягнуто швидкість передавання 10,92 Тбіт/с (273 оптичних каналу по 40 Гбіт/с). У 2009 р. лабораторії Белла за допомогою мультиплексування 155 каналів по 100 Гбіт/с вдалося передати сигнал зі швидкістю 15,5 Тбіт/с на відстань 7000 км. Це дало поштовх до появи ВОЛЗ типу *«Fiber To The Premises»* (FTTP). У зв'язку із цим останнім часом проектувальники і конструктори мереж зайнялися пошуками найбільш ефективного способу створення таких мереж і розвитку підтримуючих інфраструктур.

Волокно в кожний будинок (англ. *Fiber to the Premises, FTTP*, або *Fiber to the Home, FTTH*) — термін, використовуваний телекомунікаційними провайдерами для позначення широкополосних телекомунікаційних систем, що базуються на проведенні оптоволоконного каналу на територію кінцевого користувача для надання комплексу телекомунікаційних послуг, що включає: 1) високошвидкісний доступ в Інтернет; 2) послуги телефонного зв'язку; 3) послуги телевізійного прийому.

Будь-які впливи на волокно можуть бути зареєстровані методом моніторингу (безперервного контролю) цілісності лінії. Теоретично існують способи обійти захист шляхом моніторингу, але витрати на реалізацію цих способів настільки великі, що перевершують вартість перехопленої інформації.

NIS-система — Network Information System (Мережна інформаційна система). Термін NIS означає, що інформаційну систему призначено для роботи з електричними, тепловими, газовими, оптоволоконними мережами. NIS, як правило, крім зберігання об'єктів мережі та їх характеристик у базі даних, містить додатки, спрямовані на здійснення бізнес-функцій мережевих підприємств: планування, розрахунки, обслуговування, аналіз і под.

За останні 20 років розроблено п'ять поколінь волоконно-оптичних систем зв'язку, що відрізняються зростаючою швидкістю передавання інформації і більш досконалою елементною базою. Адже системи першого покоління використовували багатомодові волоконні світло-

води, при цьому швидкість передавання інформації становила 45 Мбіт/с, що лише на порядок вище, ніж у системах радіозв'язку. Завдяки розвитку інноваційних технологій сьогодні створено системи зв'язку з більш високими швидкостями передавання інформації [50, с. 483–486].

Таким чином, оптичні комунікації зв'язку, що використовують світло як засіб передавання різної інформації, мають низку відмінних рис, не властивих традиційним засобам зв'язку. Оскільки оптичний зв'язок використовує як носій інформації світло, що являє собою електромагнітні коливання, то за аналогією з електрозв'язком його поділяють на два види: провідний і бездротовий оптичні зв'язки. Роль оптичного зв'язку не обмежується простою заміною діючих інформаційних мереж — він відкриває зовсім нові функціональні можливості телекомунікації.

Організаційний механізм функціонування оптоволоконних комунікацій показано на схемі 2.4.

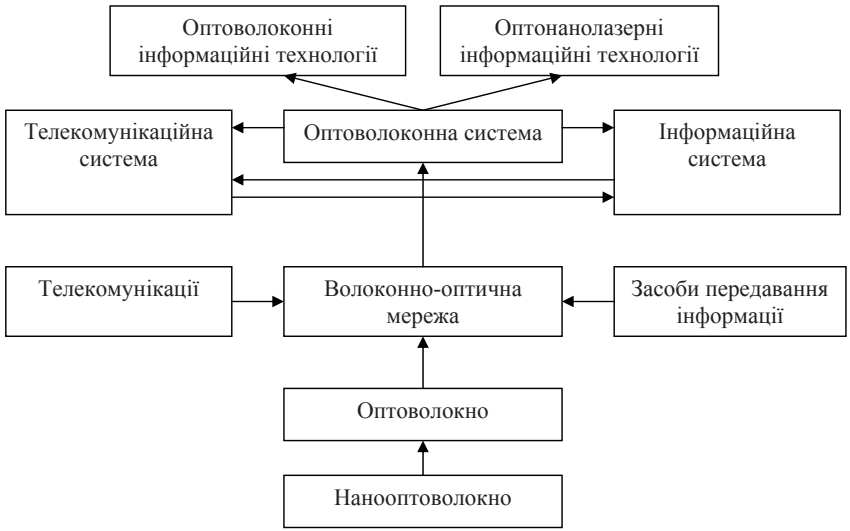


Схема 2.4

Отже, оптоволоконна система за функціональним призначенням є телекомунікаційною системою, за організаційно-правовими влас-

тивостями — інформаційною системою, де в обох випадках основним технологічним компонентом виступає волоконно-оптична мережа. Оптоволокно постає незмінним базовим елементом волоконно-оптичної мережі, а звідси — організаційною домінантою волоконно-оптичної системи.

Основним напрямом оптичного зв'язку залишається волоконно-оптичний, оскільки вже впроваджені в практичну діяльність волоконні світловоди мають чудові характеристики передавання інформації. Поряд із цим волоконно-оптичні деталі застосовують в електронно-оптичних, вимірювальних приладах, телевізійних і акустичних пристроях, фототелеграфних, телеметричних, голографічних та оптико-механічних, кібернетичних, лазерних системах і при ядерних дослідженнях. Однак волоконно-оптичний зв'язок, побудований за принципом передавання інформації у вільному просторі, також становить значний інтерес як засіб, здатний усунути недолік вільних частот, виділених для радіозв'язку, потреба в якому надалі неухильно збільшуватиметься. Сьогодні це вже не вимагає яких-небудь спеціальних підтверджень [142, с. 8].

Розроблення та застосування нової оптоволоконної технології FTPO (*Fiber To The Procurator's Office* — волокно в прокуратуру) припускає використання одного оптичного вузла, а одночасне використання як аналогових, так і цифрових систем передавання даних дозволяє у максимально використовувати існуючі інформаційно-телекомунікаційні мережі та скоротити витрати на впровадження інноваційних проектів.

Як бачимо, оптоволоконний зв'язок усе більш широко застосовується у всіх галузях — від компьютерів і бортових авіакосмічних та корабельних систем до систем передавання інформації на значні відстані, в тому числі в правоохоронній діяльності. Одним з прикладів цього може бути успішне використання магістральної волоконно-оптичної мережі зв'язку Західна Європа — Японія, більша частина якої проходить територією Росії. Крім того, збільшується сумарна довжина підводних волоконно-оптичних мереж зв'язку між континентами.

Таким чином, обґрунтовано основну тезу, згідно з якою оптичне волокно є основним матеріалом волоконно-оптичної мережі, що визначає особливості оптоволоконної системи передавання інформації.

2.3. Організаційно-правові аспекти оптоволоконних телекомунікацій

o ***Волоконна оптика і криміналістика***

Поява волоконно-оптичних технологій передавання інформації поряд з перевагами соціального, економічного, інтелектуального та інформаційного характеру містить окрему можливість їх використання у криміналістиці.

Криміналістика — це наука, яка виникла у надрах кримінального процесу в XIX ст. як сукупність прикладних прийомів і засобів, що застосовуються для виявлення та фіксації доказового матеріалу, в сучасних умовах системно вивчає закономірності механізму злочину та злочинної діяльності. Вона досліджує природу відображення інформації про злочин та його учасників в інформаційних джерелах різних видів, які слугують матеріальною основою для розроблення спеціальних засобів, прийомів і методів збирання, дослідження, оцінювання та використання доказів з метою розкриття, розслідування, судового розгляду, а також попередження злочинів.

Звідси випливає, що криміналістика залишається однією з небагатьох юридичних наук, яку фактично можна назвати наукою про розкриття злочинів та розроблення методики розслідування нового виду злочинів. Як уже зазначалося у розділі 1, одним із таких нових видів злочинів у XXI ст. є злочини у сфері високих технологій.

Перспективною сферою застосування ВОЛЗ є криміналістична техніка як найстарший розділ криміналістики, що вивчає закономірності виникнення та існування матеріальних слідів злочину, а також розроблює прийоми і науково-технічні засоби для їх збирання, фіксації та дослідження.

З метою обміну інформацією можна використати комп'ютерний багатофункціональний цифровий комплекс, призначений для реєстрації документальних фотозображень із нанесеними графічними, текстовими та звуковими коментарями. Прийняття та передавання фотографічних планів здійснюються без втрати якості завдяки низькошвидкісним каналам зв'язку. Багатофункціональний цифровий центр керування може бути використаний відповідними підрозділами правоохоронних органів з метою формування і оперативного комп'ютерного

обміну блоками електронних даних, що включають особливі прикмети злочинця, голос, текст, кольорові фотографії та іншу криміналістичну інформацію.

Висока якість виготовлення планів місць події може бути досягнута за рахунок використання із цією метою персонального комп'ютера, призначеного для роботи із графічними, відео- і звуковими файлами (наприклад, на основі комп'ютерної графічної станції). Точність фіксації місць розташування об'єктів, що можуть стосуватися справи, на місцевості повинна бути забезпечена за рахунок застосування лазерного далекоміру і компасу, а при їх значному видаленні — за допомогою приладів супутникової орієнтації, таких як «Garmin GPS-65». Тим більше, що в разі необхідності додаткового огляду місця події та проведенні перевірки показань за допомогою останнього існує можливість швидко відшукати необхідну ділянку місцевості. Ці дані можуть передаватися телефонними лініями, радіо- і супутниковими каналами зв'язку [132]. Утім, вважаємо, що найбільш ефективним засобом для передавання інформації є волоконно-оптичні мережі.

Зокрема, для поліпшення якості зображення, збільшення кута поля зору і світлосили в оптичних системах можна використовувати волоконні вирівнювачі поля, фокони, що підвищують освітленість зображення (за рахунок його масштабу), і волоконні коректори окремо або в сукупності [83, с. 262].

Отже, імовірно в майбутньому на основі лазера виникнуть численні прилади криміналістичної техніки. Однак справжній характер цих змін досить важко уявити, оскільки галузь застосування лазерів надзвичайно широка і поширюється на інформатику та телекомунікації.

Останніми роками значно зросла кількість експертних завдань, вирішення яких потребує пошуку на комп'ютерних носіях графічної інформації, що містить зображення пустих та заповнених бланків, печаток, грошових знаків, фотографій тощо. Найбільш поширеними форматами збереження та формування комп'ютерних зображень є векторний та растровий. Достатньо поширені також регулярно-комірковий та квадротомічний (квадродерево) формати. Для представлення просторових об'єктів певного типу застосовуються гіперграфова модель та її багатомірні розширення. Користувачі ПК, які

надходять для експертного дослідження, переважно використовують комп'ютерну графіка у растровому та векторному форматах.

На початку розвитку обчислювальної техніки актуальною була векторна графіка — створення зображень за допомогою так званих «векторів»-функцій, які дозволяють обчислити положення точки на екрані чи папері. Сукупність таких «векторів» і складає векторне зображення. Досвід проведення відповідних пошукових досліджень свідчить про те, що фотографічну точність у передаванні кольорів при отриманні якісних зображень документів, печаток, підписів, бланків документів, грошових знаків, фотографій тощо забезпечує частіше за все растровий формат файлів. Популярність растрового формату зумовлена ще й шляхом отримання первинних макетів цих зображень — скануванням, цифровим фотографуванням тощо. Логотипи, схеми, інші графічні елементи оформлення, навпаки, найчастіше подаються у векторному форматі, що підтверджується експертною практикою. Оскільки в комп'ютерній графіці застосовуються щонайменше три десятки форматів файлів для збереження зображень у векторному чи растровому форматах, визначимо спочатку позитивні якості файлів векторної графіки: а) малий обсяг пам'яті. При кодуванні векторного зображення зберігається не саме зображення об'єкта, а тільки деякі основні дані, використовуючи які програма відтворює зображення. Крім того, опис кольорових характеристик незначно збільшує розмір файла; б) свобода трансформації. Векторне зображення можна обертати, масштабувати без втрати його якості; в) апаратна незалежність. Векторна графіка «працює», так би мовити, з моделями, які самі пристосовуються до змін. При цьому максимально використовуються можливості роздільної здатності будь-якого пристрою виводити інформацію.

Однак слід ураховувати недоліки файлів векторної графіки: а) програмна залежність. Кожна програма будує криві Без'є за своїми алгоритмами та зберігає дані у власному форматі, тому зображення, створене в одному векторному редакторі, як правило, не конвертується у формат іншої програми або конвертується з певним погіршенням якості зображення; б) складність векторного принципу опису зображення не дозволяє автоматизувати введення графічної інформації та сконструювати для векторної графіки пристрій, аналогічний сканеру;

в) формати векторної графіки дійсно обмежені у мальовничих засобах і не призначені для створення фотореалістичних зображень.

Поряд із цим є суттєві позитивні переваги файлів растрової графіки: а) існування розвинутої системи зовнішніх пристроїв для введення зображень (сканери, відеокамери, цифрові фотокамери, графічні планшети); б) фотореалістичність (можна досягти найтонкіших нюансів при обробленні відеоінформації та відтворенні зображення); в) формати файлів, призначені для зберігання растрових зображень, є стандартними, тому не має вирішального значення, в якому графічному редакторі створювалося та було збережене зображення.

З огляду на проблему експертного пошуку графічної інформації можна зрозуміти, що зображення, які є об'єктами пошуку, ймовірніше, зберігаються у растровому форматі. Це насамперед обумовлено шляхом створення первинних макетів зображення, які для забезпечення фотореалістичності не малюють, а отримують від широко поширених пристроїв (сканерів, відеокамер, цифрових фотокамер, графічних планшетів). Але проблема пошуку не обмежується тільки дослідженням файлів растрової графіки, а стосується також файлів векторної графіки. Треба враховувати, що існує можливість взаємної конвертації векторного та растрового форматів.

Зрозуміло, що здійснити перехід від векторного способу зберігання зображення до растрового нескладно: слід задати масштаб для перерахування координат векторів у пікселі. Зворотний перехід — достатньо нетривіальне завдання. Конвертація зображення з растрового до векторного формату призводить до наслідування останнім неможливості коректного масштабування в бік збільшення.

При організації пошуку файлів графічних форматів доцільно враховувати їх внутрішню структуру. Графічні файли організовано певним чином: мають заголовок, ділянку даних та кінцівку. Структури найбільш поширених файлів растрової графіки достатньо широко представлені у літературі. Навпаки, файли векторної графіки переважно мають внутрішні формати, специфічні для тих графічних редакторів, у яких вони були створені та оброблялися. Пошук графічної інформації, розміщеної на комп'ютерному носії у вигляді файлів, можна здійснювати як за розширеннями імен файлів, так і за сигнатурами файлів у їх заголовках. При цьому також можна використову-

вати додаткову інформацію, що зберігається у файлі в текстовому вигляді (таблиця) [160, с. 238–243].

о ***Волоконно-оптичні лінії зв'язку і телекомунікаційна мережа правоохоронних органів***

Рушійною силою в розвитку високошвидкісних волоконно-оптичних систем є Інтернет. Створення волоконного світловоду і одержання безперервної генерації напівпровідникового лазера зіграли вирішальну роль у швидкому розвитку волоконно-оптичного зв'язку [83].

На жаль, дотепер не спростовано думку, відповідно якої інформаційне забезпечення правоохоронної діяльності зводиться виключно до розроблення комп'ютерів і створення програмних засобів передавання інформації [8].

Насправді передавання інформації через ВОЛЗ з високими швидкостями (1–100 Гбіт/с та вище) — винятково складна технологічна проблема. Використання оптичного (лазерного) випромінювання для передавання інформації замість радіохвиль дозволяє збільшити швидкість передавання інформації приблизно в 100 тис. разів.

Для організації магістральної аналогової оптичної лінії зв'язку в рамках проекту єдиної інформаційно-телекомунікаційної системи правоохоронних органів необхідний оптичний передавач. Слід відзначити, що при організації магістральної цифрової оптичної лінії зв'язку вимоги до характеристик передавача і приймача можуть бути значно нижче. Тому їх сумарна вартість у кілька разів менша, а звідси — застосування оптичних магістралей в інформаційно-телекомунікаційній системі правоохоронних органів може стати економічно вигідним уже на відстанях від 100 м, тобто до входів в окремо розташовані приміщення певного територіального правоохоронного органу.

При цьому оптичний кабель «заводиться» у технічне приміщення будинку, в якому розташовані працівники певного підрозділу органів внутрішніх справ чи прокуратури або спеціальна шафа (кабінет), де розміщується «активне» устаткування для перетворення оптичних сигналів в електричні. Це стає можливим завдяки тому, що технологія FTTC (*Fiber To The Cabinet* — волокно в шафу-кабінет) припускає використання одного оптичного вузла на декілька будинків [218, с. 11–14].

Розрахунки показують, що в більшості випадків побудова FTTB-мереж (*Fiber To The Building* — волокно до будинку) може бути економічно виправданою, якщо таку мережу створювати тільки при великій кількості користувачів телекомунікаційних послуг передавання даних у згаданому будинку.

Фактично така система являє собою пасивну оптичну розподільну мережу від базисного оптичного інформаційного вузла до кожного абонента. При цьому потенційний ресурс подібної волоконно-оптичної телекомунікаційної системи набагато більш значний, ніж у поширених на цей час у прокуратурі комп'ютерних мереж. Таким чином, можна спрогнозувати паралельний розвиток обох технологій протягом найближчих декількох років.

Потреба Інтернету в швидкості передавання інформації подвоюється кожні кілька місяців, тому розвиток інформаційно-телекомунікаційної системи прокуратури в найближче десятиліття визначатимуть саме інформаційні та телекомунікаційні технології, які ґрунтуються на високошвидкісних волоконно-оптичних системах зв'язку і передавання інформації. Невдовзі настане час, коли буде досягнута петабітна межа швидкості передавання інформації [51, с. 1010].

На основі волоконно-оптичних технологій створюються локальні обчислювальні мережі різної топології (кільцеві, зоряні та ін.). Такі мережі дають змогу поєднувати оперативно-розшукові, експертні, аналітичні та криміналістичні системи областей в єдину інформаційну антикримінальну систему з великою пропускною здатністю, підвищеною якістю та захищеністю від несанкціонованого допуску.

До того ж, волоконно-оптичні датчики здатні працювати в агресивних середовищах, надійні, малих габаритів і не піддаються електромагнітним впливам. Застосування ж ВОЛЗ у правоохоронній діяльності, зокрема в криміналістиці, поки що не викликало істотного інтересу. Втім, використання волоконно-оптичних приладів у сфері масштабування зображення може бути успішно використано в правоохоронній практиці. Волоконно-оптичний пристрій містить світловод, який дозволяє підвищити контраст і роздільну здатність при масштабуванні зображення, відрізняється простотою виготовлення і дешевизною.

Таким чином, викладене надає підстави припустити, що застосування розглядуваного рішення дасть змогу вирішити завдання узгодження

формату інформаційного зображення з форматом оптичного приймача при збереженні високого контрасту первинного зображення.

Високопродуктивний оптоелектронний комутатор має потенційно високі можливості для забезпечення наносекундних швидкостей комутації, низьких втрат і помірного енергоспоживання [115, с. 69–76].

Організація захисту комп'ютерних інформаційних систем та волоконно-оптичних мереж визначає порядок і схему функціонування їх основних підсистем, використання пристроїв та ресурсів, взаємовідносини користувачів відповідно з нормативно-правовими вимогами та правилами. Захист інформації на основі організаційних заходів відіграє значну роль у забезпеченні надійності та ефективності, оскільки несанкціонований доступ та витікання інформації найчастіше зумовлені умисними діями, недбалістю користувачів або персоналу. Ці чинники практично неможливо виключити або локалізувати за допомогою апаратних і програмних засобів, криптографії та фізичних засобів захисту, тому сукупність організаційних, організаційно-правових та організаційно-технічних заходів, які застосовуються разом із технічними методами, має за мету виключити, зменшити або повністю усунути збитки від дії різноманітних деструктивних чинників.

Використовуються системи з двох волоконно-оптичних кабелів, по яких передаються кодовані сигнали інфрачервоного діапазону. Якщо в сітці немає пошкоджень, то сигнали поступають на приймальний пристрій без спотворень. Спроби пошкодження сітки призводять до обривів або деформації кабелів, що викликає сигнал тривоги. Оптичні системи відрізняються низьким рівнем помилкових тривог, викликаних впливом на них дрібних тварин, птахів, зміною погодних умов та високою ймовірністю виявлення спроб вторгнення.

Таким чином, інноваційний потенціал оптоелектронних комутаторів у подальшому може віднайти широке впровадження в інформаційно-телекомунікаційну систему правоохоронної діяльності.

У розвинутих країнах існує та бурхливо розвивається графічний пейджинг, завдяки якому можливе передавання високоякісного графічного зображення фоторобота злочинця; з'явилися мобільні телефони третього покоління з можливістю відеопередавання даних, що також можна використовувати при розкритті та розслідуванні злочинів.

Перспективним напрямом розвитку комп'ютерної технології є створення програмних засобів для виведення якісного звуку та відеозображення. Технологія одержання відеозображення отримала назву комп'ютерної графіки — створення, зберігання та оброблення моделей об'єктів та їх зображень за допомогою ЕОМ. Ця технологія проникла в галузь економічного аналізу, моделювання різноманітних конструкцій, вона незамінна на виробництві, проникає в рекламну діяльність, робить цікавим дозвілля.

Отже, інтерактивна машинна графіка є одним з найбільш прогресивних напрямів серед нових інформаційних технологій.

Основними критеріями, що характеризують здатність високошвидкісних фотокамер передавати інформацію, є тимчасова й просторова розв'язна здатність, число кінокадрів, що швидко визначає можливу довжину запису, яка відповідає швидкості процесу, і ефективний відносний отвір, що характеризує світлосилу камери. Однак при оцінюванні відеокамери слід ураховувати також конструкції об'єктиву, оптики та системи затвора, а також спосіб сканування.

При реєстрації двомірної інформації основні труднощі полягають у можливості одержання більших швидкостей просування фотоплівки. Вже розроблено низку високошвидкісних камер, що використовують основні принципи цього методу. В цих системах двомірне зображення механічним або оптичним способом розкладається в регулярному порядку на низку маленьких точок або ліній, які потім систематизуються в іншому порядку, більш зручному для розгорнення зображення в часі. Розгорнуте в часі зображення швидкоплинного процесу на плівці складається з декількох розділених частин кадру.

Цей метод дозволяє за допомогою відносно простих механічних і оптичних засобів одержувати високу частоту фотозйомки зображення. Отриманий в такий спосіб негатив проектується через таку саму оптичну систему у зворотному порядку, і з елементів зображення, що належать окремому кадру, знову складається кадр вихідного формату. При передаванні у зворотному ході цих окремих знову складених кадрів у колишньої послідовності швидкоплинний процес демонструється у вигляді кінофільму [28, с. 48–51].

Запропоновано використовувати в системах технічного зору оптичні волокна за допомогою технології волоконно-оптичної головки зчи-

тування (ВОГЗ) [5, с. 102]. Цей підхід дозволяє використати переваги оптичних волокон, одночасно забезпечуючи також можливість простого сполучення з оптичними комп'ютерами, включаючи квантові, без перетворення оптичного сигналу на електричний [6, с. 369–372]. Це технічно набагато може прискорити процес виконання слідчих дій у складних (екстремальних) умовах із застосуванням науково-технічних засобів. Дороблення технології ВОГЗ до поляризаційного і фазового зчитування дасть змогу ще більше збагатити ці можливості для технічного зору. Крім того, можливості динамічної голографії дозволять проводити слідчі дії в гучних вібронезахищених приміщеннях.

Необхідність використання технічного зору зв'язана із усе зростаючим рівнем вимог до точності, швидкості оброблення та надійності в сучасному виробництві, наукових дослідженнях і діловодстві. Традиційно системи технічного зору використовують потужні лампи, коштовні відеокамери і мікропроцесори, що застосовують у реальному масштабі часу алгоритми наближені до штучного інтелекту.

Останнім часом активно впроваджуються волоконно-оптичні освітлювачі. Слід визначити основні переваги волоконно-оптичного висвітлення — можливість доступу в обмежені обсяги при огляді місця події, стійкість до підвищеної температури, хімічних і електромагнітних впливів, можливість фокусування випромінювання в потрібному місці.

Волоконно-оптичні мережі доступу одержали широке поширення завдяки стрімкому розвитку за останні роки стандартів Ethernet, що пройшли шлях від технології побудови локальних комп'ютерних мереж до магістральної технології. У результаті замість двох волокон для передавання даних у мережі Інтернет надалі може бути використано лише одне волокно, що дозволить додатково скоротити витрати на побудову на цій базі інформаційно-телекомунікаційної системи органів, які ведуть боротьбу зі злочинністю.

Крім того, як відзначають фахівці, магістральні комутатори можуть профілювати трафік, тобто фіксувати спектр пропущення під певний вид трафіку [111, с. 15–19].

Нині вартість волоконно-оптичних мереж наблизилася до такого рівня, коли ВОЛЗ стають економічно вигідним варіантом, що сприяє створенню цифрової інформаційної мережі правоохоронних органів України.

У цілому шляхами розв'язання існуючих проблем інформаційно-аналітичного забезпечення правоохоронних органів є: вдосконалення системи статистичного обліку, аналізу, оцінювання інформації та результатів виявлення порушень закону у сфері нових інформаційних технологій; створення спеціалізованих аналітичних груп, що повинні відповідати за оцінювання, узагальнення оперативно значущої інформації та пошук оперативно значущої інформації із легальних (відкритих та процесуальних) джерел; упровадження інноваційних методів отримання оперативної інформації з використанням оперативно-технічних засобів (програмних та програмно-технічних); розроблення науково обґрунтованих методик і програмного забезпечення аналізу оперативної інформації, отриманої оперативно-технічними засобами, для моделювання ситуацій, що складаються при проведенні оперативно-розшукових заходів [52; 232].

о ***Методи інформаційної безпеки та системи захисту інформації***

Поняття «захист інформації» закріплено у Законі України «Про захист інформації в автоматизованих системах» як «сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованим системам та осіб, які користуються інформацією» [66]. Таке ж визначення виписано і у підзаконних актах [128–129].

Під захистом даних розуміють будь-який правовий, організаційний, технічний (технологічний, криптографічний, програмний) захист інформації персонального змісту. Всі закони із зазначеною назвою забезпечують захист персональних даних. Для комплексного захисту даних на міжнародному рівні використовується термін «забезпечення безпеки даних», тобто в цьому разі йдеться про інформаційну безпеку.

З метою виключення термінологічної плутанини поняття «захист даних» слід тлумачити лише у тому розумінні, що встановлено у ст. 1 Конвенції № 108 Ради Європи по захисту осіб у зв'язку з автоматизованим обробленням персональних даних (м. Страсбург, 28 січня 1981 р.) [94]. Конвенція № 108 зобов'язала країни-учасниці здійснити коригування національних законодавств в частині втілення встановлених нею основних принципів захисту персональних даних.

Нині критична маса науково-практичних знань щодо розвитку суспільних інформаційних відносин дає змогу сформувати на теоретичному рівні елементи загальної теорії організації інформаційної безпеки в умовах формування інформаційного суспільства — захисту інформації в автоматизованих комп'ютерних системах.

Інформаційну безпеку можна визначити як стан надійності інформації, телекомунікаційних даних, інформаційних систем та продуктів, автоматизованих систем та їх ресурсів. У той час, як інформаційна безпека — це стан захищеності інформаційного середовища, захист інформації являє собою діяльність щодо запобігання витіканню інформації, яка захищається, попередження несанкціонованих та неумисних впливів на інформацію, що захищається, тобто є процесом, спрямованим на досягнення такого стану. Також існують інші визначення [57; 93; 171], зокрема, як діяльність, спрямована на забезпечення захищеного стану інформації про об'єкт.

У зв'язку з цим за режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Прикладом гарантування права громадян на відкриту інформацію є норми, закріплені у ст. 50 Конституції України: кожному гарантується право вільного доступу до інформації про стан довкілля, якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена.

Інформація з обмеженим доступом — це відомості конфіденційного або таємного характеру, правовий статус котрих передбачено законодавством України, які визнані такими відповідно до встановлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей.

Отже, приймемо запропоноване визначення захисту інформації з обмеженим доступом як сукупність організаційно-правових, інженерно-технічних та криптографічних заходів, які застосовуються власником інформації з обмеженим доступом або іншими особами за його замовленням, з метою запобігання заподіянню шкоди інтересам власника інформації та її неконтрольованому поширенню [122].

Організаційно-правові основи захисту інформації з обмеженим доступом стають предметом наукових досліджень [143]. До того ж, у сфері обігу інформації з обмеженим доступом нерідко вчиняються

правопорушення, що зумовлюють юридичну відповідальність, про що також є деякі розробки [122]. Так, слід мати на увазі, що застосування заходів вилучення інформації із каналів зв'язку, контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією відповідно до чинного законодавства здійснюються виключно з метою запобігання тяжкому чи особливо тяжкому злочину або з'ясування істини під час розслідування кримінальної справи, якщо в інший спосіб одержати інформацію неможливо [240, с. 342–347].

Програмний захист інформації — це система спеціальних програм, які входять до складу програмного забезпечення та реалізують функції захисту інформації. Захисні системи, що належать до засобів апаратно-програмного захисту, в частині програмного забезпечення можливо тлумачити як різновид комп'ютерної інформації [177, с. 23–27]. Поза увагою залишаються інші захисні заходи, що належать до суто апаратних, та апаратно-програмні заходи в частині апаратного забезпечення. Крім того, захисні системи можуть бути розраховані також на захист як безпосередньо комп'ютерної інформації, так і її носіїв. Дослідники свого часу вказували на те, що файлова система повинна забезпечувати захист файлів від несанкціонованого доступу [14, с. 1].

Виділяють такі напрями використання програм для забезпечення безпеки конфіденційної інформації: 1) захист інформації від несанкціонованого доступу; 2) захист інформації від копіювання; 3) захист програм від вірусів; 4) захист інформації від вірусів; 5) програмний захист каналів зв'язку. За кожним із зазначених напрямів існує достатня кількість якісних, розроблених професіональними організаціями програмних продуктів, представлених на інформаційному ринку.

Розвиток підсистеми інформаційної безпеки є важливою складовою стратегії системної інформатизації правоохоронних органів України. До найважливіших об'єктів забезпечення інформаційної безпеки у правоохоронній і судовій сферах належать: 1) інформаційні ресурси органів державної виконавчої влади, які реалізують правоохоронні функції, судових органів, їх інформаційно-обчислювальних центрів, науково-дослідних установ і навчальних закладів, що містять спеціальні відомості та оперативні дані службового характеру; 2) інформаційно-обчислювальні центри, їх інформаційне, технічне,

програмне та нормативне забезпечення; 3) інформаційна інфраструктура (інформаційно-обчислювальні мережі, пункти керування, вузли та лінії зв'язку).

Позначимо основні внутрішні загрози щодо модернізації процесів та технологій інформатизації правоохоронних органів: 1) порушення встановленого регламенту збирання, оброблення, зберігання і передавання інформації, що міститься в картотеках і автоматизованих банках даних і використовується для розслідування злочинів; 2) недостатність законодавчого та нормативного регулювання інформаційного обміну в правоохоронній і судовій сферах; 3) відсутність єдиної методології збирання, оброблення та зберігання оперативно-розшукової, довідкової, криміналістичної та статистичної інформації; 4) відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах; 5) умисні дії та помилки персоналу, безпосередньо зайнятого формуванням і веденням картотек і автоматизованих банків даних.

Поряд із загальними методами та засобами захисту інформації застосовуються також специфічні методи і засоби забезпечення інформаційної безпеки у правоохоронній і судовій сферах. Зокрема, в сучасній криптографії розглядаються два типи криптографічних алгоритмів (ключів, що засновані на використанні секретних ключів та нові криптографічні алгоритми з відкритими ключами, засновані на використанні двох типів ключів: секретного (закритого) та відкритого.

Звідси визначимо головні методи і засоби забезпечення інформаційної безпеки у сфері боротьби зі злочинністю: 1) створення захищеної багаторівневої системи інтегрованих банків даних оперативно-розшукового, довідкового, криміналістичного і статистичного характеру на базі спеціалізованих інформаційно-телекомунікаційних систем; 2) підвищення рівня професійної та спеціальної підготовки користувачів інформаційних систем [23, с. 362–363].

Таким чином, в узагальненому визначенні інформаційна безпека — це здатність держави, суспільства, організації, особистості, технічної та інформаційної систем або конструкцій забезпечити необхідні інформаційні ресурси для підтримки їх стійкого функціонування в будь-яких

складних умовах існування і розвитку. Крім цього, до поняття інформаційної безпеки слід віднести здатність зазначених суб'єктів ефективно протидіяти загрозам інформаційним ресурсам, технічним системам і джерелам передавання інформації та обміну нею.

о ***Інформаційна надійність оптоволоконних телекомунікацій***

Наголосимо, що інформаційна надійність є складовим елементом системи інформаційної безпеки, і тому від її стану залежатиме в цілому надійність цієї системи, що випливає із такого співвідношення:

$$A \geq \frac{Bt}{Bl} \geq C \ , \tag{2.2}$$

де A — інформаційна безпека; B — інформаційний захист; t — технічні засоби; l — правові засоби; C — інформаційна надійність.

Технічний захист інформації — це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Система технічного захисту інформації — це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами (організаційні структури), нормативно-правова та матеріально-технічна база.

Ефективне і належне функціонування системи технічного захисту інформації неможливе без чіткого правового регулювання відповідних суспільних відносин, адже саме право має необхідні засоби і механізми впливу на поведінку суб'єктів відповідних відносин.

Правову основу забезпечення технічного захисту інформації в Україні становлять Конституція України, закони України «Про основи національної безпеки України», «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну інформацію», інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин [45–46; 67–72].

Питання захисту інформації в інформаційно-телекомунікаційних системах, крім Закону України «Про захист інформації в інформаційно-

телекомунікаційних системах» та інших законів, регулюються також низкою підзаконних нормативно-правових актів [163–167].

Постановою від 13 березня 2002 р. № 281 КМУ уповноважив Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (Законом України від 23 лютого 2006 р. «Про Державну службу спеціального зв'язку та захисту інформації України» на базі Департаменту спеціальних телекомунікаційних систем та захисту інформації та відповідних підрозділів Служби безпеки України утворено Державну службу спеціального зв'язку та захисту інформації України) здійснювати управління захистом інформації в автоматизованих системах відповідно до Закону України «Про захист інформації в автоматизованих системах» [66].

Напрями розвитку технічного захисту інформації зумовлюють розроблення заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової, демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

Зокрема, вимоги до веб-сайту персональних даних установлюються національним законодавством про захист персональних даних. Такими головними вимогами згідно з нормами міжнародних стандартів є: 1) заборона на об'єднання веб-сайту персональних даних з вебсайтами будь-яких інших даних загального інформаційного змісту без письмової згоди власника персональних даних; 2) заборона оброблення і використання персональних даних у веб-сайтах персональних даних без письмової згоди власника персональних даних, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту і прав людини; 3) відповідальною за поширення відомостей з веб-сайту персональних даних через службу зв'язку або електронну пошту вважається та особа, що відправляє дані. Провайдер послуг відповідає за додаткове оброблення персональних даних, що необхідно йому для здійснення їх поширення; 4) обов'язок кожної фізичної особи не розголошувати персональні дані, що стали відомі у зв'язку з виконанням службових обов'язків і після закінчення службових обов'язків в органах державної влади та

органах місцевого самоврядування, організаціях, установах і підприємствах усіх форм власності [211, с. 438–439].

З метою оцінювання захищеності інформації, яка обробляється або циркулює в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, приміщеннях, інженерно-технічних спорудах тощо (об'єктах інформаційної діяльності), та підготовки обґрунтованих висновків для прийняття відповідних рішень може проводитися державна експертиза у сфері технічного захисту інформації.

Зростання загроз для інформації, спричинене лібералізацією суспільних та міждержавних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї, визначає необхідність розвитку технічного захисту інформації [93].

Комплексна система захисту інформації від несанкціонованого доступу повинна: 1) оперативно реагувати на зміни чинників, що визначають методи і засоби захисту інформації; 2) базуватися на кращих алгоритмах закриття інформації, що гарантують надійний криптографічний захист; 3) мати найважливіші елементи ідентифікації користувачів і контролю за істинністю переданої і збереженої інформації; 4) здійснювати захист від несанкціонованого доступу до інформації в базах даних, файлах, на носіях інформації, а також при її передаванні лініями зв'язку в локальних і глобальних мережах; 5) забезпечувати режим спеціально захищеної електронної пошти для обміну секретною інформацією з високою швидкістю і достовірністю передавання інформації адресату; 6) мати зручну і надійну ключову систему, що гарантує безпеку при виробленні і розподілі ключів між користувачами; 7) забезпечувати різноманітні рівні доступу користувачів до інформації, що захищається.

Таким чином, інформаційну безпеку телекомунікаційної системи можна визначити як здатність нейтралізувати такі впливи.

Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, затверджений Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 24 грудня 2001 р. № 76,

визначає основи організації та порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

Основною метою розвитку та надання доступних телекомунікаційних послуг слідчим є можливість оперативного задоволення оперативно-службових потреб у телекомунікаційних інформаційних послугах у сфері боротьби зі злочинністю. Водночас в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах правоохоронних органів, які забезпечують обмін електронними документами між різними відомчими установами (СБУ, МВС, Міністерство юстиції тощо), що містять інформацію, яка є власністю держави, або інформацію з обмеженим доступом, має забезпечуватися захист цієї інформації відповідно до законодавства. У цьому аспекті слід згадати позитивний досвід найпотужнішого в Україні пошукового правового сервера LIGA ONLINE [121–122].

Світові темпи розвитку волоконно-оптичних систем передавання інформації набагато випереджають темпи розвитку систем її оброблення та зберігання. Експериментальним шляхом підтверджено підвищення контрасту зображення пристроями більш ніж удвічі порівняно із прототипом при масштабуванні малоконтрастних зображень, що особливо істотно для криміналістики. Це розширює межі застосування вже відомих дактилоскопічних і спектрометричних систем, нічних телевізійних камер, створює передумови для побудови на їх основі детекторів брехні, дозволить підвищити надійність використання кредитних карток і под.

Прогрес у різних галузях науки і техніки сприяв створенню компактних та високоефективних ВОЛЗ, за допомогою яких можна легко підключатися до ліній телекомунікацій, та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізування розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, волоконно-оптичної, радіотеплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок. Утім, за таких умов створилися можливості витікання інформації, порушення її цілісності та блокування [75, с. 289–291].

Залишається проблемним питанням правова неврегульованість процесу надання ліцензій на «обслуговування кабельних мереж у

межах промислової експлуатації». Як правило, оператори кабельного телебачення свою діяльність відносять до сфери побутових послуг, а не промислової експлуатації. Причиною цього є факт невизначеності поняття «межа промислової експлуатації».

Не можна залишати поза увагою такий важливий напрям діяльності, як використання стандартів інформаційної надійності у критично важливих системах інформаційно-телекомунікаційної інфраструктур [149].

Таким чином, інформація, що передається з використанням волоконно-оптичних мереж, найближчим часом має стати суб'єктом спеціального правового захисту, а механізм оптоволоконного передавання інформації потребує додаткового організаційно-правового регулювання. Згідно з останньою тезою назріла актуальна потреба у розробці і впровадженні відповідних нормативно-правових інновацій.

Використання ВОЛЗ в інформаційно-телекомунікаційних системах правоохоронних органів відкриває принципово нові можливості створення і впровадження ефективних інформаційних технологій і фактично новий технологічний коридор передавання інформації у цій сфері.

Ґрунтуючись на аналізі викладеного матеріалу, спробуємо вивести певну закономірність:

$$\frac{T}{E} \cong \frac{F}{I} \ , \tag{2.3}$$

де T — телекомунікаційна мережа; E — електронні інформаційні ресурси; F — волоконно-оптична мережа; I — оптоволоконна система передавання інформації. Таке співвідношення свідчить про те, що волоконно-оптична мережа майже завжди виступає складовою сучасної телекомунікаційної мережі відповідно як носій до предмета переміщення — електронних інформаційних ресурсів.

Отже, наприкінці слід відзначити, що на сьогодні правове регулювання магістральних ВОЛЗ є недостатнім, залишається фактично на описовому рівні, а тому організаційно-правовий механізм впровадження оптоволоконних ліній передавання інформації в телекомунікаційну систему та спеціалізовані підсистеми потребує вдосконалення.

У зв'язку з цим основні положення, викладені в цьому розділі, можуть бути використані під час розроблення проекту Закону України «Про волоконно-оптичні лінії зв'язку».

Резюме. *Дослідження волоконно-оптичних інформаційних комунікацій в телекомунікаційних системах різного призначення надає підстави акцентувати увагу щодо таких підсумків: 1) визначено поняття телекомунікації, телекомунікаційної мережі та електронної інформаційної системи; 2) доведено, що національні інформаційні ресурси є основою забезпечення суверенітету та інформаційної безпеки держави; 3) ретроспективно висвітлено основні здобутки волоконно-оптичних систем зв'язку; 4) доведено, що оптичне волокно є основним матеріалом волоконно-оптичної мережі, який визначає особливості оптоволоконної системи передавання інформації; 5) з'ясовано перспективи використання ВОЛЗ в криміналістиці; 6) обґрунтовано методи інформаційної безпеки та розкрито правові засади забезпечення захисту інформації; 7) визначено особливості правових проблем інформаційної надійності оптоволоконних телекомунікацій.*

Ключові слова*: телекомунікації; інформаційні ресурси; інформаційні продукти; інформаційні системи; інформаційні процеси; оптичне волокно; оптоволоконні телекомунікації; оптоволоконна система передачі інформації; волоконно-оптичні лінії зв'язку; інформаційна безпека; системи захисту інформації; інформаційна надійність.*

Контрольні запитання

1. Поняття, функції та види телекомунікацій.
2. Суб'єкти ринку телекомунікаційних послуг.
3. Національні інформаційні ресурси як основа забезпечення суверенітету та інформаційної безпеки держави.
4. Інформаційні продукти у структурі інформаційних ресурсів.
5. Види інформаційних систем та компоненти інформаційної системи.
6. Інформаційні процеси у сфері високих технологій.
7. Організаційно-правові засади використання електронних документів.
8. Оптичне волокно та оптонановолокно.
9. Правовий зміст поняття «оптоволоконна інформаційна технологія».

10. Поняття та види волоконно-оптичних мереж.
11. Відмінність між поняттями «інформаційні системи» та «оптоволоконні системи передачі інформації».
12. Криміналістична техніка як галузь застосування ВОЛЗ.
13. Застосування волоконно-оптичних явищ і методів для аналітичних цілей у правоохоронній практиці.
14. Оптоволоконні системи передавання інформації як новий крок у мультимедійних технологіях зв'язку.
15. Правовий механізм волоконно-оптичних комунікацій.
16. Застосування волоконно-оптичних технологій передавання інформації у криміналістиці.
17. Поняття «захист інформації» та проблеми технічного захисту інформації в телекомунікаційних мережах правоохоронних органів.
18. Правова основа забезпечення технічного захисту інформації з обмеженим доступом в Україні.
19. Проблеми інформаційної безпеки телекомунікаційної системи правоохоронних органів.
20. Правове забезпечення інформаційної надійності оптоволоконних телекомунікацій.

Розділ 3

Модернізація. Інновації. Електронна юриспруденція. Цифрова юстиція

У цьому розділі ...

• ***Суперкомп'ютери та Грід-мережі: інформаційно-правовий аспект.***
Модернізація, інформатизація, формування технологічного світогляду ◄► Програмоване суспільство та високотехнологічна цивілізація ◄► Комп'ютер і суперкомп'ютер ◄► Історія Грід ◄► Інтернет і Грід-концепція ◄► Потенціал Грід-мереж і нова комп'ютерна революція ◄► Сфери застосування та класифікація Грід-технологій ◄► Грід-технології в криміналістиці.

• ***Правовий моніторинг цифрової інформаційної мережі в Інтернет-просторі.***
Цифрові права людини та мультимедіа-технології ◄► Система високотехнологічного інформаційного права та Інтернет ◄► Методологія, принципи та функції інтернет-моніторингу ◄► Мета та завдання правового моніторингу цифрових інформаційних мереж.

• ***Створення й розвиток інноваційної інфраструктури в юриспруденції.***
Інновації та інноваційна політика ◄► Управління інноваційними проектами ◄► Електронна юриспруденція та цифрова юстиція ◄► Інформаційна культура юриста ◄► Інформатизація адвокатської діяльності в умовах розвитку високих технологій ◄► Інноваційний проект «е-адвокат» ◄► Адвокатське досьє (інформаційний аспект) ◄► Електронне адвокатське провадження (інформаційний аспект) ◄► Електронний архів адвоката (інформаційний аспект) ◄► Криміналістична інформатика та високі технології ◄► Проблеми досудового слідства у сфері високих технологій та криміналістична модернізація ◄► Нові інформаційні технології в криміналістиці ◄► Види інформаційних та експертно-криміналістичних систем ◄► Характеристика інформаційних та експертно-криміналістичних систем ◄► Автоматизоване робоче місце слідчого ◄► Інноваційний проект «Оптико-електронний кабінет криміналістики».

3.1. Суперкомп'ютери та Грід-мережі: інформаційно-правовий аспект

o ***Модернізація, інформатизація, формування технологічного світогляду***

Модернізація — це вдосконалення, поліпшення, відновлення об'єкта, приведення його у відповідність із новими вимогами і нормами, технічними умовами, показниками якості. У переважній більшості модернізуються економічні процеси та технологічне обладнання [77]. Забігаючи уперед, зазначимо, що до розгляду окремих питань з модернізації економіки у контексті розвитку нанотехнологій ми ще повернемося у підрозділі 5.1 цього видання.

Поняття модернізації виникло в 50–60-х роках XX ст. в США для пояснення процесів, що змінюють традиційний суспільний порядок і сприяють входженню країн до сучасного (індустріального і демократичного) співтовариства.

Разом із цим хоча термін «модернізація» порівняно досить новий, явище, що ним позначається, існує принаймні вже три сторіччя. Постмодернізація є заперечення модернізації навіть за змістом самого терміна. Заперечується, однак, не сам по собі факт модернізації, як він мав місце в історії і продовжує зберігатися до нашого часу, а можливість досягти на цьому шляху скільки-небудь істотних результатів [123].

Як стало зрозумілим з матеріалу підрозділу 1.1, процес інформатизації є системним перетворенням продукт орієнтованого способу виробництва на постіндустріальний. В основі інформатизації лежать кібернетичні методи й засоби управління, а також інструментарій інформаційно-комунікаційних технологій. У ході інформатизації змінюється матеріально-технологічна основа суспільства, ключове значення починають набувати аналітичні інформаційні системи управління, тобто модернізується соціальний уклад життя — ми бачимо, як інформатизація набуває рис іншого феномену — технологізації.

Технологічний світогляд — це система специфічних поглядів на природу, суспільство, людину. Формування технологічного світогляду викликано наперед інформаційними особливостями суспільного буття та соціально-технічними умовами. Технологічний світогляд являє собою сукупність (систему) стійких поглядів, принципів, оцінок та переконань, які визначають ставлення до технологічних процесів, що відбуваються у навколишній дійсності, та характеризує бачення світу в цілому і місце людини у сфері високих технологій. Зміна технологічного світогляду детермінує широкі дискусії, у центрі яких

знаходиться питання стосовно стратегічної основи розвитку техніки, що не суперечить цивілізаційній перспективі.

Отже, інформатизація поетапно формує новий, високотехнологічний світогляд на природу інформаційних процесів.

Як свідчать дослідження модернізації інформаційно-аналітичного забезпечення діяльності органів влади України, в реалізації їх різних стратегій виникають типові проблеми, на які пропонується звернути увагу: 1) усвідомлення актуальності проблем першими керівниками, їх бажання і воля до розв'язання проблем; 2) недосконалість нормативно-правової бази; 3) вибір профілю технічних стандартів; 4) вибір комп'ютерного програмного середовища (інформаційних технологій); 5) створення персонального складу центру компетенції; 6) науковий моніторинг та супроводження реалізації; 7) кадрове забезпечення функціонування та розвитку; 8) фінансове забезпечення.

Звідси пропонується розуміти інформаційну модернізацію як високотехнологічний розвиток інформаційно-телекомунікаційних систем із чітко визначеною кінцевою метою. Цим інформаційна модернізація відрізняється від інформаційного розвитку, детермінованого внутрішньо зумовленою причиною. Однією з провідних ознак інформаційної модернізації є системний перехід інформаційної мережі на цифрові технології з використанням сучасних потужних комп'ютерних систем, до чого перш за все потрібно віднести суперкомп'ютери та Грід-мережі, загальна характеристика яких для усвідомлення розглядуваної проблематики аналізується пізніше.

о ***Програмоване суспільство та високотехнологічна цивілізація***

Інформаційна сфера являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збирання, формування, розповсюдження та використання інформації, а також системи регулювання суспільних відносин, що створюються при цьому. Саме в інформаційній сфері при виконанні інформаційних процесів виникають соціотехнічні відносини, що підлягають правовому регулюванню. Нагадаємо, що саме ці суспільні відносини становлять предмет інформаційного права, предмет його правового регулювання [254].

Інформатизація сьогодні виходить на четвертий етап свого розвитку. Перший був пов'язаний з появою великих комп'ютерів (мей-

нфреймів), другий — з персональними комп'ютерами, третій — з появою Інтернету, що об'єднав користувачів в єдиний інформаційний простір. Тому останнім часом в літературі можна зустріти поряд з терміном «інформаційне суспільство» новий термін «програмоване суспільство», яким позначається різновид широко поширеної в західних країнах теорії постіндустріального суспільства.

Соціальні та науково-технічні процеси високотехнологічної цивілізації вкрай складні, суперечливі та досить важко піддаються прогнозам і правовому регулюванню. Прибічники концепції програмованого суспільства вважають, що в постіндустріальному суспільстві велику роль відіграють комп'ютерні системи, з'єднані в могутні потужні суперкомп'ютерні мережі, та їх програмне забезпечення [53; 59]. Технологічна експансія поступово прирікає людину до існування в штучних умовах. Можливо, навіть, спрогнозувати відсікання людей від наукового знання шляхом встановлення блокади інформації у просторі та часі. Такий розвиток подій здатний детермінувати виникнення нової високотехнологічної цивілізації як суспільства програмованих комунікацій з мінімальним застосуванням правових механізмів.

Отже, інформаційна сфера стає особливою підвалиною майбутньої високотехнологічної цивілізації, де регулювання соціотехнологічних відносин відбуватиметься правовими засобами. Тобто, для забезпечення самого існування людства в умовах високотехнологічної цивілізації інформаційне право залишиться основним регулятором високотехнологічних відносин.

o ***Комп'ютер і суперкомп'ютер***

Комп'ютер (від лат. *computo* — обчислюю) — це компактна універсальна електронна цифрова обчислювальна машина, що складається з одного або декількох взаємопов'язаних центральних процесорів і периферійних пристроїв, завдяки чому можна без участі людини з високою ефективністю вирішувати інтелектуальні завдання. Будь-яке завдання для комп'ютера постає послідовністю обчислень. Результат виконаного завдання може бути наданий користувачеві за допомогою різноманітних пристроїв уведення-виведення інформації.

Останнім часом персональні комп'ютери використовуються як інструмент доступу до комп'ютерних мереж.

Нині проводяться ґрунтовні розробки щодо створення оптичних комп'ютерів (digital optical computer), в основі яких лежить оптичний процесор, що дозволяє використовувати замість традиційних електричних світлові сигнали. Операції виконуються за рахунок маніпуляції потоків світла, завдяки чому досягається висока продуктивність. Так, оптичний комп'ютер другого покоління «DOC-II», розроблений лабораторією «Bell», при пошуку слова може перевіряти до 80 000 сторінок тексту на секунду [254].

Таким чином, основним призначенням комп'ютера є передавання, зберігання та оброблення інформації, в тому числі з метою забезпечення «цифрового безсмертя» — «інформаційного безсмертя» даних.

Суперкомп'ютер (англ. *supercomputer*) — це обчислювальна машина, що значно перевершує за своїми технічними параметрами більшість існуючих комп'ютерів. У цей час суперкомп'ютерами прийнято називати комп'ютери з величезною обчислювальною потужністю. Такі машини використовуються для роботи над проблемами, що вимагають найбільш складних обчислень (наприклад, прогнозування погодно-кліматичних умов, виникнення Всесвіту, моделювання ядерних випробувань і под.), що в тому числі відрізняє їх від серверів і мейнфреймів (англ. *mainframe*) — комп'ютерів з високою загальною продуктивністю, покликаних вирішувати типові завдання (наприклад, обслуговування великих баз даних або одночасна робота з безліччю користувачів).

Суперкомп'ютер став формуватися перш за все як інтегратор обчислювальних ресурсів для вирішення різних «ресурсоємних» наукових завдань. Ідея ефективнішого використання обчислювальних потужностей шляхом з'єднання безлічі комп'ютерів в єдину структуру виникла в науковому співтоваристві порівняно давно — в епоху мейнфреймів. Суперкомп'ютери, не об'єднані в територіально розподілену систему, мають істотні вади.

Персональний суперкомп'ютер дає змогу дослідникам вирішувати ресурсномісткі завдання, не звертаючись до масивних кластерних систем, тим самим значно прискорюючи роботу [248]. Так, сьогодні найпотужніший у світі суперкомп'ютер фірми IBM BLUE GENE/L («Блакитний ген») складається з 65 536 обчислюваних ядер, що розміщені в 64 серверних стиках по 1024 блоки, виконує 135,5 трильйо-

нів терафлопс, при цьому займає площу, рівну половині тенісного корту, споживаючи всього 1,6 Мегават енергії.

Нагадаємо, що Ват (Вт, W) є одиницею вимірювання потужності, відповідно з чим 1 Мегават — це 10^6 Вт, а терафлопс є величиною, що використовується для виміру продуктивності комп'ютерів і показує, скільки операцій з плаваючою комою в секунду виконує дана обчислювальна система: 1 терафлопс відповідає трильйону операцій на секунду.

У червні 2006 р. уряд РФ схвалив пропозицію Міністерства освіти і науки про розроблення проекту нової суперкомп'ютерної програми «СКІФ-ГРІД» Союзної держави Росії та Білорусі. В Україні у 2006 р. відбулася презентація проекту створення Центру суперкомп'ютерних обчислень. Цей стратегічний проект веде до зміни рейтингу України в системі могутніх комп'ютерів.

Створення Центру суперкомп'ютерних обчислень підтримане державою і передбачає можливість виконання надскладних обчислень ученими, користувачами із різних регіонів України. Для цього пропонується використовувати українську телекомунікаційну мережу URAN (Ukrainian Research Academic Network), яка має регіональні центри в Харкові, Львові, Донецьку, Одесі, Сімферополі, Дніпропетровську. Параметри Центру суперкомп'ютерних обчислень за швидкістю оброблення інформації, обсягом пам'яті, можливістю нарощування кластерної структури тощо знаходяться на рівні світових показників [82, с. 29–34].

Отже, цей суперкомп'ютер — перший за потужністю в Україні і другий серед 50 кращих суперкомп'ютерів країн СНД. Очікується, що його запуск у роботу сприятиме підвищенню якості, доступності і конкурентоспроможності освіти і науки на світовому ринку праці та освітніх послуг, надасть нові можливості для наукового пошуку і технологічного розвитку.

о ***Історія Грід***

Порівняно недавно з'явився, але вже встиг стати популярним термін «Grid», що означає середовище, в якому об'єднані обчислювальні ресурси, що перебувають у різних місцях глобальної телекомунікаційної мережі. Це середовище призначене для виконання розподілених обчислень, що використовують значні ресурси.

Історія Грід починалася в 90-ті роки XX ст., коли виникла ідея створити із численних суперкомп'ютерних центрів США мега-комп'ютер, здатний надати користувачам можливість одержувати практично необмежені ресурси для обчислень і зберігання даних. Термін Grid computing було введено за аналогією з терміном power grid (електромережа). Користувачі комп'ютерних потужностей дістануть можливість прямого підключення до віддаленої обчислювальної мережі (так само, як до електроенергії через побутові розетки). Основні ресурсні елементи Грід-систем — суперкомп'ютери і суперкомп'ютерні центри, а найважливіша інфраструктурна складова — високошвидкісні мережі передавання даних.

Зараз інтерес до Грід дуже високий практично у всіх країнах світу, що виявляється у великій кількості національних і інтернаціональних проектів, дослідницьких робіт і публікацій з цієї тематики. Пояснюється це тим, що такі інститути сучасного суспільства, як банки, служби управління та моніторингу, торговельні і виробничі підприємства, мають розподілену структуру і відчувають потребу в інфраструктурі, що дозволяє організувати корпоративну та міжкорпоративну взаємодію на основі розподілених програмних мереж.

Авторами концепції Грід вважаються Ян Фостер з Арагонської національної лабораторії університету Чікаго і Карл Кессельман з Інституту інформатики Університету Південної Каліфорнії. Саме Фостер і Кессельман у 1998 р. вперше запропонували термін Grid computing для позначення універсальної програмно-апаратної інфраструктури, яка об'єднує комп'ютери і суперкомп'ютери в територіально розподілену інформаційно-обчислювальну систему. Фостер і Кессельман стояли і біля витоків розроблення першого стандарту конструювання Грід-систем, вільно поширюваного програмного інструменту з відкритим кодом Globus Toolkit. На думку Я. Фостера, підходи на основі відкритих стандартів (подібні Globus Toolkit) врешті-решт перетворять Грід на пануючий напрям розвитку корпоративних інформаційних інфраструктур. Набагато успішніше просуваються Грід-технології в науково-освітній сфері, що значною мірою пояснюється активною фінансовою підтримкою різноманітних Грід-проектів державними структурами.

У 1994 р. запроваджено проект створення всесвітньої комп'ютерної мережі GLORIAD (абревіатура від Global Ring Network for Advanced Application Development — Глобальна кільцева мережа для розвитку прикладних досліджень) — волоконно-оптичного кільця в Північній півкулі, що об'єднує обчислювальні ресурси різних науково-дослідних організацій США, Канади, Європи, Росії, Китаю і Південної Кореї (головним чином фізичних центрів).

У 2001 р. одержав розвиток проект розроблення та реалізації інформаційно-обчислювальної системи під назвою LHC Computing Grid (LCG). Проект передбачає створення регіональних центрів та розроблення специфічних комп'ютерних програм для забезпечення розрахунків. Результатом моделювання системи LHC, проведеного наприкінці 90-х років XX ст. у межах міжнародного проекту MONARC, стала розподілена модель архітектури для подальшого оброблення та аналізу до регіональних центрів.

У 2001 р. у США стартував проект TeraGrid, що фінансується Національним науковим фондом науки (NSF), основним завданням якого стало створення розподіленої інфраструктури для проведення високопродуктивних (терафлопсних) обчислень. У травні 2004 р. Європейським союзом було створено аналог американської TeraGrid — консорціум DEISA (Distributed European Infrastructure for Supercomputing Applications), який об'єднав у Грід-мережу провідні національні суперкомп'ютерні центри ЄС.

У 2004 р. завершився трирічний проект European DataGrid (EDG), в рамках якого було побудовано тестову інфраструктуру обчислень і обміну даними для потреб європейського наукового співтовариства. На основі цих напрацювань було започатковано новий міжнародний проект організації високопродуктивної Грід-мережі Enabling Grids for E-Science (EGEE). Нині в проект входять 70 наукових установ із 27 країн світу, об'єднаних в 12 федерацій. У рамках цього проекту має бути побудовано найбільший у світі Грід з сумарною обчислювальною потужністю 20 000 CPU.

У тісній взаємодії з проектом EGEE розвивається і магістральна європейська мережа для освіти і науки — GEANT. Вона здатна якісно змінити оброблення інформації радіоастрономічних комплексів, реєструючі системи яких розташовано на значному віддаленні одна

від одної. У США на базі Грід-технологій створено Національний цифровий центр мамографії із загальним обсягом даних (мамограм) 5,6 петабайта, який надає медикам можливість миттєвого доступу до записів мільйонів пацієнтів.

Великі можливості надає проект SETI@home, ініційований астрономами Університету Каліфорнії — Берклі. У рамках проекту було створено віртуальну Грід-мережу, яка регулярно аналізує дані, що надходять із радіотелескопу Arecibo в Пуерто-Ріко з метою пошуку позаземного розуму. За допомогою інтернету SETI об'єднав обчислювальну потужність понад 5 млн персональних комп'ютерів і вже виконав обчислювальну роботу, еквівалентну більш ніж 600 тис. років роботи ПК.

У США успішно функціонують чотири національні Грід-мережі: комп'ютерна мережа національного фонду наукових досліджень (NSF Comp. Grid), інформаційна мережа підтримки НАСА (NASA Information Power Grid), глобальна інформаційна мережа міністерства оборони (DOD GI Grid) і мережа суперкомп'ютерної ініціативи міністерства енергетики (DOE ASCI Grid). У 2004 р. офіційно оголошено про початок роботи президентської стратегічної GRID-програми (Strategic Grid Computing Initiative), основною метою якої є створення єдиного національного простору високопродуктивних обчислень (National High Performance Computing Environment).

У 2005 р. Єврокомісія підготувала спеціальну програму вартістю 13 млрд євро, в рамках якої Грід-компьютінгу відводиться роль стимулятора і найважливішого ресурсу для перетворення Євросоюзу на найбільш конкурентоспроможну в світі економіку знань.

З 2000 р. ведуться роботи щодо освоєння Грід-технологій у Китаї. Тривалий час інформацію про те, на якій стадії знаходиться реалізація проекту ChinaGrid, було фактично засекречено. Інформаційна бомба вибухнула у середині липня 2006 р., коли китайські ЗМІ привселюдно оголосили про завершення роботи над Китайським освітнім Грід-проектом (China Educational Grid Project, CEGP). CEGP об'єднав комп'ютерні мережі декількох десятків найбільших університетів країни і надав мільйонам китайських студентів прямий доступ до баз даних, онлайнових навчальних курсів і сервісних застосувань з різноманітних напрямів і дисциплін.

У січні 2006 р. в Афінах було офіційно оголошено про початок виконання проекту EUChinaGRID, що фінансується Європейською комісією. Головна його мета — об'єднання європейських і китайських Грід-інфраструктур з метою підвищення ефективності сумісного використання різних наукових застосувань, що працюють в Грід-середовищі. Стратегічний альянс ЄС і Китаю, що намітився, цілком можна розглядати як одну із перших спроб створення сильної Грід-противаги претензіям США на світове лідерство в цій великомасштабній технологічній гонці.

Незабаром до цього альянсу може підключитися й Індія, яка також оголосила про початок реалізації власної Національної Грід-комп'ютінгової ініціативи GARUDA, що передбачає об'єднання в Грід-мережу 17 найбільших науково-дослідних центрів країни. До теперішнього часу національні програми з розвитку Грід-технологій реалізуються практично всіма технологічно розвиненими країнами. Усі сучасні концепції та підходи до побудови глобальної Грід-системи (Грід як обчислювальна послуга — Sun Microsystems; Грід як система емуляції персонального комп'ютера і його заміни інтернет-комунікатором — AMD; Грід як єдина операційна система, що об'єднує обчислювальні потужності в глобальний суперкомп'ютер, — Google; Грід як віртуальна організація, що формує однорідний простір ІКТ-взаємодії, — Oracle) вимагають високошвидкісних мереж [251].

Найважливішим серед таких проектів став європейський проект EGEE (Enabling Grids for E-science in Europe). Його мета — об'єднати національні, регіональні і тематичні Грід-розробки, що вже ведуться, в єдину цілісну Грід-інфраструктуру для підтримки наукових досліджень. Від самого початку роботи EGEE в 2004 р. у проекті брали участь не тільки європейські, а й американські університети, вісім російських науково-дослідних інститутів, лабораторії з Ізраїлю. Загалом у ньому задіяно 70 лабораторій із 27 країн світу. Важливо зазначити, що Європейський Союз тільки для розроблення цього проекту і його розгалужень виділив 100 млн євро строком на чотири роки [54, с. 432–438].

Таким чином, створення виділеної високошвидкісної мережі передавання даних для Грід-систем — це ключовий елемент зниження

собівартості оброблення біта інформації і головна перевага в конкуренції глобальних проектів.

Отже, визначимо, що Грід (Grid) — це узгоджене, відкрите і стандартизоване середовище, яке забезпечує гнучке, безпечне, скоординоване розділення ресурсів у межах віртуальної організації.

о ***Інтернет і Грід-концепція***

Інтернет (англ. скороч. від *Inter*connected *Net*works — об'єднані мережі) — це глобальна телекомунікаційна мережа інформаційних та обчислювальних ресурсів. Рекомендується написання слова з прописної букви. Коли слово *internet* написано з рядкової літери, воно означає тільки об'єднання мереж за допомогою маршрутизації пакетів даних, при цьому в таких випадках не мається на увазі глобальний інформаційний простір Інтернет. Утім, у нетехнічній лексиці ці поняття, як правило, не розрізняють.

Всесвітня комп'ютерна мережа Інтернет разом із персональними комп'ютерами утворює технологічну основу для розвитку міжнародної концепції «Всесвітнього інформаційного суспільства». Розвиток національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним з пріоритетних напрямів державної політики у сфері інформатизації, задоволення конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства, забезпечення авторського права у сфері функціонування Інтернету [150].

Грід-концепція ґрунтується на традиційних технологіях мереж Інтернет і розвиває їх, однак уперше серйозно ставиться питання про гарантовану якість обслуговування. У цьому контексті можна говорити про Грід як про Інтернет наступного покоління [42, с. 8–16]. Наріжним каменем розвитку і використання Грід- і суперкомп'ютерних технологій є телекомунікаційна інфраструктура. Ці технології мають потребу в продуктивних каналах передавання даних — не менш 1 Гбіт у секунду. Разом із тим слід визнати, що за допомогою Інтернету створювати повноцінні корпоративні інформаційні бази даних дотепер неможливо. Дійсно, якщо припустити, що мінімальний інформаційний обсяг такої персональної бази даних повинен бути по-

рівняний з інформаційним обсягом пам'яті людини і становити, наприклад, не менш 10 терабайт (технічно це можливо), а пропускна здатність телефонного модему — 100 кілобайт, то при безперервному щоденному восьмигодинному режимі роботи для завантаження такої персональної пам'яті [4] — [10] буде потрібно 10 000 000 000 000/100 000 = 100 000 000 с = 27778 год = 3472 доби = 9,5 років. Насправді ж, якщо врахувати реальну пропускну здатність модему і реальний час пошуку користувачем потрібної інформації, то ця цифра зросте ще на декілька порядків.

Грід передусім є сервісом для сумісного доступу до географічно віддалених комп'ютерних ресурсів. Важлива обов'язкова вимога — забезпечення надійності доступу до обчислювальних ресурсів. При цьому має гарантуватися безпека як для завдання, що виконується (завдання і дані не повинні губитися і мають бути захищені від несанкціонованого доступу до них), так і для використовуваного комп'ютерного ресурсу.

о ***Потенціал Грід-мереж і нова комп'ютерна революція***

XXI ст. стає епохою масового впровадження Грід-технологій. Людство стоїть на порозі нової комп'ютерної революції: на зміну Інтернету йде супермережа — Грід, яка дозволить використовувати обчислювальні надпотужності інтелектуальних систем підтримки прийняття рішень у режимі віддаленого доступу, про що вже з'явилися наукові розробки [53].

У результаті нової хвилі комп'ютерної революції відбудеться трансформація звичного на сьогодні WWW (World Wide Web — Інтернету) в WWG (World Wide Grid — у всесвітню Грід-мережу). Магічне Грід-середовище, здатне віртуалізувати процесори, пам'ять і комунікації, обіцяє перетворити всі комп'ютерні ресурси світу на свого роду гігантський мультипроцесор, що володіє практично необмеженими обчислювальними можливостями.

Застосування Грід може дати нову якість вирішення таких класів завдань: 1) масове оброблення потоків даних великого обсягу; 2) багатопараметричний аналіз даних; 3) моделювання на віддалених суперкомп'ютерах; 3) реалістична візуалізація великих наборів даних; 4) складні бізнес-застосування з великими обсягами обчислень.

Потенціал Грід-технологій вже зараз оцінюється дуже високо: він має стратегічний характер, оскільки повинен стати провідним обчислювальним інструментарієм для розвитку високих технологій у різних сферах людської діяльності. Такі високі оцінки можна пояснити здатністю Грід на основі надійного віддаленого доступу до ресурсів глобально розподіленої інфраструктури розв'язати дві основні проблеми: а) створення розподілених обчислювальних систем надвисокої пропускної спроможності при одночасному підвищенні ефективності використання (до 100 %) наявного парку обчислювальної техніки шляхом залучення до Грід тимчасово простоюючих ресурсів; б) створення широкомасштабних систем моніторингу, управління, комплексного аналізу і обслуговування з глобально розподіленими джерелами даних, здатних підтримувати життєдіяльність державних структур, організацій і корпорацій.

Отже, Грід-технологія виглядає однією з пріоритетних інформаційно-обчислювальних інновацій XXI ст.

о ***Сфери застосування та класифікація Грід-технологій***

Хоча Грід-технології мають потенціал для багатьох застосувань, але поки що можна назвати тільки декілька проектів, близьких до практичного впровадження. Грід-технології вже активно застосовуються як державними організаціями управління, оборони, сфери комунальних послуг, освіти [41, с. 28–32], так і приватними компаніями, наприклад, фінансовими і енергетичними.

Сфера застосування Грід зараз охоплює ядерну фізику, захист навколишнього середовища, прогноз погоди і моделювання кліматичних змін, чисельне моделювання в машино- і авіабудуванні, біологічне моделювання, фармацевтику та ін. [59, с. 17–25].

Грід-технології можуть бути класифіковані на: 1) обчислювальні Грід-технології — призначені для створення віртуального суперкомп'ютера, що динамічно агрегує велику кількість індивідуальних комп'ютерів; 2) дані — Грід (DataGrid) — технології спеціалізовані на розподілі величезних обсягів даних; інформації та знань; 3) спільні Грід-технології — створюють віртуальне середовище.

Впровадження Грід-технологій ставить на порядок денний — проблему створення міжгалузевих центрів ресурсів, служб і користувачів Грід-інфраструктури. Тому перспективою Грід-технології є об'єднання

ресурсів шляхом створення комп'ютерної інфраструктури нового типу, що забезпечує глобальну інтеграцію інформаційних і обчислювальних ресурсів на основі мережевих технологій і спеціального програмного забезпечення проміжного рівня (між базовим і прикладним програмним забезпеченням), а також набору стандартизованих служб для забезпечення надійного спільного доступу до географічно розподілених інформаційних і обчислювальних ресурсів (окремим комп'ютерам, кластерам, сховищам інформації та мережам).

Одним з таких проектів може стати електронний офіс, який передбачає наявність інтегрованих пакетів прикладних програм, що включають спеціалізовані програми та інформаційні технології, котрі забезпечують комплексну реалізацію завдань предметної частини. На теперішній час все більше поширюються електронні офіси, обладнання та співробітники яких можуть знаходитися в різних приміщеннях. Необхідність роботи з документами, матеріалами, базами даних конкретної організації або закладу в домашніх умовах, в готелі, транспортних засобах призвела до появи інформаційних технологій віртуальних офісів. Такі інформаційні технології засновуються на роботі локальної мережі, з'єднаної з територіальною або глобальною мережею. Завдяки цьому абонентські системи співробітників закладу, незалежно від того, де вони знаходяться, виявляються включеними в загальну для них мережу.

о ***Грід-технології в криміналістиці***

Почнемо з того, що, на жаль, дотепер поза увагою ґрунтовного вивчення залишаються системні проблеми оновлення процесу протидії злочинності з використанням суперкомп'ютерного і Грід-технологічного потенціалів.

Що ж таке Грід-технології у сфері криміналістики? Грід-технології зможуть використовуватися для інтегрування криміналістичних знань, розвитку графіки і прогресивних засобів розкриття злочинів. Криміналістичні системи, засновані на Грід-технологіях, можуть зробити значний внесок у плані доступу до розподілених джерел оперативно-розшукових даних, поліпшення можливості використовувати комп'ютерні програми інформаційних центрів МВС та інших правоохоронних органів країн, які ввійдуть у такий актикримінальний Грід-технологічний блок. Останній має стати особливим середови-

щем, де криміналістична інформація повинна бути зібрана, оброблена та у необхідних випадках швидко надана користувачам: прокурорам-криміналістам, слідчим, оперативним працівникам та іншим відповідним посадовим особам.

Майбутній розвиток Грід-технологій характеризуватиметься повним засвоєнням сервіс-орієнтованої парадигми, технологій веб-сервісу, повною віртуалізацією ресурсів і сервісів, що зумовлено використанням семантичної інформації та онтологій. Доступність і застосовність стандартів безпеки, підтримка якості сервісу, створення моделей бізнесу в середовищі Грід мають стати чинниками розвитку і впровадження Грід-технології, що стануть специфічними для проблем оброблення криміналістичних і оперативно-розшукових даних. Адже ресурсами в криміналістичній Грід-концепції є бази даних, комп'ютерні ресурси, експертні знання, криміналістичні прилади.

Отже, кінцевою метою повинно було б стати створення антикримінальної інформаційної сфери XXI ст., що вбирає в себе всі ресурси електронної криміналістики, включаючи безпеку і авторизацію ресурсів для того, щоб управляти незалежними вузлами Грід-системи [184].

Однак у правоохоронну діяльність суперкомп'ютерні технології впроваджуються повільно і фрагментарно; тут замало високоякісного, добре документованого бізнесу, дуже мало широкомасштабних впроваджень. Тому в заявках на фінансування пріоритети мають бути розставлені так, щоб зробити життєво важливим діяльність кабінетів криміналістики обласних прокуратур, які базується на Грід-технологіях.

Таким чином, у сфері правоохоронної діяльності специфічна організація особливих режимів зберігання та оброблення інформації, зв'язок із міжнародними органами кримінальної юстиції забезпечать реалізацію активної, наступальної стратегії у боротьбі зі злочинністю за рахунок застосування Грід-технологій у розкритті злочинів.

Отже, в цьому підрозділі визначено місце суперкомп'ютерних та Грід-мереж в інформаційно-правовій сфері. Розвиток і впровадження в правоохоронну діяльність суперкомп'ютерних та Грід-технологій мають стратегічний характер. Застосування суперкомп'ютерних та Грід-технологій може забезпечити новий якісний рівень розвитку

заходів протидії щодо концептуального стримування інтелектуалізації злочинності, а іноді й реалізувати принципово новий підхід в обробленні величезних обсягів експериментальних даних, забезпечити моделювання надскладних процесів, візуалізацію великих наборів даних, у тому числі кібернетичне моделювання при розслідуванні злочинів у сфері нових технологій зі значними обсягами обчислень [52]. Тому можна сказати, що Грід-технології випереджають на 3–5 років існуючі у правоохоронних органів України, тобто фактично є антикримінальними технологіями майбутнього.

3.2. Правовий моніторинг цифрової інформаційної мережі в Інтернет-просторі

○ *Цифрові права людини та мультимедіа-технології*

Інформаційно-медійна, комунікативна системи є мережею складних, багатомірних життєвих процесів, що складається з різноманіття лінійних і нелінійних суб'єкт-об'єктних і суб'єкт-суб'єктних відносин [162, с. 18].

Пригадаємо, що цифровий (або дигітальний) формат (англ. *digit* — цифра, від лат. *digitus* — палець) є типом сигналів і форматів даних в електроніці, що використовують дискретний стан (на відміну від аналогового сигналу, що змінюється безперервно). У загальному розумінні *формат інформації* — це специфікація (однозначний опис) структури даних.

Нині розрізняють декілька видів інформаційних форматів: а) відкритий формат як загальнодоступна специфікація зберігання цифрових даних; б) тестовий формат як формат зберігання текстової інформації; в) графічні формати як формати зберігання графічної інформації — фотографій і рисунків; г) цифрові звукові формати як формати запису звуку. Крім цього, існують й інші формати зберігання інформації, зокрема, RAW-формат даних, який не має чіткої специфікації і містить неопрацьовані або мінімально опрацьовані дані, що дає змогу уникнути втрат інформації.

Цифровий зв'язок є галуззю техніки, яка пов'язана з передаванням цифрових даних на відстань. Термін «цифровий» також позначає

спосіб збереження даних у цифровому (двоїчному) форматі, адже цифрові сигнали існують як послідовності чисел у часі. Звичайно використовуються два числа: 0 та 1 (так звані біти). Цифрові види зв'язку — це категорія способів радіозв'язку, при якій використовується модуляція несучої частоти радіосигналу за допомогою цифрового сигналу. Сьогодні цифровий зв'язок з успіхом використовується також для передавання аналогових сигналів (наприклад, таких безперервних, як мова та зображення). Останні з цією метою відцифровуються (дискретизуються).

Перехід на нові формати детермінував суттєві зміни щодо зменшення розмірів при одночасному збільшенні обсягів зберігання інформації. Зокрема, до значного зростання можливостей відеомоніторингових технологій призвів перехід різних технічних пристроїв відеоспостереження в цифровий формат.

Мультимедіа-технології є технологіями одночасного використання різних форм представлення інформації та її оброблення в єдиному об'єкті-контейнері. Термін «мультимедіа» також найчастіше використовується для позначення носіїв інформації, що дозволяють зберігати значні обсяги даних та забезпечувати достатньо швидкий доступ до них (першими носіями такого типу були CD — *compact disc)*. У такому разі термін «мультимедіа» означає, що комп'ютер може використовувати такі носії та надавати користувачеві інформацію через всі можливі види даних (аудіо, відео, анімація, зображення та ін.), доповнюючи такі традиційні способи надання інформації, як текст.

У сучасних цифрових системах інформаційних технологій застосовуються кабельні (волоконно-оптичні), супутникові, радіорелейні та інші лінії і мережі зв'язку. Разом із тим до основних недоліків цифрових технологій відеоспостереження можна віднести те, що зараз більшість камер відеоспостереження програють аналоговим камерам щодо світлочутливості, передавання кольору при низьких рівнях освітленості. Крім цього, витрати на захист даних у цифрових системах трохи вище, ніж при роботі з аналоговими технологіями відеоспостереження, особливо якщо використовуються вже існуючі комп'ютери і мережі. Також слід відзначити, що аналоговий сигнал постає в цифровому вигляді з деякою неточністю.

Отже, характерними рисами електронного каналу поширення інформації є відкритість і демократичність (необмежений доступ), оперативність і інтерактивність, таргетінг (інтернет-можливість індивідуального спілкування), конективність (постійний контакт із затребуваними інформаційними потоками), мультимедийність. Утім, з другого боку, в цьому зв'язку окремо виникає проблема цифрових прав людини.

Нині інформаційна нерівність визначається низьким рівнем інформатизації, що перешкоджає широкому впровадженню інформаційних технологій. В умовах технологічного відставання і недостатнього розвитку інформаційного суспільства рівень інформаційної нерівності стрімко зростає пропорційно збільшенню сервісних та інформаційних можливостей Інтернету.

Звідси визначимо, що цифрові права — це розширення і застосування універсальних прав людини до потреб суспільства, заснованого на інформації.

У широкому розумінні термін «інформаційна нерівність» (англ. *digital divide*) означає розходження (нерівність) у доступі до інформації, до накопичених суспільством знань. У вузькому значенні під цифровою нерівністю розуміється новий вид соціальної диференціації, що випливає з різних можливостей використання новітніх інформаційних і телекомунікаційних технологій.

У глобальному контексті термін «цифрова нерівність» став активно використовуватися при аналізі нерівності між країнами у сфері нових технологічних розробок. Цифрові права передбачають подолання або зниження інформаційної нерівності, тобто доступ до інформації.

Тому для ефективної боротьби з інформаційною нерівністю необхідна активна позиція держави.

Таким чином, терміни «цифровий бар'єр», «цифрова нерівність», «інформаційна нерівність» є близькими поняттями, що означають обмеження можливостей соціальної групи через відсутність у неї доступу до сучасних засобів комунікації.

Отже, базові цифрові права людини включають право інформаційного доступу до електронної мережі, право вільно спілкуватися і висловлювати думки у телекомунікаційній системі, право на інформаційну обмеженість приватної сфери.

о ***Система високотехнологічного інформаційного права та Інтернет***

У країнах Європи з 90-х років XX ст. з'являються нормативно-правові акти, що стосуються регулювання відносин в Інтернеті, де визнається основний принцип Інтернет-індустрії — саморегуляція. Останніми роками в Україні поступово збільшується кількість нормативно-правових актів, спрямованих на регулювання такого засобу доступу до інформації, як Інтернет, що вимагає систематизації в рамках високотехнологічної теорії інформаційного права.

Важливим напрямом розвитку вітчизняного законодавства в інформаційній сфері є регулювання саме відносин, пов'язаних з цифровими технологіями мережі Інтернет. На сьогодні зусилля науковців спрямовані саме на дослідження новітніх інформаційних процесів та ефективного забезпечення їх правової регуляції [143]. Зокрема, Закон України «Про телекомунікації» визначає, що Інтернет — це всесвітня інформаційна система загального доступу, яка логічно пов'язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами.

Адміністрування адресного простору українського сегменту мережі Інтернет включає комплекс організаційно-технічних заходів, необхідних для забезпечення функціонування технічних засобів підтримки адресування, у тому числі серверів доменних назв українського сегменту мережі Інтернет, реєстру доменуUA в координації з міжнародною системою адміністрування мережі Інтернет, спрямованих на систематизацію та оптимізацію використання, обліку та адміністрування доменів другого рівня, а також створення умов для використання простору доменних імен на принципах рівного доступу, захисту прав споживачів послуг Інтернет та вільної конкуренції. Утворення адресного простору, розподіл і надання адрес, маршрутизація інформації між адресами здійснюються відповідно до міжнародних вимог [121; 122].

Таким чином, управління використанням Інтернет охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь усі зацікавлені сторони і відповідні міжурядові та міжнародні організації. Тому нині моніторинг інформаційних програм фактично постає як новий інструмент зворотного зв'язку з метою здійснення проектів, оцінювання програм чи вироблення політики.

о ***Методологія, принципи та функції інтернет-моніторингу***

Моніторинг (англ. *monitoring* — спостереження) — це процес поточного спостереження, контролю, оцінювання, аналізу і прогнозування ключових процесів у суспільстві на базі статистичних даних. У проекті Закону України «Про моніторинг телекомунікацій» визначення цього поняття сформульовано дещо інакше — як спостереження, відбір за певними ознаками, оброблення та реєстрація сеансу зв'язку в мережах телекомунікацій із застосуванням системи контролю мережі телекомунікацій.

Терміном «моніторинг мережі» називають роботу системи, що виконує постійне спостереження за комп'ютерною мережею в пошуках повільних або несправних систем, яка при виявленні збоїв повідомляє про них системному адміністратору. Система моніторингу Інтернет-мережі виконує спостереження за мережею в пошуках проблем і стежить за появою будь-яких погроз ззовні. Отже, моніторинг є інформаційним процесом, основними функціями якого виступають систематичне або безперервне збирання інформації про параметри складного об'єкта або дії.

З методологічної точки зору моніторинг інформаційних програм можна розглядати як процедуру щодо оцінювання, метою чого є виявлення та (або) фіксація ефектів триваючих загрозливих дій без з'ясування причин. Такий вид моніторингу виступає як внутрішня процедура, заснована на індикаторах та результатах, а також як інструмент збирання інформації і звітності та спрямована на збирання інформації про основні ресурси і продукти інформаційної програми. Особливою рисою моніторингу такого виду як інформаційного процесу є систематичність збирання та оброблення інформації.

Інформаційний моніторинг полягає в комплексі організаційно-правових та технологічних заходів щодо спостереження в інформаційній сфері, аналізу отриманих результатів і внесення коригувальних дій, спрямованих на усунення загрозливих показників. Обов'язковим його елементом є оцінювання та прогнозування стану соціального сприйняття у визначений проміжок часу, тобто оприлюднення результатів втручання і правового реагування щодо виявлених порушень закону в інформаційній сфері. Тобто, перш за все починати таке дослідження треба зі статистичного спостереження, а саме — зі збирання інформації.

Інтернет-моніторинг виконує одну або більше з трьох основних інформаційних функцій: 1) встановлює інформаційні відносини зі своїм оточенням в Інтернет-просторі; 2) забезпечує зворотний зв'язок та обмін інформацією з усіма суб'єктами в Інтернеті; 3) виявляє невідповідність інформації, що розміщена в Інтернеті, чинним нормам та правилам.

Система інформаційно-правового спостереження в Інтернет-просторі ще не дістала ґрунтовного впровадження в практичну діяльність, тому сьогодні вона фактично виступає інноваційним проектом. Звідси це додатково означає «проблему в проблемі». Основною умовою цього є наявність чіткої мети, вимог, параметрів інновацій [54, с. 529]. Тому моніторинг інноваційного проекту ґрунтується на декількох вирішальних припущеннях, покладених в основу будь-якої системи відстеження і контролю [200].

Слід відзначити, що до якої б галузі права не було віднесене порушення прав особистості в Інтернеті, організація своєчасного реагування є однією з найбільш ефективних форм їх правового захисту. Разом із тим можливість анонімної присутності в Мережі часто дозволяє сховати справжні імена авторів, джерел та осіб, які розмістили незаконну інформацію або вчинили інші правопорушення в Інтернеті, що становить певну складність при вирішенні питання про притягнення до відповідальності.

Таким чином, правовий інтернет-моніторинг є підвидом інформаційного моніторингу, оскільки являє собою систему спостереження в Інтернет-просторі за станом інформаційної злочинності і реалізації антикримінальних заходів.

о ***Мета та завдання правового моніторингу цифрових інформаційних мереж***

Процес спостереження, збирання інформації та попередження негативних наслідків в інформаційному просторі визначимо як правовий моніторинг цифрових інформаційних мереж. До основних стратегічних завдань у сфері надійності електронної інформаційної системи пропонується віднести постійний моніторинг різних загроз, які можуть спричинити шкоду нормальному функціонуванню органів, що ведуть боротьбу зі злочинністю, та запобігання реалізації цих загроз.

Важливим етапом модернізації і необхідною умовою освоєння нових технологічних коридорів передавання інформації у сфері боротьби зі злочинністю може стати антикримінальний моніторинг,

найефективнішим інструментом в сучасних умовах якого вважаємо правовий моніторинг цифрових інформаційних мереж. На підтвердження цього результати досліджень переконливо свідчать про те, що подібні заходи сприятимуть підвищенню результативності протидії транснаціональним злочинам і особливо тим, що вчиняються з використанням високих технологій [203–205].

Отже, потрібно погодитися з авторами, які проголошують необхідність розв'язання проблеми створення загальнодержавної інформаційної інфраструктури, відповідних організаційних структур, що формуватимуть систему збереження, опрацювання та поширення інформації, відповідатимуть за розроблення, впровадження і супровід новітніх технологій, здійснюватимуть контроль інформаційного простору і моніторинг інформаційно-психологічного впливу інформаційних ресурсів на теренах України.

Поняття інформаційної безпеки цифрової мережі органів, які ведуть боротьбу зі злочинністю, пов'язане із безпосередньо технікотехнологічними діями, що спрямовані на захист аналітичних відомостей і криміналістичних даних. Тому, про що слушно наголошують фахівці [12; 13], саме моніторинг інформаційних загроз національним інтересам дозволить визначити і територіальну локалізацію, і характер загроз. На основі даних про локалізацію загроз національним інтересам, виявлених тенденцій у стані законності і правопорядку потрібно конкретизувати антикримінальні заходи в загальнодержавному масштабі.

З метою спостереження за тенденціями розвитку інформаційної злочинності, орієнтування в причинах та умовах, що сприяють учиненню інтелектуальних злочинів, прийняття рішень щодо виконання поставлених завдань та проведення необхідних дій для досягнення мети на сучасному етапі слід орієнтуватися на пошукові, експертні, аналітичні, синтезуючі програмно-апаратні засоби, за допомогою яких можливо здійснювати розвідувально-аналітичні заходи у сфері сучасних інформаційних технологій. Використання зазначених програмно-апаратних засобів прискорить процес якісного оброблення інформації та прийняття рішень [119, с. 29–35].

Для ефективної протидії правопорушенням у сфері інформаційних технологій взаємодія правоохоронних органів має ґрунтуватися на розробленні системної програми антикримінального моніторингу.

Застосування правового моніторингу цифрових інформаційних мереж надасть змогу: 1) проводити моніторинг електронних мереж телекомунікації, збирати інформацію про злочини, що готуються злочинними формуваннями, з волоконно-оптичних каналів зв'язку, розвідки радіоефіру, комп'ютерної розвідки в Інтернеті; 2) виявляти, розкривати та розслідувати злочини, що вчиняються з використанням комп'ютерних технологій (кіберзлочинів); 3) виявляти фінансове підґрунтя організованої злочинності; 4) збирати, аналізувати та узагальнювати публікації у ЗМІ щодо окремих резонансних злочинів, тенденцій злочинності та інформаційно-психологічного впливу кримінальних структур на органи влади, зокрема на правоохоронні органи; 5) справляти інформаційно-психологічний вплив через ЗМІ з метою боротьби з організованою злочинністю та упередження негативного впливу кримінальних структур на суспільну свідомість тощо.

З метою відстеження протиправних проявів в Інтернеті, що становлять підвищену суспільну небезпечність, найбільш результативним може стати новий напрямок *«антикримінальне інтернет-патрулювання»*, що діятиме на випередження [185; 188; 191; 200].

Важливими є своєчасність і, головне, адресність доведення результатів правового інтернет-моніторингу. Порушення законів повинні бути структуровані в підгрупи (система індикаторів), які відображують стан законності в окремих галузях права, а потім, використовуючи традиційні аналітичні схеми, слід групувати їх за сферами життєдіяльності — внутрішньополітична, соціальна, економічна, екологічна, оборонна тощо, а отже, вибудовувати їх за ступенем небезпеки національним інтересам України, показувати їх прямі і опосередковані взаємозв'язки, визначати «критичні маси» таких показників. Його результати необхідно використовувати для інформування відповідних правоохоронних структур про стан інформаційної загрози і рівень захищеності національних інтересів, можливе загострення і появу нових загроз національним інтересам, підготовки пропозицій щодо вдосконалення системи засобів забезпечення національної безпеки.

Враховуючи викладене, вважаємо, що було б доцільно створити високотехнологічний центр оперативного правового моніторингу з екраном колективного користування для відображення різних да-

них — відеозображень, графіків і діаграм, текстової документації в електронному вигляді тощо. Досвід роботи подібних центрів, а також аналіз зарубіжних і вітчизняних досягнень у цій сфері свідчать про те, що їх створення істотно підвищує якість і оперативність обробления правової інформації.

З огляду на це антикримінальний моніторинг є інноваційним процесом у галузі забезпечення законності процесу кримінального переслідування як інформаційної системи спостереження, аналізу статистичної інформації про стан законності, оцінювання різнорівневих мікро- і макросоціальних чинників і прогнозування розвитку інформаційної злочинності.

Таким чином, зростанню ефективності антикримінальної діяльності в Інтернет-просторі може сприяти інноваційний проект правового моніторингу цифрової інформаційної мережі. Отже, доцільним є внесення відповідних доповнень до проекту Закону України «Про моніторинг телекомунікацій».

3.3. Створення й розвиток інноваційної інфраструктури в юриспруденції

○ *Інновації та інноваційна політика*

Інновації — це вперше створені і вдосконалені конкурентоспроможні та патентозахищені технології, товари та послуги, організаційно-технічні та економічні рішення виробничого, комерційного, адміністративного характеру, що суттєво підвищують якість виробництва і соціальної сфери. На шляху формування інноваційних зрушень в інформаційній сфері постає чимало проблем соціально-економічного і правового порядку, які гальмують їх утілення.

Інноватика — це галузь науки, що вивчає різні проблеми теорії інновацій, зокрема проблеми створення новин, реалізації нововведень, організаційного забезпечення інноваційних процесів [54, с. 646]. Інновація є основою технологічного розвитку будь-якої системи.

Базовим інструментом інноваційної діяльності сьогодні виступають програми і проекти. Проект — це унікальна (на відміну від опе-

рацій) діяльність, що має початок і кінець у часі, спрямована на досягнення певного результату (мети), створення певного унікального продукту або послуги при заданих обмеженнях по ресурсах і термінах, а також відповідає вимогам до якості і припустимого рівня ризику.

На основі системного підходу проект можна розглядати як процес переходу з вихідного стану в кінцевий. Отже, поняття «проект» поєднує різні види діяльності, що мають певні спільні ознаки: 1) спрямованість на досягнення окреслених цілей та конкретних результатів; 2) координоване виконання взаємозалежних дій; 3) обмеженість у часі з чітко визначеними початком і завершенням [103; 118]. Таким чином, під інноваційним проектом пропонується розуміти цілеспрямоване, заздалегідь обґрунтоване і заплановане новостворення, зміну або вдосконалення технології.

Інноваційний процес є процесом створення, розповсюдження та використання нововведень; перетворення нових видів і способів людської життєдіяльності (нововведень) на соціально-культурні норми та зразки, які забезпечують їх інституційне оформлення, інтеграцію та закріплення в культурі суспільства. Звідси інноваційний процес — це одна з основних соціокультурних передумов розвитку суспільної практики, збагачення її новими пізнавальними, технологічними, естетичними та всіма іншими формами людського досвіду.

Слід зазначити, що це питання розроблялося й в юридичній доктрині. Вагомий внесок у розвиток наукових розробок щодо правового регулювання окремих сторін інноваційного процесу зробили Ю. Атаманова, Ю. Жорнокуй, С. Погуляєв та ін. Зрозуміло, що саме створення та впровадження новітніх наукоємних технологій, які відповідають останнім досягненням науково-технічної еволюції, є основною метою інноваційної моделі економічного розвитку і показником ефективності інноваційного законодавства.

Неприпустимою є неузгодженість термінологічної бази в межах різних нормативно-правових актів інноваційного законодавства. Це стосується навіть законодавчих дефініцій інноваційної діяльності. В цілому ж дотепер існують два основні підходи до визначення інновацій — об'єктний і процесний (функціональний). Прихильники об'єктного підходу інтерпретують поняття інновації як результат творчого процесу. При процесному підході під інновацією розуміють-

ся процес уведення нових засобів і технологій замість чинних на сьогодні. Видається більш ґрунтовною перша точка зору, оскільки переваги дає саме кінцевий результат впровадження в конкретні заходи, а не віртуальний процес як такий.

У той же час існують розбіжності із приводу визначення самого кінцевого результату. Деякі автори поєднують поняття «інновація» і «нововведення». На нашу думку, слід розрізняти ці нетотожні поняття.

Таким чином, інноваційна політика в інформаційній сфері є складовою політики держави, оскільки визначає цілі і пріоритети інноваційної стратегії та організаційно-правовий механізм її реалізації.

о ***Управління інноваційними проектами***

Проектний формат в останні десятиріччя широко використовується державними структурами. Разом з тим залучення методології управління проектами як інструмент планування, контролю та координації здійснення проектів дозволяє заощаджувати значні ресурси, реалізовувати цілі проекту в менший строк і, найголовніше, здійснювати успішне управління. Таким чином, управління інноваційним проектом являє собою цілеспрямований процес досягнення цілей проекту при обмеженнях на фінансові, матеріальні, людські, інформаційні, технологічні та інші ресурси.

Концепцію управління проектами доцільно застосовувати в інформаційній діяльності при впровадженні інновацій. Тому ми впевнені, що згодом робота на цій ділянці може бути виділена в окремий спеціальний проектно-орієнтований напрямок діяльності у сфері нових технологій — управління інформаційними проектами [54, с. 528–529].

Методологія управління проектами дає змогу перетворити процедуру створення інноваційного продукту в добре організований і керований процес. Освоєння методів управління проектами дає можливість підходити до будь-якого проекту з єдиних позицій [54, с. 488].

Фактично «пріоритетні національні проекти» стають акмеологічною програмою щодо зростання «інтелектуального капіталу», в нашому випадку — використання інформаційних технологій нового покоління у правовій сфері.

Оскільки інновація інформаційної діяльності має визначатися як процес і як об’єкт, пропонуємо ввести такі визначення.

Інновація інформаційної діяльності як процес — комплекс інформаційних заходів, спрямованих на впровадження в процес діяльності технологічних винаходів, нововведення наукових інформаційних методик, які ще не набули достатнього розвитку та теоретичного визнання, але є перспективними для застосування та використання на практиці.

Інновація інформаційної діяльності як об'єкт — нові інформаційні технології, які є результатом досягнень науково-технічного прогресу та передового технологічного досвіду і належать як до радикальних, так і до поступових змін, що забезпечують якісне підвищення ефективності інформаційної діяльності, оскільки вони є наслідком інвестування в наукову розробку для отримання нових знань, які раніше не застосовувалися на практиці.

З огляду на це потрібно створити єдину телекомунікаційну систему управління ефективністю антикримінальних інформаційно-технологічних розробок, орієнтовану на діяльність в оновлених умовах боротьби зі злочинністю.

Одночасно потрібно погодитися із тим, що на сьогодні державна інноваційна політика залишається розбалансованою та малоефективною, такою, що вимагає перманентної корекції. Державна інноваційна політика повинна здійснюватися відповідно до закріплених законодавчо принципів. Сьогодні, на відміну від попередніх часів, абсолютно зрозумілою та науково доведеною є ключова роль інновацій в економічному розвитку.

Інформаційне забезпечення суб'єктів інноваційної діяльності віднесено до основних принципів інноваційної політики. До системоутворюючих відносять функції «запуску» та підтримки розвитку нової інноваційної моделі розвитку, як, наприклад, створення законодавства, що відповідає новій державній інноваційній політиці [46, с. 5, 10].

Оскільки сприянню розвитку інноваційної інфраструктури в юриспруденції відводиться особлива роль, цей напрям має стати одним із першочергових у структурі інноваційної політики.

Політика розвитку високих технологій передавання інформації у сфері боротьби зі злочинністю є особливим компонентом державної інноваційної політики, на який покладається розвиток конкретних заходів щодо створення соціально-економічних, технологічних, організаційних і правових умов інноваційної безпеки.

Державна інноваційна політика є процесом, що передбачає витрати ресурсів та має певний результат, – тобто продукт політики. Звідси потрібно визначити, що продуктом інноваційної політики в юридичній галузі є нові технологічні засоби, що використовуються в різних галузях юриспруденції, серед яких окремо визначаються інноваційні проекти, до розгляду чого далі ми ще повернемось.

Термін «*інноваційна безпека*» є новим у понятійному апараті. Його зміст можна розуміти у дуалістичному значенні: 1) як системні заходи безпеки в інноваційних галузях економіки та соціальної сфери, що передбачено особливим правовим режимом; 2) як інноваційні (тобто новітні, «розумні», інтелектуальні, нестандартні) заходи безпеки, зокрема кримінально-правові, кримінологічні та криміналістичні, у першу чергу із застосуванням високих технологій.

Отже, як бачимо, системні заходи інноваційної безпеки мають таку структурну побудову: 1) юридичний аспект; 2) соціальний аспект; 3) технологічний аспект; 4) економічний аспект; 5) психологічний аспект.

Вважаємо, що до основних складових інноваційної безпеки можна віднести: 1) інформаційну безпеку, що у свою чергу складається з електронної (комп'ютерна як її складова), цифрової; психологічної безпеки; історико-культурна безпека тощо; 2) техніко-технологічна безпека; 3) енергетична безпека; 4) екологічна; 5) зовнішньополітична (або міжнародна) та внутрішньополітична безпека; 6) військова безпека. При цьому невід'ємною частиною кожного з названих факторів є юридична складова, що визначає багато аспектів, але передусім визначає особливий правовий режим. Звідси бачимо, що високотехнологічне інформаційне право як особливий регулятор соціотехнологічних відносин постає найвищою ланкою в структурі інноваційної безпеки.

о ***Електронна юриспруденція та цифрова юстиція***

Інформаційні процеси й новітні інформаційні технології знаходять широке впровадження в юридичній діяльності, що стає передумовами формування інноваційної інфраструктури в юриспруденції. Це має прояви у поступовому переході до можливості трансляції відкритих судових процесів у режимі «on-line» в Інтернеті. На першому етапі такі трансляції можуть відбуватися при розгляді справ

вищими судами, а згодом це торкнеться кожного суду як елемента судової системи держави. Такий порядок допоможе вирішити цілу низко гострих питань, зокрема стати додатковим чинником мінімізації корупції в судах.

Тобто фактично розпочався процес революційних технологічних перетворень у правозастосовній діяльності, що є ознаками створення цифрової юстиції. Наголосимо, що *цифрова юстиція* та *електронна юриспруденція* є поняттями хоча й близькими за змістом та взаємопов'язаними, але у зв'язку з різною структурною побудовою ці нові терміни неможна ототожнювати.

Під терміном «юриспруденція» (лат. *juris-prudentia* — правознавство) розуміють декілька взаємопов'язаних понять, основними з яких є такі: 1) правова комплексна наука, предметом якої є вивчення змістовних властивостей держави і права; 2) сукупність правових знань та система спеціальної підготовки юристів; 3) практичне застосування юридичних знань та практична діяльність юристів.

У загальному розумінні під терміном «юстиція» (лат. *justicia* — справедливість, від лат. *jus* — право) розуміють правосуддя, оскільки це вид правоохоронної та правозастосовної діяльності, в якому реалізується судова влада. За таким підходом, стане зрозумілим, що форма реалізації судової влади не може бути цифровою, електронною, високотехнологічною й т. п., оскільки має іншу природу. Але цей термін також має інше визначення як система судових закладів або судове відомство. Крім того, у залежності від сфери судочинства визначають кримінальну юстицію, цивільну, конституційну, міжнародну, військову, ювенальну й т. п. Звідси за останньою класифікацією практика застосування нового терміна «цифрова юстиція» особливого обурення викликати не може.

Визначимо основні функції, що можуть перетинатися від *цифрової юстиції* до *електронної юриспруденції* та навпаки: 1) електронний облік усіх кримінальних справ (а згодом – юридичних справ усіх категорій), надійшовши до суду, із позначенням дати, основних реквізитів (обвинувачений, запобіжний захід, наслідки судового розгляду, апеляції); 2) можливість надсилати учасниками судового розгляду електронні повідомлення, електронні скарги (програма *е*-скарга) та електронні клопотання (програма *е*-клопотання) та своє-

часне отримання електронних відповідей; 3) у судовій системі перейти до реалізації програми створення департаменту інформаційного обліку та електронної фіксації судових процесів, що функціонально зможе замінити секретарів судових засідань, оскільки хід судових засідань повністю буде фіксуватися фахівцем у галузі інформаційних технологій на оптичний диск, що долучатиметься до справи у запечатаному конверті, наприклад, як паспорт; 4) судова канцелярія перетвориться на судову електронну канцелярію.

Звідси можна стверджувати, що *електронна юриспруденція* формується як новий інститут інформаційного права, в межах якого досліджуються правові ідеї щодо можливості внесень прогресивних змін у механізм та способи регуляції інформаційного суспільства в умовах розвитку високих технологій.

Також до структури електронної юриспруденції органічно входить інноваційна система високотехнологічної підготовки юристів та практична діяльність останніх, що відбувається з широким використанням інформаційних технологій в електронному форматі. Однією з характерних особливостей тенденцій розвитку сучасного інформаційного суспільства є експонентне зростання обсягу нових знань і технологічних досягнень у всіх галузях науки й техніки. Звідси, можна спрогнозувати, що у найближчі часи наявність фахових знань юриста у галузі інформаційних технологій стане не факультативною, а обов'язковою підставою для професійного заняття юридичною діяльністю.

Глобальний характер інформаційного розвитку, формування транснаціональної інформаційно-телекомунікаційної інфраструктури породжує низку нових проблем, що пов'язані із забезпеченням цифрової безпеки особистості. Існують також додаткові підтвердження потреби щодо подібної модернізації інноваційної інфраструктури в юриспруденції.

Отже, враховуючи викладене, підсумуємо, що *цифрова юстиція* — це особливий вид правоохоронної та правозастосовної діяльності щодо забезпечення реалізації цифрових прав людини, основною формою чого є фіксація судових процесів з використанням цифрових засобів, оптичних приладів та електронної техніки, надання та розгляд доказів, свідчень й інших фактів, що можуть мати значення при розгляді юридичної справи, за допомогою високих технологій.

о ***Інформаційна культура юриста***

Успіх юридичної діяльності сучасного юриста значною мірою визначається рівнем його інформаційної культури. Під час виконання інформаційних процесів виникають суспільні відносини, що підлягають правовому регулюванню в інформаційній сфері (точка зору інформаційного права), тобто уявляє правовий механізм вирішення інформаційних питань. Звідси нормативною основою інформаційної культури юриста є інформаційні норми та інформаційно-правові норми й принципи.

Зміст інформаційної культури юриста виражається в наступних теоретичних і практичних аспектах: 1) інформаційна свідомість (інформаційні знання, уміння й навички, інформаційна компетентність); 2) інформаційні відносини (інформаційний режим, інформаційний конфлікт, інформаційні процеси, обмін інформацією тощо); 3) інформаційна поведінка (інформаційна послуга, інформаційна діяльність, інформаційний запит, інформаційні наслідки тощо).

Юрист має право направити в будь-яку організацію мотивований *інформаційний запит* з приводу ознайомлення з офіційними документами державних органів і одержати повну та достовірну відповідь.

У другому десятиріччі XXI ст. структура інформаційної культури юриста суттєво відрізняється від минулих періодів. В умовах інформатизації більшість юридичних спеціальностей потребує технологічного переформатування, тому змістовне наповнення інформаційної культури юриста відбиває: 1) ступінь інформаційних знань (інформаційно-технологічних та інформаційно-правових); 2) усвідомлення їхньої юридичної цінності та процесуальної необхідності; 3) технологічні навички їх ефективно використовувати в окремих видах юридичної діяльності.

Інформаційна культура юриста має дві сторони: інформаційно-технологічну (знання національних і глобальних комп'ютерних мереж, у тому числі Інтернету, їхнє використання) і інформаційно-правову (своєчасна інформованість про новітні закони та інші правові акти).

Ураховуючи це, новим підвидом інформаційної культури юриста стає його *високотехнологічна культура*, де важливим показником є вміння орієнтуватися на ринку інформаційних ресурсів, послуг, інформаційних систем та технологій.

Таким чином, визначимо, що структура інформаційної культури юриста полягає в наступному:

1) оволодіння знаннями в області інформатики й інформаційного законодавства, широка інформованість про життя інформаційного суспільства, його закономірностях, правах і обов'язках громадян як учасників інформаційних відносин, у тому числі тих, що складаються у сфері розвитку високих технологій;

2) переконаність у необхідності служити суспільству шляхом використання юридичних послуг, що ґрунтуються на високотехнологічних розробках;

3) участь в інформаційних відносинах нового типу, практичне користування досягненнями в інформатиці, принципами й нормами інформаційного законодавства: збереження персональних даних (особистої інформації), забезпечення інформаційної безпеки суспільства, захист професійної таємниці, державних інформаційних стандартів та ін.

о ***Інформатизація адвокатської діяльності в умовах розвитку високих технологій***

Не викликає особливих заперечень, що адвокатура є одним із базових правових інститутів громадянського суспільства, що ґрунтується на принципах верховенства права, гуманізму, демократизму, добровільності, законності, конфіденційності, корпоративності, незалежності, самоврядності. Адвокатура не входить до системи органів державної влади та місцевого самоврядування. Одночасно із цим, держава створює належні умови діяльності адвокатури та забезпечує захист прав адвокатів та дотримання гарантій адвокатської діяльності.

Адвокатура має статус незалежного недержавного самоврядного професійного правозахисного інституту, що входить до правової системи України, який діє для забезпечення права на захист від обвинувачення, надання правової допомоги та інших юридичних послуг, а також представництва інтересів фізичних та юридичних осіб. На жаль, існуючий розвиток подій заважає остаточно визначити місце адвокатури в державі та суспільстві, а також удосконалити принципи функціонування адвокатської інституції. Звідси, існують додаткові підстави знайти пояснення причин стримування розбудови нової концепції адвокатської діяльності в Україні.

Дослідженню окремих проблем адвокатської діяльності нами присвячено низку попередніх публікацій, що систематизовано у вигляді навчального посібника [185].

Потрібно визнати що останнім часом готуються суттєві зміни з окремих проблем адвокатської діяльності. Зокрема, розглядаються більш конкретні вимоги до осіб, що мають намір займатися адвокатською діяльністю. Утім ґрунтовній розробці високотехнологічної інформаційної моделі адвокатської діяльності в нових умовах дотепер не приділено ретельної уваги.

Оскільки за змістом поняття *«адвокатська діяльність»* охоплює надання в Україні правової допомоги та інших юридичних послуг, здійснення захисту та представництва, робота адвоката припускає обробку великого обсягу інформації різних видів та з різних джерел. Така інформація міститься в справі, що веде адвокат, у документах, що особисто надаються клієнтом або витребувані адвокатом. При вирішенні складних юридичних питань адвокат обробляє великий перелік правових актів, аналізує матеріали судової практики необхідних категорій.

Джерела інформації, що використовуються в адвокатській діяльності, можна класифікувати за різними інформаційно-правовими ознаками. Річ у тому, що центральне місце в юридичній практиці відводиться фактам як джерелам інформації, більшість з яких може мати різні ступені фіксації. Наприклад, існує факт знайдення трупу певної особи. Інформаційні ступені фіксації цього факту складаються з окремих ознак: протоколу огляду місця події; фототабличок, де міститься зображення трупу; відеокасети, на магнітній стрічці якої зафіксовано хід огляду трупу учасниками слідчо-оперативної групи; акта судово-медичної експертизи трупу; довідки щодо реєстрації актів цивільного стану про смерть свідчень очевидців тощо. При цьому окремі ознаки не потребують додаткових інформаційних підтверджень, що надає підстави визначити їх як *основні* або *надійні* джерела інформації для адвоката.

Зокрема, це може бути акт судово-медичної експертизи трупу або довідка щодо реєстрації актів цивільного стану. Деякі ж ознаки, навпаки, є *додатковими* або *ненадійними*, до чого в першу чергу можна віднести пояснення осіб.

Потрібно зауважити, що це зовсім не означає, що основні (надійні) джерела інформації не можуть бути негативними (помилковими,

неправдивими), разом як і те, що додаткові (ненадійні) джерела інформації не можуть надати поштовх для виграшу юридичної справи. А тому обидві групи джерел інформації вимагають від адвоката ретельної перевірки щодо з'ясування обставин в інтересах клієнта.

Разом із тим, подібна інформаційна класифікація надає адвокатові можливість оптимального використання обмеженого часу. Тобто логічно починати перевірку з ненадійних фактів, а далі, по мірі визначення більш повної інформаційної картини юридичної справи, у випадку отримання негативних, з точку зору захисту, наслідків, поступово переходити до перевірки та аналізу надійних джерел. Зокрема, існують випадки підробки актів судово-медичної експертизи, довідок реєстрації актів цивільного стану, навіть окремих процесуальних документів кримінальної справи – протоколу огляду місця події.

Інформаційна компетентність адвоката означає професійні вміння та фахові навички у використанні права на доступ до інформації.

Структура інформаційного поля адвоката складається з сукупності різних факторів й формується в різний спосіб. Однією з найбільш ефективних форм одержання інформації є *адвокатський запит*, тобто викладена в письмовій формі, обов'язкова для виконання вимога адвоката до органу державної влади та управління, органу місцевого самоврядування, правоохоронного органу, їх посадової особи, підприємства, установи чи організації, незалежно від форм власності та підпорядкування, або їх керівника (керівного органу), об'єднання громадян або фізичної особи (далі разом – «адресат адвокатського запиту») про надання відомостей, довідок, характеристик чи інших документів (їх посвідчених копій), предметів, які можуть бути доказами у судовій справі, або надання висновків, офіційних роз'яснень чи офіційної відповіді з питань, віднесених до їх компетенції.

Фактичні документально підтверджені витрати адресата адвокатського запиту з надання відповіді на адвокатський запит, у тому числі на підготовку та передачу (пересилку) відомостей, документів (копій документів), висновків, офіційних роз'яснень та іншої інформації за запитом адвоката, мають бути відшкодовані адвокатом, який робить адвокатський запит.

Всі письмові звернення адвоката є інформаційними запитами, але не всі можуть вважатися адвокатськими запитами (наприклад, до іноземних організацій або до окремих категорій фізичних осіб).

Таким чином, поняття *«інформаційний запит»* та *«адвокатський запит»* в рівній мірі використовуються в адвокатській діяльності, але не є тотожними, а співвідносяться як ціле та частина.

Безпідставне ненадання відомостей, документів (копій документів), предметів або іншої інформації за адвокатським інформаційним запитом або ненадання мотивованої відповіді на адвокатський інформаційний запит, або надання неповної чи неточної інформації або не всіх документів (копій документів), або предметів за адвокатським інформаційним запитом, за формальними ознаками може утворювати склад адміністративного правопорушення. Враховуючи подібний підхід ми приєднуємося до пропозицій і законодавчих ініціатив щодо внесення відповідних змін, зокрема доповнити Кодекс Україні про адміністративні правопорушення ст. 185[13].

Звідси визначимо, що структура інформаційного поля адвоката в сучасних умовах складається з трьох основних видів у такий спосіб: 1) *усні інформаційні джерела* (пояснення фізичних осіб, усні заяви та відповіді службових осіб, конфіденційні розповіді); 2) *письмові інформаційні джерела* (документальні, процесуальні, позапроцесуальні, публікації); 3) *електронні інформаційні джерела* (відео, аудіо, телебачення, цифрове фото, оптичні носії, Інтернет, корпоративні комп'ютерні мережі, окремі комп'ютери тощо).

Сьогодні у професійній діяльності адвоката набуває потребу ефективне застосування високих технологій. Адже згідно зі ст. 6 Закону України «Про адвокатуру» при виконанні своїх обов'язків щодо надання правової допомоги адвокат має право застосовувати науково-технічні засоби відповідно до чинного законодавства.

Буде суттєвим спрощенням вважати, що головна особливість формування високотехнологічної культури адвоката обмежується інформаційною підтримкою адвокатської діяльності. Це безумовно важливий аспект, але в сучасних умовах пріоритетним напрямом стає як раз зворотний бік, а саме – юридична підтримка процесу розвитку високих технологій та правове забезпечення трансферу технологій (ліцензії й договори поступки).

У цьому місці можливо хтось зауважить, що адвокат не надає юридичну допомогу «процесу розвитку»; він намагається відстояти інтереси певних осіб, які звертаються до нього за такою допомогою. Ось тому суб'єктами цього процесу інноваційного розвитку

є фізичні та юридичні особи, діяльність яких повністю або частково відбувається у сфері високих технологій, і які зіштовхуються з проблемами, що мають вирішуватись в юридичній площині. Більш того, історичний досвід свідчить про високий рівень імовірності загрози виникнення негативних наслідків, що можуть мати прояви в різних формах, основною ланкою чого залишається недосконаліть механізму державної підтримки. На жаль, як раз навпаки, подібна псевдопідтримка може виявлятися як на індивідуальному рівні (від щоденних перевірок, податкового тиску до організації тенденційного кримінального переслідування), так і на системному (прийняття недосконалих законів та інших нормативних актів).

Звідси адвокат повинен знати зміст основних інформаційних прав і свобод, закріплених поточним законодавством, механізм їхньої реалізації; особливості правового статусу окремих видів інформації (масової, статистичної, науково-технічної, офіційно-документованої, інформації з обмеженим доступом та ін.).

Крім цього, юрист вправі приймати участь у всіх видах *інформаційної діяльності:* одержанні, використанні, поширенні та збереженні інформації. Уміла інформаційна діяльність юриста, що виражається в здатності вибрати достовірну й точну інформацію, вчасно її одержати в необхідній кількості, ефективно використати потрібну інформацію, здійснити режим її збереження, уникнути дезінформації постає показником його інформаційної культури.

Явища, які у теорії права називають юридичною технікою, пропонують правильніше називати *юридичною технологією*. Вживані деякими авторами терміни «навички адвоката», «навички адвокатської діяльності» мають певну спорідненість і близькість до терміна «технологія» і вказують на «технологічність» адвокатської професії.

У випадку використання комп'ютерних мереж інформаційна культура адвоката має вираз у засвоєнні сучасних технологій вільного вибору джерела, провайдеру, формату, стандарту, програми інформації.

Звідси витікає, що основні напрями діяльності адвоката по забезпеченню суспільних інформаційних відносин полягають у наступному: 1) установлення консенсусу (згоди) в інформаційних суспільних відносинах, погодженості норм інформаційного законодавства; 2) захист правомірного поводження учасників інформаційних

відносин, профілактика та боротьба із правопорушниками в цій сфері правовідносин; 3) участь у забезпеченні інформаційної безпеки громадян, їхніх об'єднань, суспільства та держави як складової національної безпеки України; 4) участь у захисті інформації від витоку, несанкціонованого доступу, знищення, підробки, модифікації, перекручення незалежно від технології обробки.

Останнім часом деякі адвокатські фірми надають безоплатну юридичну допомогу по телефону. Утім за низкою обставин така «технологія» адвокатської діяльності є застарілою і не відповідає вимогам часу.

o ***Інноваційний проект «е-адвокат»***

В Україні вже існують окремі проекти адвокатської діяльності в електронній формі, зокрема «*VIP advocate*». Але подібні інновації залишаються доступними переважно для столичної бізнес-еліти. Як же бути пересічним громадянам у випадках, коли терміново необхідна юридична допомога без виходу, наприклад, із будинку?

Сьогодні зустрічаються поодинокі спеціальні «антикризові» пропозиції, такі як щоденні *юридичні он-лайн консультації*, що надаються безкоштовно.

Ще однією тенденцією розповсюдження адвокатських компаній, які спеціалізуються на правовому забезпеченні електронного бізнесу. Зокрема, одним із напрямів професійної діяльності таких адвокатів поступово стає юридичне супроводження електронної комерції та захист інтересів клієнтів по будь-яким аспектам діяльності в Інтернет-просторі, правовий супровід Інтернет-проектів та захист і представництво по кримінальних справах про злочини у сфері комп'ютерної інформації.

Застережемо, що електронні юридичні консультації є новим *додатковим* видом адвокатських послуг, а звідси ні в якому разі не можуть претендувати в подальшому на поступове витиснення «звичайних» вербальних консультацій.

Визначимо основні переваги електронних консультацій адвоката як додаткових електронних консультацій адвоката: 1) *психологічний аспект*: клієнти, коли викладають свою проблему в письмовій формі, більш відповідально ставляться до формулювань, точніше наводять факти, перечитують свій електронний лист та можуть редагува-

ти окремі неточності, обережніше визначають свій намір; сукупність цих факторів надає можливість умовно називаному «заочному», або «електронному» адвокатові більш якісно надати юридичну консультацію та точніше окреслити подальші перспективи вирішення юридичної справи; 2) *економічний аспект* – значна економія часу та коштів на організацію зустрічей та відвідування адвоката; 3) *організаційний аспект* – мобільне одержання факсом, електронною або звичайною поштою текстового варіанту юридичної консультації у вичерпному вигляді або експертно-правового висновку, причому у вичерпній формі, у визначений термін та в погодженому обсязі.

Створювані загальнодержавні й регіональні системи й мережі інформаційно-аналітичного забезпечення діяльності органів влади припускають високу інформаційну культуру адвоката, його здатність оперативно використати новітні технології, високотехнологічні засоби комунікації, зв'язок тощо.

Тому існують підстави у межах інноваційного проекту *«е-адвокат»* запропонувати системне розроблення інноваційної підпрограми *«електронний адвокат-захисник»*.

Створення нових умов адвокатської діяльності та набуття високотехнологічних навичок потребує не тільки побудови інформаційної інфраструктури адвокатури, але й забезпечить формування нової концепції професійної діяльності адвоката у сучасних умовах.

Припускається, що здійснення правової допомоги надається за сукупністю різних категорій юридичних справ як кримінальних, так і «некримінальних» – у рамках цивільного, господарського, банківського, авторського, податкового права тощо.

У цьому контексті потрібно визначити таку важливу ознаку як дуалістичність: 1) юридичні справи різних категорій, де адвокат при здійсненні правового захисту або наданні юридичної допомоги широко використовує свої знання та навички у сфері високих технологій; 2) юридичні справи, де предметом розгляду постають окремі аспекти (договори, порушення, суперечки та ін.), що знаходяться у сфері високих технологій.

о ***Адвокатське досьє (інформаційний аспект)***

Адвокат починає працювати за дорученням юридичної або фізичної особи, як правило, в обмежених інформаційних умовах. Адже повна картина юридичної справи, стає зрозумілою, а звідси доступ-

ною для юридичного аналізу після ретельного вивчення загального інформаційного масиву всіх зібраних матеріалів.

Для зручності організації свої роботи адвокат повинен заводити та вести адвокатське досьє по кожній справі кожного клієнта (крім справ, ведення яких передбачено договорами про надання правової допомоги, які укладені в усній формі та виконуються безпосередньо під час укладання).

Використовуються декілька варіантів назви цього документа — «адвокатське досьє», «адвокатське провадження», «адвокатська справа» та ін. Назва «адвокатське досьє» не є беззаперечним варіантом, але для термінологічної однаковості надалі таке найменування приймемо за основне.

Адвокатські досьє можуть складатися практично з усіх категорій юридичних справ (адміністративні, господарські, податкові та ін.), але далі ми, корегуючи викладення матеріалу за предметом дослідження, зосередимо увагу виключно на кримінальних справах.

Матеріали адвокатського досьє є основною інформаційною базою для виконання аналізу зібраних у справі доказів. Його ведення є необхідною умовою для вироблення найбільш вірної правової позиції. Тому в адвокатському досьє мають бути зібрані й певним чином систематизовані копії і виписки постанов слідчого, висновки експертів, копії або виписки із протоколів слідчих дій та інших документів, що мають відношення до пред'явленого обвинувачення.

Усі матеріали, що надані адвокату клієнтом або іншими особами на вимогу або за дорученням клієнта, належать клієнтові і мають бути повернені йому адвокатом на вимогу клієнта. Адвокат для збереження цілісності адвокатського досьє має право зробити за власний рахунок копії матеріалів, які повертаються клієнту.

Безумовно, не існує єдиного підходу щодо формування адвокатського досьє, як не може бути єдиного підходу до роботи над юридичною справою відносно формування правової лінії. Кожний адвокат працює індивідуально, стосовно до своїх здатностей, практичному досвіду, теоретичній підготовці, умінню схоплювати сутність матеріалів, властивостям пам'яті, до вироблених професійних прийомів і способів.

Єдиною офіційною організаційно-правовою вимогою до ведення адвокатського досьє є те, що адвокат зобов'язаний вести діловодство окремо від матеріалів та документів, що належать клієнтові.

У досьє адвоката повинні бути включені: копії або виписки з основних постанов слідчого: про порушення кримінальної справи; про прийняття кримінальної справи до свого провадження; про обрання запобіжного заходу; про залучення в якості обвинуваченого; про визнання як потерпілого; цивільного позивача або відповідача; про призначення судових експертиз; про продовження строків слідства; про продовження строків утримання під вартою обвинуваченого; обвинувальний висновок; протоколів роз'яснення прав підозрюваному, допитів підзахисного в якості підозрюваного, обвинуваченого, протоколів очних ставок; протоколів допиту потерпілого, свідків, фахівців; актів документальних ревізій, висновків (актів) судових експертиз й інших матеріалів, що мають значення для обрання правової позиції захисту та її обґрунтування.

Як правило, окремо виписуються показання обвинувачуваних, потерпілого, свідків.

При цьому свідків рекомендується умовно класифікувати на декілька підгруп: 1) підтверджують винність підзахисного в повному обсязі; 2) підтверджують його винності в певній частині; 3) спростовують обвинувачення. Тому свідки перших двох груп мають потребу в детальній перевірці (зацікавленість, відносини з фігурантами в справі, фізичні й психічні якості).

Показання кожного із зазначених осіб рекомендується виписувати на окремих аркушах, з обов'язковою вказівкою дати й часу проведення слідчої дії й аркушів тому кримінальної справи. Якщо виписки дослівні, то цитати необхідно брати в лапки. Переказ же показань необхідно брати в дужки. Подібна техніка дозволяє швидко орієнтуватися в матеріалах кримінальної справи, виявляти протиріччя й неправдиві показання.

Коли вивчення кримінальної справи завершується й всі необхідні виписки з матеріалів зроблені, можна згрупувати їх у наступному порядку: 1) процесуальні документи; 2) показання підзахисного; 3) показання інших обвинувачуваних; 4) показання потерпілих і свідків; 5) очні ставки; 6) протоколи відтворень обстановки й обставин події за участю всіх осіб, що займають різний процесуальний стан; 7) висновків судових експертиз.

Той же принцип варто зберегти й при угрупованні виписок по кримінальній справі великого обсягу (багато епізодів злочинної діяльності,

кілька томів кримінальної справи). У ряді випадків доцільно виписки групувати за епізодами обвинувачення, тому що саме в такій послідовності вони будуть досліджуватися в процесі судового слідства.

Інші адвокати виписують матеріали кримінальної справи підряд, а потім систематизують на окремому аркуші опис своїх записів. При цьому аркуш ділиться на дві частини. Ліворуч записуються прізвища всіх допитаних у справі, праворуч — всі документи. Проти кожного прізвища ставиться том і аркуш справи. Для зручності користування вказуються також у дужках аркуші записів адвоката, які попередньо ним нумеруються.

В адвокатське досьє варто включати копії офіційних процесуальних документів (наприклад, позовної заяви, постанови слідчого, вироку або рішення суду й т. п.), а також інших важливих документів, що фігурують у справі (копії договорів, накладних, виписок з рахунків і т. п.), виписки по самих істотних моментах з пояснень і протоколів допитів або протоколів судового засідання. Деякі адвокати, особливо по кримінальних справах, роблять повну фотокопію всіх матеріалів. У досьє включаються також ті допоміжні документи, що відображають фактичну сторону справи, які створює сам адвокат, наприклад, складена ним схема місця злочину або схема складної господарської операції й т. д. У досьє можуть входити витримки з відповідного закону, що підлягає застосуванню по даній справі, висновок адвоката по правовій кваліфікації справи, план роботи, копії підготовлених їм процесуальних документів, переліки питань, які він має намір задати на слідстві своєму підзахисному або в ході судового засідання, стислий виклад відповідей на них. Звичайно адвокати ведуть і свій робочий протокол відповідних процесуальних дій або судового засідання, де фіксують усі найбільш важливі моменти. Такі записи також містяться в досьє.

У тих випадках, коли у зв'язку з характером справи виникла необхідність вивчення додаткового законодавства або іншого нормативного матеріалу, судової практики, спеціальної, у тому числі наукової, літератури, що відповідають відомості теж доцільно включити в досьє. Більше того, у досьє можуть бути включені методичні рекомендації з роботи з готовими юридичними документами й оглядові матеріали по юридичній техніці.

Ми бачимо, що структура побудови адвокатського досьє не є однорідною, а вимагає індивідуального підходу, виходячи з особливостей кожної юридичної справи й професійного рівня самого адвоката.

Подібна система ведення адвокатського досьє дозволяє швидко орієнтуватися в зібраних адвокатом нотатках, і що особливо важливо, надалі при судовому розгляді багатотомної кримінальної справи.

Таким чином, у сучасних умовах адвокатське досьє є надійним засобом інформаційної оптимізації адвокатської діяльності, тому поступово перетворюється з додаткового чинника в обов'язковий.

о ***Електронне адвокатське провадження (інформаційний аспект)***

Ведення діловодства в електронному вигляді відіграє більшу роль у процесі надання адвокатом клієнтам юридичної допомоги. Надалі складаються усі підстави щодо використання адвокатського досьє в електронному форматі. Для зручності з метою запобігання термінологічної тавтології й плутанини на відміну від «адвокатського досьє» пропонуємо цей новий для юридичної практики документ як «електронне адвокатське провадження» (ЕАП).

Потрібно наголосити, що електронне адвокатське провадження не є новою організаційною процедурою. Така форма створює лише додаткову можливість для адвоката й інших учасників юридичного процесу працювати із процесуальними документами, використовуючи електронну передачу даних. При цьому формування ЕАП є саме правом, а не обов'язком адвоката. Отже, ЕАП є допоміжним технологічним засобом на додаток до звичайної процедури документообігу в судочинстві. Основними технічними вимогами для ЕАП у перспективі можуть стати цифровий підпис документів, що передаються електронним шляхом, і сертифікована електронна адреса, яку повинен мати адвокат як користувач ЕАП.

Адвокатське електронне провадження формується з відомостей конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, які визнані такими відповідно до встановлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей, тобто уявляє собою інформацію з обмеженим доступом. Електронне адвокатське провадження фактично є персональною справою клієнта, що потребує додаткових заходів щодо збереження конфіденційності.

ЕАП може бути впроваджене шляхом обміну даними й електронними документами, що мають юридичну чинність, підписаними цифровим підписом і заповненими за допомогою унікальних і зашифрованих каналів передачі даних для створення електронної процедури, альтернативної традиційної «паперової».

Систематизація матеріалів справи в електронному виді за основними вузловими питаннями дозволить вирішити важливі питання: 1) сконцентрувати докази, що відносяться до конкретного аспекту, в одному місці; 2) оцінити кожний доказ із погляду його значення в загальній системі доказів; 3) полегшити роботу при аналізі доказів по конкретних питаннях; 4) установити головні, основні вузлові питання, теми, які дадуть підстави для розробки генеральної позиції в справі; 5) розробити питання для допитів, визначити тактику своїх дій на різних найближчих процесуальних етапах; 6) підготувати необхідні клопотання, заяви, скарги; 7) почати самостійні організаційні (непроцесуальні) дії щодо збору додаткової інформації, що зможе мати доказове значення; 8) розробити план захисної мови, її розділи, встановити зв'язок між ними, розташувати їх у послідовну, логічну систему доводів адвоката.

Документи, включені в адвокатське досьє, для перенесення в електронне провадження можуть бути відцифровані та збережені як копії. Виходячи із цього буде логічним помітити, що подібні документи не можуть бути використані як доказ у справі.

Потрібно обов'язково враховувати, що більшість зібраних адвокатом матеріалів не мають офіційного статусу процесуальних документів, тобто з правової точки зору фактично ще не можуть сприйматися власне як докази. Для того, щоб зібрані факти стали доказами, матеріальні носії, де відбилися інформаційні прояви, що можуть мати значення по справі, повинні бути пред'явлені слідчому, прокуророві, суду, які вирішують питання про їхню значимість і необхідність їх долучити до матеріалів кримінальної справи.

Усі матеріали адвокатського досьє, які підготовлені адвокатом по справі клієнта, отримані адвокатом на його запити або що надійшли до адвоката процесуальним шляхом, належать адвокатові. Тобто – це власність – матеріальна або інтелектуальна – самого адвоката. Викликає певні зауваження пропозиція, згідно з якою на прохання

клієнта адвокат повинен надавати йому копії матеріалів з адвокатського досьє по справі цього клієнта. У цьому випадку інтелектуальна власність адвоката залишається інформаційно відкритою для клієнта. Вважаємо, точнішим буде не зобов'язувати адвокатів подібною нормою, а вирішувати ці питання відповідно до домовленості між адвокатом та клієнтом.

З метою концентрації інформації, що надійшла до адвоката з різних інформаційних джерел, в єдиному вузлі, логічно витікає потреба у розробці відповідних інформаційних комп'ютерних програм, які в міру включення додаткових інформаційних блоків, зможуть схематично пропонувати кілька запрограмованих потенційних результатів. Подібний високотехнологічний підхід дозволить оптимізувати зусилля адвоката, сконцентрувавши потуги на найбільш перспективних вузлах.

Зберігання подібних документів поза адвокатським досьє та електронним адвокатським провадженням у деяких випадках може призвести до їхнього вилучення й використання проти інтересів довірителя, що потребує від адвоката широкого використання заходів інформаційної безпеки.

У сучасних умовах електронне адвокатське провадження стає найбільш зручним й надійним засобом фіксації інформації з юридичної справи. ЕАП дозволяє із застосуванням подібного підходу досягти систематизації зібраного матеріалу, оптимізувати аналітичну роботу з великою кількістю інформації.

Підготовка матеріалів електронного адвокатського провадження складається з декількох етапів. У якості інформаційного зразка маємо запропонувати наступний алгоритм: 1) інтерактивна бесіда з особою, що звернулася з юридичним питанням на сайт адвоката або електронною поштою; 2) занесення в електронному вигляді вихідних даних, тобто фактично відкриття адвокатського провадження, а звідси – заведення адвокатського досьє; 3) перша бесіда зі слідчим (навіть, це можливо до зустрічі з підзахисним); 4) перша зустріч із підзахисним; 5) попереднє поточне вивчення матеріалів справи; 6) самостійне збирання фактів адвокатом; 7) прилучення матеріалів під час участі в різних слідчих діях, а також перенесення їх у цифровому вигляді на електронні носії інформації; 8) вивчення матеріалів справи разом з підзахисним після закінчення досудового слідства; 9) вивчення обви-

нувального висновку; 10) аналіз останніх редакцій діючого нормативного матеріалу; 11) винесення обґрунтованих клопотань, що спрямовані на покращення правового статусу підзахисного або зміну юридичної кваліфікації у бік пом'якшення; 12) при наявності підстав привнесення скарг на дії слідчого, прокурора або інших службових осіб; 13) участь у судовому слідстві; 14) підготовка до захисної промови в судовому засіданні з критичним аналізом і можливим переглядом під час судових дебатів сторін; 15) системний аналіз інформації за наслідками судового розгляду справи та судової практики щодо перспектив апеляційного провадження; 16) кінцевий результат.

o ***Електронний архів адвоката (інформаційний аспект)***

Поступово в кожного практикуючого й професійного адвоката формується архів, що стає істотною підмогою в роботі з новими справами. У більшості адвокатів існують власні архіви, де містяться копії матеріалів з минулих юридичних справ, а інколи оригінальні, навіть унікальні документи. *Архівний документ адвоката* – це документ незалежно від його форми, виду матеріального носія інформації, місця і часу створення, що припинив виконувати функції, який є власністю адвоката і зберігається за місцем його професійної діяльності за умов його юридичної значущості.

Адвокати зберігають свої архівні документи в особливому режимі, що забезпечує збереженість інформації, що міститься в них, цілісність упорядкованих документальних комплексів. Адже судові справи однієї категорії часто мають чимало загального в правовій оцінці обставин, у судовій практиці, у складанні документів і т. п. Поряд із цим придатність території для розташування архіву визначається самим адвокатом (квартира, будинок, дача, офіс адвокатської фірми, юридична консультація), де, як правило, відсутні особливі заходи безпеки.

Ведення подібного архіву за «паперовими технологіями» хоча і є класичним, але для оптимізації роботи в сучасних умовах залишається застарілим способом. Тому адвокатам рекомендується поступово переходити до формування своїх інформаційних архівів в електронний спосіб.

Зберігання електронної інформації (електронних документів) у незмінному виді називається *електронним архівуванням*.

Систему структурованого зберігання електронних документів, що забезпечує надійність зберігання, конфіденційність і розмежування прав доступу, відстеження історії використання документа, швидкий і зручний пошук називають *«електронним архівом»*, або *«системою електронного архіву»*. Одним з видів таких архівів можна навести електронний архів юридичної документації.

Створення адвокатом електронного архіву є комплексним рішенням щодо створення і наповнення електронного архіву документів, що забезпечить ефективне використання, оперативну доступність та надійне збереження останніх. Електронний архів оптимальним чином вирішує задачі поточного збереження документів, на етапі якого найбільшу значимість здобуває оперативність доступу до інформації і наявність можливості одночасного використання документа декількома співробітниками.

У цілому ж, адвокат при формуванні свого електронного архіву може структурно розділити його на три умовних блоки: 1) практичну частину — конкретні юридичні справи й результати їхнього розгляду; 2) методичну частину — методичні рекомендації, проекти клопотань, скарг (по видах), позовних й інших заяв, судових виступів і т. п.; 3) теоретичну частину — зміни в законодавстві (по видах) і практиці його застосування; огляди підзаконних нормативних актів (відомчих наказів, інструкцій, указівок і т. п.).

Визначимо основні задачі, що вирішуються при впровадженні адвокатом електронного архіву: 1) підвищення надійності збереження інформації, зменшення ризику втрати важливої інформації внаслідок недбалості або впливу зовнішніх факторів; 2) підвищення ефективності використання інформації за рахунок зменшення часу на пошук необхідних документів; 3) забезпечення доступу до інформації практично з будь-якої територіально віддаленої точки, оскільки адвокат-власник архіву виключно володіє відповідним правом доступу; 4) при необхідності корпоративна інтеграція з іншими інформаційними системами.

Електронний архів адвоката виконує наступні функції: 1) організація збереження електронних версій позапроцесуальних документів, їхніх копій та копій процесуальних документів, облікової, довідкової та аналітичної інформації; 2) ведення класифікаторів та ру-

брикаторів та їх використання для пошуку юридичних документів; 3) встановлення і підтримка логічних зв'язків між документами як в межах однієї справи, так і у загальному масиві юридичних справ, що занесені до архіву; 4) організація пошуку документів; 5) забезпечення доступу до інформації з обмеженим доступом та електронних документів інших осіб (своїх помічників або колег) відповідно до прав доступу, процесуальних вимог та норм адвокатської етики; 6) ідентифікація електронних документів за їхніми реквізитами.

Фактично кожне адвокатське досьє спочатку переформатовується у свій електронний аналог (ЕАП), а вже потім заноситься в електронний банк інформації адвоката і залишається складовою частиною власного електронного архіву. Така динаміка утворює певний інформаційний цикл форм фіксації результатів адвокатської діяльності «адвокатське дос'є» → «електронне адвокатське провадження» → «електронний архів адвоката».

Отже, електронний архів адвоката є якісно новим рівнем використання професійної інформації, оскільки така форма збереження значно знижує можливість утрати документів і підвищує оперативність роботи за рахунок скорочення часу пошуку потрібного документа.

Правильно сформоване адвокатське досьє з урахуванням досягнень сучасних інформаційних технологій свідчить про високотехнологічний професіоналізм у діяльності сучасного адвоката. Добре сформоване адвокатське досьє може послужити не тільки при роботі з конкретної справи, тому зберігання в електронному вигляді сьогодні є найбільш зручною формою, тому його збереження в електронному вигляді можна вважати допоміжним методичним чинником у роботі адвоката по наступних справах.

Якщо адвокат, який працює індивідуально, буде не в змозі здійснювати свою професійну діяльність з будь-яких підстав, він має негайно, але не пізніше одного місяця з дати виникнення таких підстав, після консультацій з клієнтом та отримання його згоди, передати справу клієнта, яку він веде (разом з адвокатським досьє або його електронною чи паперовою копією), іншому адвокатові з його згоди та письмово повідомити про це клієнта.

Після припинення договору про надання правової допомоги адвокату (адвокатському об'єднанню) рекомендується зберігати всі

матеріали адвокатського досьє протягом трьох років з моменту закриття адвокатського досьє (припинення договору про надання правової допомоги). Такий термін обумовлений тим, що охоплює максимальний час циклу проходження справи по всім судовим інстанціям. На відміну від цього, електронне адвокатське провадження має передумови для необмеженого терміну зберігання, наприклад, на оптичних носіях (CD та DVD).

Окремо зауважимо, що електронне адвокатське провадження у ході досудового слідства або судового розгляду залишається допоміжною (факультативною) формою, оскільки частково дублює свій «паперовий» варіант: перше є подвійною копією (копією з копії), а друге, умовно кажучи – оригінальною (першою) копією. Тобто адвокатське досьє є чернеткою і після кінцевого розгляду (закінчення повного юридичного циклу руху справи) на відміну від ЕАП може знищуватися.

Архів адвоката ж, навпаки, визначально формується виключно в електронному вигляді, де електронні адвокатські провадження виступають основними складовими.

Такий технологічний підхід надає помітну допомогу в професійній діяльності адвоката. Якщо питання про зміст, структуру й час зберігання адвокатського досьє не вирішені на рівні локального нормативного акта адвокатського об'єднання, то рішення по них адвокат приймає самостійно.

Врешті-решт ми намагалися підкреслити, що в основу розвитку інформаційної електронної культури професійної діяльності адвоката-захисника може бути покладена *концепція тактично-технологічної інноваційності*.

Отже, окреслено інформаційно-правові перспективи модернізації адвокатської діяльності в умовах розвитку високих технологій. Викладений матеріал, а також наслідки попередніх досліджень [183], надають нам ґрунтовні підстави висловити переконання з приводу перспективності розвитку *галузевої спеціалізації адвокатів у сфері високих технологій*.

Додатковим аргументом такого сценарію юридичного розвитку в умовах технологічного переоснащення виробництва нової продукції або впровадження високих технологій є неупереджене застосування

законодавства. Одним із факторів, що зможе гарантувати правову підтримку інноваційної діяльності в інформаційному суспільстві може стати *нова високотехнологічна адвокатура* як професійний інститут правової допомоги.

Таким чином, підсумуємо, що система знань, умінь і навичок юриста у сфері високих технологій, інформаційних й інформаційно-правових відносин, використовуваних для забезпечення різних видів юридичної діяльності та надання різноманітних правових послуг у суспільстві, обумовлена рівнем розвитку інформаційного суспільства і складає основний зміст *високотехнологічної культури адвоката*.

о ***Криміналістична інформатика та високі технології***

Стрімкий розвиток нових технологій в криміналістичній практиці детерміновано потребами у швидкому переробленні величезних масивів криміналістично значущої інформації [92]. Від традиційної криміналістичної науки криміналістична інформатика відрізняється також характером своїх міждисциплінарних зв'язків та функціями. В рамках цієї наукової теорії розробляються загальнометодологічні основи математизації і автоматизації розкриття та розслідування злочинів у сфері високих технологій [232]. Тому криміналістична інформатика набуває рис загальної теорії розв'язання криміналістичних завдань з використанням високотехнологічних методів інформатики і в цьому сенсі виконує функції, подібні до функцій загальної теорії держави і права у сфері конкретних юридичних наук [211, с. 516].

Зміст діяльності слідчого під час побудови ним інформаційної моделі злочину пов'язаний з виявленням, дослідженням, збиранням, оцінюванням, збереженням та використанням криміналістичної інформації.

Програмне забезпечення експертно-криміналістичної діяльності, на думку деяких дослідників, може класифікуватися так: 1) програми для автоматизації пошуку криміналістичної інформації; 2) програмні продукти, що дають змогу автоматизувати процес виявлення та дослідження ознак об'єктів; 3) спеціальні програми для оцінювання виділених ознак різноманітних об'єктів дослідження; 4) програми, що дають змогу автоматизувати процес складання експертного висновку [211, с. 542].

Для документування злочинів у сфері високих технологій з метою пошуку та фіксації фактичних даних широко застосовуються програмні та технічні засоби, використовуються наукові, технічні та інші спеціальні знання. Це зумовлено такими чинниками: 1) зміст заходів та умови їх проведення (об'єкт пошуку — інформація, яка оброблюється автоматичним шляхом або передається технічними засобами; об'єкти дослідження — носії інформації, засоби зв'язку, комп'ютерна і телекомунікаційна техніка, їх системи та мережі); 2) електронне середовище як місце вчинення протиправних діянь; 3) механізм слідоутворення в електронному середовищі; 4) способи фіксації, збереження, дослідження та відображення доказової інформації у формі, зрозумілої для сприйняття слідчим та судом.

Для фіксації факту користування певною особою зазначеним обладнанням необхідно створити ситуацію, яка б однозначно свідчила про винність конкретної особи (комбінація, затримання «на гарячому», відеофіксація, дактилоскопія тощо).

Як слушно визначають дослідники цієї проблематики, багато правопорушень учиняються вже на рівні надання доменних імен [43, с. 98–101]. Водночас треба погодитися із твердженням деяких експертів про те, що довести подібні злочини практично неможливо, оскільки виготовлена порнопродукція, як правило, зберігається на цифрових носіях, які, якщо буде потрібно, ліквідуються протягом секунд [109, с. 124–126]. Тобто, знищуються речові докази, а тому злочинці залишаються безкарними.

Утім, залишається питання про допустимість доказів, отриманих у результаті застосування телекомунікаційних засобів. Вирішуючи це питання, слід виходити з того, що допустимість визначається законністю джерела доказу, суб'єкта, який отримав доказ, умов та способів його отримання. Так, інформація, отримана телекомунікаційним шляхом, може бути віднесена до справи, як й інші непроцесуальні дані. Але така інформація може використовуватися як орієнтуюча, тактична. Але для того, щоб бути доказами в кримінальній справі, фактичні дані повинні набути ще й ознак допустимості, тобто вони мають бути отримані: 1) належним суб'єктом доказування; 2) належним способом збирання доказів; 3) із належного джерела доказів.

Модернізацію технологічних коридорів передавання інформації у сфері боротьби зі злочинністю наведено на схемі 3.1.

Схема 3.1

о ***Проблеми досудового слідства у сфері високих технологій та криміналістична модернізація***

Особливості розслідування злочинів у сфері мобільних телекомунікацій привертають неабияку увагу дослідників [213]. Утім, вітчизняне кримінально-процесуальне законодавство не враховує потенційні можливості використання телекомунікаційних технологій при розслідуванні злочинів. Проблеми телекомунікаційного забезпечення кримінального процесу останнім часом розглядають російські дослідники [90]. Слід зазначити, що в ч. 4 ст. 303 КПК України (згідно зі змінами, внесеними у 2000 р.) [64] також закріплена можливість проведення дистанційного допиту (тобто допиту з віддаленою присутністю допитуваної особи). Але КПК України не регламентує особливості такого допиту, зокрема пов'язані із застосуванням спеціальних науково-технічних засобів, робота яких має забезпечувати належну якість зв'язку під час допиту. Крім того, має бути вирішене питання щодо процедури встановлення судом у таких випадках особи допитуваного.

Деякі вчені, а саме Д. В. Лебедєв, М. І. Пашковський, А. Сизоненко, М. І. Смирнов, пропонують використовувати телекомунікаційні технології при проведенні окремих слідчих дій, зокрема, допиту, очної ставки, пред'явлення для впізнання, експертиз тощо.

Питання застосування інформаційних технологій у кримінальному судочинстві має бути вирішено при виконанні будь-яких процесуальних дій як у звичайному, так і в інтерактивному (дистанційному)

режимі, з одночасним веденням документообігу і діловодства на паперових та електронних носіях, з яких для учасників процесу у випадках, передбачених процесуальним законодавством, виготовлюються автентичні копії процесуальних документів [182, с. 191].

Доказова інформація у справах про злочини у сфері нових інформаційних технологій полягає в тому, що виявлені особливості не можуть сприйматися безпосередньо, а мають бути інтерпретовані та проаналізовані за допомогою спеціальних технічних засобів, у тому числі комп'ютерного програмного забезпечення.

Специфіка виявлення та проведення слідчих дій в Інтернет-просторі вимагає розроблення спеціальних криміналістичних методик, глибоких знань сучасних інформаційних технологій, наявності відповідного апаратного та програмного забезпечення, налагодження міжнародного співробітництва для розслідування комп'ютерних злочинів та ліквідації злочинних угруповань [191]. При вчиненні злочинного посягання у мережі Інтернет злочинець змушений з метою впливу на інформацію переборювати протидію як захисних апаратних пристроїв, так і захисного програмного забезпечення, залишаючи при цьому сліди на вузлах комп'ютера потерпілого, сервера та маршрутизаторів мережі. Сліди злочинних діянь залишаються у вигляді змін електронного середовища, а саме змін інформації (баз даних, програм, текстових файлів), що розташована на жорстких дисках, дискетах, магнітних стрічках, лазерних і магнітооптичних дисках. Крім того, магнітні носії можуть мати сліди знищення чи зміни інформації (видалення з каталогів імен файлів чи стирання окремих записів, фізичне руйнування чи розмагнічування носіїв) [191].

Фіксація фактичних даних про злочини у мережі Інтернет, як правило, передбачає проведення оперативно-технічних заходів. Процедури збирання в електронній формі доказів по комп'ютерних злочинах відповідно до Конвенції про кіберзлочинність передбачають необхідність: 1) збирання комп'ютерних даних у реальному масштабі часу; 2) збирання даних про рух інформації у реальному масштабі часу; 3) збирання за допомогою технічних засобів або запис даних про рух інформації у реальному масштабі часу, що пов'язано з визначеним передаванням інформації через комп'ютерні системи; 4) пере-

хоплення даних змісту інформації; 5) збирання за допомогою технічних засобів або запис даних змісту інформації у реальному масштабі часу, які належать до визначеного передавання інформації [170].

До заходів зі зняття інформації з технічних каналів зв'язку належать такі: пошук в інформаційних та телекомунікаційних мережах місць, де може зберігатися інформація, яка становить оперативний інтерес; забезпечення негласного доступу до носіїв такої інформації (у тому числі електронних поштових скриньок, трафіку IP-телефонії, повідомлень інтернет-пейджингу тощо), а також фіксація цієї інформації [76].

Для виявлення схеми вчинення злочину є потреба у застосуванні певних технологій та програмно-апаратних засобів, для чого пропонують залучати сертифікованих спеціалістів. Консультації спеціалістів допоможуть визначити: 1) місця, в яких можуть залишитися сліди вчинення злочину, вигляд останніх; 2) необхідні програмно-технічні засоби для виявлення цих слідів та їх фіксації у вигляді, зручному для безпосереднього сприйняття; 3) технічні та програмні засоби, якими, можливо, користувався правопорушник, його фаховий рівень; 4) найбільш оптимальні схеми виявлення, моніторингу та фіксації злочинної діяльності правопорушника, необхідність залучення спеціалістів.

Слід враховувати, що прямими доказами використання правопорушником певних програмно-технічних засобів зі злочинною метою будуть сліди злочину на них, які перебувають у причинно-наслідковому зв'язку із зафіксованими на обладнанні потерпілого. Тому обов'язковими є вилучення програмно-технічних засобів, які використовувалися під час учинення злочину, та проведення їх комп'ютерно-технічної експертизи.

Ще одним із напрямів модернізації використання у кримінальному судочинстві інформації, що міститься в електронному вигляді, є дані, що знаходяться в електронних повідомленнях (електронна пошта). Діапазон її використання залежить від технічних можливостей та засобів комп'ютерної мережі. Якщо розглядати електронну пошту з технічного погляду, то вона являє собою систему з відповідним програмним забезпеченням, яка дозволяє передавати повідом-

лення, використовуючи глобальні чи локальні комп'ютерні мережі [56, с. 35–38].

Водночас проблематичною є процедура отримання електронного повідомлення, яке міститься на сервері у провайдера. Для обмеження доступу до повідомлення використовуються відповідні паролі [114, с. 185–198].

Використання інформації, отриманої телекомунікаційним шляхом, у кримінальному судочинстві має визнаватися допустимим, якщо її використання: 1) передбачене законом, відповідає цілям і завданням судочинства, не суперечить принципам кримінального процесу; 2) є науково правомірним, тобто відповідає науковим положенням; 3) забезпечує ефективність провадження по кримінальній справі; 4) відповідає моральним нормам, не заподіює шкоди і не принижує людську гідність.

У сучасних умовах комп'ютерна техніка може фіксувати докази злочинів не тільки в Інтернет-мережі. Доцільність та ефективність одержання доказів із застосуванням телекомунікаційних технологій очевидні. У кримінальному судочинстві пропонують за необхідне як найшвидше введення в кримінально-процесуальне законодавство норм, що визначають специфіку доказів, одержаних з використанням телекомунікаційних засобів, детально регламентувавши особливості такого способу отримання доказів [56; 90; 93; 125]. Так, під час обшуків постійно виникатимуть питання стосовно доцільності вилучення електронних пристроїв з діючих автоматизованих систем. Невдалі підходи до вирішення цих питань можуть призвести до знищення доказів, порушення роботи цих систем, а це у свою чергу — до законних судових позовів. Інша причина необхідності поглиблених знань — складність виявлення злочинів із застосуванням нових інформаційних технологій, чим і користуються злочинці.

Шляхами розв'язання проблем, що виникають під час розслідування кримінальних справ про злочини, вчинені у сфері нових інформаційних технологій, є модернізація системи статистичного обліку, аналізу та оцінювання криміналістичної інформації у сфері нових технологій.

Отже, назріл час створення інтегрованої інформаційно-аналітичної системи правоохоронних органів України. Одним з напрямів щодо розв'язання проблеми криміналістичної модернізації є ство-

рення інтегрованої інформаційно-аналітичної системи правоохоронних органів, яка передбачена Концепцією національної програми інформатизації України [71] та впроваджується в ОВС України [130; 174].

Технічний аспект пов'язаний перш за все з вивченням проблем надійності, швидкості та точності передавання інформації, методами, технічними засобами побудови каналів передавання сигналів тощо [100, с. 144–147; 101, с. 70–77].

Необхідно розробити науково обґрунтовані методики програмного забезпечення аналізу оперативної інформації, отриманої оперативно-технічними засобами, для моделювання ситуацій, які складаються при проведенні оперативно-розшукових заходів [52; 232]. З метою створення бази для проведення аналітичної роботи у сфері нових інформаційних технологій пропонується вдосконалити систему обліку оперативної інформації та показників щодо розкриття цих злочинів [231]. Не слід забувати, що інформаційні системи правоохоронних органів теж можуть піддаватися атакам хакерів. Тому треба постійно проводити копітку роботу щодо технічного та криптографічного захисту інформаційної інфраструктури [128].

Модернізаційний проект створення цифрової телекомунікаційної мережі органів, які ведуть боротьбу зі злочинністю, представлено на схемі 3.2.

Отже, пріоритетним напрямом криміналістичної модернізації є науково-технічне розроблення та впровадження в досудовий кримінальний процес інноваційних проектів експертно-пошукових систем. Особливої актуальності це набуває у сфері розслідування злочинів у сфері високих технологій. Тому викладені пропозиції доцільно використати під час розроблення проекту Закону України «Про інформаційно-телекомунікаційну систему правоохоронних органів».

Пропонуємо визначати *антикримінальні інформаційні технології* як сукупність криміналістичних, кримінологічних, кримінально-правових та кримінально-процесуальних знань та інших відомостей про інформаційне забезпечення послідовності окремих оперативно-тактичних операцій з будь-якими об'єктами у сфері боротьби зі злочинністю з метою досягнення ефективних результатів.

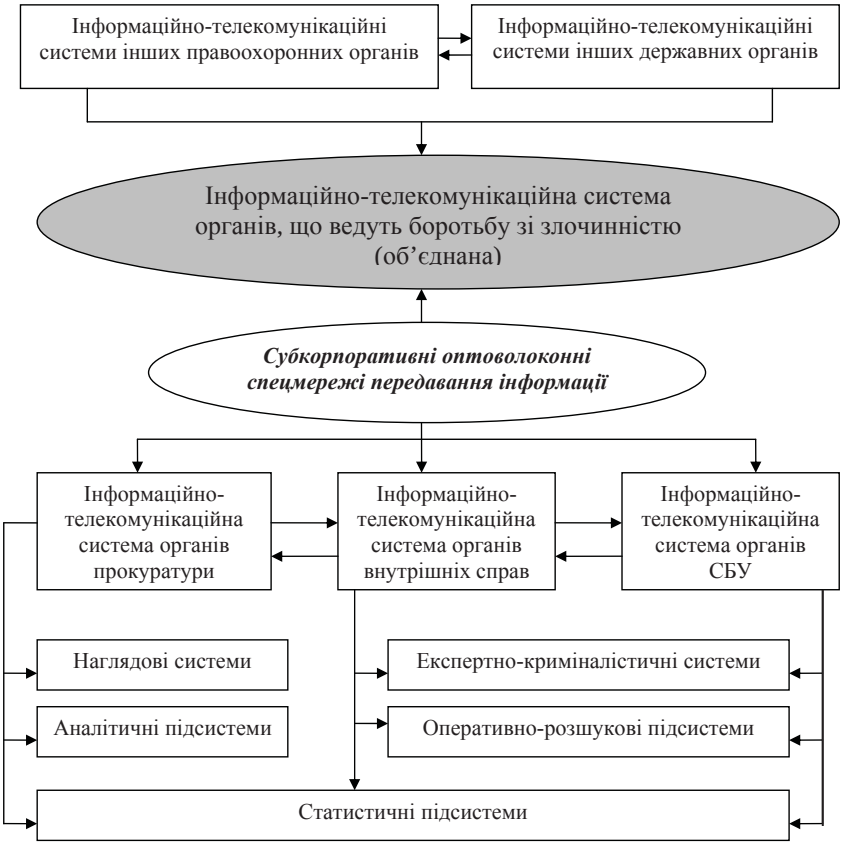


Схема 3.2

o ***Нові інформаційні технології в криміналістиці***

Впровадження у професійну діяльність правоохоронних органів інноваційних проектів у сфері застосування інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та комунікаційних мережах на значних територіях. Можна констатувати, що на сьогодні вироблено певне теоретично-методологічне підґрунтя, базуючись на якому можна розпочати розроблення безпосередніх заходів щодо модернізації інформаційних процесів у правоохоронних органах.

Ідея нової інформаційної технології полягає у розгляді системи понять предметної галузі і відповідності між нею та системою формальної моделі як похідної інформації для вирішення прикладного завдання.

Основне завдання нової інформаційної технології — перетворення ЕОМ на зручного партнера під час виконання професійних функцій. Тобто, на відміну від традиційного використання ЕОМ, де процес оброблення інформації визначається як виконання програми, за новою технологією — це отримання потрібних знань. Структурно така інформаційна технологія повинна складатися з виконавчої системи, бази знань та інтелектуального інтерфейсу.

Експертні системи (ЕС) започаткували розвиток комплексу методів і технічних прийомів використання штучного інтелекту, що в цій галузі є одним з найсуттєвіших практичних досягнень.

ЕС — це обчислювальна система, в якій зібрано знання фахівців про певну конкретну проблемну галузь і яка у межах цієї галузі здатна приймати експертні рішення на рівні експерта-професіонала та на вимогу користувача надавати пояснення своїм міркуванням зрозумілим для користувача способом. Основою кожної експертної системи є широкий запас знань про конкретну проблемну галузь.

ЕС повинна мати такі головні властивості: 1) бути обмеженою певною сферою експертизи; 2) бути компетентною (рівень рішень, які вона пропонує, мусить бути на рівні експерта-фахівця); 3) здатність до внутрішнього оцінювання, якщо дані сумнівні; 4) здатність вирішувати реальні завдання у межах певної предметної галузі та надавати пояснення прийнятим рішенням; 5) факти та механізм виведення чітко розмежовані; 6) відкритість (можливість нарощування системи); 7) бути здатною переформульовувати запити та завдання; 8) бути здатною до самоаналізу (міркувань про свою роботу та структуру); 9) надавати на виході чітку пораду; 10) бути економічно вигідною.

Ці властивості характеризують експертні системи як певний клас систем штучного інтелекту, в складі яких неодмінно присутні база знань та певна схема міркувань, що має назву системи (машини) логічного виведення.

Ідеальна експертна система містить у своєму складі такі головні компоненти: базу знань та систему логічного виведення (складають

ядро ЕС), інтерфейс з користувачем та модуль надбання (засвоєння) знань і модуль відображення та пояснення рішень. У теперішній час ЕС вже використовуються для інтерпретації даних, прогнозування подій (за наявності, як правило, неповної інформації), діагностики, моніторингу, планування, налагодження, ремонту, управління та ін.

Отже, системи підтримки прийняття рішень призначено для допомоги в отриманні ефективного способу розв'язання експертного завдання.

o ***Види інформаційних та експертно-криміналістичних систем***

У системі правоохоронних органів існують інформаційні та експертно-криміналістичні системи різних видів і різного призначення.

Інформаційні обліки в системі органів внутрішніх справ створюються для оперативного інформаційного забезпечення службової діяльності всіх підрозділів. На територіальному рівні управління в міськрайлінорганах на основі документів первинного обліку формуються банки даних оперативно-розшукового, оперативно-довідкового, адміністративного та статистичного призначення. Прикладами використання систем, які сприяють прийняттю рішень під час розслідування злочинів, є майже всі системи автоматизації дактилоскопічних обліків, а також системи розпізнавання голосу людини, ідентифікації аудіо- та відеопристроїв, балістичних експертиз та багато інших систем, що базуються на знаннях експертів [80].

Нині в системі правоохоронних органів використовуються дві основні методики побудови таких систем: 1) засновані на статистичному аналізі слідчих ситуацій; 2) засновані на збиранні, класифікації та використанні узагальненого досвіду розслідування у вигляді знань окремих професіоналів.

Методики, засновані на статистичному аналізі слідчих ситуацій, дають добрі результати при виявленні закономірностей у зв'язках між злочинною подією, особою злочинця, місцем та засобами вчинення злочину, особливостями злочинної поведінки. На жаль, процедура формування похідних даних бази знань на основі стандартних карток обліку злочинів, яка широко використовується, неналежним чином ураховує динаміку злочинних проявів. Це призводить до значних втрат інформації, оскільки ознаки, суттєві для окремих категорій злочинних посягань, можуть зовсім не потрапити до розгляду.

Другий тип методик відповідає розглянутому класичному способу побудови експертних систем [211, с. 548–549].

Слід зазначити, що інформаційні системи в органах, які ведуть боротьбу зі злочинністю, за своїм призначенням умовно можна розділити на такі, що забезпечують (автоматизовані системи фінансових підрозділів, кадрів, матеріально-технічного забезпечення, електронного документообігу тощо), і функціональні, що випливають безпосередньо із завдань, покладених на практичні підрозділи.

Ця класифікація не претендує на абсолютну безумовність та повноту, тому надалі вона може бути доповнена і вдосконалена. Ми розглядатимемо програми і автоматизовані комплекси, вказуючи клас програми за раніше наведеним розподілом.

о ***Характеристика інформаційних та експертно-криміналістичних систем***

Інформаційно-пошукова система «Оперативно-довідкова картотека» (ОДК) містить обліки оперативно-довідкової картотеки та дактилоскопічні обліки ДІТ МВС України та Державного науково-дослідного експертно-криміналістичного центру МВС України і забезпечує: 1) зберігання, накопичення, введення, облік та видання в установленому порядку ОВС, СБУ, прокуратурі, судам та іншим правоохоронним органам оперативно-довідкової інформації на осіб (у тому числі іноземців та осіб без громадянства), які вчинили злочини на території України, були заарештовані, засуджені, затримані за бродяжництво, уникають слідства та суду; 2) ідентифікацію осіб, які приховують свої біографічні дані від правоохоронних органів; 3) пошук злочинців за слідами, виявленими на місці злочину.

Дактилоскопічна та оперативно-довідкова картотеки накопичують таку інформацію: 1) основні установчі дані (прізвище, ім'я, по батькові, у тому числі й російською мовою, дата і місце народження, дактилоформула); 2) додаткові установчі дані (місце проживання, професія, місце роботи, посада, національність, громадянство); 3) відомості про арешт, судимість; 4) відомості про притягнення до кримінальної відповідальності; 5) відомості про місце та час відбування покарання, переміщення, дату і підставу звільнення; 6) відомості про номери слідчих та архівних справ; 7) відомості про пере-

бування у розшуку (коли, ким оголошений, у зв'язку з чим), призупинення розшуку (дата), запобіжні заходи; 8) відомості про затримання; 9) дактилоскопічну інформацію.

Інтегрована інформаційна система базується на центральному банку даних комп'ютерних систем ДІТ МВС України та даних, які накопичені у вигляді облікових карток за прізвищами, дактилокарт та слідів, вилучених з місць злочинів експертно-криміналістичними підрозділами ОВС [130].

Порядок ведення оперативно-довідкових і дактилоскопічних фондів регламентується наказом МВС України від 23 серпня 2003 р. № 823/188 [78].

Щоб автоматизувати формування та оброблення запитів в ОДК, фахівці ДІТ створили поштовий автомат «РУБІН», який успішно використовується в усіх обласних підрозділах ОВС України в областях та забезпечує оперативний доступ до центрального банку даних ОДК [211, с. 490–491].

Інформаційна система «Автоматизований банк даних» (АБД-центр) забезпечує збирання, оброблення та аналіз інформації, яка регламентується відповідними наказами МВС України. Автоматизований банк даних призначено для оперативного забезпечення працівників і підрозділів ОВС інформацією для розшукової діяльності, розслідування і попередження злочинів у повному і зручному для використання вигляді, надання аналітичної, статистичної та контрольної інформації. На центральному рівні управління збирається інформація, що використовується під час аналізу, планування, прийняття рішень та проведення в межах України оперативно-розшукових, слідчих та інших спеціальних заходів по боротьбі зі злочинністю.

До складу інформаційних фондів першого рівня входять банки кримінологічної інформації, що містять відомості про: а) надзвичайні події; б) нерозкриті тяжкі та резонансні злочини; в) викрадені, загублені та вилучені предмети, знаряддя вчинення злочинів, речові докази, у тому числі номерні речі, антикваріат, автомототранспорт, вогнепальну зброю, документи; г) криміналістичні обліки; ґ) викрадені та вилучені наркотичні речовини; д) об'єкти виготовлення, перероблення, зберігання та використання наркотичних речовин; е) осіб

таких категорій: особливо небезпечні рецидивісти; злочинці-«гастролери»; злочинці, оголошені у міждержавний розшук; організатори і члени злочинних угруповань, кілери; засуджені за злочини, пов'язані з наркотиками, торговці та розповсюджувачі наркотичних речовин з міжрегіональними та міжнародними зв'язками; схильних до вчинення злочинів, пов'язаних з посяганнями на інтереси держави; зниклі безвісти; невпізнані трупи та невідомі хворі; є) банк оперативно-довідкової інформації, що містить дані алфавітного та дактилоскопічного фондів раніше засуджених осіб; ж) банк статистичної інформації про стан злочинності та результати боротьби з нею; з) банк спеціальної інформації, що містить повідомлення спецапарату та іншу оперативну інформацію загальновідомчого значення; і) банк паспортних даних громадян; ї) банк з інформацією про зареєстрований автотранспорт; к) банк з інформацією про зареєстровану вогнепальну зброю; л) банки даних адміністративно-управлінського призначення; м) банки даних спеціалізованого призначення галузевих служб; н) банки даних архівів, спеціальних фондів та ін.

Повнота даних на кожному рівні за категоріями обліку визначається відповідними нормативними документами [112].

Водночас зараз активно використовуються телекомунікаційні технології при проведенні оперативно-розшукової діяльності. Зокрема, найбільш поширеними є такі галузі телекомунікацій, як мобільний та пейджинговий зв'язок. Наприклад, про номер, марку та ознаки викраденого автомобіля, мобільного телефону можна повідомити протягом години після вчинення злочину через радіо, мобільний і пейджинговий зв'язок; фоторобот можна розмістити на телебаченні. На користь застосування мобільного і пейджингового зв'язків для поширення розшукової інформації свідчить і те, що їх абонентами є, як правило, люди, що ведуть активний спосіб життя, пересуваючись територією міста і країни. Тому вони можуть допомогти у розкритті злочинів по «гарячих слідах».

Інформаційну підсистему «Розшук» призначено для централізованого збирання та оброблення інформації від ініціаторів розшуку про осіб, що розшукуються і встановлюються, які оголошені в регіональ-

ний, державний, міждержавний розшук, і надання інформації за запитами працівників ОВС, інших зацікавлених міністерств і відомств.

Технологія оброблення інформації передбачає її тиражування каналами електронної пошти в ГУ МВС областей з метою забезпечення доступу до цієї інформації на регіональному рівні. Крім цього, інформація, зосереджена в банку даних, використовується під час оперативно-розшукових заходів регіонального, державного, міждержавного рівнів.

Інформаційна підсистема «Пізнання» забезпечує централізоване збирання інформації на: 1) осіб, що безвісно зникли; 2) невпізнані трупи; 3) невідомих хворих.

Документом для формування бази даних та оброблення запитів є пізнавальна карта, яка надсилається із ГУ МВС в областях до МВС України. Запити на перевірку надсилаються поштою, телетайпом або каналами електронної пошти.

Міжвідомчий банк даних (МБД) «Наркобізнес» використовується для оброблення, накопичення та аналізу інформації про осіб та злочини, пов'язані з незаконним обігом наркотичних засобів, психотропних речовин та прекурсорів. Інформація МБД «Наркобізнес» використовується під час розкриття та розслідування злочинів, пов'язаних із наркоманією та наркобізнесом.

Інформаційна підсистема (ІПС) «Арсенал» — це система централізованого номерного обліку вогнепальної зброї в системі МВС України, створена для здійснення всебічного контролю за зброєю. ІПС «Арсенал» — система, що складається із джерел формування і надання початкової та коригуючої інформації, інформаційної бази, технічних і програмних засобів реалізації, споживачів інформації та інформаційного апарату, який забезпечує функціонування ІПС. До складу ІПС «Арсенал» входять дані про вогнепальну, пневматичну калібру понад 4,5 мм та швидкістю польоту кулі понад 100 м/с зброю, холодну зброю, спеціальні засоби самооборони, заряджені речовинами сльозоточивої та подразнюючої дії (газові пістолети та револьвери, що перебувають у користуванні громадян та організацій), дані про зброю органів внутрішніх справ, військових частин, навчальних закладів системи МВС та про зброю, яка зберігається на складах військових баз МВС [212].

Завдяки наявності волоконно-оптичної інформаційної мережі та спільної співпраці підрозділу комп'ютеризації з підрозділом правового забезпечення з'явилася можливість використання мережної версії інформаційної правової бази (ІПБ) «Експерт» для пошуку нормативно-правових актів України. Система «Експерт» є не тільки джерелом повноцінної правової інформації, а й потужним програмним інструментом аналітичної роботи. ІПБ «Експерт» постійно оновлюється в автоматизованому режимі.

Бази даних, як зовнішні, так і внутрішні (відомчі), повинні бути забезпечені надійним і ефективним програмним засобом систематизації і пошуку інформації. Тому мають бути запропоновані до впровадження відповідні програмні засоби. До того ж, паралельно вивчається можливість використання універсальної інтегрованої інформаційної системи «Портрет 4.3». Вона являє собою комплекс програмно-апаратних засобів для побудови багатокористувальницьких розподілених ІПС різного призначення і складності.

ІПС, які можуть бути побудовані на основі комплексу «Портрет 4.3», мають архітектуру «клієнт-сервер» і використовують сервери баз даних, завдяки чому забезпечуються зберігання і керування інформаційними масивами великого обсягу. «Портрет 4.3» надає слідчому, який може не мати спеціальної технічної кваліфікації, можливості для створення баз даних, що мають складну розгалужену структуру, і забезпечення максимальної гнучкості як при побудові складних запитів до баз даних, так і при аналізі результатів пошуку. Утім, подібна конструкція не є вичерпною.

Зокрема, інформаційна підсистема «ІБД» містить інформацію про осіб криміногенних категорій (особливо небезпечні рецидивісти, «гастролери», оголошені у міждержавний розшук, бродяги), нерозкриті тяжкі злочини, викрадену, вилучену, знайдену зброю, номерні речі, викрадені в Україні та країнах СНД транспортні засоби [211].

о ***Автоматизоване робоче місце слідчого***

Автоматизоване робоче місце (АРМ) слідчого — це комплекс індивідуальних технічних і програмних заходів, спрямованих на автоматизацію інформаційної підтримки процесу досудового слідства у кримінальних справах.

Комп'ютерну програму «Автоматизоване робоче місце слідчого» розроблено для організації роботи слідчого з інформаційними базами даних, призначеними для службового використання (правова інформація, накази, методики тощо). Система дозволяє оптимізувати виконання основних завдань, пов'язаних з роботою слідчого при розслідуванні кримінальних справ [17].

Система надається слідчому на компакт-диску типу CD-ROM і розроблена таким чином, що вона може як використовуватися слідчим з компакт-диску, так і встановлюватися на комп'ютер слідчого для індивідуального використання. До структури АРМ слідчого входять такі функціональні блоки: правова інформація (включає нормативно-правову базу, яка забезпечує процес досудового слідства); функціональні системи (методика розслідування кримінальних справ, типові зразки процесуальних документів, судові експертизи) тощо.

АРМ слідчого надають можливість користувачам (слідчим) працювати в діалоговому режимі, оперативно вирішувати окремі поточні завдання, викликати необхідну інформацію для оброблення, визначати вірогідність результативної інформації та виводити її на екран, принтер або передавати її каналами волоконно-оптичного зв'язку [23, с. 202–203].

Отже, головне призначення АРМ — надання допомоги слідчому при розслідуванні злочинів. Головними завданнями, для розв'язання яких мають використовуватися такі системи, є визначення можливих напрямів розслідування (формування версій про подію з урахуванням різних джерел отримання інформації); обрання найбільш ймовірних напрямів і надання користувачу рекомендацій щодо подальших дій (призначення експертиз, проведення оперативно-пошукових заходів, перевірочні та слідчі дії тощо).

о ***Інноваційний проект «Оптико-електронний кабінет криміналістики»***

Слід відзначити, що на сьогодні, незважаючи на розроблені В. І. Лебеденком, І. П. Козаченком, С. С. Овчинським, О. П. Снігерьовим, О. Б. Утевським та іншими вітчизняними і російськими вченими теоретичні основи такої роботи і концепцію розвитку інформаційного забезпечення органів внутрішніх справ, у відділах криміналістики

органів прокуратури вона обмежується тільки констатуванням та реєстрацією деяких подій, осіб та способів учинення злочинів. Тому, дещо забігаючи уперед, торкаючись проблем інформатизації прокурорської діяльності, про що окремо викладено матеріал у наступному розділі, пропонуємо обґрунтування проекту створення цифрової інформаційної мережі кабінетів криміналістики із застосуванням високих технологій.

Слідчі як суб'єкти електронного документообігу в рамках програми «Оптико-електронний кабінет криміналістики» (ОЕКК) користуються правами та мають можливість оперативно звернутися за практичною або методичною допомогою з питань організації досудового слідства та впровадження новітніх експертних технологій до централізованого масиву електронного офісу криміналістичної служби прокуратури області, що працює цілодобово, при цьому не виїжджаючи з району до обласного центру в різні установи. Звернення слідчих фіксуються та зберігаються в електронній пам'яті антикримінальної інформаційної мережі.

За ознаками надання телекомунікаційні послуги слідчим поділяються на основні та додаткові, що нерозривно пов'язані технологічно з наданням певних основних телекомунікаційних послуг. Перелік додаткових послуг визначається технічними можливостями обладнання операторів та провайдерів телекомунікацій [166].

Універсальний доступ має відповідати таким вимогам:

1) забезпечення за вимогою слідчих районних прокуратур з'єднанням його кінцевого обладнання з телекомунікаційними мережами корпоративного користування в мережі органів прокуратури;

2) телекомунікаційні мережі спеціального користування (закриті відомості), факсимільний зв'язок, передавання даних на рівні, достатньому для доступу споживачів до мережі Інтернет;

3) електронні паролі ОЕКК забезпечують універсальний доступ слідчих до телекомунікаційної антикримінальної мережі корпоративного користування, що не залежить від технології доступу або способу підключення.

Метою стандартизації у сфері телекомунікацій програмними засобами проекту ОЕКК є створення єдиної системи антикримінальних

інформаційних стандартів та інших нормативних документів, які визначають вимоги до телекомунікаційних мереж, їх технічних засобів та якості телекомунікаційних послуг, а також гармонізація цих вимог з вимогами міжнародних нормативних документів.

Разом із тим технологічні аспекти надання практичної або методичної послуги слідчим визначаються готовністю електронного інформаційного масиву криміналістичної служби прокуратури області надавати відповідну послугу в електронній формі.

Під час навчально-методичної роботи зі слідчими, ще одним з процесуальних засобів доведення винності осіб у вчиненні комп'ютерних злочинів, є судова експертиза комп'ютерної техніки і програмних продуктів, основними завданнями якої мають бути: 1) установлення технічного стану комп'ютерно-технічних засобів; 2) установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів інформації та програмного забезпечення; 3) виявлення інформації та програмного забезпечення, що міститься на комп'ютерних носіях; 4) установлення відповідності програмних продуктів певним параметрам [11, с. 84–94].

Для дослідження інформації, що міститься на комп'ютерних носіях, експерту потрібно надавати сам комп'ютерний комплекс, до складу якого входить досліджуваний носій. Щоб визначити, які саме об'єкти слід надавати експерту в кожному конкретному випадку, прокурор-криміналіст має навчити слідчих, як правильно відбирати їх для дослідження.

Видається за доцільне і в подальшому розвивати напрямок впровадження електронного документообігу не тільки в прокуратурі вищого рівня, а й в прокуратурах першої і другої ланок. Причому для реалізації цієї ідеї потрібно вдосконалити чинне законодавство даної сфери, зокрема те, що регулює індивідуалізацію особи — учасника документообігу, електронний підпис, захищеність системи від стороннього втручання тощо. І в такому розвитку не слід зупинятися лише на обігу документів відомчого характеру, треба йти далі і використовувати електронний документообіг при провадженні судових справ, у тому числі кримінальних. Це сприятиме прискоренню роботи щодо пересилання документів та реагування на них, скороченню строків провадження у справах. Наприклад, якщо слідчий зі Львова

у Донецьк надсилає окреме доручення в порядку ст. 118 КПК України, то десять передбачених законом днів будуть витрачені тільки на пересилання, і часу на його виконання практично не залишається. Завдяки комп'ютерній техніці при належному законодавчому забезпеченні час на пересилання зменшився б практично з десяти днів до декількох секунд.

Впровадження комп'ютерної програми «Автоматизована система тестування» в органах прокуратури надає можливість для незалежної перевірки знань працівників органів прокуратури. Ця програма дозволяє створювати різноманітні групи тестів для проведення незалежного тестування працівників органів прокуратури, які підлягають атестації.

Інформаційно-комунікаційні та дистанційні педагогічні технології навчання прокурорсько-слідчих працівників та інноваційність заходів з підвищення їх кваліфікації без відриву від основної діяльності зможуть забезпечити слідчих прокуратури на місцях інформаційно-практичними, науково-технологічними та навчально-методичними ресурсами для самостійного опрацювання, електронними індивідуальними завданнями для самостійного виконання під дистанційним контролем з боку прокурора-криміналіста. Це дасть змогу реалізувати індивідуальний підхід до надання методичної допомоги кожному слідчому. Звідси — доцільність використання сучасних наукових методів, розроблення та впровадження інноваційних методик практичного навчання прокурорсько-слідчих працівників на електронних навчально-методичних семінарах, про що ми вже наголошували [184; 187].

Крім того, в роботі кабінетів криміналістики органів прокуратури треба ширше застосовувати конференцзв'язок, у тому числі відеоконференцзв'язок, а також різного роду телемости, які дозволяють у режимі живого спілкування вирішувати функціональні завдання цього правоохоронного органу. Так, для чого свідку із Одещини їхати за викликом до слідчого Генеральної прокуратури, якщо можна було б з'явитися до прокуратури місцевого рівня, і, спілкуючись із цим слідчим наживо, за допомогою інформаційних систем пройти процедуру допиту за місцем проживання? На сьогодні залишається високою вартість цієї процедури, але є надія, що із швидким розвитком техніки вона стане більш доступною.

У цій дистанційній формі могли б організовуватися як на загальнодержавному, так і на регіональному рівні заходи з обміну досвідом чи з підвищення кваліфікації певних категорій прокурорських працівників, що звільнило б від необхідності доставлення їх до місця проведення заходу, розміщення для проживання, відриву від основної роботи, витрат на відрядження тощо.

Необхідно визначитися, за яких умов, з використанням яких методів та засобів інформаційно-комунікаційні та дистанційні технології будуть ефективними при реалізації проекту ОЕКК. Зокрема, деякі офісні програмні продукти (текстові та графічні редактори планування діяльності СОГ, програми підготовки та призначення судових експертиз, електронні інформаційно-статистичні таблиці тощо) можуть бути використані прокурорами-криміналістами для підготовки навчально-методичного матеріалу (наприклад, шаблонів програми розслідування за окремими категоріями кримінальних справ) та надання слідчим-користувачам такої електронно-комунікаційної мережі результатів перевірки і виконання індивідуальних та групових завдань в електронній формі.

Таким чином, прокурор-криміналіст зможе дистанційно ефективно здійснювати координаційні заходи щодо практичної діяльності слідчого.

Як слушно зазначається, професійна діяльність прокурора-криміналіста передбачає наявність певного рівня знань у сфері телекомунакацій [31, с. 2–4]. З цього приводу слід визнати, що неприпустимим є призначення на посади прокурорів-криміналістів працівників без відповідної кваліфікації в надії на засвоєння ними основ інформаційних технологій у подальшій роботі. Це може призвести до неефективної роботи у нових технологічних умовах.

Окремо треба підкреслити, що особливий інтерес до проблеми правового і технологічного захисту проекту ОЕКК викликається зростаючою роллю інноваційних технологій в інформаційній сфері і чисельними випадками використання корпоративних комп'ютерних мереж та Інтернету для проникнення в конфіденційні бази відомчих даних правоохоронних органів.

Кабінети криміналістики окремих областей вже сплановані навіть частково реалізують комплекс організаційних і практичних заходів.

На основі узагальнення пропозицій криміналістичних підрозділів прокуратури розроблено структуру і уведено в експлуатацію внутрішній інформаційний сервер ГПУ, за допомогою якого на основі web-технологій забезпечується доступ користувачів системи до відомостей за напрямами роботи.

Вдосконалення інформаційного забезпечення кабінетів криміналістики органів прокуратури має бути спрямоване на загальну організацію цієї діяльності, а саме: на розвиток законодавства, що регулює відносини у сфері інформаційно-телекомунікаційних технологій, організаційно-кадрове та матеріально-технічне забезпечення, підвищення рівня інформаційно-аналітичної роботи. Для реалізації цього слід забезпечити доступ практично всіх комп'ютерів прокуратури (у тому числі районного рівня) до постійно обновлюваних криміналістично значущих інформаційних масивів, які мають бути зосереджені в оптико-електронному кабінеті криміналістики.

Прокурор-криміналіст має змогу самостійно створювати дистанційні електронні курси підвищення кваліфікації і проводити навчання на відстані, в тому числі надсилати повідомлення стажистам прокуратури, розподіляти, збирати та перевіряти результати виконання навчально-методичних та практичних завдань [203–205]. Усі електронні навчально-методичні курси, що розроблюються криміналістичною службою прокуратури та впроваджуються в практичну діяльність слідчих, розміщені в системі ОЕКК, повинні мати уніфіковану структуру та відповідати певним критеріям якості.

З метою впровадження нових методів пропонуємо використовувати інноваційну модель індивідуального підвищення кваліфікації при кабінеті криміналістики, зміст якої полягає в інтеграції двох форм навчання — стажування і семінарів, що відбуваються з виїздом до прокуратури області, з інформаційно-комунікаційними та дистанційними технологіями навчання з підсумковим автоматизованим тестуванням слідчих. Електронні методичні вказівки в рамках проекту ОЕКК можуть стати корисними для обережного постійного керування самостійною роботою слідчих.

Аналіз накопиченої в базі даних інформації дозволить слідчим районних прокуратур одержувати із бази даних електронного кабінету криміналістики результати, неочевидні при розгляді розрізнених

подій. Крім цього, в антикримінальній інформаційній системі передбачено оптико-волоконні засоби щодо візуального аналізу даних.

Ми переконані, що інноваційний проект ОЕКК насамперед має стати супертелекомунікаційним центром, що показано на схемі 3.3.

Схема 3.3

Однією з інформаційних інновацій, впроваджених за допомогою волоконно-оптичних технологій, може стати участь прокурора-криміналіста не тільки в проведенні телеконференцій та відеоконсультацій слідчих з метою надання ним на відстані практичної та методичної допомоги. З цього приводу телеконференцію потрібно визначити як: 1) систему, що ґрунтується на використанні персональних комп'ютерів та приєднаних до них за допомогою засобів зв'язку терміналів, яка дає змогу користувачам, незважаючи на їх взаємну віддаленість у часі і просторі, пересилати і приймати текстові, графічні та усні повідомлення, брати участь у спільних заходах; 2) інтегральний набір послуг, що надається за допомогою комп'ютерів та мереж і застосовується з метою обміну відеозображеннями, звуком та даними

між двома або більшою кількістю користувачів; 3) вид електронної пошти, коли поштові повідомлення надсилаються не окремим користувачам, а в спеціально організовані дискусійні групи. Учасники телеконференції можуть бачити і чути один одного в реальному часі, а також обмінюватися даними та спільно їх обробляти.

Аудіоконференція включає живий обмін мовними повідомленнями за допомогою телефонного зв'язку. Якщо є можливість обміну текстами та всіма зображеннями (графіками, діаграмами або малюнками) поряд з мовними повідомленнями, то цей тип конференції називається аудіографічним [224].

За допомогою відеоконференцій існує можливість обміну не тільки мовою та графікою, а й переміщенням зображень. Технологія відеоконференцій не застосовує телефонні лінії, але використовує супутниковий зв'язок або телевізійну мережу. Інтернет-конференція відповідно до своєї назви включає передавання тексту та графічних, звукових і візуальних засобів інформації через Інтернет. Для цього необхідне використання комп'ютера з браузером, тоді зв'язок може бути або синхронним, або асинхронним. Через цю корпоративну електронну мережу слідчий може дистанційно ознайомитися з програмою підготовки чи підвищення кваліфікації, що подається у вигляді різнотипних інформаційних ресурсів (текст, відео, шаблонні проекти певних процесуальних документів, алгоритми вирішення окремих слідчих ситуацій, електронні навчально-методичні посібники тощо).

Для використання пропонується нова глобальна/регіональна інформаційна мережа Теланнет (не плутати зі службою Telnet існуючого Інтернету). Істотною перевагою Теланнета порівняно з Інтернетом є забезпечення в ньому повної інформаційної безпеки, тобто захисту від хакерів, комп'ютерних вірусів, шпигунських програм (якими зараз уражено 80 % комп'ютерів, підключених до Інтернету), непрошеної кореспонденції рекламного характеру (спам) тощо. Такі комп'ютери для інформаційної підтримки, підключені до мережі Теланнет з метою використання її служби комп'ютерного інтелекту, в майбутньому здатні вирішувати окремі завдання.

Метою технологій інтелектуального аналізу даних є побудова моделей і виявлення залежностей, прихованих в даних великого об-

сягу, представлених таблицями (кількість ознак порівняна з кількістю об'єктів), уражених шумами та пропусками з ознаками, виміряними в різнотипних одиницях, за відсутності підстав для висунення гіпотез про закони розподілу [61, с. 136–139]. Для цього в персональній пам'яті головного комп'ютера єдиної інформаційно-телекомунікаційної системи має бути закладено досить повний масив криміналістичної інформації.

Антикримінальна інформаційна система може бути призначена для підтримки діяльності аналітичних підрозділів правоохоронних органів. Вона забезпечує уведення оперативної інформації про кримінально значущі події (щодо фактів, об'єктів і зв'язків між ними) до бази даних, її прив'язку до вже зафіксованих фактів (об'єктів) і аналіз. Магнітооптичні пристрої вже сьогодні дозволяють сформувати високоякісний масив бінарної інформації, причому швидкість його оброблення за алгоритмом нейронної мережі на декілька порядків перевершує можливості людського мозку. Такий тип комп'ютера при його використанні в галузі кримінального переслідування пропонуємо визначити як *інтелектуальний антикримінальний комп'ютер*.

Таким чином, на інтелектуальний антикримінальний комп'ютер слід покласти виконання таких завдань: 1) аналіз стану протидії організованій злочинності у сфері високих технологій та злочинності транснаціонального характеру; 2) складання стратегічних прогнозів; 3) процесуальне закріплення можливості самостійно порушувати кримінальні справи та в разі необхідності, проводити розслідування в повному обсязі; 4) науково-методичне забезпечення впровадження актикримінальних суперкомп'ютерних технологій в єдину слідчу практику; 5) координація діяльності правоохоронних органів у сфері протидії злочинам, що вчиняються з використанням технологічного потенціалу.

Враховуючи викладене, визначимо:

$$M \diagup K \xrightarrow{2} \frac{S+G}{P}, \tag{3.1}$$

де модернізація передавання інформації (M) передбачає знайдення та застосування нових технологічних коридорів передавання інформації (K), що стане удвічі ефективнішим завдяки впровадженню

суперкомп'ютерних технологій (*S*) та Грід-мереж (*G*), дослідним зразком чого має стати інноваційний проект антикримінального моніторингу Інтернет-простору *(P)*.

Резюме. *Дослідження системних проблем модернізації та освоєння нових технологічних коридорів передавання інформації у сфері боротьби зі злочинністю надає підстави резюмувати: 1) визначено поняття інформаційної модернізації; 2) розкрито передумови формування технологічного світогляду в сучасних умовах; 3) проведено міжнародно-порівняльний огляд досягнень суперкомп'ютерних і Грід-технологій в різних країнах; 4) висвітлено перспективи створення міжнародних центрів антикримінальних обчислень; 5) обґрунтовано стратегічний потенціал суперкомп'ютерних і Грід-мереж у галузі боротьби зі злочинністю; 6) охарактеризовано види інформаційних та експертно-криміналістичних систем; 7) запропоновано інновації стосовно інформаційного забезпечення розслідування злочинів, що вчиняються із застосуванням високих технологій; 8) доведено, що на сучасному етапі моніторинг цифрової інформаційної мережі в Інтернет-просторі є пріоритетним напрямом антикримінального впливу.*

Ключові слова*: модернізація; інформатизація; інноваційні проекти; суперкомп'ютер; Грід; інтернет-моніторинг; криміналістична інформатика; інформаційні системи; експертно-криміналістичні системи; оптико-електронний кабінет криміналістики.*

Контрольні запитання

1. Зміст поняття «модернізація».
2. Проблеми теорії інновацій та зміст інноватики у сфері діяльності органів, що ведуть боротьбу зі злочинністю.
3. Інновація інформаційної діяльності як процес і об'єкт.
4. Об'єкти і суб'єкти інноваційної діяльності у сфері високих технологій.
5. Історія, потенціал та міжнародний розвиток Грід-концепції.
6. Перспективи використання суперкомп'ютерних і Грід-мереж у галузі боротьби зі злочинністю.
7. Високотехнологічні проблеми антикримінальних інформаційних технологій.
8. Поняття та види антикримінального моніторингу цифрової інформаційної мережі в Інтернет-просторі.

9. Допустимість доказів, отриманих у результаті застосування телекомунікаційних засобів.
10. Специфіка виявлення злочинних проявів та особливості проведення слідчо-криміналістичних дій в Інтернет-просторі.
11. Криміналістична інформатика як міждисциплінарна галузь знання.
12. Основні завдання системної інформатизації правоохоронних органів України.
13. Інформаційні обліки в системі органів внутрішніх справ.
14. Програмне забезпечення експертно-криміналістичної діяльності.
15. Інформаційно-пошукові системи «Оперативно-довідкова картотека» і «Автоматизований банк даних».
16. Інформаційні підсистеми «Розшук» і «Впізнання».
17. Міжвідомчий банк даних «Наркобізнес» та інформаційна підсистема «Арсенал».
18. Інформаційна правова база «Експерт» та автоматизоване робоче місце слідчого.
19. Універсальна інтегрована інформаційна система «Портрет 4.3».
20. Оптико-електронний кабінет криміналістики.

Розділ 4

Органи прокуратури як спеціальні суб'єкти високотехнологічного інформаційного права

У цьому розділі ...

- ***Інформаційно-телекомунікаційна система органів прокуратури України.***

Інформаційна сфера і сфера боротьби зі злочинністю ◄► Правоохоронна діяльність і система правоохоронних органів ◄► Суб'єкти інформаційного права України у сфері боротьби зі злочинністю ◄► Інформаційне забезпечення органів прокуратури ◄► Інфраструктура прокурорських телекомунікацій ◄► Досвід розвитку інформаційно-телекомунікаційної системи прокуратури.

- ***Електронні наглядові системи та аналітичні системи обробки інформації.***

Електронний документообіг в органах прокуратури ◄► Інформаційно-аналітична підсистема «Статистика» ◄► Електронна система «Нагляд» ◄► АРМ «Прокурор-кримінолог-аналітик» ◄► Розбудова інформаційних технологій нового покоління.

- ***Стратегії розвитку інформатизації органів прокуратури України.***

Поняття стратегії інформатизації ◄► Основні завдання інформатизації прокурорської діяльності ◄► Концептуальні засади інформатизації органів прокуратури.

4.1. Інформаційно-телекомунікаційна система органів прокуратури України

o *Інформаційна сфера і сфера боротьби зі злочинністю*

У цілому дослідженням проблем у сфері боротьби зі злочинністю присвячено велику кількість фундаментальних праць. Власне стосов-

но процесів боротьби зі злочинністю вживається безліч термінів, при цьому кожний викликає наукові спори і не може оцінюватися однозначно. Тому впорядкування понятійного апарату має не тільки наукове, а й важливе практичне значення щодо розроблення концепції боротьби зі злочинністю.

Не заглиблюючись в аналізі різних точок зору з цього приводу, пропонуємо застосовувати поняття «сфера боротьби зі злочинністю».

Слід визначити, що сфера боротьби зі злочинністю є складною системною діяльністю, яка являє собою єдність таких трьох підсистем: 1) загальної організації боротьби; 2) попередження злочинності; 3) правоохоронної діяльності.

З першого погляду інформаційна сфера і сфера боротьби зі злочинністю є нібито двома абсолютно різними виявами соціального буття. Але ці соціальні інституції мають низку спільних рис, основою чого залишається право як універсальний регулятор соціальних відносин усіх типів.

У сфері боротьби зі злочинністю виникають різні правовідносини, в першу чергу інформаційні. Зокрема, якісно нова організація специфічних режимів зберігання та оброблення інформації, зв'язок з міжнародними правоохоронними органами забезпечать реалізацію активної, наступальної стратегії в боротьбі з правопорушеннями, корупцією, організованою злочинністю завдяки застосуванню нових інформаційних технологій у розкритті злочинів. Звідси соціальні відносини, що системно складаються в цих сферах, інформаційно розширюються і навіть перехрещуються, що умовно показано нижче на схемі 4.1.

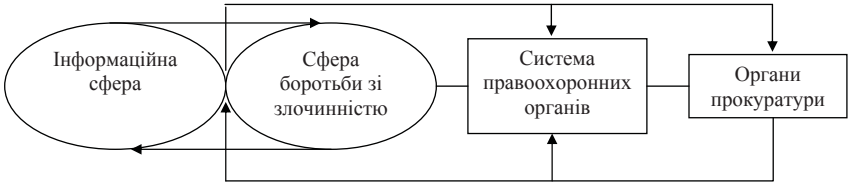


Схема 4.1

Утім, існує й зворотний зв'язок. Так, модернізація соціотехнічних процесів, що відбуваються у сфері боротьби зі злочинністю, детермі-

нує формування та розвиток інформаційних відносин нового виду, в тому числі високотехнологічного змісту.

о ***Правоохоронна діяльність і система правоохоронних органів***

Правоохоронна діяльність — це специфічна державна форма активності, реалізована у сфері забезпечення правопорядку і законності за допомогою спеціальних інститутів, форм і методів здійснення.

На жаль, дотепер в Україні відсутнє конституційне закріплення як поняття правоохоронних органів, так і правоохоронного органу та її системи. Система може бути визначена як сукупність закономірно впорядкованих, взаємопов'язаних елементів, кожен з яких є внутрішньою одиницею даної сукупності, що у взаємодії з іншими елементами утворює систему як ціле із наявною відповідною структурою і здатністю до саморозвитку. Структурний аспект системного дослідження передбачає з'ясування елементів системи, а також встановлення зв'язку між цими елементами. Взаємодія елементів системи спрямована на збереження системи, здійснення її головної функції.

Система органів, що ведуть боротьбу зі злочинністю, становить складне утворення і може бути розглянута як така, що охоплює систему слідчих органів та систему оперативних (оперативно-розшукових) органів.

Правоохоронні органи одного виду як складові системи правоохоронних органів являють собою певні підсистеми, що характеризуються цілісністю, якісною своєрідністю і відносною самостійністю. Інакше кажучи, правоохоронні органи кожного виду є елементами загальної системи правоохоронних органів. Така централізована система має організаційно-правову самостійність, створюється у законодавчому порядку, здійснюється за допомогою специфічних методів і пріоритетних форм (виходячи з головних напрямів правоохоронної діяльності) від імені держави, на основі і в межах закріпленої за ним компетенції, обсяг і характер якої залежать від його місця в системі правоохоронних органів.

Таким чином, між елементами (правоохоронними органами) даних підсистем існують субординаційні зв'язки, тобто правоохоронні органи одного виду будуються в ієрархічному порядку, в підпорядкуванні нижчих правоохоронних органів вищим із урахуванням адміністративно-територіального поділу держави, тобто компетенція

того чи іншого правоохоронного органу поширюється відповідно на певну територію держави.

Питання про визначення поняття «правоохоронні органи» є дискусійним не тільки в теорії. Відсутня одностайність у його розумінні і серед практичних працівників цих органів. Усе це призводить до колізій і непорозуміння при застосуванні тих чи інших законодавчих положень.

Ураховуючи певну кількість підходів, з метою єдиного розуміння пропонуємо сприймати правоохоронні органи як державні і суспільні установи та організації, що покликані забезпечувати законність і вести боротьбу зі злочинністю та іншими правопорушеннями [197, с. 440].

о ***Суб'єкти інформаційного права України у сфері боротьби зі злочинністю***

На даний час інформатизація правоохоронних органів здійснюється шляхом створення та експлуатації кожним органом власних інформаційних систем, які в цілому забезпечують виконання покладених на відповідний орган завдань, пов'язаних, зокрема, з боротьбою зі злочинністю. Звідси більшість правоохоронних органів мають субкорпоративні інформаційно-телекомунікаційні системи, окремі з яких співвідносяться між собою або доповнюють одна одну, тим самим підвищуючи ефективність інформаційного забезпечення системи правоохоронних органів у цілому.

Незважаючи на підвищену увагу з боку науковців та практиків до інформаційного забезпечення правоохоронних органів, на цьому шляху залишається багато нерозв'язаних проблем, пов'язаних, у першу чергу, з повільним впровадженням в управлінську практику інформаційних технологій та недостатнім використанням усіх можливостей сучасної обчислювальної техніки, засобів зв'язку тощо.

Визначимо основних *суб'єктів інформаційного права України у сфері боротьби зі злочинністю*, якими є правоохоронні органи України та їх службові особи, державні експертні установи, експерти, прокурори, слідчі та оперативні працівники органів прокуратури, внутрішніх справ, СБУ, податкової міліції, органи дізнання, міждержавні спеціальні організації та недержавні формування, які відповідно до свого правового статусу беруть участь у боротьбі зі злочинністю.

о ***Інформаційне забезпечення органів прокуратури***

У цілому питання діяльності прокуратури в різних напрямах розглянуто в працях О. А. Банчук, В. С. Бабкової, Д. М. Бакаєва, А. Д. Бойкова, Ю. М. Грошевого, Т. Б. Вільчик, Л. Р. Грицаєнка, Л. М. Давиденка, В. В. Долежана, Л. Б. Ільковця, Б. М. Ковріжного, Т. К. Кожевникова, І. М. Козьякова, М. В. Косюти, В. В. Кулакова, М. Й. Курочки, А. М. Ларіна, Д. Р. Марочкіна, М. М. Міхєєнка, Г. О. Мурашина, В. Т. Нора, О. П. Петриненка, В. П. Півненка, М. А. Погорецького, Ю. Е. Полянського, В. Я. Тація, М. В. Руденка, В. М. Савицького, Н. В. Сибільової, Т. А. Сульженко, С. К. Трофімова, П. В. Шумського, Г. М. Ясинського, В. Д. Фінько та ін. [84; 85; 98; 108; 134; 154; 155; 172; 178; 179; 199; 201; 222; 228].

Про необхідність, доцільність і перші кроки щодо проблем формування правової інформатики в прокуратурі України свідчать публікації на рівні статей М. Гаврилюка, В. Загороднього, А. Іщенка, А. Карпуся, А. Куліша, О. Черв'якової, Є. Шевченка та ін. [87; 107; 215; 234; 235; 238; 241].

Використання сучасної інформаційної техніки, нових інформаційних технологій дає реальну можливість організувати забезпечення прокурорських працівників такою інформацією, яка об'єктивно їм необхідна для здійснення функціональних обов'язків. Виконання функцій, покладених на прокуратуру, потребує всебічного володіння інформацією, котра б характеризувала як систему в цілому (внутрішня інформація), так і стан зовнішнього середовища, який безпосередньо або опосередковано впливає на прокурорську діяльність, потребує прокурорського втручання (зовнішня інформація).

Проблеми, пов'язані з визначенням інформаційного забезпечення організації прокурорського нагляду у сфері слідчо-оперативної діяльності, як правило, у переважній більшості були предметом уваги з боку правознавців, що досліджували проблеми правоохоронних органів.

Слід зазначити, що з метою поліпшення координації організаційних, оперативно-розшукових, правових та інформаційних заходів правоохоронних органів стосовно боротьби зі злочинністю, підвищення рівня роботи в цій сфері Указом Президента України від 31 січня 2006 р. № 80/2006 запроваджено створення Єдиної

комп'ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю (далі — Єдина комп'ютерна система) [227]. Відповідно до цього Указу утворено Міжвідомчу координаційну групу з питань створення і функціонування Єдиної комп'ютерної системи.

Дослідження заходів впровадження комп'ютерних інформаційних технологій в прокуратурі України свідчать про те, що вони зводилися переважно до комп'ютеризації — насичення комп'ютерною технікою (на базі персональних комп'ютерів) та типовими комп'ютерними програмними продуктами, а також створення локальних комп'ютерних мереж. При цьому комп'ютерні інформаційні технології дозволяли суттєво поліпшити організацію індивідуальної діяльності працівників прокуратури, але істотно не вплинули на організаційно-управлінську складову прокуратури України в цілому.

З точки зору організаційного аспекту зазначена проблема була зумовлена тим, що в системі прокуратури України тривалий час не існувало функціональної галузевої наукової структури, яка б напрацьовувала для її практики цільові теоретичні, методологічні, методичні розробки щодо інформатизації та її взаємопов'язаних аспектів: організаційних, правових, наукових, технічних та ін.

20 листопада 1996 р. затверджено Концепцію створення корпоративної інформаційної системи органів прокуратури. Зі змісту Концепції, а також практики її реалізації, публікацій науковців і практиків можна зробити висновок про те, що впровадження досягнень науково-технічного прогресу у сферу інформатики в органах прокуратури України здійснювалося ситуативним чином. Концепцією не передбачаються зміни в організаційній структурі, перерозподіл функцій між структурами та зміни в системі інформаційного забезпечення при впровадженні комп'ютерної техніки і технологій. І це цілком закономірно, адже теорія комп'ютеризації таких питань не вирішує. За її науковою концепцією модернізації піддаються тільки технічна та відповідна їй технологічна складові на рівні комп'ютерних програм.

Під системною інформатизацією прокуратури України пропонується розуміти множину взаємопов'язаних наукових, технічних, організаційних, правових, соціально-економічних, фінансових та інших процесів, спрямованих на модернізацію інформаційного забезпечення

діяльності прокуратури через створення, застосування та розвиток комп'ютерних інформаційних систем, у тому числі мереж, ресурсів і технологій [234, с. 73–77].

Треба відзначити, що до цього часу ще спостерігається відставання від потреб практики наукового забезпечення інформатизації органів прокуратури.

Отже, стратегія вдосконалення інформаційного забезпечення діяльності прокуратури України має базуватися на алгоритмізації інформатизації.

о ***Інфраструктура прокурорських телекомунікацій***

На теперішній час спостерігається тенденція до об'єднання різноманітних типів інформаційних технологій в єдиний комп'ютерно-технологічний комплекс, який має назву інтегрованого. Особливе місце в ньому належить засобам телекомунікації, які забезпечують не тільки надзвичайно широкі технологічні можливості автоматизації управлінської діяльності, а й самі власне є основою створення найрізноманітніших мережних варіантів інформаційних технологій: локальних, багаторівневих, розподілених, глобальних обчислювальних мереж, електронної пошти, цифрових мереж інтегрального обслуговування. Усі вони зорієнтовані на технологічну взаємодію об'єктів, створених засобами передавання, оброблення, нагромадження та зберігання, захисту даних, являють собою інтегровані комп'ютерні системи оброблення інформації (даних) великої складності, практично необмежених експлуатаційних можливостей для реалізації управлінських процесів.

Інтегровані комп'ютерні системи оброблення даних проектуються як складний інформаційно-технологічний та програмний комплекс. Він підтримує єдиний спосіб подання даних та взаємодію користувачів з компонентами системи, забезпечує інформаційні та обчислювальні потреби фахівців в їх професійній роботі. Особливе значення в таких системах надається захисту інформації при її передаванні та обробленні. Найбільш поширеними при захисті інформації є апаратно-програмні способи. Зокрема, використання системи зв'язку, обраної за захисними властивостями та якістю обслуговування, гарантує збереження інформації в процесі передавання та доставлення її адресату; шифрування та розшифровування даних абонентами мережі

загального користування здійснюються за домовленістю користувачів про загальні технічні засоби, алгоритми шифрування і под.

За типом інтерфейсу користувача інформаційні технології можна розглядати з точки зору можливостей доступу користувача до інформаційних та обчислювальних ресурсів. Так, пакетна інформаційна технологія виключає можливість користувача впливати на оброблення інформації, поки вона здійснюється в автоматичному режимі. Це пояснюється організацією оброблення, яка заснована на виконанні програмно заданої послідовності операцій над заздалегідь накопиченими в системі та об'єднаними в пакет даними.

На відміну від пакетної діалогова інформаційна технологія надає користувачу необмежену можливість взаємодіяти інформаційними ресурсами, які зберігаються в системі, в реальному масштабі часу, одержуючи при цьому всю необхідну інформацію для виконання функціональних завдань та прийняття рішення. Інтерфейс мережної інформаційної технології надає користувачу засоби теледоступу до територіально розподілених інформаційних та обчислювальних ресурсів завдяки розвиненим засобам зв'язку, що робить такі інформаційні технології багатофункціональними та передбачає їх широке застосування.

о ***Досвід розвитку інформаційно-телекомунікаційної системи прокуратури***

Інформаційно-телекомунікаційну систему органів прокуратури України змістовно включено в систему органів прокуратури України. Органи прокуратури у своїй сукупності складають злагоджену триланкову систему [65]. Обидві системи є відносно автономними системами різних рівнів, які мають взаємну узгодженість, підпорядкованість, спільні риси та функціональні відмінності. Що ж стосується інформатизації системи органів прокуратури України, то при визначенні змісту відповідного поняття, можливо, доцільно говорити про систему певних інформаційних процесів.

Інформаційно-телекомунікаційну систему органів прокуратури України пропонується розглядати як комплекс програмних, технічних та організаційних засобів для оперативного обміну даними оперативного, статистичного, експертного, інформаційно-довідкового та адміністративно-управлінського характеру між центральним апаратом ГПУ і підрозділами органів прокуратури на місцях.

Основою інформаційної мережі прокуратури є комп'ютерна мережа, яка поєднує всі програмно-технічні комплекси інформаційних підсистем на всіх рівнях. Інформаційна волоконно-оптична мережа створюється в інтересах усіх галузевих служб прокуратури і надає можливість оперативної інформаційної взаємодії як у системі прокуратури, так і з іншими правоохоронними органами, експертними та державними установами, міністерствами та відомствами України, а також з правоохоронними органами інших держав.

Під час створення Єдиної комп'ютерної системи вже частково використовуються новітні інформаційні технології, застосовуються оптиковолоконні, провідні та радіоканали передавання даних, сертифіковані програмно-апаратні засоби, які забезпечують надійність, достовірність та конфіденційність обміну інформацією.

В окремих випадках створюються галузеві інформаційні мережі, що входять до складу інформаційно-телекомунікаційної мережі прокуратури і забезпечують інформаційну взаємодію підрозділів з дотриманням протоколів обміну інформацією, що визначаються Департаментом інформаційних технологій (ДІТ) МВС України.

Разом із цим сьогодні в органах прокуратури ще використовуються здебільшого застарілі інформаційні технології, що призводить до непомірно великого обсягу «ручної» праці. Оскільки діловодство здебільшого ще достатньою мірою не автоматизовано, атестовані працівники змушені відволікатися на виконання не властивих їм канцелярських функцій, що негативно позначається на використанні робочого часу висококваліфікованими прокурорсько-слідчими працівниками.

Структурна побудова інформаційних підсистем прокуратури поєднує принципи територіально розподіленої та централізованої топології і організована у вигляді трирівневої ієрархічної моделі. Управляють інформаційною мережею центральна та регіональна системи адміністрування, підпорядковані відповідно інформаційним підрозділам прокуратури.

До цього часу в органах прокуратури України не створено єдиної волоконно-оптичної мережі зв'язку та передавання інформації з можливістю подальшого розширення. Зазначена мережа охоплює основні підрозділи апарату прокуратури області і надає можливість створити єдиний інформаційний простір. Встановлено та налагоджено сервер

корпоративної електронної пошти прокуратур областей, сервер управління розподіленою локально-обчислювальною мережею та центральний сервер бази даних.

Наявні локальні волоконно-оптичні мережі нині дають можливість використовувати лише мережний варіант комп'ютерної правової бібліотеки «Закон» інформаційно-аналітичного центру «Ліга», мережний варіант комп'ютерної інформаційно-пошукової правової бази «Законодавство» Секретаріату Верховної Ради України, мережний варіант опрацювання стат-звітності, мережний варіант опрацювання карток за скаргами та зверненнями, мережний варіант електронного документообігу («Експедиція-Картотека»), мережний варіант сучасного пакету прикладних бухгалтерських програм «ІС-бухгалтерія» та використання мережних принтерів, що є явно недостатнім. Єдиною інформаційною мережею на цей час не з'єднано навіть дві адміністративні будівлі ГПУ, розміщені поруч.

Розвиток волоконно-оптичної інформаційної мережі прокуратури характеризується такими етапами.

Перший етап — використання діючої комп'ютерної мережі на основі електронної пошти ГПУ. На цьому етапі забезпечується розвиток системи електронної пошти всіх рівнів на основі оптоволоконних каналів зв'язку, впроваджується доступ користувачів до інформаційних підсистем оперативно-розшукового призначення.

Другий етап — розвиток діючої електронної пошти на основі використання виділених каналів волоконно-оптичного зв'язку між центральною та регіональними інформаційними мережами, застосування технології Інтранет. Впроваджується зв'язок з банками даних у режимі Off-Line та On-Line, забезпечується адміністрування на центральному та регіональному рівнях.

Третій етап — побудова глобальної інформаційної мережі прокуратури з обміном інформацією між територіальним, регіональним та центральним рівнями і забезпечення формування банків даних верхнього рівня з використанням телекомунікаційних технологій. На цьому етапі широко застосовуються волоконно-оптичні канали зв'язку між регіональними та центральним рівнями, основою яких мають бути супутникові та цифрові канали. Реалізується доступ до комп'ютерної мережі з рухомих об'єктів.

Таким чином, волоконно-оптичні інформаційні мережі всіх рівнів системи органів прокуратури — це відомчі мережі закритого типу, що не допускають під'єднання до інформаційних мереж загального користування.

Належність інформаційної підсистеми до певного рівня визначають принципи територіальності, специфіка використання, а також обсяг інформації, що оброблюється. Перший рівень — *центральний,* інтегрує інформаційні підсистеми правоохоронних органів загальновідомчого значення та галузевих служб. Другий рівень — *регіональний,* охоплює інформаційні обліки, які є складниками загальновідомчих інформаційних підсистем. Третій рівень — *територіальний,* охоплює інформаційні обліки, що є складниками загальновідомчих інформаційних підсистем. Цей поділ стосується як загальновідомчих, так і галузевих інформаційних підсистем.

Основою системи збирання, контролю та використання інформації є третій рівень. На цьому рівні забезпечуються первинне накопичення інформації, ведення територіальних банків даних, захист інформації, актуалізація інформаційних фондів та передавання інформації до банків даних другого та першого рівнів.

На другому рівні формуються регіональні банки даних, оброблюється інформація, забезпечуються доступ територіальних підрозділів для санкціонованого використання інформації, інформаційний зв'язок між регіонами та центром. Забезпечується зв'язок з територіальними правоохоронними органами та іншими установами держави. Здійснюються контрольні функції щодо виконання вимог повноти, достовірності, актуальності та збереження інформації відповідно до законів України та відомчих нормативних актів.

На першому рівні забезпечуються інтеграція та оброблення інформації для формування банків даних інформаційних підсистем, міжвідомчий та міжрегіональний інформаційний зв'язок, керування системою інформаційного забезпечення прокуратури та дотримання стратегії її розвитку, розроблення нормативно-правової бази впровадження сучасних інформаційних технологій.

Досягнення зазначеного дасть змогу органам прокуратури України сприяти становленню відкритого демократичного інформаційного суспільства, в якому державою буде гарантовано дотримання

конституційних прав громадян, у тому числі щодо їх участі у суспільному житті, прийняття рішень органами державної влади та органами місцевого самоврядування у межах і в способи, визначені законодавством.

4.2. Електронні наглядові системи та аналітичні системи обробки інформації

Електронний документообіг в органах прокуратури

Провідним напрямком розвитку інфраструктури прокурорських інфотехнологій має стати впровадження кращих здобутків правової інформатики — інформатики у правотворчості, правозастосуванні та правовій освіті, формування галузевого електронно-цифрового інформаційного простору під умовною назвою «Електронна прокуратура», де особливе місце відведено питанням електронного документообігу в органах прокуратури.

У цілому організаційно-правові засади електронного документообігу та використання електронних документів визначає Закон України «Про електронні документи та електронний документообіг» [68].

Електронний документообіг в органах прокуратури переважно здійснюється без електронного підпису. За таких умов говорити про надання процесуальним документам правового статусу, звичайно, неможливо. Це далеко не повний перелік проблем, пов'язаних з організацією та управлінням, впровадженням та застосуванням сучасних комп'ютерних інформаційних технологій в діяльність органів прокуратури.

Важливим показником системності інформатизації є розроблення автоматизованого класифікатора даних галузевої інформаційної системи. Цей класифікатор має узгоджуватися з відповідними класифікаторами інших галузевих (відомчих) інформаційних систем. Тільки за такої умови можна говорити про підвищення якості інформаційно-аналітичного забезпечення діяльності органів прокуратури України.

Зазначене є особливо актуальним у контексті агрегації автоматизованої обліково-реєстраційної підсистеми органів прокуратури з автоматизованими базами даних, обліково-реєстраційних систем, які адмініструються інформаційно-аналітичними службами різних органів влади (у тому числі регістри, кадастри тощо).

Відсутність єдиної інформаційної структури в органах прокуратури породжує такі негативні наслідки: а) паралельність інформації (ті ж самі показники частково опрацьовуються різними підрозділами, зв'язок між якими не завжди впорядковано); б) відсутність єдиного підходу до роботи з інформацією, внаслідок чого окремі показники не в усіх випадках можуть бути якісно опрацьовані на різних рівнях прокурорської системи; в) нерегулярність, невпорядкованість потоків інформації внаслідок відсутності юридично закріпленої форми та невизначеності періодичності потреби в ній; г) надходження надлишкових обсягів інформації або її неповнота внаслідок відсутності єдиних вимог та умов щодо збирання інформації, що спричиняє, з одного боку, одержання випадкових, недостовірних відомостей, а з другого — надмірні витрати часу на їх опрацювання; ґ) диспропорційність інформації внаслідок розбіжностей у періодичності та формі отримання даних у різних ланках прокурорської системи, що не дозволяє оперативно та безпомилково зіставити інформацію, проаналізувати відповідні відомості; д) знецінення інформації через її несвоєчасне оброблення, що ставить під сумнів її використання в прокурорській діяльності.

Звідси очевидно, що вдосконалення прокурорської діяльності тісно пов'язане з реформуванням інформаційного забезпечення, його систематизацією, потребою забезпечення даними, які адекватно відображують процеси, що відбуваються як в самій системі (внутрішнє управління прокурорською системою), так і ззовні (зовнішні, спрямовані на реалізацію функцій прокуратури). Цим зумовлена необхідність розроблення сучасної моделі інформаційно-аналітичного забезпечення прокурорської діяльності, яка, на жаль, залишається на рівні, коли кожна структура прокуратури по суті займається інформаційним самозабезпеченням, витребовуючи та накопичуючи відомості про процеси, що відбуваються у правозастосовній та правоохоронній сферах без відповідної системи їх збирання та опрацювання.

У зв'язку з концепцією комп'ютеризації прокуратури останнім часом починають активніше використовуватися різноманітні загальнодоступні комп'ютерні інформаційно-пошукові системи правової інформації та засоби комп'ютерної телекомунікації масового застосування: електронна пошта, інформаційні ресурси в мережі Інтернет.

Загалом інформаційне забезпечення прокуратури спрямоване на забезпечення таких чинників: а) актуальність інформації, яка відображує реальний стан справ у відповідних сферах прокурорської діяльності за визначений період; б) об'єктивність даних, які відображують достовірність стану справ; в) повнота відбиття явищ таким чином, що дає можливість визначитися стосовно пріоритетних напрямів прокурорської діяльності; г) погодженість та інформаційна єдність показників, завдяки чому первинні дані не суперечать зведеним та похідним; ґ) можливість виконання таких функцій управлінського процесу, як облік та аналіз, прогнозування та планування, координація та контроль [238, с. 119–122].

Що стосується впровадження сучасних інформаційних технологій в їх повному обсязі (мережний варіант, прикладне програмне забезпечення високого рівня, законодавчі бази, електронний документообіг та ін.), то технічним вимогам відповідає не більше третини засобів комп'ютерної техніки, що експлуатується центральним апаратом ГПУ.

У контексті зазначеного у проекті майбутньої стратегії інформатизації прокуратури України має бути закладено перспективи безпосереднього звернення громадян через Інтернет до районних, обласних прокуратур та прирівняних до них за статусом інших прокуратур, ГПУ, в тому числі із заявами та скаргами, а також за довідками стосовно розгляду цих заяв, загальнодоступної статистики діяльності органів прокуратури в цілому та в регіонах тощо. Цей сегмент галузевої інформаційної системи прокуратури пропонується реалізувати через відповідний проект під назвою «Інтернет-приймальня (портал) прокуратури України», який пропонується інтегрувати через модернізацію галузевої автоматизованої інформаційної системи (ГАІС) «Скарга» в ГАІС «Звернення в прокуратуру».

Важливим аспектом техніко-технологічної структури галузевої інформаційної системи прокуратури України має стати галузева Інтра-

нет. Її пропонується розглядати як інтегроване інформаційне середовище функціонування електронного документообігу із застосуванням електронного підпису та як середовище здійснення контрольних функцій в управлінні органами прокуратури її керівниками. Розвиток технологій Інтранет дозволить модернізувати режим проведення електронних реєстрів та інтеграції їх з обліками результатів діяльності як окремих працівників, так і структурних підрозділів. При цьому у керівників та окремих працівників виникає можливість з меншими затратами робочого часу раціонально планувати та розподіляти навантаження, оформлювати різні звіти тощо, а резерв вивільненого часу застосовувати на реалізацію основних галузевих функцій.

Реалізація стратегії інформатизації прокуратури на методології під умовною назвою «Електронна прокуратура» передбачається у складі реалізації формування ідеї «Електронний уряд» як складової стратегії «Електронна Україна» з метою гідного представлення нашої країни у глобальному кіберпросторі. Таким чином, показано роль і розкрито значення модернізації галузевого інформаційного забезпечення, що передбачає розвиток автоматизованого інформаційно-обчислювального середовища для підвищення якості задоволення інформаційних потреб усіх підрозділів прокуратури, на всіх рівнях її організації та управління.

о ***Інформаційно-аналітична підсистема «Статистика»***

Аналіз стану інформаційного забезпечення прокурорської діяльності дає змогу погодитися з висновком про те, що прокурору необхідно відстежувати дані понад ста форм державної статистичної звітності під час здійснення нагляду за додержанням і застосуванням закону. Проте очевидно, що з часом така інформація потребує певного перегляду та переосмислення. Деякі процеси, які відбуваються у суспільстві, потребують удосконалення діяльності державних органів статистики і можуть знайти відображення у нових формах звітності. Перш за все це стосується роботи зі зверненнями громадян, яка обліковується на рівні відомств.

Інформаційно-аналітична підсистема «Статистика» забезпечує реалізацію обліків згідно з Інструкцією про порядок заповнення та подання документів первинного обліку злочинів, осіб, які їх вчинили, руху кримінальних справ, затвердженою відповідними наказами ГПУ,

МВС, СБУ, Державної податкової адміністрації і Міністерства юстиції України.

Облік злочинів, осіб, які їх вчинили, кримінальних справ в органах прокуратури (зокрема у військових прокуратурах), внутрішніх справ, податкової міліції та СБУ здійснюється на підставі таких облікових документів: 1) статистична картка на виявлений злочин; 2) статистична картка про наслідки розслідування злочину; 3) статистична картка про результати відшкодування матеріальних збитків та вилучення предметів злочинної діяльності; 4) статистична картка на особу, яка вчинила злочин; 5) статистична картка про рух кримінальної справи; 6) статистична картка на злочин, за вчинення якого особі пред'явлено обвинувачення; 7) єдиний журнал обліку злочинів, кримінальних справ і осіб, які вчинили злочини.

Систему показників у перелічених обліково-реєстраційних документах побудовано на кримінально-правовій основі і спрямовано на зміцнення законності під час здійснення обліку злочинів та їх розкриття.

Забороняється вносити в зазначені документи первинного обліку будь-які доповнення і зміни, оскільки вони єдині для всіх органів прокуратури та правоохоронних органів і можуть змінюватися і доповнюватися тільки за узгодженням з ГПУ.

Під час заповнення документів первинного обліку (статистичних карток, журналів, довідок) належить керуватися правилами реєстрації і обліку злочинів та осіб, які їх учинили, викладеними в Інструкції про єдиний облік злочинів, та положеннями, що зазначені в цій Інструкції.

Працівник з обліково-статистичної роботи зобов'язаний перевірити в картках правильність дублювання відомостей відповідних пунктів цифровими індексами, які розміщені в графоклітинках з правого боку карток, та правильність заповнення даних, які відзначаються в картках за довідниками, зробити відповідні позначки в документах первинного обліку. Протягом 24 годин з моменту одержання карток у прокуратурі працівник з обліково-статистичної роботи повинен зробити в Єдиному журналі обліку злочинів, кримінальних справ і осіб, які вчинили злочини, необхідні записи і направити облікові документи безпосередньо до обліково-реєстраційного підрозділу.

Обліково-реєстраційні підрозділи зобов'язані негайно врахувати всі надіслані і підписані прокурором документи первинного обліку і не мають права відкладати постановку на облік або виключати їх з обліку. У разі відсутності підпису прокурора або його заступника чи неможливості врахувати картку у зв'язку з неналежним її оформленням вона повертається для дооформлення через відповідного прокурора.

Усі вміщені в документах первинного обліку інформаційні показники і додаткові дані, що їх уточнюють, необхідні для реєстрації, обліку злочинів і осіб, які їх учинили, а також для подальшого складання статистичної звітності правоохоронними органами про злочинність і заходи боротьби з нею, мають бути пронумеровані.

У пронумерованих пунктах карток потрібні відомості або вписуються, або підкреслюються, а в розміщених з правого боку графоклітинках, там, де це необхідно, дублюються цифровими індексами.

Якщо правоохоронний орган розташований у тому самому місці, де й обліково-реєстраційний підрозділ, документи первинного обліку здає працівник з обліково-статистичної роботи органу особисто до обліково-реєстраційного підрозділу під підпис у реєстрі, в якому вказуються: назва картки, номер справи та дата одержання картки. Якщо правоохоронний орган і обліково-реєстраційний підрозділ розташовані в різних населених пунктах, документи первинного обліку може направляти працівник з обліково-статистичної роботи начальнику обліково-реєстраційного підрозділу поштою із супровідним листом, у якому вказуються ті самі реквізити, що і в реєстрі.

Реєстри і копії супровідних листів зберігаються у діловодстві працівника з обліково-статистичної роботи. Документи первинного обліку підлягають зберіганню в обліково-реєстраційних підрозділах упродовж одного року після складання на їх підставі статистичної звітності про злочини і осіб, які вчинили злочини, за умови, що по справах, які направлені до суду, в обліково-реєстраційний підрозділ надійшла із суду довідка про наслідки розгляду кримінальної справи судом (форма 6) та по закритих кримінальних справах, у разі їх наявності в архівах інформаційних підрозділів.

Документи первинного обліку про злочини, по яких справи зупинено за пунктами 1, 3 ст. 206 КПК, не знищуються, а зберігаються у спеціальній картотеці обліково-реєстраційного підрозділу до роз-

криття злочину або закриття справи на підставі, що виключає кваліфікацію діяння як злочину [211, с. 502–505].

о ***Електронна система «Нагляд»***

У прокуратурах областей з 2002 р. впроваджено інформаційну систему електронного обліку документообігу «Нагляд». Ця система забезпечує в автоматизованому режимі реєстрацію вхідної кореспонденції, наглядових проваджень, ведення баз даних за особами, організаціями, контроль визначених законодавством строків розгляду звернень та заяв, руху документів та виконання інших функцій щодо документообігу. Таке програмне забезпечення дозволяє проводити пошук осіб, організацій чи документів за багатьма параметрами, формувати в автоматичному режимі звіти за будь-який строк з контролю, обліку, статистики тощо.

Автоматизована система електронного обліку документообігу «Нагляд» відповідає всім вимогам законів України «Про прокуратуру», «Про звернення громадян», «Про статус народного депутата України», «Про Концепцію Національної програми інформатизації», Інструкції з діловодства в органах прокуратури України, затвердженої наказом ГПУ від 28 грудня 2002 р. № 90.

Впровадження цієї системи в секретаріатах прокуратур областей значно поліпшило контроль за документами, які надходять до прокуратури, що дало змогу скоротити формування статистичної звітності. Наприклад, по скаргах за рік по будь-якому відділу до кількох секунд скорочено виявлення прострочених строків контролю. Система дала змогу чітко розмежувати обов'язки співробітників секретаріату, рівномірно розподілити їх навантаження.

Заплановано завершити встановлення системи «Нагляд» в усіх міжрайпрокуратурах області, що дозволить працівникам апарату всіх обласних прокуратур одержувати інформацію та контролювати стан справ на місцях.

Водночас триває робота зі створення захищеної мережі зв'язку, яка вже використовується у форматі корпоративної електронної пошти.

До користування корпоративною електронною поштою підключено 68 структурних підрозділів прокуратури області, а 28 підрозділів апарату прокуратури області в разі необхідності напряму спілкуються з 40 міськрайпрокуратурами.

Використання електронного зв'язку відчутно підвищило ефективність роботи, забезпечило збереження робочого часу працівників, призвело до відмови від непродуктивних дій, що сприяє активній інтелектуальній діяльності. Зокрема, у оперативних та технічних працівників прокуратури з'явилася можливість відмовитися від використання факсимільних апаратів. Робота цієї системи здійснюється відповідно до Положення про організацію розсилання та прийняття документів в електронному вигляді за допомогою «Корпоративної системи електронної пошти прокуратури області».

З огляду на актуальність розвитку та впровадження новітніх технологій у діяльності органів прокуратури вже розроблена та опробована нова версія інформаційної системи електронного обліку документообігу «Нагляд». Нова версія значно поліпшує систему пошуку, зберігання, захищеності інформації, надає можливість керівникам структурних підрозділів прокуратури самостійно організовувати роботу з документами та контроль за строками розгляду скарг, заяв, які надходять до відділів [60, с. 116–120].

о ***АРМ «Прокурор-кримінолог-аналітик»***

Функціонально АРМ «Прокурор-кримінолог-аналітик» дає змогу:

1) створювати банки статистично-аналітичних даних з інформацією в інтересах діяльності галузевих служб органів прокуратури;

2) аналізувати та формувати у табличному або графічному вигляді (графіки, діаграми тощо) стан злочинності в Україні згідно з визначеними показниками та формами звітності;

3) аналізувати та формувати у таблицях або графіках прогнозований стан злочинності за визначеними напрямами;

4) аналізувати стан і прогнозувати можливість застосування додаткових методів та засобів для підвищення ефективності боротьби зі злочинністю з визначених напрямів;

5) аналізувати та визначати напрями та методи вдосконалення діяльності прокурорських працівників та інших галузевих служб для підвищення ефективності попередження злочинності тощо.

Програмно-технічний комплекс «Прокурор-кримінолог-аналітик» працює з будь-якою операційною системою, починаючи з Windows 9x, та з будь-якої версії MS Office (MS Office 97, MS Office 2000 та ін.)

У програмному забезпеченні використовується Microsoft Excel [23, с. 509]. Зазначений сегмент стратегії подальшої інформатизації прокуратури пропонується здійснювати в рамках проекту модернізації «АІС — Нагляд» у напрямі формування та розвитку її агрегованих складових: автоматизованих робочих місць (АРМ): «АРМ — прокурора», «АРМ — слідчого» тощо, які передбачається інтегрувати в підсистему комп'ютерної інформаційно-аналітичної системи управлінського призначення під умовною назвою проекту «КСІАЗ-Прокуратура УП».

За таких умов можна створити і багатофункціональну інформаційну підсистему електронного архіву е-сховище. Важливою складовою цієї підсистеми мають стати бази даних і знань у галузі держави і права.

Система «Закони та підзаконні акти України в Інтернеті» надає абонентам мережі Інтернет можливості: 1) пошуку документів за реквізитами (реєстраційним номером, датою прийняття, типом, органом влади, станом (чинні, нечинні); 2) пошуку документів за словами в текстах з урахуванням «відстані» між ними; 3) перегляду текстів знайдених документів, копіювання їх у файл. Бази даних поновлюються щоденно. Блоки поновлення для системи «Законодавство» передаються користувачам через електронну пошту і виставляються на FTP-сервер [148, с. 84–85].

Система «Інформаційна система розслідування, прокурорського нагляду, попередження кримінальних подій» розроблена на основі СУБД Oracle8i з використанням пакету Oracle Internet Developer Suite і працює в трирівневій архітектурі. В рамках наших пропозицій слід зауважити, що доступ слідчих районних прокуратур, що знаходяться на значній відстані від системних інформаційних криміналістичних ресурсів, може здійснюватися в межах закритої корпоративної системи прокурорського зв'язку.

Досить загальними та орієнтованими на кількісні аспекти інформатизації (збільшення кількості комп'ютерів та локальних мереж) є пропозиції за результатами дисертаційних досліджень щодо організаційно-управлінських аспектів діяльності органів прокуратури України [98; 246].

З огляду на викладене виникає ґрунтовна пропозиція щодо утворення в органах прокуратури відповідних структур — інформаційно-

аналітичних відділів (управлінь), здатних збирати від єдиних джерел єдину достовірну інформацію (як зовнішню, так і внутрішню), опрацьовувати її, перетворюючи на результативну. Це, по-перше, звільнить інших оперативних працівників від технічної роботи, пов'язаної зі збиранням, опрацюванням та елементарним аналізом такої інформації. По-друге, потребують визначення обсяг та джерела такої інформації, тобто вона має регламентуватися управлінськими актами Генерального прокурора України для всіх органів прокуратури. Видання таких актів передбачає розроблення переліку та структури інформаційних масивів відповідно до предмета прокурорської діяльності, створення таблиць регламентуючої інформації, вдосконалення аналітичної роботи, визначення та розрахунок якісних показників ефективності системи інформаційного забезпечення.

o ***Розбудова інформаційних технологій нового покоління***

Інформаційні технології можуть ефективно використовуватися також в організаційно-управлінській діяльності усередині прокурорської системи. Так, фіксування тієї чи іншої інформації в електронних службових блокнотах за типом «прокурорського досьє» зможе допомогти розумінню, засвоєнню, аналізу і використанню наявних матеріалів для наступних висновків. Це, зокрема, такі напрями, як доведення управлінських директив до виконавців, контроль за виконанням, облік і розстановка кадрів, перевірка професійної придатності, внутрішня безпека органів прокуратури.

Використання нових інформаційних технологій створило в органах прокуратури принципово нові умови для протидії злочинам в інформаційній сфері. Ці методи отримання та збереження оперативно-розшукової інформації означені як «аналітична розвідка», «забезпечення інформаційної безпеки», «комп'ютерна розвідка» [138]. З метою розв'язання проблеми централізованого збирання та накопичення оперативної інформації щодо злочинів у сфері нових інформаційних технологій на сучасному етапі пропонують залучити до автоматизованої інформаційно-пошукової системи «Оріон» підсистему «злочини у сфері нових інформаційних технологій». За аналізом наслідків опитувань необхідність такої системи підтримують 45,7 % респондентів [231].

Створення в Україні окремого відомчого чи міжвідомчого спеціалізованого підрозділу, завданням якого має бути вирішення лише

цього питання, безумовно, сприятиме підвищенню ефективності протидії злочинності у сфері високих технологій. Як завдання такого підрозділу запропоновані: 1) розроблення та проведення конкретних заходів із запобігання та розкриття фактів незаконних дій у сфері інформаційно-телекомунікаційних технологій; 2) проведення заходів щодо розшуку та затримання осіб, які вчиняють комп'ютерні злочини; 3) організація взаємодії з іншими оперативними підрозділами органів внутрішніх справ, СБУ, Департаменту виконання покарань у вирішенні питань боротьби з комп'ютерними злочинами, а також з операторами зв'язку, інтернет- та контент-провайдерами, банківськими, фінансовими установами, державними та громадськими організаціями; 4) узагальнення відомостей про факти комп'ютерних інцидентів, інформування про це вищестоящих та зацікавлених органів внутрішніх справ, інших правоохоронних органів, а також відповідних установ; 5) використання наявних сил і засобів, а також залучення фахівців інших державних органів та підприємств, громадських організацій [26, с. 319–328].

З метою підвищення ефективності заходів протидії злочинності у сфері нових інформаційних технологій необхідними є: 1) створення міжвідомчої робочої групи для розроблення та координації спільних заходів протидії комп'ютерній злочинності між правоохоронними органами та операторами зв'язку, інтернет- та контент-провайдерами, банківськими, фінансовими установами, державними та громадськими організаціями; 2) створення міжвідомчої системи моніторингу оперативної обстановки у сфері телекомунікаційних технологій; 3) розроблення нормативно-правового забезпечення доступу до інформації про протиправні дії при використанні корпоративних інформаційно-телекомунікаційних технологій; 4) розроблення нових програм навчання при кабінетах криміналістики, проведення електронних навчально-методичних семінарів слідчих прокуратури, які спеціалізуються на розслідуванні справ про комп'ютерні злочини; 5) розроблення та впровадження ефективних криміналістичних заходів реагування на комп'ютерні інциденти.

Важливого значення набувають створення єдиної системи оперативно-розшукової реєстрації, заснованої на високих інформаційних технологіях [34, с. 270–271], та формування інтегрованого

електронного банку даних для використання в рамках цього проекту. В цьому зв'язку загальнодержавний підхід вимагає регулярного доведення до органів прокуратури перспективних планів щодо централізованого впровадження у діяльність програмного забезпечення і технологій збирання інформації. При цьому доречно розглянути можливість створення єдиного банку даних криміналістичної служби органів прокуратури на територіальному рівні з наступним об'єднанням на загальнодержавному рівні.

Останнім часом на порядок денний постала проблема щодо розгляду питання про можливість створення відомчого (корпоративного) телекомунікаційного середовища, призначеного для об'єднання різних елементів інформаційної системи підрозділів прокуратури і забезпечення стійкого доступу до інформаційних ресурсів.

Отже, наглядово-аналітичні системи оброблення інформації є корпоративними інформаційними мережами спеціального призначення і інтегрованими компонентами єдиної телекомунікаційної інфраструктури органів прокуратури.

4.3. Стратегії розвитку інформатизації органів прокуратури України

о *Поняття стратегії інформатизації*

Взагалі, під стратегією розуміють загальний план дій з метою досягнення необхідного результату (на відміну від тактики, що вирішує окремі проміжні завдання). Звідси пропонуємо визначити стратегію розвитку як можливі згідно з чинними правилами (правовими нормами) способи дій суб'єктів суспільних відносин.

Окремо слід наголосити на тому, що стратегії вирішення інноваційних завдань, які виникають у сфері боротьби зі злочинністю і в сучасних умовах у переважній більшості потребують нестандартного підходу, пов'язана із застосуванням евристичних прийомів (евристик).

Серед основних завдань інформатизації прокуратури України — задоволення потреб громадськості в поінформованості про діяльність органів прокуратури, підвищення авторитету прокуратури в державі,

забезпечення співвідношення інтересів людини, суспільства та держави, а також перехід від паперових технологій документообігу до комп'ютерних [98].

Стратегії розвитку інформаційно-телекомунікаційної системи органів прокуратури є складовою частиною процесу інформатизації правоохоронних органів і представляють її найвищий рівень. До того ж, стратегії в цій галузі міцно пов'язані з державною політикою розвитку високих інформаційних технологій. Вони охоплюють питання теорії та практики підготовки інформаційно-телекомунікаційної системи до роботи у сфері боротьби зі злочинністю, тобто фактично питання інформаційної діяльності в екстремальних або надзвичайних умовах.

Сьогодні в органах прокуратури швидкими темпами провадиться робота із забезпечення всіх підрозділів як в центрі, так і на місцях комп'ютерною технікою, програмними продуктами, засобами зв'язку за останнім словом техніки. На тлі цього треба окреслити основні завдання інформатизації органів прокуратури.

Подальший розвиток інформатизації прокуратури України як напрямку науково-практичних досліджень має забезпечити формування вітчизняної наукової школи правової інформатики.

о ***Основні завдання інформатизації прокурорської діяльності***

Інформатизація прокурорської діяльності має створити теоретичну базу переходу від комп'ютеризації до високотехнологічної автоматизації виконання професійних завдань та інформаційного забезпечення прокурорських заходів з використанням сучасних електронно-обчислювальних (комп'ютерних) засобів.

Створення корпоративної волоконно-оптичної та обчислювальної (комп'ютерної) мережі здійснюватиметься поетапно і послідовно з урахуванням трирівневої системи органів прокуратури України. Першим етапом є модернізація та розвиток локальної обчислювальної (комп'ютерної) мережі ГПУ, другим — створення або модернізація і розвиток локальних обчислювальних мереж у прокуратурах обласного рівня і з'єднання їх із локальною системою ГПУ, третім — створення АРМ на базі персональних комп'ютерів у прокуратурах районного рівня і з'єднання їх з локальними системами прокуратур обласного рівня.

Згідно з вимогами тендерної документації комплексна інформаційна система органів прокуратури України (перша черга) включатиме такі інформаційні модулі: 1) розроблення проектно-технологічної документації щодо створення корпоративної телекомунікаційної локальної мережі органів прокуратури України; 2) створення структурованої кабельної мережі ГПУ; 3) створення системи електронного документообігу органів прокуратури України; 4) створення корпоративного порталу органів прокуратури України (внутрішня та зовнішня частини); 5) створення комплексної системи захисту інформації органів прокуратури України; 6) придбання та налаштування ліцензійного системного програмного забезпечення системи керування базами даних Oracle або аналогічної; 7) придбання та налагодження комп'ютерного обладнання.

Прогнозованими результатами реалізації генеральним підрядником першого етапу створення корпоративної волоконно-оптичної комп'ютерної мережі органів прокуратури України є впровадження системи в експлуатацію, де результативність впровадження визначатиметься якістю розроблення, повнотою та глибиною охоплення ділових процесів, якістю освоєння функцій системи користувачами. Очевидним є зменшення часу на пошук інформаційних ресурсів, ведення фінансового, бухгалтерського і господарського обліку та контролю виконання бюджету, доручень, узгодження документів, що розробляються, та матеріалів судових справ, поліпшення їх якості і як наслідок — розширення інформаційної бази. Завдяки впровадженню цієї системи можна прогнозувати загальне підвищення продуктивності праці співробітників прокуратури [241, с. 3–7].

Звідси з метою ефективної реалізації стратегії інформатизації прокурорської діяльності пропонується створення ситуаційно-аналітичного та сервісного центрів.

Такі центри мають здійснювати моніторинг заходів, накопичувати інформацію стосовно досягнення мети прокурорської діяльності, а також напрацьовувати рекомендації щодо координації, корегування, визначення нових завдань і заходів, виходячи із аналізу проблемних ситуацій.

Опановуючи юридичну науку та постійно підвищуючи кваліфікацію, органи прокуратури могли б на базі існуючих в її системі

бібліотек накопичувати спеціальну літературу на електронних носіях із різних галузей юридичної та інших наук — підручники, посібники, монографії, методичні комплекси тощо. Для цього також із використанням системи Інтернет можна заходити на сайти тих бібліотек, де є така електронна література. Це зекономить час та кошти на купівлю коштовних паперових носіїв, а також час на відвідування бібліотек.

Результати інвентаризації системного та прикладного програмного забезпечення, яке використовується в ГПУ, засвідчили, що майже третина його застаріла, звідси виникають проблеми з придбанням необхідного програмного забезпечення. І це пояснюється не тільки об'єктивними причинами, які полягають у недостатньому обсязі бюджетних коштів, а й суб'єктивним чинником — недостатнім розумінням важливості вирішення завдань і відповідно відсутністю ініціативи та творчого підходу під час реалізації положень єдиної інформаційної системи органів прокуратури. Це характерно як для центрального апарату, так і для більшості прокуратур областей, не кажучи вже про прокуратури міського та районного рівнів.

Саме з найбільш підготовлених областей слід розпочати реалізацію другого етапу створення єдиної інформаційної системи органів прокуратури України, що значно полегшить та оптимізує працю співробітників цих прокуратур.

Отже, основні складові стратегії інформатизації прокурорської діяльності пропонується визначити таким чином:

1) розвиток електронно-інформаційних зв'язків органів прокуратури України всіх рівнів між собою, а також з громадянами та різними організаціями, державними установами, службами, відомствами України, які знаходяться на території України та за її межами;

2) формування інтегрованої системи сховища електронних баз даних як єдиного електронного архіву, який забезпечуватиме відповідний правовий режим доступу до інформації, її аналітичне опрацювання при здійсненні працівниками прокуратури своїх функцій щодо статистики, переймання кращого досвіду роботи, наукових здобутків у галузі держави і права, правової інформатики тощо;

3) створення в органах прокуратури повноцінного електронного документообігу із застосуванням електронного підпису;

4) інтеграція галузевої комп'ютерної інформаційної системи прокуратури в єдине автоматизоване інформаційне середовище правоохоронних органів України та до загальнодержавної електронної інформаційної мережі на засадах методології формування в країні електронного управління як складових інформаційного суспільства, глобального кіберпростору;

5) співпраця з різними вітчизняними науковими та конструкторськими установами стосовно розроблення та впровадження новітніх комп'ютерних інформаційних технологій в усі сфери діяльності органів прокуратури України з урахуванням нових розробок щодо діяльності інших органів державної влади та органів місцевого самоврядування;

6) забезпечення підвищення комп'ютерної грамотності та інформаційної культури працівників органів прокуратури, насамперед шляхом інформатизації системи галузевої освіти, орієнтованої на застосування новітніх комп'ютерних інформаційних технологій, інтегрованих у загальнодержавні комп'ютерні інформаційні системи у сферах освіти, науки тощо;

7) сприяння застосуванню новітніх Інтернет-технологій в об'єктивному висвітленні діяльності органів прокуратури різними ЗМІ, у тому числі щодо протидії спеціальним інформаційним операціям з боку тих, хто намагається підірвати у суспільстві авторитет прокуратури в цілому чи окремих її підрозділів, а також окремих її працівників, зокрема змусити їх приймати рішення на користь правопорушників;

8) застосування комп'ютерних інформаційних технологій органами прокуратури при виконанні ними своїх функцій як складової вдосконалення державного управління, відносин між державою і громадянами, становлення електронних форм взаємодії між органами державної влади та органами місцевого самоврядування, фізичними та юридичними особами;

9) здійснення функцій прокуратури стосовно захисту інформаційних прав громадян, насамперед щодо доступності інформації, захисту інформації про особу (персональних даних), підтримки демократичних інститутів, поліпшення стану інформаційної безпеки людини, суспільства, держави в умовах розвитку інформаційного суспільства в Україні.

Для створення інформаційно-аналітичного центру можна було б застосувати науковий потенціал Академії прокуратури України, на базі якої проводити спільні оперативні наради відповідних працівників органів прокуратури та науковців.

Таким чином, здобутки правової інформатики відкривають нові можливості підвищення якості інформаційно-аналітичного забезпечення прокурорської діяльності, модернізації організації управління в органах прокуратури з використанням високих технологій.

о ***Концептуальні засади інформатизації органів прокуратури***

Стосовно управління в прокуратурі можна зазначити, що організація системної інформатизації можлива тільки тоді, коли в її необхідності переконані перші керівники ГПУ та керівники їх структурних підрозділів. Саме вони, у тому числі методами адміністративного та економічного стимулювання, спонукають підлеглих постійно підвищувати рівень інформаційної культури та організаційно забезпечують впровадження досягнень науково-технічного прогресу інформаційної сфери в практику [215, с. 14–19].

Узагальнені моделі стратегії розвитку системи інформаційно-аналітичного забезпечення прокуратури України можуть складати: 1) модель організації управлінських процедур та інформаційних послуг; 2) модель організаційно-функціональної структури; 3) моделі повноважень і відповідальності; 4) ресурсна модель у контексті моделі документообігу; 5) модель системи показників і оцінювання ефективності роботи; 6) модель ієрархії даних (інформаційних ресурсів); 7) модель концепцій модернізації інформаційно-аналітичної системи (у дворічному циклі); 8) модель програм впровадження концепцій модернізації.

Основні інформаційно-аналітичні завдання, які потребують вирішення на стратегічному рівні, пропонується сформулювати таким чином: 1) технологічна підтримка діяльності органів прокуратури України (наприклад, розроблення моделей типових управлінських та процесуальних процедур за функціями); 2) типові АРМ за посадами із доступом до централізованих та розподілених електронних сховищ даних і знань на основі комп'ютерних баз даних і знань в галузі держави і права тощо; 3) розроблення та застосування моделей, а також розрахунків для оперативного і довгострокового прогнозування, пла-

нування кримінологічних, соціальних та економічних ситуацій, математичних моделей динаміки зазначених процесів; 4) інформаційне забезпечення прийняття рішень у різних ситуаціях та оцінювання наслідків їх реалізації в умовах відповідного масштабу часу; 5) розроблення алгоритмів прийняття рішень у типових процедурах; 6) інформаційна безпека функціонування системи, моделювання, прогнозування випередження та подолання наслідків інформаційних загроз; 7) підвищення правової та інформаційної культури посадових осіб на різних рівнях управління системою прокуратури України; 8) підвищення комп'ютерної культури працівників органів прокуратури з урахуванням нових можливостей інформатики; 9) підвищення інформаційного рівня якості надання правових послуг громадянам, установам, організаціям через Інтернет.

У правовій сфері заслуговує на увагу поглиблення роботи із систематизації нормативно-правових актів для використання практичними працівниками органів прокуратури.

До таких баз даних мали б входити акти не тільки вищих чи центральних органів влади і управління, а й нормативні акти органів місцевої влади та самоврядування, державних підприємств, установ і організацій.

Слід також опрацювати ідею акумулювання органами прокуратури в електронному варіанті актів індивідуально-розпорядчого характеру, виданих органами влади, управління та самоврядування всіх рівнів, а також державними підприємствами, установами і організаціями (щось на кшталт того, як органи юстиції реєструють нормативні акти, так і органи прокуратури мали б брати до відома індивідуальні розпорядчі акти). Це служило б стримуючим чинником від різного роду порушень закону, а також інформативно сприяло б здійсненню прокуратурою своєї діяльності.

Для проекту Стратегії інформатизації прокуратури України пропонується таке: 1) автоматизований класифікатор адміністративно-територіального устрою України з екстраполяцією на геоінформаційні системи певного типу; 2) інформаційні інтерфейси обміну даними між підсистемами обласного, районного і міського рівнів та із зовнішнім інформаційним середовищем; 3) системи документообігу із застосуванням електронного підпису; 4) алгоритми підтримки при-

йняття рішень; 5) функціональні АРМ; 6) системи галузевої інформаційної безпеки.

Передбачені Концепцією технічні та програмні засоби забезпечать виконання завдань, зумовлених створенням інформаційно-обчислювальної мережі органів прокуратури: 1) здійснення міжвідомчих зв'язків — тобто забезпечення двосторонніх електронно-інформаційних зв'язків між органами прокуратури України всіх рівнів з різними організаціями і службами України, а також приватними особами, що перебувають як на території України, так і за її межами; 2) створення єдиного архіву даних — тобто створення системи збереження даних як єдиного архіву, який забезпечуватиме доступ до даних та їх аналітичне опрацювання при здійсненні прокурорами функцій стосовно нагляду за виконанням законів і проведення профілактичних заходів щодо запобігання порушенням закону; 3) забезпечення документообігу — тобто формування, збереження, пошук, аналіз і видання документів, контроль за їх виконанням, а також робота із законодавчо-нормативними базами; 4) запровадження безпаперових технологій — тобто впровадження безпаперової технології групової роботи — системи автоматизації ділових процедур (електронного документообігу).

Концепція враховує можливість інтеграції корпоративної інформаційно-обчислювальної мережі органів прокуратури України в загальну інформаційну систему правоохоронних органів, а також у загальнодержавну інформаційно-обчислювальну мережу України.

Зараз проводяться підготовчі організаційні заходи щодо створення єдиного банку даних прокуратур областей, за допомогою якого передбачається забезпечити повноту інформації, що збирається, і провести агрегацію розрізненої системи даних для більш цілісного й оперативного одержання необхідних відомостей (у режимі досьє) по конкретній особі або організації, що проходила за матеріалами органів прокуратури (кримінальні справи, матеріали про відмову в порушенні кримінальної справи, позовні вимоги, протести, попередження, подання та ін.).

Беручи до уваги зазначене, А. М. Куліш вважає, що невідкладними заходами у сфері інформатизації органів прокуратури України має бути створення електронної бази даних, в якій би містилися накази

та розпорядження Генерального прокурора, інформаційні листи Генеральної прокуратури та інші документи, обізнаність щодо яких необхідна для ефективного виконання прокурорсько-слідчими працівниками своїх функціональних обов'язків. Поновлення цієї бази в прокуратурах на місцях може здійснюватися двома шляхами: через мережу Інтернет або за допомогою компакт-дисків з останніми змінами у нормативній базі, які щотижня мають надсилатися із ГПУ у прокуратури на місцях [107, с. 75].

Одним із форвардних сегментів є інформатизація досудового провадження у кримінальних справах, де роль прокуратури провідна.

Важливим є також те, що інформаційна безпека органів прокуратури характеризується мірою захищеності держави (суспільства) та стійкості основних галузей прокурорської діяльності відносно небезпечних (дестабілізуючих, деструктивних, кримінальних тощо) інформаційних впливів, причому як з упровадження, так і добування оперативно-службової інформації.

Таким чином, стратегії розвитку інформаційно-телекомунікаційної системи органів прокуратури України передбачають використання волоконно-оптичних систем передавання даних у правоохоронних органах, що дозволить продуктивно використовувати існуючі інформаційно-телекомунікаційні мережі, скоротити витрати та строки на впровадження в телекомунікаційну систему прокуратури нових видів інформаційних послуг.

Побудова ефективної інформаційної системи, організація проходження інформаційних потоків мають охоплювати всі підрозділи. Для цього в районних прокуратурах необхідно встановити модеми і через мережу Інтернет організовувати доступ до поштового сервера електронного кабінету криміналістики прокуратури області, що дозволяє значно оптимізувати інформаційний обмін і скоротити відповідні фінансові витрати. Вважаємо, що при розробленні перспективних планів розвитку електронного кабінету криміналістики необхідно передбачити її розширення за рахунок підключення районних і міських прокуратур.

Важливою складовою системної інформатизації прокуратури України є техніко-технологічна структура її галузевої інформаційної системи. Ця структура повинна мати дві складові: 1) можливість до-

ступу до відкритих засобів електронної телекомунікації, зокрема Інтернет; 2) внутрішню галузеву комп'ютерну мережу (Інтранет), яка б забезпечувала реалізацію норм інформаційного законодавства про інформацію з обмеженим доступом.

Стосовно зовнішніх інформаційних зв'язків прокуратури України вбачається можливим розширення доступу до відповідних Інтернет-ресурсів прокуратури сторонніми користувачами (громадянами та ін.) відповідно до Закону України від 23 вересня 1997 р. «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» [67; 128; 166].

Таким чином, розв'язання поточних методологічних, методичних та інформаційно-технологічних проблем передбачає: 1) забезпечення єдності інтерфейсу різних інформаційних систем через стандартизацію; 2) розроблення електронної бібліотеки документів із стандартною внутрішньою структурою, ефективною системою пошуку і надійною схемою розмежування прав користувачів; 3) подання розробником технічної документації та додатків для замовника системи, чіткого опису складових її архітектури, інтегруючих різноманітні компоненти облікових підсистем; 4) створення нових прототипів інформаційного сервісу для підтримання робочих процесів працівників різних підрозділів органів прокуратури на основі стаціонарних та мобільних АРМ, CASE-технологій тощо; 5) уніфікацію та стандартизацію робочих процесів при виконанні функцій працівниками органів прокуратури [235, с. 92–99].

На основі узагальнення цих пропозицій слід розробити структуру і увести в експлуатацію внутрішній інформаційний сервер органів прокуратури, за допомогою якого на основі web-технологій забезпечується доступ користувачів системи до відомостей за напрямами роботи, а саме: статистичної інформації про результати діяльності органів прокуратури; аналітичної інформації з пріоритетних напрямів діяльності; статистичної, аналітичної та текстової інформації про результати діяльності правоохоронних і контролюючих органів, органів державної влади, наукових і навчальних закладів; інформації, що публікується в ЗМІ, про події і соціально-політичні процеси. Розглядається можливість створення єдиного банку даних органів про-

куратури за рахунок організації уніфікованої системи обліків результатів наглядової діяльності на територіальному рівні з наступним об'єднанням на загальнодержавному рівні [52; 232].

Визначено, що основним завданням, що вирішується в рамках цієї програми, є створення Єдиної інформаційно-телекомунікаційної системи (ЄІТС) органів прокуратури України, яка повинна об'єднати в інтегрований інформаційний простір розподілені і локальні цифрові (електронні) ресурси — інформаційні, наукові та адміністративні, програмні (алгоритмічні) — територіальних прокуратур та інших правоохоронних і експертних відомств на місцях. Користувачами ЄІТС можуть стати насамперед керівництво органів прокуратури, організаційно-управлінський апарат ГПУ, окремі колективи і співробітники. У рамках цієї програми створюється комплекс оптоволоконних засобів, що забезпечують використання її ресурсів і повнофункціональне управління ними. Більш того, найважливішою складовою проекту є створення власного інформаційно-телекомунікаційного Web-порталу.

Процес створення такої програми пропонується розбити на чотири послідовні етапи: а) формування цілісної системи цілей і вимог до програми і доведення її до кожного працівника, зокрема з використанням волоконно-оптичної мережі спеціально розробленого Інтернет-порталу; б) збирання і систематизація пропозицій щодо включення інноваційних заходів у програму, спільна робота з ініціаторами пропозицій, що сприяє підвищенню вірогідності наданої ними інформації; в) проектування найбільш повного варіанта програми, попередньо розробленої і затвердженої концепції інформатизації, можливостей і перспектив інформатизації прокуратури, аналізу пропозицій, що надійшли, для одержання повноцінного вихідного переліку заходів програми; г) розроблення декількох попередніх варіантів програми, що відповідають різним ресурсним обмеженням і цільовим настановам, використанням спеціально розробленого математичного апарату і оптимізаційного комп'ютерного моделювання (управлінської моделі) [153, с. 65–73].

Оскільки оптоволоконна інформаційна технологія є комплексом методів, способів і засобів пошуку, збирання (придбання), реєстрації, збереження, поширення (реалізації), захисту і відображення інфор-

мації за допомогою високотехнологічних інформаційних систем і волоконно-оптичних мереж передавання даних, першим етапом організаційних заходів у цьому напрямку має бути інформаційно-аналітична робота, а саме: створення єдиної системи обліку способів учинення злочинів, статистичної звітності, розроблення порядку аналітичної діяльності органів, які здійснюють протидію таким злочинам, розроблення нормативно-правових актів, що регламентують діяльність (взаємодію) спеціалізованих підрозділів з протидії правопорушенням у сфері інформаційно-телекомунікаційних технологій, розроблення відповідних методик.

Розв'язання проблеми створення єдиної оптоволоконної мережі в інформаційно-телекомунікаційній системі органів прокуратури України можливе шляхом: а) визначення потреб органів прокуратури в інформаційних ресурсах; б) удосконалення наявних та розроблення нових нормативно-правових актів, які чітко визначатимуть порядок, стандарти, механізм та обсяги інформаційної взаємодії; в) організаційного та кадрового забезпечення розроблення і функціонування системи; г) залучення інформаційних ресурсів інших державних органів для використання їх органами прокуратури в порядку, встановленому законодавством; ґ) розроблення та запровадження єдиної уніфікованої технології оброблення інформації в системі, а також типових і спільних програмних засобів; д) створення телекомунікаційної складової системи як окремої підсистеми Національної системи конфіденційного зв'язку із забезпеченням можливості інформаційної взаємодії з наявними системами правоохоронних органів; е) залучення до створення системи вітчизняних науково-дослідних установ; є) створення в органах прокуратури технічної бази для впровадження системи; ж) впровадження комплексної системи захисту інформації та підтвердження її відповідності в порядку, встановленому законодавством; з) визначення принципів можливої інтеграції системи в міжнародні спеціалізовані інформаційні системи у сфері запобігання злочинності [45].

Виходячи з аналізу нормативно-правових актів, а також з доктринальних положень щодо інформатизації України, можна запропонувати концептуальне визначення інформатизації прокуратури України як множини взаємопов'язаних наукових, технічних, організаційних, правових, соціально-економічних та інших процесів, спрямованих на

модернізацію інформаційного забезпечення діяльності прокуратури через створення, застосування та розвиток комп'ютерних інформаційних систем, мереж, ресурсів і технологій.

Отже, органи прокуратури виступають суб'єктами інформаційного права, які мають особливий статус, тобто фактично є спеціальними суб'єктами, що підтверджує співвідношення

$$Il = \frac{S \xrightarrow{1} C}{S \xrightarrow{2} P} \Leftarrow HTl \ , \tag{4.1}$$

де *Il* — інформаційне право; *S* 1 — суб'єкти; *C* — сфера боротьби зі злочинністю; *S* 2 — спеціальні суб'єкти; *P* — прокуратура; *HTl* — право високих технологій.

Слід відзначити такий системний недолік, як недостатній рівень надійності правового та організаційно-технічного захисту інформаційно-телекомунікаційної системи органів прокуратури.

Нарешті, підбиваючи підсумки з розгляду проблеми високотехнологічної інформатизації прокуратури, визначимо системну кореляцію основних категорій:

$$\frac{O}{T} \neq \frac{E}{I} \ , \tag{4.2}$$

де наглядово-аналітичні системи оброблення інформації (*O*) є спеціальними компонентами телекомунікаційної інфраструктури прокуратури (*T*). У той же час експертно-пошукові системи (*E*) становлять більш масивну інформаційну систему, яка організаційно підпорядковується інфраструктурі органів внутрішніх справ (*I*). Подібна конструкція містить приховану загрозу міжвідомчих неузгодженостей, що можуть виникати в інформаційній сфері зазначених відомств.

Для розв'язання цих проблем вважаємо перспективним створення в органах прокуратури спеціалізованого наукового підрозділу, до завдань якого має бути включено розроблення науково-методичної бази щодо розкриття злочинів у сфері нових інформаційних технологій, підвищення професійної підготовки прокурорів та слідчих, узагальнення передового досвіду використання можливостей високих технологій у сфері боротьби зі злочинністю.

Резюме. *Результати дослідження органів прокуратури як спеціальних суб'єктів високотехнологічного інформаційного права України дає підстави для таких основних висновків: 1) з'ясовано особливий статус суб'єктів інформаційного права у сфері боротьби зі злочинністю; 2) висвітлено основні засади інформаційного забезпечення прокурорської діяльності; 3) охарактеризовано особливості інфраструктури прокурорських телекомунікацій; 4) визначено види наглядово-аналітичних систем оброблення інформації та окремих підсистем; 5) розкрито загальні положення стратегії інформатизації органів прокуратури; 6) з'ясовано призначення та обґрунтовано ефективність інформаційно-телекомунікаційної системи органів прокуратури; 7) систематизовано напрями розвитку інформатизації органів прокуратури України.*

Ключові слова*: правоохоронні органи; органи прокуратури; інформаційно-аналітичні системи; електронний нагляд; «електронна прокуратура»; електронна статистика; прокурор-кримінолог-аналітик; інформатизація прокуратури.*

Контрольні запитання

1. Поняття системної інформатизації прокуратури, основні завдання та функції.
2. Органи прокуратури як спеціальні суб'єкти високотехнологічного інформаційного права**.**
3. Архітектоніка інформаційної мережі правоохоронних органів.
4. Етапи розвитку інформаційної мережі органів прокуратури.
5. Інформаційно-телекомунікаційна система органів прокуратури України
6. Структурна модернізація галузевої інформаційної системи прокуратури.
7. Організаційно-правові засади електронного документообігу в органах прокуратури.
8. Волоконно-оптичні мережі системи органів прокуратури як відомчі інформаційні мережі закритого типу.
9. Характеристика інформаційно-аналітичної підсистеми «Статистика».
10. Порядок та умови застосування комп'ютерної програми «Автоматизована система тестування» для атестування прокурорсько-слідчих працівників.

11. Інформаційна система електронного обліку документообігу «Нагляд» та проект «Електронна прокуратура».
12. Корпоративна система електронної пошти прокуратури області.
13. Автоматизоване робоче місце «Прокурор-кримінолог-аналітик».
14. Інтернет-приймальня (портал) прокуратури України.
15. Модернізація галузевої автоматизованої інформаційної системи «Скарга» в систему нового покоління «Звернення в прокуратуру».
16. Розвиток технологій електронних реєстрів та інтеграція їх з обліками результатів діяльності структурних підрозділів прокуратури.
17. Проблеми високотехнологічної модернізації інформаційного забезпечення діяльності органів прокуратури.
18. Впровадження інформаційних технологій нового покоління в інформаційно-телекомунікаційну систему прокуратури.
19. Проблеми створення волоконно-оптичних інформаційних комунікацій та обчислювальної (комп'ютерної) мережі прокуратури.
20. Перспективи застосування нової оптоволоконної технології «волокно в прокуратуру».

Розділ 5

Нанотехнологія як особливий об'єкт високотехнологічного інформаційного права

У цьому розділі ...

- ***Нанотехнологія: інновації, можливості та розвиток правового забезпечення.***

Інноваційне законодавство у сфері високих технологій ◄► Поняття нанотехнології ◄► Наноіндустрія як об'єкт права високих технологій ◄► Організаційно-правові проблеми нанотехнологій ◄► Модернізація економіки, інвестиційна політика та концепція розвитку нанотехнологій.

- ***Нанонаукові засади експертних досліджень об'єктів надмалих розмірів.***

Нанонаука ◄► Судова експертиза та високі експертні технології ◄► Поняття і види об'єктів надмалих розмірів ◄► Нанотехнології в судово-експертній практиці ◄► Види наноматеріалів і криміналістична нанотехніка ◄► Судова медицина і нанотехнології ◄► Судова хімія і нанохімія ◄► Судова (криміналістична) фізика і нанотехнології.

- ***Проблеми інтелектуалізації інформаційної та міжнародної злочинності і перспективи інноваційних розробок антикримінальних наносистем.***

Інформаційна злочинність ◄► Міжнародна злочинність ◄► Інтелектуалізація злочинності ◄► Інфотероризм ◄► Злочини у сфері нанотехнологій і нанозлочинність ◄► Штучний інтелект і нанороботи ◄► Ядерний тероризм ◄► Психотероризм ◄► Авіатероризм ◄► Антитерористичні нанотехнології ◄► Інформатизація Збройних Сил і військові нанотехнології.

5.1. Нанотехнологія: інновації, можливості та розвиток правового забезпечення

o *Інноваційне законодавство у сфері високих технологій*

Як вище було доведено, високотехнологічне інформаційне право є окремою підгалуззю (науковою теорією), що формується у рамках

науки інформаційного права. Невиправдане виключення теоретико-правових засад високих технологій із інформаційного права обмежує сферу правового регулювання останнього і фактично залишає його на тупиковій гілці розвитку. Оскільки провідним методом інформаційного права вважається метод комплексного застосування методів конституційного, адміністративного, цивільного, трудового та кримінального права, стає зрозумілим, що методи права високих технологій ґрунтуються на методах цивільно-правового, адміністративно-правового, господарсько-правового регулювання та деяких інших.

Отже, інші інститути права агрегуються з інформаційним правом. Окремі з них у певних умовах мають статус міжгалузевих субінститутів. Саме до таких можна віднести право високих технологій. У цьому зв'язку нижче показано місце високотехнологічної теорії у системі інформаційного права (схема 5.1).

Схема 5.1

До функцій права високих технологій мають бути віднесені правове регулювання клітинних технологій, правове регулювання технології біоінженерії, правове регулювання водневої енергетики, правове регулювання нових джерел енергії, правове регулювання технологій оброблення, зберігання, передавання і захисту інформації, правове регулювання інтелектуальних систем навігації, правове регулювання ядерного виробництва, правове регулювання космічної діяльності тощо.

Слід зазначити, що в нашій країні поки що немає спеціального систематизованого законодавства стосовно високих технологій. Інноваційне законодавство виконує функцію своєрідного полігону для

відпрацювання нових категорій права інтелектуальної власності та високих технологій, що можуть бути складовими в переліку вже закріплених законодавством об'єктів. Йдеться перш за все про категорії «нанотехнологія» та «нанотехнології». Сьогодні рівною мірою використовуються обидва зазначені терміни.

Нанотехнологіями вважаються міждисциплінарні технології, які розроблені для об'єктів розмірами менш як один мікрон і дають змогу проводити дослідження, маніпуляції та оброблення речовин у діапазоні розмірів від 0,1 до 100 нанометрів [95].

Утім, вважаємо, що з юридичної точки зору для визначення поняття цього нового соціально-правового феномену вірніше буде базове застосування в єдиному числі, тобто «нанотехнологія». У свою чергу термін «нанотехнології» є похідним, оскільки означає декілька видів основної технології. Тому з метою мінімізації термінологічної плутанини треба визначити основні нормативно-правові джерела, що регулюють соціотехнічні відносини, пов'язані з нанотехнологією. Перш за все потрібно назвати Концепцію Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010–2014 роки [95] та розпорядження КМУ від 3 квітня 2009 р. «Про схвалення Концепції Державної цільової науково-технічної програми "Нанотехнології та наноматеріали" на 2010–2014 роки» [175].

Отже, право високих технологій не обмежується регулюванням виключно інформаційних правовідносин, а системно регулює усі соціальні відносини, в тому числі ті, які виникають під час розроблення та впровадження нанотехнологій.

Без сумніву, нанотехнології є одним з найбільш прогресивних видів високих технологій як загальної системи вищого рівня. У зв'язку з цим зазначені норми мають створити гармонійно узгоджену комплексну систему правового регулювання суспільних відносин щодо нанотехнологій.

Законодавство у цій сфері достатньо швидко розвивається, намагаючись відобразити розвиток соціальної складової впливу нанотехнологій на інформаційні правовідносини. Водночас слід відзначити, що сьогодні існує система відносно відокремлених від інших та пов'язаних між собою правових норм стосовно нанотехнологій, що регулюють відповідну групу суспільних відносин. Так,

до них можна віднести закони України «Про Національну програму інформатизації» [70] та «Про Концепцію Національної програми інформатизації» [71], Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки [147], постанову ВРУ від 16 червня 2004 р. «Про дотримання законодавства щодо розвитку науково-технічного потенціалу та інноваційної діяльності в Україні» [163], Указ Президента України від 24 вересня 2001 р. «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» [226], Комплексну програму фундаментальних досліджень НАН України «Наноструктурні системи, наноматеріали, нанотехнології» та ін.

Виникнення численних правових колізій у сфері створення нанотехнологій та впровадження наноматеріалів свідчить про те, що існуючий на сьогодні механізм правового регулювання є недостатнім. У зв'язку з тим, що суспільні відносини у цій сфері активно розвиваються, система правового регулювання потребує відповідних змін. Зокрема, з метою координації діяльності у наносфері, здобуття передових позицій на світовому ринку високотехнологічної продукції, а також забезпечення конкурентоспроможності та безпеки країни, захисту і розвитку високих технологій нормативне регулювання нанотехнологій має виділитися в окремий правовий напрямок.

Разом із тим віднесення нанотехнології до високих технологій передавання інформації потребує додаткового розроблення, прийняття та систематизації окремих правових норм у сфері інформаційного права та суміжних галузях.

У зв'язку з цим постають проблеми організаційного та правового забезпечення нанотехнологій:

$$O + L \Rightarrow Nt \ , \tag{5.1}$$

де організаційне забезпечення нанотехнологій (O) є сукупністю документів, що встановлюють організаційну структуру процесу розроблення, виробництва та впровадження експериментальних, дослідних та промислових зразків нанопродукції, права і обов'язки персоналу та користувачів при експлуатації нанопродукції; правове забезпечення нанотехнологій (L) — сукупність норм, що регламентують

правові взаємовідносини при функціонуванні нанопродукції та юридичний статус результатів їх функціонування.

Нанотехнологія стала найбільш перспективною складовою процесу використання інформаційних ресурсів суспільства. Тому назріла потреба в розробленні нормативно-правових документів у сфері нанотехнологій та наноіндустрії, де окремо слід передбачити норми щодо правового забезпечення нанотехнологій спеціального призначення (схема 5.2).

Схема 5.2

Можна зробити висновок про те, що нині існують засади визначення права високих технологій як складової спеціальної частини інформаційного права. Звідси потрібно навести ґрунтовну аргументацію щодо необхідності та обґрунтованості подібних організаційних і правових заходів у цій новій сфері суспільних відносин.

о ***Поняття нанотехнології***

Будь-яка технологія, як-то оброблення матеріалу на макро-, мікро- або нанорівні, не може обходитися без засобів виміру відповідних величин [38]. У перекладі із грецького слово «нано» означає карлик. Один нанометр (нм) — це одна мільярдна частина метра (10^{-9} м). Більшість атомів мають діаметр від 0,1 до 0,2 нм, а товщина ниток ДНК — близько 2 нм. Діаметр еритроцитів — 7000 нм, а товщина людського волосся — 80 000 нм.

Одними з перших інструментів, які допомогли ініціювати нанотехнологічну революцію, були створені в 80-х роках XX ст. так звані зонди, що сканують. Згодом на їх основі з'являлися перші тунельні мікроскопи.

Слід визначити, що основними галузями нанотехнології є наноматеріали, наноінструменти, наноелектроніка, мікроелектромеханічні системи та нанобіотехнології [151, с. 18–26]. Розвиток наноелектроніки ґрунтується на елементній базі, яка складається з кристалічних структур, розміри яких становлять нанометри [120]. Вже сьогодні на основі нанотехнологій створено нові лазери і зносостійкі покриття магнітних дисків нанометрової товщини, високоселективні наноструктурні каталізатори, нанопокриття лопастей вертольотів і ефективні присадки до ракетного палива, нові лакофарбувальні матеріали і косметичні товари.

Виготовлені із застосуванням нанотехнологій речовини та матеріали знайшли і в недалекому майбутньому знайдуть ще ширше застосування в енергетиці (ультрадисперсне ядерне паливо, матеріали для сонячної енергетики, нові хімічні джерела живлення), технологіях створення нових поколінь авіаційно-космічних апаратів (легкі, жаростійкі матеріали та покриття, елементи систем живлення, орієнтації і управління, нові види палива), засобів наземного і супутникового зв'язку та інформації (мініатюрних, енергоекономічних, безпечних, інформаційно високоємнісних елементів і систем), систем безпеки і оборони (нові засоби виявлення і розвідки, засоби колективного та індивідуального захисту особового складу, нові роботизовані системи озброєння, нові матеріали з високою міцністю).

Завдяки застосуванню нанотехнологій електроніка наближається до рівня мініатюризації, коли робочими елементами інтегральних

схем будуть невеликі ансамблі атомів і молекул або окремі спеціально синтезовані молекули.

Отже, визначимо нанотехнологію як сукупність наукових знань, способів і засобів, спрямованого, регульованого складання (синтезу) із окремих атомів і молекул різних речовин, матеріалів і виробів із лінійним розміром елементів структури до 100 нм.

о ***Наноіндустрія як об'єкт права високих технологій***

За багатьма прогнозами, XXI ст. визначатиме наноіндустрія.

Дотепер нерідко термін «індустрія» використовується як синонім терміна «промисловість». Утім, сьогодні це вже не зовсім коректно. Індустрія (від лат. *industria* — діяльність, ретельність) — це сфера діяльності, що поєднує в собі виробництво, збут певних товарів, сполучені сектори та споживчу аудиторію.

Наноіндустрія — сфера суспільних відносин та сектор економіки, що включає виробничо-технологічне впровадження інноваційних здобутків науково-дослідницької діяльності у пріоритетний сектор економіки відповідно до концепції державної програми створення, виготовлення, впровадження та розповсюдження нанопродукції. При цьому під пріоритетом пропонуємо розуміти першість у відкритті та винаході.

Складовими частинами наноіндустрії є: 1) науково-дослідницька діяльність — сукупність інноваційних наукових заходів, спрямованих на розроблення дослідних зразків нанопродукції нової якості; 2) виготовлення нанопродукції — виробничо-технологічний процес організаційно-виробничих заходів, спрямованих на підготовку і випуск у світ нанопродукції; 3) розповсюдження нанопродукції — на ринкових засадах доведення до споживача економічних переваг промислових зразків нанопродукції.

Нині на ринку високих технологій виробляються дослідницькі тунельні і атомно-силові мікроскопи. Проводиться комплекс дуже важливих робіт з лінійного виміру і взагалі з нанометрології.

Одна з проблем наноіндустрії України — це відсутність спеціального технологічного обладнання. Слід особливо зазначити, що наноіндустрія — це технологія багатопланового призначення. Якщо сьогодні робляться наночастки, то їх можна застосувати для зубної пасти (наприклад, наночастки срібла), а завтра — для якихось зовсім інших цілей, включаючи військову техніку.

Не секрет, що у світі ведуться активні роботи з дослідження і розроблення нанозброї. Міністерство оборони США створила інститут нанотехнологій для розвитку напрямів військового використання нанотехнологій за лінією Агентства передових оборонних розробок США (DARPA). Наприклад, у цього агентства є програма з наноелектроники. У ній перераховано більше 50 напрямів, і за кожним з них, принаймні, у відкритій частині, закріплено конкретний американський університет, у деяких випадках — окремі фірми. В Україні поки що немає нічого подібного.

Пріоритетним вектором політики розвитку високих технологій має стати становлення наноіндустрії, тобто промисловості принципово нового типу, особливість якої — в розробках вимірювального та експертного обладнання, різних наноматеріалів, спеціальних покрить, що можуть бути використані в судово-експертній практиці.

о ***Організаційно-правові проблеми нанотехнологій***

Існують підстави для твердження, згідно з яким правове регулювання стосовно нанотехнологій є правовим феноменом, що формується в інформаційному праві, джерелами якого поряд з інформаційним правом є цивільне, адміністративне, кримінальне право та низка комплексних галузей права (господарського права, права інтелектуальної власності тощо). Нанонаука, нанотехнології і наноіндустрія за своїм змістом можуть охоплювати різні галузі знань.

Організаційно-правова структура наносфери неоднорідна, але можна визначити три об'єкти, які одночасно постають основними етапами розвитку політики державного регулювання, а саме: нанонауку, нанотехнологію, наноіндустрію.

1-й етап) *нанонаука* — новий особливий вид людської пізнавальної діяльності, спрямований на напрацювання об'єктивних, системно організованих та фундаментальних знань про наноявища, що дозволяють теоретично обґрунтувати і побудувати причинно-наслідкові зв'язки і як наслідок — прогнозувавати подальший розвиток нанознань.

2-й етап) *нанотехнологія* — практичні методи дослідження, аналізу і синтезу, а також процес фундаментального розроблення методів виробництва і застосування продуктів із заданою атомарною струк-

турою шляхом контрольованого маніпулювання окремими атомами та молекулами.

3-й етап) *наноіндустрія* — сфера високотехнологічної діяльності, сектор інноваційної економіки, що включає дослідне та серійне виробництво, промислове впровадження і реалізацію як нанопродукції, так і нанотехнологій, а також допоміжні сектори та споживчу аудиторію.

Наведене надає підстави щодо висновку про те, що нанонаука, нанотехнології та наноіндустрія є об'єктами цивільних правовідносин у інформаційній сфері. Що стосується співвідношення нанонауки і нанотехнологій, то останні є складовою частиною цієї комплексної науки майбутнього.

Спробуємо визначити наноявища і нанопроцеси як об'єкти високотехнологічного інформаційного права (схема 5.3).

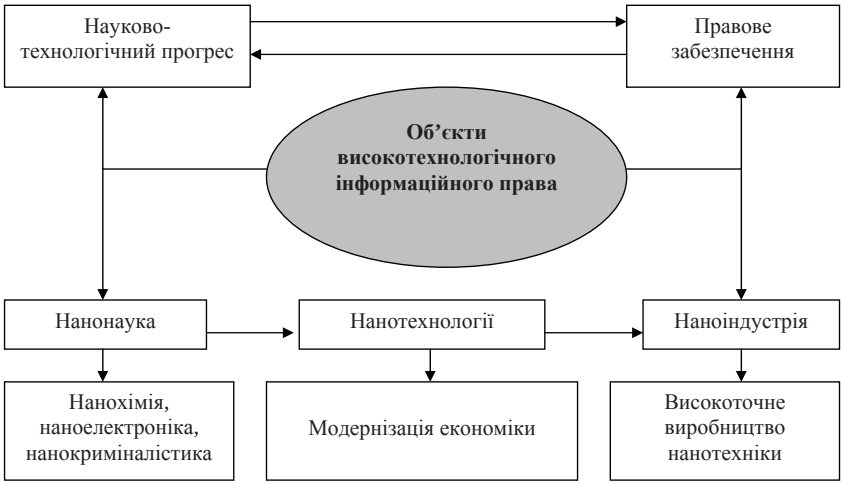


Схема 5.3

Таким чином, розроблення надпотужних інформаційних систем надмалих розмірів є найбільш перспективним напрямом розвитку нанотехнологій.

Нарешті, підсумуємо, що нанотехнологічне суспільство є фактично наступною стадією розвитку інформаційного суспільства, що ґрунтується на розвитку та використанні нанотехнологій.

о ***Модернізація економіки, інвестиційна політика та концепція розвитку нанотехнологій***

У цілому економіку країни можна визначити як організацію, структуру та стан господарського життя.

Формування та розвиток національної інноваційної системи є необхідною умовою реалізації інноваційного сценарію модернізації держави.

Інноваційна економіка є типом економіки, в якій прибуток створюється не за рахунок матеріального виробництва (індустріальна економіка) і не за рахунок концентрації фінансових центрів. Інноваційна економіка фактично постає економікою знань або інтелектуальною економікою і дозволяє генерувати надлишковий потік інновацій, постійно підвищуючи наступний рівень у технологічному змаганні.

Інноваційна економіка забезпечує світову економічну перевагу країни, що її здійснює. За своїм змістом інноваційна діяльність є економічною діяльністю, оскільки поєднує низку внутрішніх ознак: комерційну мета, інтелектуальну основу та отримання прибутку як кінцеву мету.

Одним з основних пріоритетних напрямів є модернізація та комплексний розвиток української економіки за допомогою побудови національної інноваційної системи, розширення нових конкурентоспроможних секторів у сфері високих технологій, усунення внутрішніх бар'єрів, що перешкоджають інноваційному росту. У зв'язку з цим останнім часом на найвищому рівні висловлюється припущення, згідно з яким розвиток економіки у сучасних умовах має ґрунтуватися на п'яти «І» — ІНСТИТУТИ (1) + ІНВЕСТИЦІЇ (2) + ІНФРАСТРУКТУРА (3) + ІННОВАЦІЇ (4) + ІНТЕЛЕКТ (5). Оскільки в сучасних соціотехнологічних умовах більшість з компонентів вибудовується на новому інформаційному підґрунті, можна відшукати системну незавершеність концептуальної конструкції «5-І». Адже ефективність національної інноваційної системи у майбутньому стане визначатися не тільки її структурою, а й інформаційною чіткістю та системною узгодженістю виконання завдань, що поставлені державною політикою перед її елементами, збалансованим інформаційним розвитком підсистем генерації та трансферу знань, а також виробництвом наукомісткої високотехнологічної продукції. Тому неврегульованість останнього зумовлює

модифікацію цієї формули шляхом додаткового включення важливого шостого елемента ІНФОРМАЦІЯ (6).

Такий шлях залишається практично неможливим без вирішення багатьох питань, пов'язаних з правовим регулюванням інноваційної діяльності у сфері високих технологій, що додаткового підкреслює актуальність удосконалення та кодифікації інформаційного законодавства.

З метою якісного задоволення матеріальних, інформаційних та духовних потреб суб'єктів інвестиційної діяльності у процесі її здійснення виникають суспільні відносини стосовно продуктивної реалізації інвестицій національних та іноземних інвесторів, що потребує наявності механізму правової регуляції.

Незважаючи на наявність окремих футуристичних визначень та прогнозів, техносфера тим не менш залишається виробничою сферою, де основною детермінантою є технологічна еволюція.

У цьому зв'язку можна припустити, що для забезпечення нормального і стабільного розвитку промисловості у сучасних умовах потрібні якісні та органічні модернізаційні зміни у структурі економіки, що неможливо стихійно, без свідомого проведення відповідної державної політики, у тому числі у сфері розвитку високих технологій.

Отже, визначимо гіпотезу, згідно з якою сьогодні змінити економіку можливо лише активно використовуючи високі технології.

При цьому інвестиційна політика у сфері високих технологій має бути послідовною і не залежати від зміни певних політиків та державних діячів, персонального складу уряду тощо. Стрижень цієї політики становлять її фундаментальні принципи, що визначають рішення, порядок та умови реалізації. Саме такий механізм зможе забезпечити прогнозування, послідовність і спадкоємність інноваційних рішень.

Спрямованість зміни економічних показників обумовлюється обробленням інформації та установленням на цій основі тенденцій економічного зростання або спаду, що в літературі позначається як тренд. Оскільки тренд є загальною тенденцією спрямованості змін показників, що розглядається у рамках технічного аналізу, фінансові плани суб'єктів діяльності у сфері високотехнологічних інновацій мають ґрунтуватися на аналізі більш точних прогнозів визначальних чинників.

Важливі результати для оздоровлення економіки України може надати впровадження інноваційного проекту, що отримав назву парку високих технологій. До речі, використовуються також інші назви: технопарк, науково-технологічний або регіональний індустріальний парк, що свідчить про існування різних моделей технопарків.

Метою цього проекту є створення в державі сприятливих умов для модернізації індустрії експортноорієнтованого програмування, розвитку інших експортних виробництв, що ґрунтуються на високих технологіях, а також для концентрації кадрового, науково-виробничого та інвестиційно-фінансового потенціалів.

Звідси технопарк уявляється спеціальною територією, де об'єднані науково-дослідні організації, об'єкти соціальної індустрії, ділові центри, виставочні площадки, заклади освіти, а також допоміжні об'єкти: транспортні засоби, автомагістралі, відокремлений мікрорайон або містечко-супутник для проживання персоналу, заклади освіти, система охорони тощо.

Технопарки, що створюються у сфері високих технологій, обов'язково повинні мати відповідну інвестиційно-банківську та юридичну інфраструктуру.

Отже, як ми усвідомлюємо, основним завданням створення технопарків є концентрація на окремій території фахівців різного профілю з метою забезпечення запуску та функціонування єдиного високотехнологічного циклу.

Наголосимо, що практична реалізація проекту регіональних індустріальних та технологічних парків (РІТ-парків) забезпечить створення нових підприємств, діяльність яких відповідає пріоритетам розвитку економіки регіону з метою нарощування промислової, інвестиційної та інноваційної компоненти регіональної економіки.

Як пріоритетні напрями кожного технопарку логічно визначати окремі спеціалізації. У певному сенсі технопарками можна вважати академмістечки. У таких умовах учені зможуть проводити дослідження у науково-дослідних інститутах, викладати у навчальних закладах та брати участь у процесах впровадження результатів своїх розробок в інноваційні проекти. З метою ефективного запровадження проекту технопарків в Україні потрібно не чуратися радянського (Зеленоград, Новосибірськ, Томськ) та сучасного російського (Казань, Обнінськ, Санкт-Петербург, Тюмень) досвіду.

За більшістю прогнозів інноваційної діяльності технопарків у сфері високих технологій, вартість сукупного обсягу виробленої продукції та наданих послуг зможе перевищити 20 млрд гривень.

У сучасних умовах досягнення науки і високих технологій стали визначати динаміку економічного зростання, рівень конкурентоздатності держав у світовому співтоваристві, ступінь забезпечення їх національної безпеки та інтеграції у світову економіку [163, с. 68–72]. Так, з метою реалізації науково-технічних програм та інноваційних проектів на просторі Євразійського економічного співтовариства створюється Центр високих технологій ЄврАзЕС.

Використання можливостей нанотехнологій у найближчій перспективі сприятиме збільшенню обсягу виробництва внутрішнього валового продукту та істотному економічному ефекту в галузі наноелектроніки [95]. До 2015 р. світовий ринок продукції нанотехнологій оцінюватиметься експертами у трильйон доларів і потребуватиме два мільйони фахівців. Уряди і найбільші корпорації світу інвестують мільярди доларів щорічно на розвиток і впровадження у виробництво нанотехнологій. До 2015 р. у РФ на розвиток нанотехнологій буде виділено 318 млрд руб. Це найпотужніша в світі державна інвестиційна програма у цій сфері.

Ґрунтуючись на цьому, слід визначити, що соціально-технологічна сфера знаходиться у рамках інвестиційної діяльності, де особливе місце в модернізації економіки відводиться інвестиційній політиці.

Інвестиційна політика у цілому розуміється як система господарських рішень, які визначають обсяг, структуру та спрямованість капітальних вкладень, що забезпечує зростання та оновлення фондів. З цього випливає, що ефективність інноваційної діяльності у сфері високих технологій визначається інвестиційною політикою держави. Тому стратегічним завданням модернізації і технологічного розвитку економіки України є визначення пріоритетних напрямів, форм і методів державного регулювання, у тому числі у сфері високих технологій. Це додатково підкреслює актуальність розробок механізму правової регуляції, оскільки правові норми впорядковують соціальні процеси у сфері високих технологій та інформаційної діяльності, встановлюючи однакові правила поведінки для суб'єктів.

Отже, зрозуміло, що успішний розвиток нанотехнологій можливий тільки при якісних перетвореннях в економіці і соціальній сфері. Тому сформульовано п'ять пріоритетів технологічного розвитку країни — це енергетика, у тому числі енергоефективність, енергозбереження, нові види палива, ядерні технології, інформаційні технології, наземна і космічна інфраструктури передавання інформації, медицина, фармацевтика [16].

Але, незважаючи на розуміння значення нанотехнологій, дослідження у галузі нанометрології, наноелектроніки, біотехнології, точного приладобудування, наноматеріалів, фотоніки тощо в Україні проводяться безсистемно [99, с. 119–135]. Оскільки дотепер не існує центру координації з нанотехнології, програм цільової підтримки таких робіт на державному рівні, обмежуються фінансові ресурси, що виділяються на науку та високі технології, спостерігаються факти роздріблення ресурсів.

За Концепцією Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010–2014 роки потрібно визначити такі пріоритетні заходи розвитку нанотехнологій: 1) створення структури управління, безпосередньо підпорядкованої вищому керівництву держави, яка була б наділена особливими повноваженнями для створення нанотехнологічної наукової школи і промисловості в стислий строк; 2) розгортання нанотехнологічних досліджень і розробок, створення відповідної системи підготовки наукових кадрів, кваліфікованого персоналу, спроможного працювати з нанотехнологічним устаткуванням і об'єктами; 3) розроблення стратегії і тактики бойових дій із застосуванням нанотехнологічної зброї, засобів захисту, устаткування і приладів індикації та ідентифікації такої зброї, а також її нейтралізації і знищення; 4) створення в державних зовнішньоекономічних органах і розвідслужбах спеціальних підрозділів з особливими правами і можливостями для придбання за кордоном сировини, устаткування, зразків техніки цільового призначення; 5) імпорт устаткування і продуктів нанопромисловості, що дозволяє створювати компоненти нанотехнологічного устаткування; 6) створення можливостей для молекулярного моделювання, розрахунку і тестування складних наноструктур, придбання комп'ютерів відповідної потужності; 7) створення системи захищених лабораторій, ви-

робництв, складських сховищ для нанооб'єктів і спеціалізованих засобів їх транспортування підвищеної безпеки; 8) широка поінформованість населення щодо потенційних загроз нанотехнологій та необхідності мобілізації сил на науково-технічний розвиток; 9) розвиток військово-технічного співробітництва із зарубіжними державами в галузі нанотехнологій; 10) розроблення і введення в експлуатацію системи наносенсорів для антикримінального випередження терористичної діяльності.

За аналітичними даними Американського національного наукового фонду (NSF), уряди і промислові кола розвинених країн очікують в найближчі 10–15 років бурхливого зростання обсягів ринку нанотехнологічних матеріалів, приладів та іншої продукції з виходом на такі обсяги: наноструктурні матеріали і технологічне обладнання — 340 млрд дол./ рік; наноелектроніка — понад 300 млрд дол./ рік; фармацевтичні нанопрепарати — понад 180 млрд дол./ рік; хімічна продукція на основі нанотехнологій — 100 млрд дол./ рік; наноматеріали для аерокосмічної промисловості — 70 млрд дол./ рік. Таким чином, світовий ринок цієї продукції може досягти 1 трильйона доларів до 2015 р.

Широкомасштабні нанотехнологічні розробки почали здійснюватися у більшості розвинених країн з початку 90-х років XX ст. і тепер такі програми мають більше 50 країн, а щорічні світові обсяги інвестицій в нанотехнології обчислюються мільярдами доларів і мають стійку тенденцію до зростання.

Практично весь світовий обсяг (~90 %) таких інвестицій сконцентровано в 15 країнах: США, Японії, Великій Британії, Австралії, Німеччині, Ізраїлі, Індії, Китаї, Канаді, Південній Кореї, Франції, Фінляндії, Сінгапурі, Тайвані і РФ, де частка державних витрат на роботи в галузі нанонауки і нанотехнологій перевищує 50 % від загального обсягу їх фінансування.

Світовими лідерами за обсягами інвестицій в нанотехнології всі останні роки були США і Японія, а в поточному році до них приєдналася РФ, де сконцентровано більше половини світового обсягу інвестицій. У США бюджетне фінансування розвитку нанотехнологій та виготовлення нових наноматеріалів становить більш як 1 млрд доларів США на рік. В Японії на розроблення в цій галузі у 2005–2008 рр. було виділено 3 млрд доларів США.

Європейські країни також своєчасно зрозуміли стратегічну важливість розвитку нанотехнологій. У 6-й Рамковій програмі Євросоюзу (2002–2006 рр.) дослідження і розробки в галузі нанотехнологій були оголошені пріоритетними і на їх фінансування протягом п'яти років витрачено 1,3 млрд євро. У 7-й Рамковій програмі (2007–2013 рр.) на цей напрямок передбачено 3,5 млрд євро.

У 2007 р. в РФ утворено урядову Раду з нанотехнологій з метою ефективної реалізації державної політки РФ у галузі нанотехнологій і наноіндустрії. На Раду покладено також формування ринку нанопродукції і нанопослуг, координацію вкладання бюджетних і приватних коштів у конкретні проекти. На розвиток наноіндустрії в РФ до 2015 р. планується виділити 200 млрд руб., з них 130 млрд руб. увійде до траншу цього року.

З метою сприяння реалізації державної політики у цій сфері в РФ створено корпорацію «Роснанотехнологія», яка у 2007 р. отримала з федерального бюджету близько 1 млрд доларів США.

У НАН України протягом багатьох років виконуються фундаментальні і прикладні дослідження, що мають безпосереднє відношення до нинішніх розробок у галузі нанотехнологій. З метою координації і цілеспрямованої підтримки цих робіт Президія НАН України в 2003 р. започаткувала Комплексну програму фундаментальних досліджень «Наноструктурні системи, наноматеріали, нанотехнології».

За час виконання Програми (2003–2006 рр.) при сумарному фінансуванні близько 33 млн грн, яке слід визнати досить обмеженим, враховуючи складність і масштаб вирішуваних завдань, вдалося створити: оригінальні наноструктурні композити для нових технологій зварювання перспективних конструкційних металевих матеріалів, непіддатливих зварюванню в звичайних умовах; зразки жаростійкого нанодисперсного алюмокомпозиту — перспективного матеріалу для авіаційної і космічної техніки; технології отримання покрить у наноструктурному стані, які значно підвищують стійкість і міцність лопаток газових турбін і конструкційних матеріалів; серію магнітом'яких нанокристалічних сплавів і на їх основі — зразки сердечників для високоекономічних трансформаторів різного призначення; методи отримання металевих та металоксидних наноплівок для створення датчиків магнітного поля і захисних фільтрів у систе-

мах мобільного зв'язку; зразки композитів з вуглецевими нанотрубами і наночастинами, що ефективно поглинають випромінювання радіо- та НВЧ-діапазону; зразки матеріалів з квантовими точками германію на кремнії для створення неохолоджуваних приладів нічного бачення; зразки нанокомпозитів на основі оксидів титану, що мають зворотний фотохромний ефект, для пристроїв оптичного запису інформації; технологію отримання і спікання нанопорошків титанату барію для багатошарових конденсаторів на основі керамік; тверді, радіаційно стійкі, електропровідні мастила для космічного і наземного використання на основі інтеркальованих наносистем; нанокомпозити для світловипромінюючих діодів, матеріали для літієвих акумуляторів високої ємності, систем запису інформації та перетворення сонячної енергії в інші види енергії; наноструктуровані каталізатори для спалювання метану в процесах газового очищення, а також знешкодження промислових та автотранспортних викидів; наноструктуровані біосумісні з кістковою тканиною людини керамічні композити на основі гідроксоапатиту кальцію та біоактивних фаз; дослідні зразки магнітокерованих наноносіїв лікарських препаратів у медицині; низькотемпературний і екологічно чистий метод нанесення на поверхню медичних імплантантів з титану і монокристалічного сапфіру біосумісних кальцієво-фосфатних покриттів; нові методи отримання наноматеріалів з високими міцнісними і корозійностійкими властивостями шляхом інтенсивної пластичної деформації для потреб машинобудування, електроніки та медицини; наноматеріали з високою стійкістю до абразивного зношення для інструментів прецизійного оброблення матеріалів.

Реалізація таких масштабних завдань в Україні можлива лише за умов суттєвого, не менше ніж десятикратного порівняно з сучасним, збільшення фінансування нанорозробок [249]. Значні фінансові ресурси необхідно передбачити для закупівлі відповідного сучасного обладнання.

Головною проблемою, яку необхідно розв'язати, є визнання стратегічного значення розроблення і впровадження нанотехнологій та наноматеріалів на державному рівні і подолання відставання України у здійсненні наукового та методичного забезпечення координації досліджень і розроблень, формуванні та розвитку технологічної бази,

задоволенні потреби у спеціально підготовлених кадрах з наданням для цього відповідної фінансової підтримки.

Хоча висловлюються різні погляди відносно того, що окрема програма стосовно нанотехнологій не потрібна, а достатньо окремих розділів, присвячених нанотехнологіям у загальній великій національній програмі під назвою «Національна технологічна база», але саме в програмі має бути позначена якась мета. Такою метою може стати створення в Україні промисловості нового типу — індустрії наносистем і матеріалів.

Формування пріоритетних напрямів і переліку критичних технологій доречно здійснити у два етапи: I етап — підготовка довгострокового прогнозу науково-технологічного розвитку; II етап — підготовка пропозицій щодо формування і корегування пріоритетних напрямів і переліку критичних технологій на основі експертизи відповідних пропозицій.

Корегування пріоритетних напрямів і переліку критичних технологій пропонується здійснювати не рідше ніж один раз на чотири роки.

Науковий рівень вітчизняних розроблень у галузі розробки нанотехнологій і виготовлення нових наноматеріалів в основному відповідає світовому. Однак на цей час спостерігаються недостатня координація робіт, пов'язаних із розробленням нанотехнологій, низька готовність промисловості до широкого впровадження дослідних зразків, істотне заниження потреб вітчизняного ринку в нанотехнологічній продукції у багатьох соціально значущих сферах (медицина, енергетика, екологія) порівняно з обсягами її реального виробництва.

Державна цільова науково-технічна програма «Нанотехнології та наноматеріали» розроблятиметься відповідно до нормативно-правової бази, яка регулює функціонування науково-технологічної та інноваційної сфер, зокрема законів України «Про наукову і науково-технічну діяльність» і «Про пріоритетні напрями інноваційної діяльності в Україні» [95].

Мета Програми — створення сучасної національної наноіндустрії.

Основними завданнями Програми є: 1) формування інфраструктури для проведення ефективних фундаментальних досліджень у галузі нанотехнологій; 2) координація робіт із розроблення та застосування нанотехнологій та наноматеріалів; 3) розроблення нових

підходів до підготовки кваліфікованих фахівців з питань розв'язання наукових, технологічних і виробничих проблем розвитку нанотехнологій і виготовлення нових наноматеріалів шляхом лібералізації податкової політики, оптимізації фінансової політики і системи захисту прав інтелектуальної власності.

Можливі такі варіанти розв'язання проблеми: 1) створення умов для залучення зовнішнього інвестора і позабюджетних коштів для розвитку наноіндустрії. У такому разі інвестиційна активність приватного капіталу буде спрямована в основному на досягнення її найвищої рентабельності та забезпеченості її гарантованими ринками збуту. Однак інтереси інвесторів можуть не збігатися з державними інтересами, внаслідок чого роботи за напрямами, в яких Україна має істотний доробок або які необхідні для сталого розвитку економіки країни, залишаться без інвестиційної підтримки і практично не розвиватимуться; 2) залучення державних кредитів на закупівлю необхідного обладнання для виготовлення нових наноматеріалів. Однак без державної цільової програми цей традиційний шлях технічного переоснащення підприємств не дасть економічного ефекту, оскільки у ньому відсутній системний підхід; 3) створення системи державного фінансування науково-дослідницьких і дослідно-конструкторських робіт у рамках державної цільової програми та залучення позабюджетних коштів для реконструкції існуючих та створення нових промислових потужностей.

Аналіз цих варіантів свідчить про те, що найбільш ефективним є третій варіант.

Для цього необхідно: 1) визначити пріоритетні напрями розроблення нанотехнологій з урахуванням перспектив їх подальшої комерціалізації, конкурентоспроможності та попиту, в першу чергу на внутрішньому ринку, найважливіші серед яких — наноелектроніка, наноінженерія, функціональні та конструкційні наноматеріали, нанобіотехнології і наноматеріали медичного призначення, колоїдні нанотехнології, нанотехнології щодо каталізу та інших хімічних галузей, наноматеріали і нанотехнології для захисту довкілля, нанотехнології для енергетики, нанотехнології спеціального призначення; 2) забезпечити вітчизняних дослідників сучасним обладнанням, необхідним для виготовлення нових наноматеріалів і дослідження їх

властивостей; 3) створити спеціальну систему підготовки дослідників, матеріалознавців і технологів, які володіють міждисциплінарними фундаментальними знаннями і вмінням працювати на сучасному спеціальному обладнанні; 4) забезпечити стандартизацію та сертифікацію наноматеріалів; 5) розробити систему заходів для залучення бізнесових кіл до розвитку наноіндустрії, зокрема шляхом запровадження безмитного імпорту (експорту) нанотехнологічного обладнання, введення пільг для споживачів і виробників нових наноматеріалів.

Сьогодні в Україні в число першочергових завдань необхідно включити: а) проведення аналізу тенденцій світового науково-технічного і технологічного розвитку та оцінки конкурентоспроможності України на світовому ринку; б) виявлення першочергових потреб країни в наукових і технічних досягненнях, виходячи зі стратегічних цілей соціально-економічного і оборонного будівництва, наявності природних, фінансових, матеріальних і кадрових ресурсів, а також науково-технічного і технологічного потенціалу; в) проведення аналізу наукових досліджень, що відбивають публікаційну діяльність, коефіцієнт цитованості українських учених, а також аналізу патентних документів; г) визначення основних секторів економіки, в яких Україні необхідно забезпечити світове лідерство, а також технологій, що забезпечують рішення завдань національної обороноздатності і безпеки; ґ) проведення аналізу соціальних, технологічних, економічних, екологічних і політичних аспектів розвитку національної інноваційної системи; д) використання в разі потреби інших методів оцінювання тенденцій науково-технічного і технологічного розвитку України та зарубіжних країн.

Для цього у рамках Національної програми впровадження моделі розвитку і комерціалізації нанотехнологій мусить бути доручено недержавній структурі [4]. Фінансування Програми планується здійснювати за рахунок коштів державного бюджету та інших джерел. Інвестиційні кошти спрямовуватимуться насамперед на закупівлю сучасного імпортного обладнання, організацію та налагодження виробництва нанопродукції [95].

Отже, нанотехнології є не менш важливим для держави напрямом з погляду економічної, соціальної та військової безпеки. Така програма не може бути прирівняна до програми щодо розвитку, напри-

клад, металургії, нафти або газу. У цьому зв'язку необхідно вжити заходів, які б не тільки стосувалися формування державної програми, а й передбачали відповідні політичні кроки. Перераховані заходи могли б стати поворотним моментом у розвитку країни, початком загальнонаціонального технологічного прориву.

Нарешті, є сенс зауважити: останнім часом висловлюються певні спрощення, що призвело до впровадження у літературний обіг окремих хибних тез, спростування яких потребує додаткової аргументації.

Зауваження перше. Інновація розглядається як системне перетворення технологічної модернізації, яке за своїм змістом залишається глибоко соціокультурним явищем. На перший погляд, ця теза не може викликати особливих заперечень. Однак разом із тим як основний двигун інновацій формується оптимальна комбінація інвестицій великих наукомістких корпорацій, середнього бізнесу переважно малих компаній плюс елемент державної політики. При цьому останній передбачає докорінні зміни механізму правової регуляції, оскільки неузгодженість більшості норм інформаційного законодавства у нинішньому вигляді гальмує впровадження інновацій.

Зауваження друге. За своєю новизною багато інститутів інформаційного права ще не укорінилися і процес їх становлення триває. Але існуючий різнобій в юридичній термінології стосовно визначення високотехнологічних інновацій не може бути виправданий, оскільки подібний стан вже провокує різні підходи судів у вирішенні типових категорій справ. Ось чому особливе місце в інформаційному законодавстві має бути відведено гарантіям інноваційної політики у сфері високих технологій. Такі гарантії можуть мати декілька рівнів: перший — стабільність інформаційного законодавства; другий — стабільний правовий режим інновацій у сфері високих технологій; третій — стабільний правовий стан інвесторів та учасників інноваційної діяльності; четвертий — можливість ефективного юридичного захисту порушених прав.

Зауваження третє. Нанотехнології — виключно науково-технологічна сфера, для розвитку якої правова регуляція є факультативною ознакою, а тому правовий механізм нанотехнології не потребує додаткової уніфікації. Тобто, домінанта ефективного вирішення цього питання — це наука і техніка.

Вважаємо, що з цією спрощеною тезою неможливо погодитись у повному обсязі, адже загальні норми права регулюють центральні для певної галузі законодавства суспільні відносини і визначають їх належність. Утім, нанотехнологія як процес становить особливий інформаційний феномен, завдяки чому вимагає наявності спеціального механізму правового регулювання.

Нарешті, стає зрозумілим, що саме за допомогою спеціальних норм інформаційного права повинні вирішуватися конкретні стратегічні і особливо тактичні завдання розвитку нанотехнологій.

Таким чином, сукупність викладених аргументів додатково зумовлює потребу в кодифікації законодавства у сфері високих технологій, а звідси вимагає структурного перероблення існуючих проектів Інформаційного кодексу України, про що вже частково йшлося у підрозділі 1.2.

З цього є підстави підсумувати, що нанонаука, нанотехнології та наноіндустрія потребують ґрунтовного дослідження як об'єкти нової підгалузі інформаційного права, яка останнім часом стрімко формується, — права високих технологій, що можна визначити так:

$$Ol = \frac{Ns + Nt + Ni}{W} \xleftrightarrow{3} \{I\}, \tag{5.2}$$

де *Ol* — об'єкти правового регулювання; *Ns* — нанонаука; *Nt* — нанотехнології; *Ni* — наноіндустрія; *W* — право високих технологій; *I* — інформаційне право.

Отже, вважаємо доведеним висловлене припущення, згідно з яким нанотехнології є правовим феноменом особливої природи, що формується в інформаційному праві. Відповідно до цього правові норми, що регулюватимуть суспільні відносини у сфері нанотехнологій, пропонується викласти окремим підрозділом у відповідному розділі спеціальної частини проекту Інформаційного кодексу України.

Треба наголосити на тому, що у найближчі десять років саме розвиток наноіндустрії, а саме — синтез та використання нових наноматеріалів стане одним із основних стимуляторів інноваційних заходів у провідних галузях економіки, в тому числі в судово-експертній практиці, до розгляду чого ми ще повернемося. Отже, соціотехнічна революція в інформаційній сфері має стати можливою завдяки нанотехнологіям.

І останнє: стратегія розвитку нанотехнології передбачає внесення відповідних системних змін не тільки до інформаційного, а й до кримінального, адміністративного, цивільного, податкового, митного законодавства тощо. Тому з метою реалізації викладених вище принципів необхідно найближчим часом підготувати проект Закону України «Про нанотехнології».

5.2. Нанонаукові засади експертних досліджень об'єктів надмалих розмірів

Нанонаука

Нанотехнологія є символом науково-технічного прогресу XXI ст., оскільки сьогодні вона визначає майбутнє науки і всього нашого життя, про що слушно наголошується в останніх науково-практичних розробках [1; 16; 33; 37; 99; 151; 156; 229].

З одного боку, нанотехнологія одночасно є наукою і технологією виробництва, орієнтована на одержання унікального обладнання і речовин із заздалегідь заданими структурою та властивостями. З другого боку, нанонауку слід розглядати як один із важливих аспектів цивілізаційного розвитку, що порушує широке коло інформаційно-правових проблем. Нанонаука включає найновіші досягнення фундаментальних досліджень з фізики, хімії, математики, матеріалознавства, біології, генетики, медицини. Нанонаука та нанотехнології вимагають думати, створювати, вимірювати, використовувати і проектувати в наномасштабі, який неможливо, навіть психологічно, уявити, тому процес дослідження у цій сфері є досить складним.

Нанотехнології вже уражають своїм потенціалом у сфері захисту інформації [161]. Враховуючи це, ми безумовно погоджуємося з твердженням, що ера нанотехнологій вже настала [176, с. 207].

Останнім часом не викликає сумнівів перспектива існування зв'язку нанонауки з фізикою високих енергій, що вивчає взаємодії елементарних часток та/або ядер атомів при енергіях зіткнення, істотно вище, ніж маси самих часток, що зіштовхуються. При цьому

експерименти проводяться за допомогою прискорювачів заряджених часток та ядерних реакторів. У цьому напрямі проводяться й інші дослідження [156].

Отже, нанонаука є не тільки кількісним, а й якісним стрибком від теоретичних досліджень речовини до маніпуляції окремими атомами.

Вважаємо за доцільне у цьому контексті сказати декілька слів про колайдери. Колайдер (від англ. *collide* — зіштовхуватися, стикатися) — це прискорювач заряджених часток на зустрічних пучках, призначений для розгону протонів і важких іонів та вивчення продуктів їх зіткнень, а після їх зіткнень — для спостереження утворення інших часток. За видами колайдери поділяються на кільцеві (Великий андронний колайдер (*Large Hadron Collider*) у науково-дослідному центрі Європейської ради ядерних досліджень — найбільша експериментальна установка у світі) та лінійні.

Сонячна енергія залишається ключовим напрямом використання досліджень у галузі нанотехнології, оскільки чиста, оновлювана енергія, що може обіцяти втілення подібних проектів, приваблива з економічного, політичного, інформаційного, екологічного та соціального аспектів. У цілому енергія розуміється як механічна робота, що є єдиним виявом потенційного оцінювання різних форм матерії та мірою переходу руху матерії з одних форм в інші. Як свідчать наслідки досліджень, світлом, яке локалізоване у нанорозмірному обсязі, можна управляти. Застосування лазерів у спектроскопії зумовило бурхливий розвиток її нового напряму — лазерної спектроскопії, що відкриває нові перспективи розвитку судово-експертних технологій.

Нанонаука пропонує різні можливості створення магнітних та оптичних запам'ятовуючих пристроїв. Зокрема, для запису інформації та її подальшої зміни можуть бути використані лазери з різним рівнем інтенсивності. Однією з переваг таких наноскопічних оптичних структур є те, що вони можуть існувати у трьох вимірах [176, с. 180]. Найбільш очевидною сферою застосування нанонауки до цього часу залишаються електронні технології.

Високотехнологічна інформатизація судово-експертної діяльності сприятиме підвищенню ефективності наукових досліджень у цій сфері, створенню потужної міжкорпоративної системи науково-технічної інформації та її використанню на всіх етапах наукової діяльності за

умови активізації всіх її форм. Це дозволить сформувати у майбутньому «об'єднаний», чи «колективний», експертний інтелект як високотехнологічний інформаційно-експертний центр найвищого рівня.

о ***Судова експертиза та високі експертні технології***

Судова експертиза — це дослідження експертом на основі спеціальних знань матеріальних об'єктів, явищ і процесів, що містять інформацію про обставини справи, яка знаходиться у провадженні органів дізнання, досудового та судового слідства [74].

Наукова і науково-технічна експертиза — це діяльність, метою якої є дослідження, перевірка, аналіз та оцінювання науково-технічного рівня об'єктів експертизи і підготовка обґрунтованих висновків для прийняття рішень щодо таких об'єктів [73].

Підприємства, установи, організації зобов'язані надавати безоплатно інформацію, необхідну для проведення судових експертиз, державним спеціалізованим установам, а також за згодою натурні зразки або каталоги своєї продукції, технічну документацію та іншу інформацію, необхідну для створення і оновлення методичної та нормативної бази судової експертизи.

Державні спеціалізовані установи, судові експерти та спеціалісти, що проводять судові експертизи, у разі отримання інформації, яка становить державну, комерційну чи іншу охоронювану законом таємницю, повинні забезпечити нерозголошення цих відомостей [74]. Остання норма узаконює обов'язковість надання інформації про об'єкт, що може бути корисним у разі необхідності обстеження такого об'єкта, який вже знаходиться у приватній власності, і перебуває під захистом відповідного законодавства. Державні спеціалізовані установи, що проводять судові експертизи, мають право одержувати від судів, органів дізнання та досудового слідства знаряддя злочину та інші речові докази, щодо яких закінчено провадження у справах, для використання в експертній і науковій діяльності [74]. Цим підкреслюється зміст ст. 20 Закону України «Про судову експертизу» щодо її інформаційного забезпечення.

Таким чином, судова експертиза — це процесуальна форма вивчення об'єктів різних видів з метою одержання доказової інформації методами наукового дослідження, яка інформаційно відображується у висновку експерта.

Судова експертологія як самостійне вчення методологічно та методично об'єднує усі види судових експертиз і не є предметом інших наук [91].

Традиційно судово-експертна методика є описом конкретних прийомів, способів, технік експертної діяльності в окремих видах судових експертиз. Утім, в теорію і практику судово-експертної діяльності у 80-х роках XX ст. було введено термін «експертні технології», проте до цього часу він уточнюється [242].

Фактично термін «експертні технології» можна вважати синонімом терміна «експертне дослідження», тобто сукупністю управлінських засобів і техніко-оформлюючих актів. Сьогодні в судово-експертній практиці поступово використовуються вже не тільки автоматизовані експертні системи, про що вже йшлося, а й системно запроваджуються сучасні високі технології [159]. У зв'язку з цим зміст поняття високих експертних технологій системно знаходиться вже на новому методологічному рівні.

Високі експертні технології, як і «звичайні» експертні технології, складаються з таких інформаційних складових: 1) знання методичних основ експертного дослідження; 2) знання структури експертного висновку; 3) знання критеріїв оцінки даних, отриманих у ході дослідження; 4) формування переконання експерта в обґрунтованості своїх висновків; 5) формування кінцевих висновків; 6) оформлення результатів експертизи [49, с. 164].

Однак суттєвою різницею є техніко-експертні засоби, які застосовуються експертами, що може бути представлено таким чином (схема 5.4).

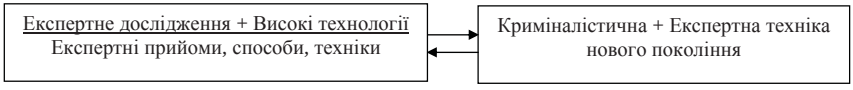


Схема 5.4

Отже, інформаційне забезпечення експертного процесу не можна вважати тотожним високотехнологічному забезпеченню, оскільки під останнім пропонується розуміти сукупність нових науково-методичних прийомів та інноваційних операцій для виконання експертного дослідження, які здійснюються експертом (експертами) за дорученням

слідчих і судових органів на основі спеціальних знань у технологічній послідовності з метою пошуку відповідей на поставлені інформаційні питання.

Слід зазначити, що високі експертні технології, зокрема нанотехнології, є ефективним способом організації проведення судової експертизи з використанням інноваційних методів та продуктів (схема 5.5).

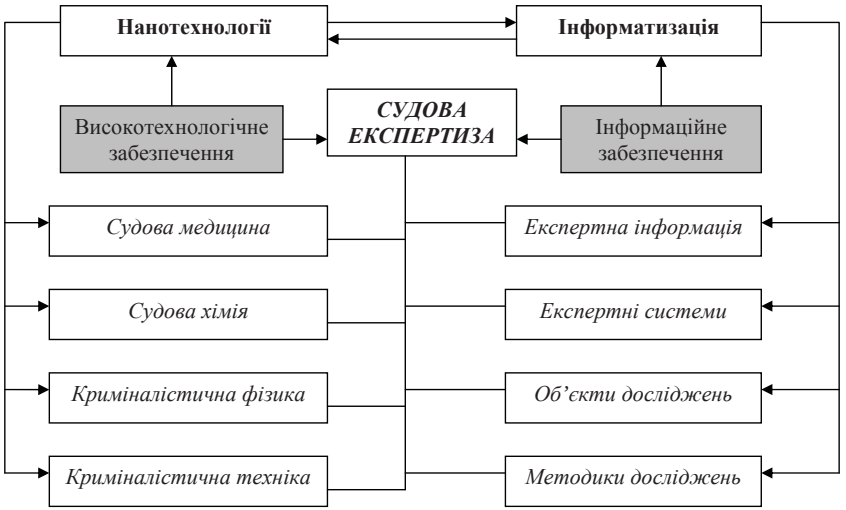


Схема 5.5

о ***Поняття і види об'єктів надмалих розмірів***

Під об'єктами надмалих розмірів у судовій експертизі слід розуміти об'єкти з мінімальною інформаційною складовою, до яких треба віднести два основні види: мікрооб'єкти та нанооб'єкти, що видно із формули

$$\frac{CE}{M} = \int o \xleftarrow{2} Mo \diagup No \,, \tag{5.3}$$

де *CE* — судова експертиза; *M* — експертні методи; *o* — об'єкти надмалих розмірів; *Mo* — мікрооб'єкти; *No* — нанооб'єкти.

Мікрооб'єкти і нанооб'єкти є сукупними термінами, що можна віднести до малих об'єктів, одні з яких вважаються безструктурними,

інші ж мають складну внутрішню структуру, однак розділити їх на складові частини ще неможливо. Нагадаємо, що мікро (грец. *маленький*) означає зменшення величини в мільйон раз, тобто наступним є вже нанорівень.

В експертній практиці по-різному вирішується питання про пошук і дослідження мікрооб'єктів, особливо тоді, коли немає інших джерел доказової інформації. Більшість науковців виділяють два варіанти вилучення мікрооб'єктів: разом з об'єктом-носієм (фрагментом об'єкта-носія); окремо від об'єкта-носія. Так, у практиці розслідування мікрооб'єкти найчастіше виявляються у волоссі, наружному слуховому проході, носовій порожнині.

Мікрооб'єкти та нанооб'єкти слід надсилати до експертного закладу щодо встановлення природи їх походження, а також перевірки за колекцією мікрооб'єктів, що вилучаються з місць нерозкритих злочинів, з метою встановлення фактів учинення декількох злочинів однією й тією самою особою (злочинцем). Ця колекція створюється у фізико-хімічних і біологічних лабораторіях Науково-дослідного експертно-криміналістичного центру (НДЕКЦ) при МВС. Мікрооб'єкти в таких колекціях систематизуються за видами злочинів, а також можуть поділятися за природою походження на текстильні волокна, лакофарбові покриття і под.

Отже, визначимо два напрями використання об'єктів надмалого розміру під час розслідування злочинів. По-перше, об'єкти надмалого розміру є засобом маркування продукції, різних предметів і злочинців. Тому потрібно заздалегідь визначити характеристики об'єктів надмалого розміру, умови і порядок їх використання. По-друге, встановлюється факт взаємного пересування (або перенесення в одному напрямку) об'єктів надмалого розміру при контактній взаємодії. У цьому разі мікрооб'єкти служать лише проміжною ланкою, а дослідження спрямовано на ідентифікацію їх слідоутворюючого об'єкта, встановлення тотожності з яким є важливим у процесі доказування кримінальної справи. Характеристики нанооб'єктів, умови і порядок їх використання значною мірою залежать від обставин події, що розслідується.

о ***Нанотехнології в судово-експертній практиці***

У судово-експертній практиці застосовуються два підходи до впровадження нанотехнології. Перший ґрунтується на послідовному

зменшенні розмірів об'єктів, оскільки синтез нанодисперсних речовин та матеріалів, процес регулювання хімічних перетворень тіл нанометрового розміру, запобігання хімічної деградації наноструктур становлять предмет нанохімії [33].

У судово-експертній практиці нанотехнології вже впроваджуються при дослідженні відбитків пальців. Для контрастування жирних слідів пальців використали суспензію золотих наночасток, що володіють гідрофобними властивостями, тобто здатністю прилипати до поверхонь, покритих жиром. Ці наночастки, прилипаючи до жирних борозенок відбитків пальців, формували значно більш чіткий рисунок, ніж той, який можна було б одержати за допомогою традиційної технології. При цьому час процедури не перевищував 3 мін. У цілому дотепер у криміналістиці нанотехнології обмежено застосовуються при дослідженні прихованих (латентних) відбитків пальців. Зокрема, металеві наночастки і наноструктуровані частки використовуються для проявлення відбитків.

Технічні засоби і прийоми та організаційні заходи профілактичного характеру розробляються експертами на основі власного досвіду і власних спеціальних знань з використанням при цьому даних інших наук. Утім, вивчення експертної практики свідчить про те, що нанотехнологічні експертні дослідження ще не отримали належного науково-практичного розвитку в Україні. Застосування нанотехнологій в судово-експертній практиці до цього часу ще неможливо через низку об'єктивних причин.

На наш погляд, перспективним є системне використання наукових методів нанотехнологій, що дозволить виконувати складні експертні дослідження мікрооб'єктів та мікрослідів уже на нанорівні. Звідси відкриваються інноваційні шляхи для розвитку нового класу експертних методик — експертизи нанооб'єктів і нанослідів. Це може стати новою ерою в розслідуванні практично всіх категорій злочинів, але для реалізації цієї програми організаційно-методичні та процесуально-правові аспекти потребують істотного нормативного вдосконалення на законодавчому та відомчих рівнях.

o ***Види наноматеріалів і криміналістична нанотехніка***

Завдяки стрімкій технізації наносвіту отримала розвиток нанотехніка як галузь техніки, в якій використовуються наноструктури, де на

молекулярному та кристаличному рівнях можливо принципово змінювати властивості речовини, одержуючи досконало новий клас матеріалів, тобто фактично нанотехніка вже стала прогресивною технологією сьогодення й майбутнього, основою чого є наноматеріали.

Поняття «нанотехника» було уведено в обіг в 1974 р. японцем Норіо Танігучі [254]. Зазначений термін є збірним, де в дослідний спосіб реалізовано високотехнологічні можливості нанонауки. Фактично цим терміном позначається будь-яка фізико-технічна продукція, виготовлена, як правило, малою серією, за допомогою нанотехнологій. Класичними прикладами цього можуть бути растровий тунельний мікроскоп (1982), атомний силовий мікроскоп (1986) та нанотрубки (1991). Безумовно, це визначення потребує уточнення, оскільки в ньому залишаються змістовні неясності.

Під терміном «наноматеріал» розуміється будь-який матеріал, що має наноскопічні розміри і вироблений для виконання певного завдання [176, с. 89].

Наноматеріали — це матеріали, які створені з використанням наночастинок або завдяки нанотехнологіям, мають унікальні характеристики і властивості, що випливає з мікроскопічних розмірів їх складових, обґрунтованих наявністю цих частинок у матеріалі. До наноматеріалів належать об'єкти, один з характерних розмірів яких знаходиться в інтервалі від 1 до 100 нм.

Наноматеріали, як правило, відрізняються від аналогічних матеріалів у масивному стані. Нанотехнології дають можливість здійснювати маніпуляції з речовиною на рівні одного нанометра, що фактично означає управління фізичними, хімічними і біологічними процесами на атомарному і молекулярному рівнях. Саме це дає змогу створювати принципово нові матеріали, криміналістичні технічні прилади та судово-медичні препарати, розробляти нові технологічні процеси з небаченими раніше можливостями.

Утім, застосування наноматеріалів у криміналістичній техніці дотепер не отримало широкого розвитку, оскільки докладне вивчення цього феномену тільки почалося і зараз йде накоплення знань про такі нові матіріали.

Разом із тим можна припустити, що інноваційний розвиток криміналістичної техніки у XXI ст. визначатимуть саме нанотехнології,

що призведе до істотних змін у цій галузі криміналістики і стане фундаментом окремого напряму — криміналістичної нанотехніки.

о ***Судова медицина і нанотехнології***

Судова медицина — особлива галузь медичної науки, що має бути умовно віднесена до групи так званих прикладних наук і досліджує питання медичного, біологічного, медико-криміналістичного характеру, які найчастіше виникають у кримінально-правовій та цивільно-правовій сферах суспільної практики і вирішити які можна виключно за допомогою спеціальних медичних знань.

Доцільність використання наноматеріалів, які виготовляються із застосуванням нанотехнологій, зумовлена тим, що у таких розмірах об'єктів речовина має властивості, не притаманні її макрокількості. Звідси зрозуміло, що нові напрями судових експертиз свідчать про постійний динамічний процес розвитку і вдосконалення судово-експертних технологій.

Моделювання і теорія є базисом розуміння та проектування наноструктур, а також у більш загальному випадку всього наукового всесвіту. Проектування на молекулярному рівні та молекулярна біологія надають множину нових інтелектуальних матеріалів. Так, моделювання показує, що нанотрубки — це найбільш міцний синтезований матеріал з усіх можливих.

Наночастинки застосовують для наукових розробок у галузі судової медицини, зокрема для створення біомаркерів. Магнітні наночастинки, на які нанесено антитіла та фрагменти ДНК, мають властивість посилювати сигнал біомолекул [33]. Це дозволить виконувати судово-медичні дослідження з на декілька порядків вищою точністю.

Термін «геном» означає сукупність генів організму людини, його повний хромосомний набір. Генетичний код містить інформацію про фізичний стан певної людини та її предків. Не існує окремого гена, що описує расу, але багато генів описують різні компоненти характеристик рас: колір і текстуру волосся, колір шкіри, форму очей і носа, схильності та імунітети до хвороб тощо. Прилад з генетичним наведенням може бути запрограмований на виконання тих чи інших руйнівних дій залежно від генетичної структури ДНК-клітини, в яку він потрапив. Можна запрограмувати як умову активації пристрою унікальну ділянку генетичного коду людини або шаблон для дій над групою людей.

При цьому відрізнити звичайну епідемію від бактеріологічної етнічної зброї буде важко навіть фахівцю, хоча б тому, що вчені держави-розробника такої зброї можуть свідомо дезінформувати громадськість. Безпосередні ж докази одержати навряд чи видається можливим.

Ця зброя може спрацьовувати не тільки проти наміченої групи людей, а й за чітко визначеними умовами, тобто йдеться про відкладене на невизначений строк захворювання. Потрапивши в організм жертви, бактерії спочатку аж ніяк не виявлятимуть себе. Але як тільки заражена людина, наприклад, занедужавши ангіною, прийме антибіотик, бактерії активуються і починають розмножуватися, викликаючи смертельне захворювання, що не піддається діагностиці. Летальна доза токсину ботулізму для людини становить близько 100 нанограмів. Комплект із десятка пристроїв, здатних здалека розпорошити смертельну дозу над великими містами-«мільйонниками», може вміститися в невеликому кейсі терориста. Медикам складно буде вжити заходів, оскільки спроби лікування лише прискорюватимуть розвиток захворювання.

о ***Судова хімія і нанохімія***

Судова, або, інакше, криміналістична, хімія — це частина прикладної (переважно аналітичної) хімії, яка за обсягом у широкому сенсі є практично неосяжною стосовно численності та розмаїтості завдань, що нею вирішуються, оскільки будь-яке хімічне дослідження може стати предметом судово-хімічної експертизи, якщо цього вимагають питання, які виникли у правовій (переважно правоохоронній) практиці і вирішити які можна виключно за допомогою спеціальних хімічних, токсикологічних або фармацевтичних знань. Таким чином, фактично криміналістична хімія досліджує якісний та кількісний хімічний аналіз об'єктів, що були надіслані на експертизу слідчими і судовими органами.

Зв'язок судової хімії з нанотехнологією очевидний. Сьогодні судова хімія з успіхом досліджує такі нові питання, що постають у правовій сфері, як техногенні системи та екологічний ризик, криміналістичний аналіз мікроволокон, проблеми хімічного матеріалознавства та деякі інші.

Нанохімія — це наука, яка вивчає синтез нанодисперсних речовин та матеріалів, регулювання хімічних перетворень об'єктів надмалих

розмірів (нм), запобігання хімічної деградації наноструктур, способи лікування хвороб з використанням нанокристалів [214].

Слід указати на такі напрями нанохімії, як синтез наноструктур у біологічних тканинах, розроблення методів складання великих молекул із атомів за допомогою наноманіпуляторів та запровадження нових нанокаталізаторів для судово-хімічної лабораторної практики, що відкриває додаткові перспективи розвитку методів судової хімії.

У сучасних умовах наявні переваги методів мікрокристалоскопії — висока чутливість, специфічність, наочність реакцій. Це отримало визнання серед провідних експертів-хіміків. Специфічність мікрокристалічних реакцій під час проведення судово-хімічних досліджень значно підвищується при сполученні зовнішнього виду нанокристалів з їх оптичними властивостями.

Електрохімія широко застосовується не тільки у виробництві наноструктур, а й для їх аналізу, що має виняткове значення для судово-експертної практики. Детектування ДНК є потенційно великою сферою, де нанонаука може детермінувати модернізацію окремих методів судової медицини. Зокрема, практично неможливо помилитися з ідентифікацією ДНК-відбитком пальця хвороби. Імовірність помилки становить усього одну мільярдну. До того ж, наноскопічні фотосенсори зможуть розширити основи науки судової фотографії.

Різноманітні периферійні пристрої дозволяють використовувати мас-спектрометри *DELTA V Plus і DELTA V Advantage* для експертних досліджень і аналізу інтегрального та компонентного ізотопного складу в будь-яких середовищах для практичного застосування в криміналістиці, зокрема з метою виявлення фальсифікації продукції, а також біохімічних досліджень. Так, «електронний ніс» вже може забезпечити нові можливості в боротьбі з контрабандним увезенням і поширенням наркотиків, попередити терористичні диверсії. Відчуваючи запах метану, можна швидко виявити й усунути витік із газопроводів. Нанотехнологія сприяє створенню потужних вибухових, запалювальних й отруйних речовин. Нанопокриття — це покриття товщиною від 1 до 100 нм, які використовуються в лазерній техніці завдяки здатності якісного відображення.

Однією з важливих проблем, що постає перед нанохімією, є проблема пошуку можливостей змусити молекули групуватися пев-

ним порядком, щоб у підсумку одержати нові матеріали або пристрої. Цією проблемою і займається нанохімія, яка вивчає не стільки окремі молекули, скільки процеси взаємодії між молекулами, які здатні впорядкувати молекули в певний спосіб, створюючи нові речовини і матеріали.

Загальновідомий факт, що дрібні частинки хімічно активніші через більше співвідношення площі поверхні до обсягу. Дослідження підтверджують, що навіть нешкідливі речовини у вигляді наночастинок стають смертельною отрутою. Тому наночастинки можуть бути використані як потужний каталізатор для широкого діапазону хімічних реакцій — основи надпотужних вибухових запалювальних речовин.

Звідси перспективним напрямом є розроблення низки нових нанокаталізаторів для хімічної промисловості та лабораторної практики, що може бути з успіхом використано в експертно-криміналістичній діяльності.

o ***Судова (криміналістична) фізика і нанотехнології***

Останніми роками завдяки інтенсивному освоєнню та впровадженню досягнень фізики відбувається значна модернізація криміналістичної техніки, що додатково аргументує доцільність формування судової або криміналістичної фізики як окремої підгалузі судової експертизи.

За великим рахунком фізико-технічна експертиза не є попередницею медико-криміналістичної експертизи, а тому не буде зовсім вірним ототожнювати її з останньою. За допомогою фізико-технічної експертизи вивчається структурний склад матеріалів, адже від структури матеріалів залежать їх майбутні властивості. Структура матеріалів може бути або однорідною, або неоднорідною, причому визначити, яка з них є більш довговічною, можливо лише під час розгляду кожного окремого випадку.

У криміналістиці методологічно важливо при враховуванні фізичних властивостей об'єктів у нерозривному зв'язку розрізняти їх зовнішню і внутрішню побудову.

Основними методами криміналістичної фізики є атомно-емісійна спектрометрія, атомно-абсорбційна спектрометрія, рентгеноспектральний аналіз, молекулярний спектральний аналіз, методи виявлення мікродефектів. Наприклад, рентгеноструктурний аналіз є типовим

методом фізики, тому його розвиток і вдосконалення неможливі поза фізикою. Використання цього методу для дослідження речових доказів вимагає розроблення певних специфічних прийомів, тобто фактично особливого підходу, відносно як техніки, так і оцінювання результатів, що не пов'язані із загальною фізикою. Тим не менш метод залишається фізичним, оскільки він пов'язаний насамперед з фізикою і тому належить до судово-фізичної експертизи. Таким чином, судовий фізик насамперед має спиратися на дані фізики, що створює науковий фундамент відповідного виду судово-фізичної експертизи [253].

Для того щоб розглянути і дослідити мікрочастинки, необхідно вдаватися на допомогу різних фізичних приладів та технологічних інструментів. Одним з перших таких інструментів судової фізики позначився мікроскоп. За досить тривалу історію свого застосування оптична мікроскопія стала універсальним і дуже ефективним методом одержання судових доказів.

Одним із ключових елементів нанотехнології є молекулярне розпізнавання, що фактично виконує роботу «зору» [176, с. 49–50].

Комбінації молекулярного розпізнавання та збирання зможе дати нові експертні матеріали, побудова чого можлива виключно в наносвіті.

Ґрунтуючись на цьому, мікроскопи, що сканують, дозволяють побачити об'єкти атомного розміру. Першими нанорозмірними структурами, побудованими на молекулярному рівні, були вуглецеві трубки, які демонструють дійсно унікальні властивості [176, с. 79]. Нанотрубки зможуть вивести експертні технології на новий рівень, але до цього часу їх виробництво ще не набуло статусу промислової інновації у сфері судової експертизи, хоча яскраво демонструє експертний потенціал і величезні можливості нанотрубок. Наприклад, такі надміцні наноматеріали, як нанотрубки, неможливо знайти на об'єкті, використовуючи металопошукачі або хімічні «носи». Єдиний можливий шлях виявлення особи, яка проносить подібну зброю до літака чи в будинок, — ретельний обшук.

Упровадження волоконно-оптичного пристрою для одержання контактного зображення відбитку пальця дає змогу задовольнити будь-який експертно-криміналістичний стандарт якості.

Сьогодні саме фізико-технічна експертиза зможе досліджувати параметри наноматеріалів та інших нанооб'єктів. Вона покликана допомогти у вивченні фізичних властивостей матеріалів, завдяки чому стає можливим визначити їх майбутні механічні параметри.

До того ж, слід зазначити, що цікавими для криміналістичної фізики можуть стати розробки у галузі нанооптики як розділі оптики та нанотехнології, де використовується світло, локалізоване в просторі значно меншому довжини хвилі (λ) або обсязі, набагато меншому за λ^3. Практичний розвиток цієї галузі ґрунтується на створенні лазерів на наноструктурах (кластери, плівки, трубки). Нанофотоніка є розділом нанооптики, в якому досліджуються нановипромінювання з малою кількістю фотонів та вивчається поведінка світла в наномасштабах. Використання структури нанометрових розмірів надало можливість створити мікроскоп, за допомогою якого подолано дифракційну межу в оптиці, яка завдяки розвитку цієї технології може досягти 1 нм.

Усі ці галузі активно розвиваються з упровадженням нанонауки у сферу електроніки, оптики та магнітних матеріалів. Зважаючи на класифікацію видів високих технологій, про що вже йшлося, це, мабуть, і є «найвищими технологіями» нанонауки, оскільки вони становлять оптимальну взаємодію нанотехнології з високою інформаційною технологією [176, с. 180].

Класичний приклад, що додатково підтверджує, зокрема, перспективи використання нанотехнологій у криміналістичній фізиці, — це послідовне зменшення довжини хвилі випромінювання при фотолітографії (від видимого світла до рентгенівського).

Другий підхід полягає у відтворенні об'єкта з мікроелементів (атомів, молекул, структурних фрагментів біологічних клітин і под.). Сьогодні продуктивність цього підходу невисока, однак, за прогнозами аналітиків, саме їм належить майбутнє в нанотехнології, оскільки методи першого підходу обмежуються фізичними межами самої природи цих методів [42, с. 8–16].

У теперішній час інтенсивно розвиваються напрями нанофотоніки, до якої можна віднести в першу чергу нанохвилеводи, нанолазери, оптичне маніпулювання мікро- і наночастинками [99, с. 119–135].

Фактично нанотехнологія має ознаки універсальності, оскільки системно може поліпшити багато з судово-експертних технологій.

Тому відкриття, зазначені вище, можуть мати революційні наслідки для формування нових судово-експертних методів, фактичного втілення нанометодик у практику експертних досліджень об'єктів надмалих розмірів.

Нарешті, слід резюмувати, що організаційно-правовий механізм регулювання судово-експертних стандартів нанотехнологій ще є недосконалим. До цього потрібно додати необхідність правового з'ясування ефективності експертних стандартів. У зв'язку із цим існують підстави стверджувати, що теоретичне розроблення системи оцінок ефективності використання нанотехнологій у судово-експертній практиці є важливим напрямом політики розвитку високих технологій у сфері боротьби зі злочинністю [193].

5.3. Проблеми інтелектуалізації інформаційної та міжнародної злочинності і перспективи інноваційних розробок антикримінальних наносистем

о ***Інформаційна злочинність***

Стійке функціонування інформаційної інфраструктури, забезпечення інтересів особи, суспільства і держави у цій сфері перетворюються на важливий чинник збалансованого розвитку будь-якої країни.

Інформаційні ресурси та інформаційна інфраструктура відіграють дедалі більшу роль у міждержавній боротьбі за світове лідерство і досягнення політичних, економічних, воєнних переваг. З приводу оцінок та реагування на нову кримінальну ситуацію проводяться наукові дослідження та з'являються певні практичні розробки [36; 57; 93; 119; 135; 137; 139; 243].

Термін «інформаційна злочинність» ще не є загальноприйнятим [40]. Одні автори віддають перевагу терміну «злочинність у сфері інформаційних відносин» [58]. Інші ж пропонують увести термін «інформаційна злочинність» у науковий обіг, визначаючи її як різновид злочинності, що виявляє себе в інформаційній сфері, де інфор-

маційний зв'язок виступає стосовно злочинності її істотною детерміністською ознакою [40, с. 93–96].

Пропонуємо визначати *інформаційну злочинність* як протиправні дії в інформаційній сфері, що порушують установлені законом права особи, організації або держави, чим заподіюють останнім моральну шкоду або матеріальний збиток. Істотною ознакою є те, що *інформаційна злочинність* має організований і міжнародний (транснаціональний) характер, базується на стрімкому розвитку і використанні телекомунікаційних засобів повідомлень.

Має здійснитися якісний перехід від нині існуючої системи протидії інформаційній злочинності до нової, більш сучасної, що потребує переосмислення накопиченого досвіду для визначення концепції, загального підходу до цієї проблеми як правоохоронних структур, так і суб'єктів ринку інформаційно-телекомунікаційних технологій. Інформаційна епоха розширила сферу діяльності тероризму, що призвело до появи «інформаційного тероризму», який визначається як злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій [36, с. 162].

Особливу небезпечність сучасності становить відносно новий вид терористичної діяльності — інформаційний тероризм, розгортання якого зумовлено широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства, що вимагає розроблення комплексної системи протидії «інформаційному тероризму» правовими та організаційно-технічними заходами з боку правоохоронних органів з відповідними науковими нововведеннями.

Основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передавання даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупованнями або окремими особами. Наслідки такої атаки — проникнення до інформаційно-телекомунікаційної системи, перехоплення управління, пригнічення засобів мережевого інформаційного обміну та вчинення інших деструктивних дій.

o ***Міжнародна злочинність***

Міжнародну злочинність як особливий вид злочинності називають по-різному, найчастіше злочинністю міжнародного характеру або транснаціональною злочинністю [37], однак від цього її зміст не змінюється, оскільки міжнародна злочинність являє собою сукупність усіх злочинних діянь, учинених у певний період на території більш ніж однієї держави.

У теорії склався загальновизнаний поділ злочинів, що зачіпають інтереси держав і всього міжнародного співтовариства, на декілька груп. У цьому зв'язку сучасні дослідники пропонують різні класифікації міжнародних злочинів, що ґрунтуються на критеріях, які характеризують джерело криміналізації правопорушення і юрисдикцію, під яку воно підпадає [36].

Боротьбою з міжнародною злочинністю (англ. *struggle against international criminality*) визнається будь-яка діяльність репресивного або превентивного характеру, заснована на праві і здійснювана правоохоронними органами, що зачіпає правові інтереси щонайменше двох суверенних держав.

Оскільки дотепер власне не існує ні міжнародного кримінального права, ні наднаціонального виконавчого органу, який був би наділений відповідною компетенцією вести боротьбу з міжнародною злочинністю, залишається виходити з існування «міжнародного» випадку тоді, коли порушені дві суверенні системи права.

o ***Інтелектуалізація злочинності***

У першому десятиріччі XXI ст. перед суспільством виникли нові виклики у вигляді не тільки суттєвого зростання злочинності, а й появи таких нових ознак, як структуризація, спеціалізація, професіоналізація та інтелектуалізація злочинності, тобто, інформаційна злочинність як соціально-правовий феномен залучила собі на службу досягнення у сфері високих технологій.

Обережно висловлюючись щодо прогнозів розвитку злочинності в Україні найближчими роками, слід визнати основні тенденції як вкрай несприятливі. Головним є те, що характерною прикметою сьогодення стала *інтелектуалізація злочинності* [216]. У цілому інтелектуалізація злочинності як відносно новий соціально-правовий

феномен постає складною і багатогранною проблемою, що умовно можна відобразити таким чином:

$$\frac{[M+I]\,c}{I \underset{2}{\longleftrightarrow} HTc} \Uparrow Nc, \tag{5.4}$$

де *M* — міжнародна злочинність; *I* — інформаційна злочинність; *I*2 — інтелектуалізація злочинності; *HTc* — злочинність у сфері високих технологій; *Nc* — нанозлочинність.

Більш того, в Україні слід очікувати і потрібно завчасно готуватися до зростання масштабів політичної злочинності, що не виключає її детермінування до тероризму. У цьому зв'язку існує небезпека доступу кримінальних угруповань і терористичних організацій до зброї масового знищення. Звідси слід очікувати нових видів злочинів у сфері інформаційних технологій, також передбачати збільшення обсягів залучення до злочинної діяльності наукових співробітників, колишніх офіцерів збройних сил і правоохоронних органів, кваліфікованих юристів, тобто, зросте інтелектуалізація злочинності внаслідок її озброєння останніми досягненнями високих технологій, у тому числі військових нанотехнологій [32].

о ***Інфотероризм***

Злочинність терористичної спрямованості можна визначити як сукупність злочинів терористичної спрямованості, або тероризм у широкому сенсі слова [105, с. 640]. У рамках предмета нашого дослідження поняття «терор» розглядається як метод політичної боротьби і протиставляється всім неекстремістським та іншим насильницьким методам зовнішньополітичної боротьби [135]. При цьому помітимо, що нерідко такі поняття, як «тероризм», «терор», «терористична діяльність» і «терористичний акт», ототожнюються. У статті 258 КК України передбачено кримінальну відповідальність за терористичний акт, тобто застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого само-

врядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з подібною метою [104].

Під тероризмом також розуміють залякування населення органів влади з метою досягнення злочинних намірів. Він полягає у погрозі насильством, підтриманні стану постійного страху з метою досягнути певних політичних чи інших цілей, спонукати до певних дій, привернути увагу до особи терориста або організацій, які він представляє. Реальність загрози визначається з урахуванням місця та часу терористичного акту, наявності людей чи матеріальних цінностей, використовуваних знарядь та засобів, їх вражаючих властивостей і потужності тощо. Заподіяння чи загроза заподіяння шкоди є своєрідним попередженням про можливість спричинення більш тяжких наслідків, якщо вимоги терористів не буде сприйнято. Характерною ознакою тероризму є його відкритість, коли про мету заподіяння шкоди чи погрози широко розголошується.

Сучасні високоінтелектуальні інформаційні мережі є середовищем для вчинення терористичних планів, розгортання кібертероризму взагалі, що становить реальну загрозу не тільки національній безпеці окремих країн, а й всієї світової спільноти. Новітні інформаційні технології стають інструментом міжнародного тероризму [141].

Розростання «інформаційного тероризму» вимагає запровадження правових основ для створення захищених від нелегального проникнення механізмів інформаційного обміну та загальних стандартів зберігання, аналізу та обміну інформацією у складі національних та міжнародних інформаційних ресурсів [36, с. 162–166].

Кібертероризм орієнтується на використання різних форм і методів виведення з ладу інформаційної інфраструктури держави або на використання інформаційної інфраструктури для створення обставин, які призводять до катастрофічних наслідків у суспільстві.

На жаль, правоохоронні органи не завжди були здатні надати адекватну відповідь розростанню «інформаційного тероризму», хоча спостерігалося намагання адаптуватися до складної ситуації, змінити форми антикримінального впливу відповідно до нових завдань і нових викликів.

Сучасний стан розвитку інформаційного суспільства та досить великий ревень потенційних загроз тероризму (зокрема, «інформаційного тероризму») визначає порядок забезпечення оперативного доступу до необхідних та актуальних даних у складі сучасних національних і міжнародних інформаційно-аналітичних систем з метою протидії терористичним проявам. Тому важливим завданням постає міжнародне співробітництво з використанням інформаційних технологій, оскільки розроблення заходів протидії злочинним проявам у глобальній мережі тільки на національному рівні залишається малоефективним. У зв'язку з цим необхідно розробити і прийняти такі норми, що будуть пристосовані до законодавств інших держав.

о ***Злочини у сфері нанотехнологій і нанозлочинність***

З одного боку, вже не викликає сумнівів, що нанотехнологічне суспільство є новим виміром соціальної реальності, де перед людиною відкриваються нові позитивні можливості, але, з другого — містить високий рівень загрози, що у майбутньому може створити певні проблемні ситуації, чого раніше не спостерігалося. Однією із таких проблем може стати протиправна діяльність у сфері високих технологій, у першу чергу з використанням нанопристроїв.

На жаль, певні кола, зацікавлені в підтримці міжнародного тероризму, теж використовують нові технологічні можливості для порушення міжнародної стабільності і створення нових загроз національній безпеці України та безпрецедентного силового тиску на неї.

Основні пріоритети провідних західних держав у галузі розвитку перспективних засобів ураження спрямовані на створення зброї з використанням електромагнітної енергії, роботизованої зброї, непомітних непілотованих бойових платформ, призначених для цілодобової розвідки і таємного застосування різних видів високоточної зброї.

Водночас здійснюються заходи щодо подальшого підвищення можливостей невеликих підрозділів стосовно ведення інформаційних, спеціальних і повітряно-морських десантних операцій у віддалених регіонах світу, а також операцій в умовах великих міст. Має велике значення розроблення нових препаратів, заснованих на досягненнях нанобіотехнології, що дозволять бойовикам не утрачати боєздатність.

Нові мініатюрні пристрої спостереження можуть бути легко вмонтовані в деталі обладнання, які Україна купує з-за кордону через неконтрольовані канали [29, с. 50–51]. Будь-яка система може містити ворожу підсистему, здатну перехоплювати, спотворювати, знищувати інформацію як в автономному режимі, так і за командою супротивника.

Подальший розвиток нанотехнологій дозволить з незначними витратами вбудовувати закладки в з'єднувальні проводи, конденсатори, кріпильні деталі та інші елементи техніки. Зміниться і характер закладок — вони стануть більш автономними і функціональними, зможуть бути знаряддям широкого діапазону впливів на техніку і особовий склад, від указівки на ціль для крилатих ракет до викиду токсинів.

Упродовж наступних років буде винайдено багато малогабаритних пристроїв, здатних накопичувати і передавати інформацію. В Японії і США вже створено зразки «цифрового паперу» — тонких і гнучких, немов паперовий лист, плівкових масивів наноелектронних схем [220]. Нові технології тривимірного друку дають змогу наносити з порошків металу і пластика об'ємні структури за заданою програмою. Портативні прилади допомагають терористам друкувати будь-які документи в потрібній кількості.

Отже, цей перелік не є вичерпним, однак він додатково надає підстави для постановки проблеми правового забезпечення соціальних процесів, що відбуваються з використанням нанотехнологій. І у першу чергу це потребує певних змін у кримінально-правовому законодавстві.

Як уже зазначалося, до злочинів у сфері високих технологій більшість дослідників невиправдано обмежено відносять виключно «комп'ютерні злочини». Тому, повертаючись до обґрунтування висловленого раніше зауваження, зазначимо, що фактично під «справжніми» високотехнологічними злочинами слід розуміти сукупність інтелектуальних злочинів, які вчиняються з використанням нанотехнологій.

Звідси стає зрозумілим необхідність розроблення кримінально-правових новацій і внесення відповідних змін до КК України.

Нагадаємо, що злочинність є не тільки особливим соціально-правовим явищем, а й сукупністю злочинів. Фактично з часом можуть

з'явитися підстави щодо введення терміна «нанозлочинність». Тому для з'ясування цього спочатку пропонуємо запропонувати правове визначення цих злочинів.

Вважаємо, що злочини у сфері нанотехнологій слід розуміти у вузькому та широкому сенсах. Так, пропонуються такі дефініції.

1. Злочини у сфері нанотехнологій у широкому сенсі — це окремі види злочинів, що вчиняються з використанням нанотехнологічних засобів, методів та пристроїв.

2. Злочини у сфері нанотехнологій у вузькому сенсі — це протиправні дії, спрямовані на свідоме порушення наноструктури або структурну перебудову будь-яких матеріалів та інших об'єктів на нанорівні з метою подальшої протиправної діяльності, в тому числі вчинення, як мінімум, ще одного злочину, передбаченого КК України.

Нанозлочинність проходить декілька еволюційних етапів, які визначаються у позитивному сенсі розвитком науково-технічного прогресу, в негативному — появою нових інформаційно-технічних засобів здійснення протиправного впливу. Відповідно нанозлочинність також можна розглядати у двох значеннях: 1) як підвид інформаційної злочинності інтелектуального спрямування, об'єктом посягань якого виступають нанотехнології; 2) як підвид міжнародної злочинності терористичного спрямування, основні засоби протиправного впливу якої ґрунтуються на використанні нанотехнологій.

Отже, можна вивести поняття нанозлочинності як сукупності таких структурних компонентів: 1) окремі види злочинів, передбачених чинним КК України, що вчиняються з використанням нанотехнологічних засобів, методів та пристроїв; 2) діяльність, спрямована на свідоме порушення та перебудову молекулярної структури наноматеріалів та інших об'єктів з метою досягнення протиправних намірів; 3) інші види злочинів, у тому числі терористичної спрямованості.

Зрозуміло, що такі протиправні наміри, можливо, буде досить складно довести. Звідси ця системна проблема потребує додаткового розв'язання в організаційно-процесуальній та криміналістичній площині.

Отже, нанозлочинність як новий негативний соціотехнічно-правовий феномен несе надвисокий рівень суспільної загрози.

o ***Штучний інтелект і нанороботи***

Сьогодні на стиці нанотехнологій, біотехнологій та інформаційних технологій у синергетичній площині фактично виникає нова наука штучного інтелекту (англ. *artificial intelligence,* AI) , предметом якої стає розроблення інтелектуальних машин та інформаційних систем, особливо інтелектуальних комп'ютерних програм, спрямованих на те, щоб зрозуміти людський інтелект.

Під проблемою комп'ютерного інтелекту ми розуміємо підпроблему штучного інтелекту, необхідну для вирішення завдань з використанням нових інформаційних технологій.

Зазначена проблема стає предметом докладного наукового розгляду [131]. До того ж, інтегрування із робототехнікою можна вважати ще одним напрямом досліджень — створення інтелектуальних нанороботів.

Нанороботи — це автоматичні пристрої з антропоморфною дією, які частково або повністю замінюють людину при виконанні робіт, що відбуваються у небезпечних для життя умовах або при відносній неприступності об'єкта, розміри яких порівняні з молекулою (менш 10 нм), що можуть виконувати інформаційні програми, обробляти та передавати інформацію. Нанороботи фактично є нанорозмірними машинами, здатних рухатися під час енергетичного впливу. Навіть звичайних роботів, які можуть переміщатися з нанорозмірною точністю, можна вважати нанороботами. Крім слова «наноробот», також використовують такі назви, як «наніт», «наноген» і «наномураха». Вже існують нанороботи, які називаються реплікаторами, що можуть створювати свої копії, тобто здатними до самовідтворення.

Нанороботи можуть виявляти токсичні хімічні речовини у навколишньому середовищі і вимірювати рівень їх концентрації. Можливо військове застосування нанороботів як засобів спостереження і шпигунства, а також для використання нанороботів як зброї [146]. Оскільки наноробот може управлятися оператором або працювати за заздалегідь складеною програмою, неймовірно широким може бути використання «кримінальних нанороботів» у протиправних цілях, що не тільки потенційно несе в собі інформаційну загрозу найвищого рівня, але й взагалі може призвести до переформатування існуючих

знань про злочинність та способи боротьби з нею, що випливає із визначеної закономірності:

$$Nc = \sum \frac{1+2...A+B...}{Nr} \to \infty , \tag{5.5}$$

де *Nc* — нанозлочинність; 1+2... — окремі види нанозлочинів терористичної спрямованості; *A+B*... — інші види злочинів, учинених з використанням нанотехнологій, нанозасобів та наноприладів; *Nr* — нанороботи (кримінаніти).

Таким чином, існують усі підстави вважати штучний інтелект спеціалізованим напрямом наукових досліджень, пов'язаним зі створенням нейрокомп'ютерів, здатних навчатися, аналізувати та розуміти.

Використання можливостей нанотехнологій у найближчій перспективі сприятиме інформатизації за рахунок багаторазового збільшення обсягу пам'яті та продуктивності системи оброблення, зберігання і передавання інформації, а також створення нових високоефективних швидкісних пристроїв з наближенням можливостей обчислювальних систем до властивостей, притаманних об'єктам живої природи з елементами інтелекту.

Далі наведено виразні приклади нових загроз, інформація про які базується на офіційних джерелах, державних документах західних держав та публікаціях визнаних експертів [29; 32; 96; 135; 139; 220; 223 та ін.].

о ***Ядерний тероризм***

Місцезнаходження більшості боєприпасів відоме зацікавленим колам. Оскільки вбудовані захисні та сигнальні системи є перешкодою для наноприладів перших поколінь, терористи можуть зосередитися на атаках засобів доставлення і системи управління ядерною зброєю. Тому вірогідною може стати атака на ядерне озброєння з метою таємного знешкодження або навіть активізації його на території країни-власника.

Засоби доставлення — це підводні човни, авіація, підземне та наземне пускове обладнання. Їх можна швидко і раптово знешкодити, якщо не будуть розроблені і встановлені спеціальні засоби протидії нанозброї. Місцезнаходження та маршрути цих засобів доставлення, їх детальний технічний опис можуть передаватися терористам іно-

земними розвідками. Порушення роботи електронних мереж і механіки за допомогою малогабаритних роботизованих пристроїв — очевидний варіант такого впливу.

Дуже небезпечною вважається атака на заводи боєприпасів — вони захищені набагато гірше, ніж окремий боєзаряд, і як наслідок — можливі пошкодження унікальних заводських потужностей, а найгірше — це вибух і радіоактивне зараження величезних площ [32].

Атака на заводи з регенерації ядерного палива при дефіциті кваліфікованих фахівців-ядерників може позбавити країну фізичної можливості виробництва плутонію для зброї. Виробництво ядерного палива та видобуток сировини не є метою для атаки, тому що така війна закінчиться раніше, ніж будуть розроблені боєприпаси. Однак «господарі» терористів можуть мати свої плани щодо всієї території України або її окремих областей, і тому, можливо, намагатимуться уникнути її радіоактивного зараження. І вони мають цьому зручну альтернативу — безпосередню атаку на керівництво держави.

Якщо створення ядерної зброї вимагає складної і прихованої інфраструктури, то інфраструктура виробництва технологічної зброї є малопомітною для виявлення та ідеально підходить для тероризму.

о ***Психотероризм***

Ґрунтовні дослідження ведуться у галузі нейронних технологій і зчитування нервових імпульсів. Ми звикли вважати подібні речі фантастикою, але нещодавно у лабораторіях NASA створено дійові зразки устаткування для перехоплення внутрішньої природної мови, що виявляється у слабких нервових імпульсах, виникаючих у відділі мозку, який керує голосовими зв'язками. Подальший розвиток цих технологій призведе до появи бойових наноприладів, що здійснюють шпигунство або перехоплюють контроль над функціями організму людини, використовуючи підключення за допомогою розроблених у Каліфорнії «нейротранзисторів» до нервової системи людини [220, с. 23–29].

Ще один проект — мікрохвильове випромінювання, яке уражає людину, не даючи змоги для оборони. Active Denial System за принципом мікрохвильової печі змушує водяні молекули під шкірою активно рухатися, нагріваючи шкіру до 130 градусів за Цельсієм протягом 2 с, при цьому люди стають абсолютно безпорадними на великих територіях.

о ***Авіатероризм***

Систематичне і вибіркове ураження найважливіших об'єктів військового і економічного призначення, виведення з ладу систем забезпечення життєдіяльності населення на всій території країни з метою її капітуляції є звичайною практикою збройних конфліктів останніх років.

Гіперзвукові апарати, здатні маневрувати, зможуть доставити заряди вибухівки до складів боєприпасів і палива, до реакторів або будь-яких запасів енергії, здатних до швидкої детонації. Малогабаритні ракети з поліпшеними системами «Стелс» і пристроями електромагнітних перешкод спроможні розпорошити будь-що в атмосфері площею радіусом тисячі кілометрів на будь-якій відстані від місця запуску.

Програма «Advanced Standoff Cruise Missile» передбачає створення снарядів, що застосовуються у низці систем, від супутникових до лазерних, здатних до перепрограмування у польоті і забезпечених великою кількістю сенсорів для розвідки та наведення на ціль. Нанокомпозитні матеріали, компактна електроніка і нові види палива дозволяють звільнити значну частину обсягу носія для вибухівки.

Проте міжнародним авіатерористам не обов'язково мати власні бойові речовини. Існують великі склади зброї масового ураження, заводи з її перероблення, військові дослідницькі лабораторії. Спеціально запрограмовані або дистанційно керовані пристрої зможуть швидко і таємно доставити вибухівку для підриву сховищ агресивних речовин, а потім розповсюдити їх дію по численних населених пунктах і промислових об'єктах. Терористи зможуть за добу перетворити життєво важливий, наприклад, для України, агропромисловий комплекс на мертву пустелю.

Подібні напрями терористичних атак стають усе реальнішими у міру відставання України в розвитку нанотехнологій від тих, хто прагне використати досягнення науки на користь терору. Ефективна боротьба з терористами можлива тільки при високотехнологічному оснащенні армії і сил безпеки.

о ***Антитерористичні нанотехнології***

Активізація антитерористичної діяльності з використанням новітніх досягнень у галузі інформаційних технологій припускає налагодження міжнародних контактів. Як свідчить аналіз досвіду роботи

спеціальних підрозділів поліції зарубіжних країн, організаційно боротьба зі злочинами у сфері високих технологій забезпечується двома основними способами: покладенням додаткових функцій на вже існуючі підрозділи або створення спеціалізованих галузевих служб.

До основних функцій таких спеціальних підрозділів, що займаються виявленням і розслідуванням комп'ютерних злочинів, а також моніторингом інформаційних технологій, можна віднести: 1) моніторинг мережі Інтернет з метою виявлення кіберзлочинів, нових вірусів; 2) здійснення оперативно-розшукових та розвідувальних заходів з метою документування протиправної діяльності кіберзлочинців; 3) розслідування кіберзлочинів і надання методичної і практичної допомоги іншим галузевим службам та правоохоронним органам у межах своєї компетенції; 4) накопичення, узагальнення та аналіз інформації про кіберзлочинність.

Слід зауважити, що у більшості країн на базі підрозділів боротьби зі злочинами у сфері високих технологій або НЦБ Інтерполу створено контактні пункти з питань протидії інформаційній злочинності, які покликані забезпечувати оперативну взаємодію правоохоронних органів різних країн у розслідуванні відповідних злочинів. Характер сучасних терористичних погроз висуває підвищені вимоги щодо оперативності, злагодженості та уміння діяти на випередження. На розв'язання цієї проблеми спрямовано процеси структурного реформування правоохоронної системи з використанням нових технологій в інформаційній сфері, приклади чого, зокрема при розслідуванні організованої діяльності у сфері торгівлі людьми [180; 221] та деякі інші [181], додатково підтверджують правильність обраного курсу.

Пропонуємо декілька прикладів досягнень українських учених, що при належному застосуванні створять суттєві проблеми терористам і тим, хто їх підтримує: 1) нанотехнологічні біосенсори, здатні виявити присутність у повітрі навіть поодиноких молекул отруйних чи біологічно небезпечних речовин; 2) універсальні вакцини проти певних класів біологічної зброї, спроможні швидко налагоджуватися на боротьбу навіть з раніше невідомими його модифікаціями; 3) нановуглецеві матеріали, здатні витримувати величезні температури при високій міцності і легкості — незамінний матеріал для літаючих апаратів і військової техніки; 4) наночастинки металів, що мають

дезинфікуючу дію на декілька порядків і вищу за стандартні засоби; 5) наноелектронні компоненти і схеми, здатні цілком витиснути імпортні комплектуючі з вітчизняної електроніки та інформаційних технологій; 6) лазери, що базуються на новітніх досягненнях нанофотоніки, які перетворюють електричну енергію на світлове випромінювання з високим коефіцієнтом корисної дії; 7) квантові пристрої для захищених телекомунікацій та обчислень; 8) мікроелектромеханічні прилади і нові матеріали для авіакосмічної техніки, які можна використовувати у надкомпактних гіперзвукових літальних апаратах; 9) біоелектронні чіпи, що можуть стати компонентами активних інтелектуальних систем охорони стратегічних об'єктів від високотехнологічного нападу [48].

Отже, визначимо основні зовнішні загрози, що становлять найбільшу небезпеку для об'єктів забезпечення інформаційної безпеки у військовій та правоохоронній сферах: 1) розвідувальна діяльність спеціальних служб іноземних держав, міжнародних злочинних угруповань, організацій і груп, пов'язана зі збиранням відомостей, що розкривають завдання, плани діяльності, технічне оснащення, методи роботи та місця дислокації спеціальних підрозділів і органів внутрішніх справ України; 2) діяльність іноземних державних і комерційних структур, що прагнуть одержати несанкціонований доступ до інформаційних ресурсів правоохоронних і судових органів.

З метою докладного вивчення сучасної проблематики нанотехнологій та інших критичних технологій, а також захисту інтелектуальної власності в системі правоохоронних органів України створено спеціальні підрозділи, у складі яких працюють аналітичні групи, що відслідковують напрацювання сотні світових джерел у сфері нанотехнологій. У той же час, як показує зарубіжний досвід, спроби подолати інфотероризм виключно силовими засобами в сучасних умовах малоперспективні. Тому державна політика у сфері запобігання тероризму [47] має посідати особливе місце щодо розроблення та впровадження антитерористичних нанотехнологій, чому, на жаль, до цього часу приділяється недостатньо уваги.

о ***Інформатизація Збройних Сил і військові нанотехнології***

Інформатизація Збройних Сил України — складова частина національної програми інформатизації [30, с. 19–22]. Високотехнологіч-

на інформатизація є складовою цього процесу і включає створення, впровадження, застосування і модернізацію в різних сферах діяльності у мирний та воєнний час нових високотехнологічних методів, систем і засобів одержання, оброблення, зберігання, передавання та використання інформації.

Головний акцент високотехнологічної модернізації Збройних Сил України становить інформатизація. Висока ефективність інформаційної боротьби на міжнародній арені стимулює інтенсивні розробки нової техніки, високотехнологічних телекомунікаційних засобів, радіоелектронних апаратів та інших інформаційних пристроїв. Тому однією з головних цілей забезпечення інформаційної безпеки у військовій сфері є підтримка постійної готовності Збройних Сил до адекватних заходів, у тому числі в інформаційному протиборстві.

У цьому зв'язку потрібно визначити особливу загрозу такого злочину, як диверсія у сфері комп'ютерної інформації, яка може бути пов'язана з інформаційною війною, що планується і ведеться з метою досягнення інформаційної переваги над супротивником у військовій ситуації.

Стратегічні, оперативні та тактичні потреби боротьби з інформаційним ресурсом породили новий клас інформаційної зброї — ракети і бомби різних класів, що наводяться на джерела випромінювань, засоби радіоелектронної боротьби. Тому змагання в модернізації інформаційних засобів є важливою умовою ефективного застосування високотехнологічної бойової техніки.

Нові можливості в розвитку інформатизації Збройних Сил відкриває комп'ютеризація, заснована на широкому застосуванні комп'ютерних мереж. У зв'язку з цим до основних вимог ефективної діяльності систем управління військами слід віднести здатність функціонувати в умовах різкого збільшення потоку інформації при одночасному зменшенні часу на її передавання, оброблення та використання.

Таким чином, висока ефективність і значущість інформатизації стали одним з найважливіших чинників підвищення бойової готовності Збройних Сил на новому витку їх розвитку і вдосконалювання. Це зумовлює істотний перегляд військово-політичних, стратегічних та оперативно-тактичних поглядів на зміст і характер військового протистояння в сучасних умовах.

Окрема загроза в інформаційному протистоянні виходить з військових нанотехнологій. Наприклад, мікроскопічні датчики «Smart Dust» («розумний пил») виявили свою ефективність під час застосування у військових операціях. Сигнали таких елементарних датчиків аналізуються з центрального вузла управління, і, що важливо, датчики дуже дешеві у виробництві. Розвідувальні та бойові пристрої невеликих розмірів (сантиметрових діапазонів), що літають, повзають, плавають, можуть проникнути куди завгодно. У цьому зв'язку потрібно наголосити на тому, що у найближчі 10–20 років можуть бути створені супермалі комп'ютери, більш легкі та міцні матеріали, нові типи зброї та, навіть, імплантанти, що вводитимуться в організм військовослужбовців.

Звідси перспективи *військових нанотехнологій* необхідно розглядати з погляду міжнародної безпеки та запобігання новим перегонам озброєнь. Як відзначають дослідники, до 2025 р. на Землі можливо прогнозувати справжню війну наномашин [3]. Це, навіть, можливо уявити: сидить який-небудь президент у себе на дачі. Чує, що комар дзижчить. Почуває, що кусає. Шльопає його. І, начебто б, убиває, оскільки дзижчання затихає. Але насправді цей «комар-кримінаніт» уже проник усередину тіла і затаївся, чекаючи злочинного наказу.

Нанотехнології потенційно надають можливість для створення системи, яка повинна здійснити автоматичний ядерний залп у разі виявлення ядерної атаки. Некерований наноробот, запрограмований виключно на побудову копій самого себе, використовуючи підручні матеріали, може дуже швидко переробити усю біосферу Землі у свої копії — так звану «сіру слиз» як велику масу наномашин, що самовідтворюються, і при цьому не мають структури у великому масштабі. Такі події можуть трапитися через умисне включення або від випадкову мутацію наноструктурних утворень.

Отже, інформатизація Збройних Сил та правоохоронних органів має відбуватися у рамках єдиного процесу, що відображує відповідний напрям державної інформаційної політики.

Розглянутий матеріал дозволяє спрогнозувати подальше зростання інформаційної злочинності та появу її нових підвидів як в Україні, так і за кордоном, що викликає необхідність розроблення невідкладних заходів щодо її попередження у сфері використання нових інте-

лектуальних технологій, де найбільше помітне наше технологічне відставання від злочинного середовища.

Нанотехнології можуть стати для правоохоронних органів тим науково-технічним інструментом, завдяки якому можна радикально підняти ефективність боротьби зі злочинністю на якісно новий рівень. Зрозуміло, що шляхи використання інформаційних наносистем у сфері протидії інформаційній злочинності та стримуванні рівня її інтелектуалізації потребують ґрунтовного осмислення і визначення подальших перспектив розвитку в цій галузі знань.

Сьогодні вже не може виникати спорів щодо доцільності створення антикримінального мега-інформаційного середовища, здатного найбільш повно і оперативно задовольняти інформаційні потреби органів усіх рівнів, які ведуть боротьбу зі злочинністю, при здійсненні ними своїх функцій і повноважень.

Процес інтеграції інформаційних систем правоохоронних органів має бути продовжений і ще глибше охоплювати інформаційні масиви, починаючи зі слідчих та закінчуючи експертними установами.

Отже, наведені аргументи надають підстави щодо виведення формули високотехнологічної теорії інформаційного права:

$$\frac{X}{Y} = \frac{N \xrightarrow{1} N \xrightarrow{2} N \xrightarrow{3}}{W \xrightarrow{1} W \xrightarrow{2}} \Rightarrow HT, \tag{5.6}$$

де інформаційне право (X) виступає правовим регулятором суспільних відносин у сфері високих технологій (Y), новими об'єктами чого є нанонаука (N^1), нанотехнології (N^2) і наноіндустрія (N^3), детермінуючи особливий характер розвитку високотехнологічних інформаційних правовідносин (W^1), а звідси — становлення високотехнологічного інформаційного права (W^2) як окремої теорії права високих технологій (HT).

На завершення слід зазначити, що концептуалізація інформаційної політики у сфері боротьби зі злочинністю — це науково обґрунтована системна докорінна видозміна об'єкта державного впливу на інноваційний процес програмної інформатизації з метою досягнення кінцевої мети — модернізації засобів антикримінального впливу згідно з сучасними умовами інтелектуалізації злочинності.

На підставі системного аналізу наслідків дослідження, спробуємо схематично вивести передостанню формулу:

$$P = \frac{D}{L+R} S\sqrt{In + If}\ , \tag{5.7}$$

де P — політика розвитку високих інформаційних технологій складається з D — державного регулювання високотехнологічних інформаційних правовідносин, L — правового механізму, R^{-} стратегій розвитку, окремим напрямом чого виступає сфера боротьби зі злочинністю (S), модернізувати яку пропонується завдяки високотехнологічному прориву, а саме впровадженню інформаційних наносистем (In) та оптоволоконних систем передавання інформації (If).

Логіку цих міркувань показано на схемі 5.6.

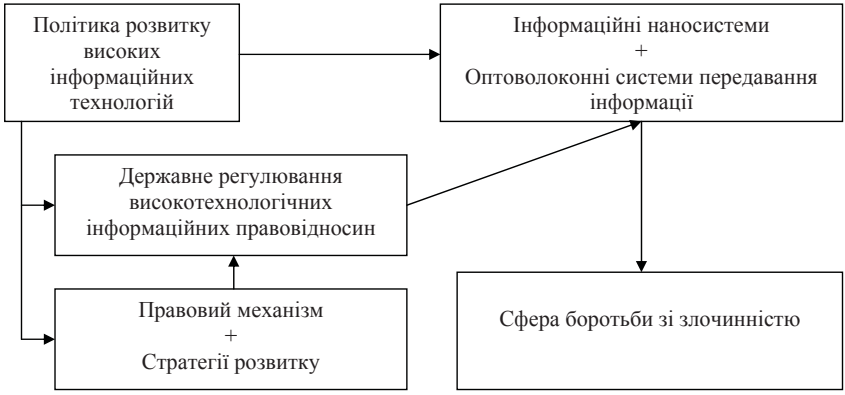


Схема 5.6

Резюме. *Дослідження національних програм розвитку нанотехнологій як антикримінальних метатехнологій XXI ст., надає підстави підсумувати: 1) визначено правовий зміст поняття «нанотехнологія»; 2) з'ясовано основні наукові підходи щодо тлумачення змісту понять «нанонаука», «нанотехнології» та «наноіндустрія» як об'єктів права високих технологій; 3) висвітлено нанонаукові засади судово-експертних досліджень; 4) з'ясовано напрями використання нанотехнологій в експертній практиці; 5) обґрунтовано доцільність уведення нового поняття «нанозлочинність» у контексті уточнених визначень «інформаційна злочинність», «міжнародна злочин-*

ність», «інтелектуалізація злочинності»; б) запропоновано нове бачення перспектив використання наносистем у галузі протидії міжнародному тероризму; 7) виведено концептуальні засади розвитку нанотехнологій у сфері боротьби зі злочинністю та військовій галузі.

***Ключові слова**: нанонаука; нанотехнології; наноіндустрія; тунельні мікроскопи; судова експертиза; експертні технології; нанохімія; криміналістична фізика; нанооб'єкти; наноматеріали; інформаційна злочинність; міжнародна злочинність; інтелектуалізація злочинності; тероризм; нанороботи.*

Контрольні запитання

1. Поняття права високих технологій та його об'єкти.
2. Проблеми правового регулювання суспільних відносин щодо нанотехнологій.
3. Нанонаука, нанотехнології та наноіндустрія як нові об'єкти права високих технологій.
4. Техносфера і нанотехнологічне суспільство.
5. Правове регулювання суспільних відносин у галузі наноіндустрії.
6. Концепція та основні завдання Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010–2014 роки.
7. Національні стратегії політики та програми розвитку нанотехнологій у контексті модернізації економіки.
8. Проблеми розвитку експертних стандартів нанотехнологій.
9. Наночастинки як носії інформації в судово-експертних дослідженнях.
10. Нанотехнологія як нова методика експертних досліджень об'єктів надмалих розмірів.
11. Криміналістична фізика та фізика високих енергій.
12. Інформатизація Збройних Сил України як складова частина національної програми інформатизації та військові нанотехнології.
13. Основні кількісно-якісні показники злочинності у сфері високих технологій.
14. Перспективи застосування туннельних мікроскопів як нанотехнологій в судовій експертизі та криміналістиці.
15. Нанотехнології як протидія ядерному тероризму, психотероризму та біотероризму.

16. Штучний інтелект, розробки нейронних нанотехнологій і зчитування нервових імпульсів.
17. Використання нанотехнологічних біосенсорів у галузі протидії міжнародній злочинності.
18. Кримінальні нанороботи (кримінаніти) як потенційні засоби та способи вчинення високотехнологічних злочинів.
19. Проблеми концептуального стримування інтелектуалізації злочинності та ефективної боротьби з міжнародним інформаційним і кібертероризмом.
20. Шляхи інноваційного розвитку нанотехнологій як антикримінальних метатехнологій XXI ст.

₪ Якщо ми прагнемо створити новий світ,
матеріал для нього вже готовий.
Перший також був створений з хаосу.
(Роберт Куіллен)

₪ Нановиробництво — це побудова
на граничному рівні добірності.
(Ричард Смеллі)

Висновки

Підсумовуючи викладене, можемо констатувати, що наука інформаційного права, а звідси й відповідна навчальна дисципліна, ще перебувають на стадії формування. Проведений нами аналіз більшості проблемних аспектів засвідчив, що в інформаційному праві чимало питань залишаються дискусійними.

Монопарадигмальність є критерієм, що визначає право дисципліни на самостійність. Оскільки високотехнологічне право — підгалузь інформаційного права, предметом якої є правова регуляція високотехнологічних процесів, що відбуваються в інформаційній сфері, логічно спрогнозувати системний розвиток цієї наукової теорії. Адже еволюція наукового знання й зводиться до формування, розвитку і революційних змін парадигм. Тому ми намагалися показати різні точки зору стосовно побудови окремої наукової теорії, детермінованої розвитком нових правовідносин, що активно складаються у сфері високих технологій.

Зрозуміло, що висвітлені наукові погляди, концепції та практичні рекомендації не беззаперечні, а у деяких моментах навіть різняться з прийнятими у вітчизняній юридичній науці. Втім, сподіваємося, що систематизація раніше здобутих і нових унікальних даних сприятиме становленню високотехнологічної теорії інформаційного права.

Викладений матеріал не охопив усе коло проблем, що існують у сфері державного регулювання високотехнологічних інформаційних правовідносин. Основна авторська ідея полягає у тому, що високі технології є предметом суспільних відносин в інформаційному праві. Ця концепція є новою в теорії права. Вона ще не набула глибокого

наукового обґрунтування, проте активно впливає на формування своїх методологічних основ і поглиблення міжгалузевих зв'язків, застосовується у правотворенні, зокрема щодо створення правових норм у сфері нових інформаційних технологій. Це відкриває нові перспективи для подальших наукових досліджень.

Правова регуляція суспільних відносин, що складаються у високотехнологічній сфері, залишається безсистемною. І дійсно, адже в різних сферах людської діяльності інформаційні нововведення багато в чому мають загальний характер, а займаються ними фахівці різних галузей права, що стримує розвиток високотехнологічних інновацій.

Звідси за структурою роботи ми знаходимо зв'язок унікальних міждисциплінарних зв'язків високотехнологічної теорії інформаційного права з теорією держави і права (підрозділ 1.2), філософією (підрозділ 3.1), політикою (підрозділ 1.1), економікою (підрозділ 5.1), технікою (підрозділи 2.2, 2.3, 3.1), навіть футурологією (підрозділ 5.3) та основними дисциплінами кримінально-правого циклу — кримінальним правом і кримінологією (підрозділи 1.3, 5.3), кримінальним процесом і криміналістикою (підрозділ 3.3), судовою експертизою (підрозділ 5.2) та прокуратурою (розділ 4).

Врешті-решт ця праця охоплює виключно базові засади цієї теорії, не вичерпуючи увесь її зміст, оскільки автор і не ставив перед собою такого завдання. Проблема полягала в тому, щоб визначити методологічну основу, навколо якої можна було б синтезувати предмет високотехнологічної теорії інформаційного права в системі права України, доповнюючи його існуючими парадигмами, концепціями і результатами емпіричних досліджень.

Відповідно до цього пріоритетні напрями і перелік високих (критичних) технологій повинні бути взаємопов'язані зі стратегічними цілями і пріоритетними напрямами, визначеними у прогнозах і програмах соціально-економічного розвитку країни на середньострокову та довгострокову перспективу. Тож вважаємо цілком доведеним, що одним з першочергових завдань постає розроблення та вдосконалення законодавства, що регулює високотехнологічні підвалини інформаційних правовідносин.

У цьому зв'язку, розвиваючи логіку співвідношення, зазначеного у формулі 5.6, визначимо перспективи політики розвитку високих

технологій передавання інформації у сфері боротьби зі злочинністю у вигляді центральної формули

$$\sum \frac{1+2+3+4+5}{M \xrightarrow[1]{} M \xrightarrow[2]{} M \xrightarrow[3]{} M \xrightarrow[4]{} M \xrightarrow[5]{}} = P,$$

де основними компонентами є: політика розвитку високих технологій передавання інформації у сфері боротьби зі злочинністю (*P*); системна інформатизація правоохоронних органів (1), що передбачає модернізацію єдиної інформаційно-телекомунікаційної системи (*M* 1); нові інформаційні технології (2), в тому числі суперкомп'ютери та Грід-мережі (*M* 2); освоєння нових технологічних коридорів передавання інформації (3), що ґрунтуються на впровадженні ВОЛЗ (*M* 3); моніторинг цифрової інформаційної мережі (4), в тому числі антикримінальне Інтернет-патрулювання (*M* 4); розвиток нанонауки, впровадження нанотехнологій, становлення наноіндустрії (5), в тому числі у військовій, експертно-криміналістичній та інформаційній сферах (*M* 5).

Пропоноване дослідження орієнтоване не тільки на змістовну систематизацію проблеми теоретико-правових засад політики розвитку інформаційних процесів у сфері високих технологій. Одним з основних завдань був пошук оптимальних шляхів стосовно ефективного розв'язання інформаційно-правових проблем, що виникають в нових соціотехнологічних умовах. З цією метою, спираючись на методологію синергетичного підходу, нові і вже відомі теоретичні розробки систематизовано в єдину теорію і тим самим структурно окреслено системні заходи модернізації та освоєння нових технологічних коридорів передавання інформації у сфері боротьби зі злочинністю.

Проведене дослідження дозволило обґрунтувати гіпотезу відносно перспектив розвитку політики інноваційної безпеки, що підтверджується низкою концептуальних положень. Зокрема, визначено теоретичні засади формування високотехнологічних (електронних, цифрових) інститутів інформаційного права та концептуальні проблеми розвитку нанотехнології в Україні і Російській Федерації у сфері боротьби зі злочинністю.

Не повторюючись зазначимо, що головні висновки в концентрованому вигляді та основні логіко-правові формули сформульовано наприкінці кожного з розділів цієї праці.

Аналіз матеріалу надає підстави вважати доведеною основну тезу, згідно з якою інноваційний розвиток та модернізація економіки поступово призводять до появи нових високотехнологічних інститутів інформаційного права.

Отже, дана праця є цілісною теоретико-методологічною розробкою, де розглянуто проблеми організаційно-правового регулювання низки високотехнологічних явищ, а саме нанотехнологій та оптоволоконних систем передавання інформації, відсутніх у деяких підручниках і монографіях. З часом в її зміст можуть бути включені додаткові матеріали без порушення структури, оскільки запропонований загальний підхід до концептуалізації політики розвитку високих технологій (нанотехнологій та оптоволоконних систем передавання інформації) у сфері боротьби зі злочинністю не суперечить рекомендаціям провідних дослідників у галузі інформаційного права.

Переорієнтація інтересів і цілей національної політики з модернізації на глобальний розвиток нових інформаційних технологій — це єдиний послідовний напрям, що відповідає реаліям сьогодення.

Виконання комплексу визначених заходів має призвести до модернізації і технологічного розвитку інноваційної економіки в цілому. Саме в цьому напрямі слід шукати систему цінностей, здатну стимулювати економічне зростання і соціальний розвиток. Лише увімкнувшись у розв'язання проблем високотехнологічної цивілізації глобального порядку, Україна одержить суттєвий імпульс розвитку, зможе перебороти кризу, заявити про себе як про спроможну країну XXI століття. Розвиток нанотехнологій надасть Україні можливість повернутися в коло світових лідерів у науковій, економічній і політичній сферах, розв'язати проблеми у сфері боротьби зі злочинністю. Не повторювати і копіювати те, що вже пройдено іншими, а разом з ними брати участь у створенні нового світу — тільки так можна і надолужити упущене, і зберегти себе в цьому світі. І Україні, якщо вона не обмежуватиметься гаслами і ґрунтовно розбереться у своєму минулому, є що сказати й запропонувати світовому співтовариству.

Довідково-контрольна частина

Сучасний світ активно змінюється. У глобальному контексті особливого значення набуває модернізація процесу підготовки майбутніх юристів, де окреме місце посідають інформаційно-технологічні інновації. Звідси сьогодні впровадження нових програм навчання в юридичних закладах, неминуче починаються з інформаційного перелому свідомості як викладача, так і студентів. У першу чергу це стосується навчальної дисципліни «Інформаційне право України». Адже на цьому шляху існує певна кількість проблемних питань, частину з яких ми спробували вирішити у процесі підготовки цього видання. Так, студенти-юристи часом не мають уявлень щодо своїх можливостей у реалізації читання навчальної літератури, особливо з тих юридичних дисциплін, де використовується складна технічна та природнонаукова термінологія. Такий стан ускладнюється тим, що нині студенти-юристи, як правило, не оперують спеціальними знаннями, навіть у мінімальному обсязі. До того ж, вони не мають відповідних навчально-методичних рекомендацій щодо засвоєння незрозумілих питань.

У цьому зв'язку ми рекомендуємо викладачам, ґрунтуючись на матеріалі навчального посібника «Високотехнологічне інформаційне право України» та виходячи з середньої швидкості читання у групі, визначати оптимальний обсяг навчального матеріалу для самостійного вивчення з кожної теми. Подібний реалістичний підхід до визначення обсягу матеріалу для самостійного освоєння знижує формальне ставлення до позааудіторної навчальної діяльності студентів і дає можливість підвищити рівень його засвоєння.

Крім того, для покращення сприйняття навчального матеріалу при вивченні навчального курсу «Інформаційне право України» додаються різні експериментальні форми практичних робіт — ділові ігри за фабулами юридичних справ у сфері високих технологій, постановка окремих інформаційно-правових проблем і розв'язання соціально-правових конфліктів, що можуть виникати в інформаційній галузі, аудиторні відеоконференції, виконання юридичних завдань з використанням комп'ютерної техніки тощо.

Отже, допомога викладачів у складанні системи уявлень про продукт своєї навчальної діяльності, ступені системної сформованості знань у сфері правового регулювання високих технологій може й повинна стати основою модернізації самостійної роботи студентів при вивченні навчального курсу «Інформаційне право України».

Як засвідчила практика, спроби повністю або частково виключити контроль з навчального процесу призводять до зниження якості навчання. Тож, запроваджувані на сучасному етапі інтенсивні методи навчання неминуче зумовлюють нові пошуки у царині підвищення якості та ефективності педагогічного контролю і впровадження інноваційних форм у контексті розвитку кредитно-модульної системи освіти.

Загальновідомо, що, виходячи з поставлених до методів педагогічного контролю основних вимог, їх можна поділити на методи набування знань; формування вмінь і навичок; здійснення творчої діяльності; закріплення і перевірка знань. Утім, інформаційні методи навчання спрямовані на формування педагогом у студентів нових знань. Використання цих методів у процесі модульного навчання підкріплює інформаційну функцію модуля.

У зв'язку з цим викладання матеріалу має плануватися таким чином, щоб викликати у студентів зацікавленість до проблеми, збагатити їх інформацією в конкретній галузі, визначити місце даної проблеми в суміжних галузях, що ми спробували розробити у вигляді тестів чотирьох рівнів складності, куди включено як загальні питання з навчального курсу «Інформаційне право України» (до речі, загальні з яких у цій роботі не висвітлювалися), так і організаційно-правові проблеми високих технологій передавання інформації у сфері боротьби зі злочинністю, про що докладно йшлося в основному тексті.

Тести містять чотири рівні складності: а) відмінний; б) добрий; в) достатній; г) мінімальний. Кожне тестове завдання має п'ять варіантів відповідей, із яких правильними відповідями можуть бути як одна, так дві або, навіть, три.

Підсумкові тести різних рівнів складності

Рівень «Г» (мінімальний)

Тест 1. Інформація — це:

а) документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі;

б) документовані або публічно оголошені відомості про події та явища, що мали або мають місце у суспільстві, державі та навколишньому середовищі;

в) документовані або публічно оголошені відомості про події та явища, що можуть мати місце у суспільстві, державі та навколишньому середовищі;

г) відомості в будь-якій формі і 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.

Тест 2. Поняття «інформаційне суспільство» виражає:

а) ідею нової фази в історичному розвитку передових країн;

б) не прихід «постіндустріального» суспільства, а створення нового соціального зразка;

в) результат «другої індустріальної революції», яка в основному ґрунтується на мікроелектронній технології;

г) результат «третьої індустріальної революції», що створила соціально-економічні відносини нового типу, основу яких складатимуть нанотехнології.

Тест 3. Головні складові поняття «інформаційне суспільство»:

а) інформаційна економіка;

б) наноіндустрія;

в) високоінтелектуальні інформаційні технології;

г) оптоволоконні телекомунікаційні мережі зв'язку.

Тест 4. Законодавство України визначає види інформаційної діяльності:

а) діяльність друкованих засобів масової інформації;

б) діяльність інформаційних агентств;

в) науково-технічна діяльність;

г) рекламна діяльність.

Тест 5. Науково-інформаційна діяльність — це:

а) сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні;

б) сукупність дій, спрямованих на задоволення політичних потреб держави в науково-технічній інформації, що полягає в її пошуку та контролі за розповсюдженням;

в) сукупність дій, спрямованих на задоволення економічних потреб громадян та юридичних осіб, що полягає в аналітично-синтетичній обробці науково-технічної інформації та засекречуванні;

г) збирання, оброблення, творення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції.

Тест 6. Архівна справа — це:

а) збирання, оброблення, творення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції;

б) збирання, аналітично-синтетичне оброблення, фіксація, зберігання, пошук і поширення інформації;

в) галузь життєдіяльності суспільства, що охоплює наукові, організаційні, правові, технологічні, економічні та інші питання діяльності юридичних і фізичних осіб, пов'язані із нагромадженням, обліком, зберіганням архівних документів та використанням відомостей, що в них містяться;

г) галузь життєдіяльності українського суспільства, що охоплює політичні питання діяльності юридичних і фізичних осіб у радянський період, пов'язані із накопиченням, обліком, зберіганням архівних документів та використанням відомостей, що в них містяться.

Тест 7. Державна статистична діяльність — це:

а) сукупність організаційних, творчих, виробничих заходів, спрямованих на підготовку і випуск у світ видавничої продукції;

б) сукупність дій, пов'язаних з проведенням державних статистичних спостережень та наданням інформаційних послуг, спрямована на збирання, опрацювання, аналіз, поширення, збереження, захист та використання статистичної інформації, забезпечення її достовірності, а також удосконалення статистичної методології;

в) планомірний, науково організований процес збирання даних щодо масових явищ та політичних процесів, які відбуваються в економічній, соціальній та інших сферах життя України та її регіонів;

г) комплекс видів професійної діяльності, пов'язаної з виробництвом, зберіганням статистичних відомостей та демонструванням їх вищим посадовим особам України.

Тест 8. Книжкова палата України — це державна наукова установа у сфері видавничої справи та інформаційної діяльності, що здійснює:

а) організацію книготоргівлі та книгообміну;

б) державну бібліографічну реєстрацію та централізовану каталогізацію всіх без винятку видів видань, випущених в Україні;

в) аналіз тенденцій розповсюдження видавничої продукції, вивчення книжкового ринку, його регіональних особливостей;

г) розроблення та обґрунтування короткострокових і довгострокових прогнозів розвитку видавничої та бібліографічної справи в Україні.

Тест 9. Інформатизація — це:

а) процес, що використовує сукупність засобів і методів збирання, оброблення та передавання даних (первинної інформації) для одержання інформації нової якості про стан об'єкта, процесу або явища (інформаційного продукту);

б) множина взаємопов'язаних організаційних, правових, науково-технічних та інших процесів, спрямованих на формування умов для задоволення потреб громадян і суспільства, реалізації їх прав, обов'язків через створення, застосування та розвиток комп'ютерних інформаційних систем, мереж, інформаційних ресурсів і технологій;

в) виробництво інформації для її аналізу людиною і прийняття на його основі рішення про виконання будь-якої дії;

г) динамічна система інформаційних взаємодій суб'єкта із зовнішнім світом, у процесі чого відбуваються створення образу, вті-

лення його в об'єкті, здійснення та перетворення опосередкованих психічним чином відносин суб'єкта в предметній діяльності.

Тест 10. Інформаційне право є:

а) сукупністю правових норм, що регулюють соціальні відносини, які так чи інакше пов'язані з інформацією;

б) правовим інститутом, що регулює інформаційні правовідносини, що виникають виключно у сфері високих технологій;

в) галуззю права, що вивчає правову регуляцію суспільних відносин в інформаційному просторі;

г) сукупністю норм щодо правового регулювання соціально-економічного процесу розвитку постіндустріального суспільства.

Рівень «В» (достатній)

Тест 1. У навчальному курсі «Інформаційне право України» виділяється такі основні проблеми:

а) розроблення і просування універсальних принципів та норм з метою вирішення світових і національних проблем інформаційної галузі;

б) забезпечення обмеженого доступу та прихованого використання глобальних інформаційних ресурсів;

в) пошук правових заходів на виклики міжнародного тероризму;

г) розвиток багатостороннього співробітництва України в галузі інформації та комунікації, свободи вираження та розвитку нових інформаційних технологій.

Тест 2. Інформаційна безпека — це:

а) організаційно-правовий механізм мінімізації негативних наслідків застосування інформаційних технологій;

б) стан захищеності інформаційних інтересів держави, при якому запобігається заподіяння шкоди;

в) стан захищеності приватних інтересів людини, при якому діє правовий механізм щодо запобігання заподіянню шкоди;

г) стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається заподіяння шкоди.

Тест 3. Інформаційна діяльність — це:

а) сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави;

б) діяльність органів влади щодо оприлюднення офіційних нормативно-правових актів;

в) сукупність інформаційних дій, спрямованих на задоволення політичних потреб України;

г) будь-яка діяльність щодо збирання, зберігання, використання і поширення інформації, спрямована на задоволення інформаційних потреб різноманітних суб'єктів.

Тест 4. Одержання інформації — це:

а) набуття, придбання, накопичення виключно публічно оголошуваної інформації державою та її уповноваженими органами;

б) набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою;

в) накопичення документованої інформації громадянами та юридичними особами;

г) набуття, придбання, накопичення відповідно до міжнародно-правових норм документованої або публічно оголошуваної інформації юридичними особами або державою.

Тест 5. Поширення інформації — це:

а) задоволення інформаційних потреб громадян, юридичних осіб і держави;

б) забезпечення належного стану інформації та її матеріальних носіїв;

в) поширення, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації;

г) набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою.

Тест 6. Складовими частинами видавничої справи є:

а) видавнича діяльність — сукупність організаційних, творчих, виробничих заходів, спрямованих на підготовку і випуск у світ видавничої продукції;

б) виготовлення видавничої продукції — виробничо-технологічний процес відтворення певним тиражем видавничого оригіналу поліграфічними чи іншими технічними засобами;

в) розповсюдження видавничої продукції — доведення видавничої продукції до споживача як через торговельну мережу, так і іншими способами;

г) юридичні особи, які здійснюють господарську діяльність у сфері видавничої діяльності.

Тест 7. Залежно від території розповсюдження програм визначається територіальна категорія мовлення та територіальна категорія каналу мовлення або багатоканальної телемережі:

а) загальнонаціональне мовлення — мовлення не менше ніж на дві третини населення кожної з областей України;

б) регіональне мовлення — мовлення на регіон (область, декілька суміжних областей), але менше ніж на чверть областей України;

в) місцеве мовлення — мовлення на один чи кілька суміжних населених пунктів, яке охоплює не більше половини території області;

г) закордонне мовлення — мовлення на територію поза межами державного кордону України.

Тест 8. Видавнича справа спрямована на:

а) задоволення потреб особи, суспільства, держави у видавничій продукції та отримання прибутку від цього виду діяльності;

б) створення можливостей для самовиявлення громадян як авторів незалежно від раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак;

в) поступове зменшення книговидання російською мовою, при цьому слід забезпечувати культурні потреби російськомовного населення в Україні з урахуванням обмеженого імпорту друкованої продукції;

г) збільшення кількості видань іноземними мовами, які поширювали б у світі знання про Україну.

Тест 9. Забороняється реклама:

а) проведення цілительства на масову аудиторію;

б) нових методів профілактики, діагностики, реабілітації та лікарських засобів, які знаходяться на розгляді в установленому порядку, але ще не допущені до застосування;

в) алкогольних напоїв та тютюнових виробів;

г) послуг народної медицини (цілительства) та осіб, які їх надають, дозволяється лише за наявності відповідного спеціального до-

зволу на заняття народною медициною (цілительством), виданого Міністерством охорони здоров'я України або уповноваженим ним органом, і повинна містити номер, дату видання зазначеного дозволу та назву органу, який його видав.

Тест 10. Модернізація — це:

а) удосконалення та відновлення об'єкта, приведення його у відповідність із новими вимогами і нормами, технічними умовами, показниками якості;

б) розвиток, детермінований внутрішньо обумовленою причиною, спрямований на формування умов для задоволення потреб громадян і суспільства, реалізації їх прав, обов'язків через створення, застосування та розвиток комп'ютерних інформаційних систем, мереж, інформаційних ресурсів і технологій;

в) розвиток із заздалегідь планованим результатом, зі свідомо прогнозованим фіналом, із чітко визначеною кінцевою метою;

г) інноваційне поліпшення технологічного процесу з метою досягнення вищого рівня ефективності.

Рівень «Б» (добрий)

Тест 1. У сфері соціального захисту головним завданням інформатизації є:

а) створення для управлінських і регіональних структур програмних систем та засобів обліку всіх рівнів, аналізу і моделювання зайнятості населення, запобігання масовому безробіттю та для широкого залучення населення до нових галузей матеріального виробництва та інших сфер;

б) створення єдиної структурованої інформаційної системи обліку стану здоров'я громадян України на основі автоматизованої реєстрації пацієнтів у лікувальних установах, збирання даних профілактичних обстежень з метою їх подальшого використання в статистичних, аналітичних та експертних системах;

в) створення системи дистанційного консультування та діагностики на основі комп'ютерних мереж, що об'єднують великі лікувальні та наукові заклади;

г) організація державних і приватних центрів масового навчання населення новим спеціальностям з урахуванням вимог міжнародних

стандартів для кадрового забезпечення усіх напрямів інформатизації за рахунок інтенсифікації підготовки відповідних фахівців.

Тест 2. З метою складання статистичної інформації органи державної статистики можуть використовувати такі джерела інформації:

а) первинні та статистичні дані щодо респондентів, що підлягають статистичним спостереженням;

б) оперативні дані органів, які згідно із законодавством України можуть проводити оперативно-розшукові заходи;

в) дані банківської і фінансової статистики, статистики платіжного балансу тощо;

г) статистичну інформацію міжнародних організацій та статистичних служб інших країн тощо.

Тест 3. Забороняється розташовувати засоби зовнішньої реклами:

а) на пішохідних доріжках та алеях;

б) у населених пунктах на висоті менш ніж 10 метрів від поверхні дорожнього покриття, якщо їх рекламна поверхня виступає за межі краю проїжджої частини;

в) поза населеними пунктами на відстані менш ніж 5 метрів від краю проїжджої частини;

г) поза населеними пунктами на відстані менш ніж 3 метри від краю проїжджої частини.

Тест 4. Державні інформаційні ресурси — це:

а) організаційно-технічна сукупність, що складається з автоматизованої системи та мережі передавання даних;

б) інформація, яка передається мережею передавання даних незалежно від способу її фізичного та логічного представлення;

в) інформація, яка є власністю держави та (або) необхідність захисту якої визначено законодавством;

г) організаційно-технічна система, яка складається з комплексів телекомунікаційного обладнання (вузлів комутації) та реалізує технологію інформаційного обміну з використанням первинної мережі зв'язку.

Тест 5. Інформаційна система — це:

а) організаційно-технічна система оброблення інформації за допомогою технічних і програмних засобів;

б) сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації;

в) сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання (випромінювання) або приймання сигналів, знаків, звуків, рухомих чи нерухомих зображень або іншим способом);

г) система обліку, зберігання, використання та знищення документів, справ, видань, магнітних та інших матеріальних носіїв інформації, що містять конфіденційну інформацію, яка є власністю держави.

Тест 6. Правова інформація — це:

а) сукупність документованих або публічно оголошених відомостей про особу;

б) систематизовані, документовані або публічно оголошені відомості про суспільне, державне життя та навколишнє природне середовище;

в) сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо;

г) документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій та явищ, процесів, фактів.

Тест 7. Інформація з обмеженим доступом — це:

а) відомості конфіденційного або таємного характеру, правовий статус яких передбачено законодавством України, що визнані такими відповідно до встановлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей;

б) відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов;

в) інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (банківську, комерційну, службову, професійну, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству і державі;

г) матеріали, документи, інші відомості, якими користуються в процесі та у зв'язку з виконанням своїх посадових обов'язків посадові особи державних органів, що здійснюють регулювання ринків фінансових послуг, та особи, які залучаються до здійснення цих

функцій, і які забороняється розголошувати у будь-якій формі до моменту прийняття рішення відповідним уповноваженим державним органом.

Тест 8. Комерційна таємниця — це:

а) 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, і 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;

б) вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані такою (державною таємницею) у порядку, встановленому Законом України «Про державну таємницю», і підлягають охороні державою;

в) будь-які відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці;

г) 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 і розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

Тест 9. Волоконно-оптичний зв'язок — це:

а) передавання інформації на значні відстані з більш високою швидкістю передавання даних, ніж в електронних засобах зв'язку, в тому числі надання широкого доступу в Інтернет;

б) вид провідного електрозв'язку, що використає як носій інформаційного сигналу електромагнітне випромінювання оптичного діапазону, а як напрямні системи — волоконно-оптичні кабелі;

в) високотехнологічний вид системи бездротового передавання інформації;

г) новий вид зв'язку, при якому інформація передається по оптичних діелектричних хвилеводах, відомих за назвою «оптичне волокно».

Тест 10. Високотехнологічне інформаційне право охоплює:

а) сукупність правових норм, що регулюють соціальні відносини, які так чи інакше пов'язані з технологічними розробками в інформаційній сфері;

б) сукупність правових норм, що регулюють інформаційні правовідносини, які виникають у сфері високих технологій;

в) особливості нормативно-правового регулювання процесу розвитку високотехнологічного інформаційного суспільства;

г) правові засади діяльності друкованих засобів масової інформації (преси) та правовий статус інформаційних агенцій, бібліотечну та архівну діяльність, телебачення, радіомовлення і кінематографію, законодавство у сфері видавничої справи, правове регулювання державної статистики та організаційно-правові основи рекламної діяльності.

Рівень «А» (відмінний)

Тест 1. Електронний цифровий підпис — це:

а) дані в електронній формі, що додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

б) обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;

в) 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;

г) програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів доступу.

Тест 2. Несанкціоновані дії щодо інформації в системі — це:

а) виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

б) перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності;

в) дії, що провадяться з порушенням порядку доступу до цієї інформації, встановленого відповідно до законодавства;

г) несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.

Тест 3. Адміністрування адресного простору українського сегмента мережі Інтернет здійснюється для:

а) створення реєстру доменних назв і адрес мережі українського сегмента мережі Інтернет;

б) впровадження правового механізму саморегулюції доменних назв і адрес українського сегмента мережі Інтернет;

в) забезпечення унікальності, формування та підтримки простору доменних назв другого рівня в домені.UA;

г) представництва та захисту у відповідних міжнародних організаціях інтересів споживачів українського сегмента мережі Інтернет.

Тест 4. Захист інформації з обмеженим доступом — це:

а) організаційно-правові заходи, які вживаються власником інформації з обмеженим доступом або іншими особами за його замовленням, з метою запобігання заподіянню шкоди інтересам власника інформації та її неконтрольованому поширенню;

б) інженерно-технічні заходи, які вживаються власником інформації з обмеженим доступом або іншими особами за його замовленням, з метою запобігання заподіянню шкоди інтересам власника інформації та її неконтрольованому поширенню;

в) криптографічні заходи, які вживаються власником інформації з обмеженим доступом або іншими особами за його замовленням, з метою запобігання заподіянню шкоди інтересам власника інформації та її неконтрольованому поширенню;

г) сукупність організаційно-правових, інженерно-технічних та криптографічних заходів, які вживаються власником інформації з обмеженим доступом або іншими особами за його замовленням, з метою запобігання заподіянню шкоди інтересам власника інформації та її неконтрольованому поширенню.

Тест 5. Блокування інформації в системі — це:

а) дії, внаслідок яких унеможливлюється доступ до інформації в системі;

б) результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

в) позбавлення користувачів можливості обробляти інформацію в системі;

г) дії, внаслідок яких інформація в системі зникає.

Тест 6. Користування персональними даними передбачає:

а) дії їх власника щодо користування ними або дії володільця персональних даних, якому їх власником чи законом надано часткове або повне право оброблення персональних даних, а також покладені обов'язки щодо їх захисту;

б) будь-які дії їх власника щодо оброблення цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншими суб'єктами відносин, пов'язаних із персональними даними;

в) право володільця персональних даних на надання часткового або повного права оброблення персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, за згодою власника персональних даних чи відповідно до закону;

г) право держави тимчасово обмежувати права володільця персональних даних у випадках, передбачених законом.

Тест 7. Принципами формування і проведення державної політики у сфері технічного захисту інформації є:

а) додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;

б) єдність підходів до забезпечення технічного захисту інформації, які визначаються загрозами безпеці інформації та режимом доступу до неї;

в) виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту конфіденційної інформації, що належить державі

г) скоординованість дій та розмежування сфер діяльності організаційних структур системи технічного захисту інформації з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки.

Тест 8. Сучасними напрямами розвитку нанотехнологій є:

а) розроблення надпотужних інформаційних систем надмалих розмірів та пристроїв оптичного запису інформації;

б) розроблення засобів протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом;

в) розроблення нових психотехнологій гіпнорепродукційного опитування і нейролінгвістичного програмування;

г) розроблення наноматеріалів та наноінструментів щодо методик виявлення латентних слідів та дослідження мікрооб'єктів.

Тест 9. Інтелектуальні технології — це:

а) високі наукоємні технології, що відтворюють елементи інтелекту людини;

б) процес приєднання локальних (регіональних) суспільств, держав до сучасної світової комп'ютерної інформаційної культури;

в) новий спосіб організації технологічної сфери як результат «другої індустріальної революції», що ґрунтується на мікроелектронних технологіях;

г) умови для створення нового соціального зразка «об'єднаного» чи «колективного» інтелекту, що в основному ґрунтується на високих технологіях.

Тест 10. Оптоволоконна інформаційна технологія — це:

а) процес, що використовує сукупність засобів і методів збирання, обробки і передавання даних (первинної інформації) для одержання інформації нової якості про стан об'єкта, процесу або явища (інформаційного продукту);

б) комплекс методів, способів і засобів пошуку, збору (придбання), реєстрації, зберігання, поширення (реалізації), захисту і відображення інформації за допомогою високотехнологічних інформаційних систем і волоконно-оптичних мереж передавання даних;

в) виробництво інформації для аналізу її людиною та прийняття на його основі рішення на виконання будь-якої дії;

г) цілеспрямовано організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечує високу швидкість оброблення даних, швидкий пошук інформації, розміщення даних, доступ до джерел інформації незалежно від місця їхнього розміщення.

Ключі до вірних відповідей

¥ *Мінімальний рівень: 1 (Г) — а, б, г; 2 (Г) — а, б, в; 3 (Г) — а, в, г; 4 (Г) — а, б, г; 5 (Г) — а; 6 (Г) — в; 7 (Г) — б; 8 (Г) — б, в, г; 9 (Г) — б; 10 (Г) — а, в.*

¥ *Достатній рівень: 1 (В) — а, г; 2 (В) — а, г; 3 (В) — а, б, г; 4 (В) — б; 5 (В) — в; 6 (В) — а, б, в; 7 (В) — а, в, г; 8 (В) — а, б, г; 9 (В) — а, б, г; 10 (В) — а, в, г.*

¥ *Добрий рівень: 1 (Б) — а; 2 (Б) — а, в, г; 3 (Б) — а, в; 4 (Б) — в; 5 (Б) — а; 6 (Б) — в; 7 (Б) — а; 8 (Б) — а, в; 9 (Б) — а, б, г; 10 (Б) — а, б, в.*

¥ *Відмінний рівень: 1 (А) — в; 2 (А) — в; 3 (А) — а, в, г; 4 (А) — г; 5 (А) — а; 6 (А) — б; 7 (А) — а, б, г; 8 (А) — а, г; 9 (А) — а, г; 10 (А) — б.*

Індивідуальні завдання

Завдання А

Підготовте доповіді (реферати) з визначених тем:

Тема № 1. Основні засади розвитку інформаційного суспільства.

Тема № 2. Поняття та види інформаційної діяльності.

Тема № 3. Друковані засоби масової інформації (преса) в Україні.

Тема № 4. Правовий статус інформаційних агентств в Україні.

Тема № 5. Бібліотечна діяльність в Україні.

Тема № 6. Архівна діяльність в Україні.

Тема № 7. Телебачення, радіомовлення і кінематографія в Україні.

Тема № 8. Законодавство у сфері видавничої справи в Україні.

Тема № 9. Правове регулювання державної статистики в Україні.

Тема № 10. Рекламна діяльність в Україні.

Тема № 11. Електронний документообіг та правове регулювання телекомунікацій.

Тема № 12. Національна складова глобальної інформаційної мережі Інтернет.

Тема № 13. Основні засади політики розвитку високих технологій передачі інформації у сфері боротьби зі злочинністю.

Тема № 14. Правове регулювання інформаційних відносин у сфері високих технологій.

Тема № 15. Оптоволоконні інформаційні комунікації в системі правоохоронних органів України.

Тема № 16. Інформаційно-телекомунікаційна система органів прокуратури.

Тема № 17. Модернізація передачі інформації у сфері боротьби зі злочинністю.

Тема № 18. Національні програми розвитку нанотехнологій як антикримінальних метатехнологій XXI століття.

Завдання Б

Продовжіть думку:

1. Інформація — це документовані або публічно оголошені відомості про події та ... .

2. Інформаційне право є сукупністю правових норм, що регулюють соціальні відносини, які ... .

3. Правова інформація — це сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію ... .

4. Інформатизація — це політика й процеси, які спрямовані на побудову й розвиток телекомунікаційної інфраструктури, що поєднує ... .

5. Інформаційна технологія — це процес, що використовує сукупність засобів і методів збирання, обробки і передачі даних ... .

6. Високотехнологічне інформаційне право — це є основний нормативним регулятором інформаційних відносин найвищого (критичного) рівня, які виникають у сфері ... .

7. Інформаційна діяльність — це сукупність дій, спрямованих на задоволення інформаційних ... .

8. Інформаційні ресурси — це організована сукупність інформації, інформаційних продуктів і інформаційних ... .

9. Телекомунікації — це процес дистанційного передавання даних на засадах ... .

10. Під системною інформатизацією прокуратури розуміють взаємопов'язані правові, організаційні, технічні, наукові, фінансові та інші процеси, спрямовані на модернізацію інформаційного забезпечення діяльності прокуратури через створення ... .

Завдання В

Порівняйте:

1. Поняття волоконно-оптична мережа та оптоволоконна система.

2. Організаційно-правові принципи забезпечення інформаційної безпеки в комп'ютерних та телекомунікаційних системах.

3. Правовий зміст визначень захист інформації та інформаційний захист.

4. Завдання регіональних і територіальних інформаційних мереж правоохоронних органів.

5. Функції органів прокуратури і органів внутрішніх справ як суб'єктів високотехнологічного інформаційного права у сфері боротьби зі злочинністю.

Завдання Г

Розв'яжіть задачі:

Задача 1. Назвіть відсутню ланку, вкажіть пропущені значення *X*, *Y*, *Z* та обґрунтуйте логічність формул: «Техніка + Наука = Технологія» ~ «*X* + *Y* = *Z*» ~ «Високі технології + Інформаційне право = Високотехнологічне інформаційне право».

Задача 2. Проаналізуйте дефініцію (визначити, чи правильна вона, якщо ні — то які категорії учасників інформаційних правовідносин пропущено): «Громадяни України, іноземні громадяни, особи без громадянства, юридичні особи усіх форм власності, господарські товариства, науково-дослідні та професійно-освітні заклади, органи влади і управління та їхні посадові особи є суб'єктами високотехнологічного інформаційного права України».

Задача 3. Розкрийте вид і структуру визначення: «Інформаційні інновації антикримінальної діяльності — це виключно нові інформаційні технології, які є результатом досягнень науково-технічного прогресу й передового антикримінального досвіду, оскільки є наслідком інвестування в наукову розробку і отримання нового знання, яке раніше не застосовувалося в практиці органів, які ведуть боротьбу зі злочинністю». Порівняти поняття інформаційної інновації як процесу та об'єкта.

Задача 4. Визначте тип відношення між поняттями і зобразіть його за допомогою колових схем: а) «несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»; б) «комп'ютерний злочин»; в) «злочини у сфері високих технологій»; г) «інформаційна злочинність».

Задача 5. К. зі свого домашнього комп'ютера надіслав 1500 адресатам сумнівну інформацію щодо імовірності вірусної атаки, рекомендувавши в цей період автономно використовувати комп'ютери, вимкнувши їх з мережі. Вірусна атака відбулася в зазначений у повідомленні час, за наслідками чого було порушено роботу 1250 електронно-обчислювальних машин. Які обставини додатково потрібно з'ясувати для вірної кваліфікації дій К. Скласти план розслідування і проект обвинувачення.

Завдання Д

Спираючись на матеріал відповідного розділу навчального посібника, іншу навчальну та наукову літературу, складіть словник основних понять та термінів:

1. Інформація як об'єкт суспільних відносин.
2. Інформаційні процеси у сфері високих технологій.
3. Джерела високотехнологічного інформаційного права України.
4. Особливості правового регулювання високотехнологічних інформаційних відносин.
5. Інститути високотехнологічного інформаційного права.
6. Види високотехнологічної інформації та типи її носіїв.
7. Основна мета та суб'єкти національної інформаційної політики.
8. Система інформаційних ресурсів та інформаційна инфраструктура.
9. Виробництво та розвиток високих інформаційних технологій.
10. Роль інформаційної політики в становленні інформаційного права високих технологій.
11. Загальносистемні проблеми інформаційної безпеки у сфері високих технологій.
12. Концепція кодифікації українського інформаційного законодавства та мета Інформаційного кодексу України.
13. Національна програма інформатизації та політика розвитку високих інформаційних технологій у сфері боротьби зі злочинністю.

Завдання Є

Завершіть схеми або складіть нові, при цьому аргументуйте свої зауваження:

Схема 1

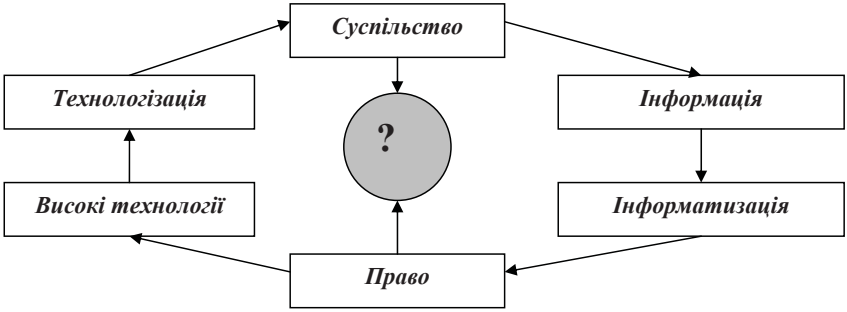
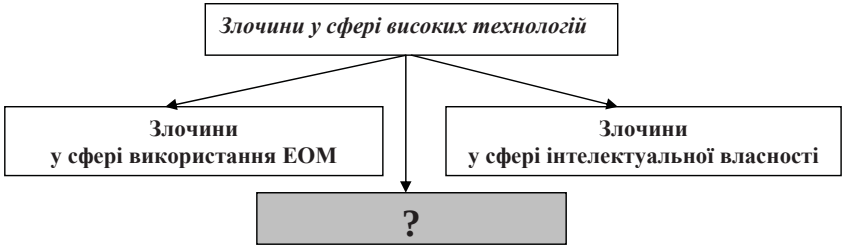


Схема 2



Завдання Ж

До кожного поняття підберіть правильне визначення й укажіть його порядковий номер:

1	Інформаційна інновація		обчислювальна система, де зібрані знання фахівців про певну конкретну проблемну галузь і яка, у межах цієї галузі, здатна приймати експертні рішення
2	Оптоволоконний зв'язок		створення, формування, сберігання, обробка, розповсюдження, використання інформаційних продуктів, управління процесом використання інформаційного продукту та надання інформаційних послуг, розвиток та застосування нових технологій передачі інформації в системах і мережах комунікацій, посилення безпеки в інформаційній сфері, а також юридична відповідальність суб'єктів інформаційного права
3	Експертна система		інформаційна система спостережень, яка складається зі збору, обробки та аналізу інформації про стан об'єкта, обов'язковим елементом чого є оцінка та прогноз стану соціального сприйняття у певний період часу
4	Грід-технологія		практичні методи дослідження, аналізу і синтезу, процес фундаментальної розробки методів виробництва й застосування продуктів із заданою атомарною структурою шляхом контрольованого маніпулювання окремими атомами та молекулами
5	Об'єкти інформаційного права		протиправні дії в інформаційній сфері, що порушують установлені законом права особистості, організації або держави, що заподіюють ним моральну шкоду або матеріальний збиток
6	Суб'єкти інформаційного права		вид проводового електрозв'язку, при якому інформація передається за оптичними діелектричними хвилеводами, відомими за назвою «волоконно-оптичні кабелі»

7	Моніторинг		сфера високотехнологічної діяльності, сектор інноваційної економіки, що включає дослідне та серійне виробництво, промислове впровадження й реалізацію як нанопродукції, так і нанотехнологій, а також допоміжні сектори та споживча аудиторія
8	Нанотехнологія		учасники інформаційних відносин, які володіють інформаційними правами та обов'язками, організаційно здійснюючі їх на нормативно-правовій основі, що у передбачених законом випадках несуть відповідну правову відповідальність
9	Інформаційна злочинність		об'єднання ресурсів шляхом створення комп'ютерної інфраструктури нового типу, що забезпечує глобальну інтеграцію інформаційних і обчислювальних ресурсів на основі мережевих технологій і спеціального програмного забезпечення, а також набору стандартизованих служб
10	Наноіндустрія		вперше створена та модернізована нова технологія в інформаційні сфері, що суттєво підвищує рівень інформатизації

Ключі: 1 — 10; 2 — 6; 3 — 1; 4 — 9; 5 — 2; 6 — 8; 7 — 3; 8 — 4; 10 — 7; 9 — 5.

Питання для самоперевірки

1. Розкрийте зміст понять «інформаційне право», «високотехнологічне інформаційне право» та «право високих технологій».

2. У чому співвідношення високотехнологічного інформаційного права з іншими галузями права та юридичними дисциплінами?

3. Визначте поняття «інформаційно-телекомунікаційна система».

4. Доведіть особливості правовідносин між суб'єктами в процесі оброблення інформації в інформаційно-телекомунікаційній системі.

5. Охарактеризуйте законодавство України про захист інформації в інформаційно-телекомунікаційних системах.

6. На чому ґрунтується побудова системи захисту інформації в конкретній інформаційно-телекомунікаційній системі?

7. Аргументуйте тенденції розвитку правового регулювання захисту інформації в мережі Інтернет.

8. Розкрийте поняття і види юридичної відповідальності за правопорушення у сфері обігу інформації з обмеженим доступом.

9. Які дії та процеси підпадають під визначення «несанкціонований доступ», «витік інформації»?

10. Визначте організаційно-технологічні засади інформаційного забезпечення діяльності органів, які ведуть боротьбу зі злочинністю.

11. Охарактеризуйте законодавство України про Національну систему конфіденційного зв'язку.

12. Що таке спеціальна телекомунікаційна система (мережа)?

13. Дайте визначення Національної системи конфіденційного зв'язку.

14. Розкрийте зміст поняття «конфіденційна інформація, що є власністю держави».

15. Які права та обов'язки оператора зв'язку (телекомунікацій)?

16. Обґрунтуйте високотехнологічну концепцію стримування інтелектуалізації злочинності.

17. Назвіть типові положення міжурядових Угод про співробітництво в галузі технічного захисту інформації.

18. Зазначте принципи національних проектів розвитку нанотехнологій у сфері протидії ядерному тероризму.

19. Розкрийте перспективи створення правового механізму регуляції українського інтелектуального ринку високих технологій.

20. Прилади та методи криміналістичної фізики.

Модельна програма кредитно-модульного контролю

МОДУЛЬ 1

Високотехнологічне інформаційне право в системі права України та основи правового регулювання у сфері високих технологій

1. Державна політика розвитку високих технологій передачі інформації.
2. Інформація та інформатизація.
3. Поняття інформаційного суспільства.
4. Повноваження державних органів у сфері розбудови інформаційного суспільства.
5. Характеристика основних нормативно-правових актів, що регламентують розвиток інформаційного суспільства в Україні.
6. Поняття інформаційної діяльності, її основні напрями та види.
7. Інформаційна діяльність органів державної влади та органів місцевого самоврядування в Україні.
8. Сутність та мета інформаційної політики органів державної влади.
9. Концепція Національної програми інформатизації та основні напрями інформатизації в Україні.
10. Політика інформатизації правоохоронних органів.
11. Місце високотехнологічного інформаційного права в системі права України та його зв'язок з іншими юридичними дисциплінами.
12. Теорія правової информатики.
13. Поняття та види високих технологій.
14. Особливості правового регулювання інформаційної діяльності у сфері високих технологій.
15. Методи та методологія права високих технологій.
16. Основні функції та принципи високотехнологічного інформаційного права.
17. Об'єкти і суб'єкти високотехнологічного інформаційного права.
18. Проблеми кодифікації інформаційного законодавства та проекти Інформаційного кодексу України.
19. Поняття, правові ознаки та види інформації.
20. Правовий статус інформації як об'єкта цивільних прав.

21. Поняття та види конфіденційної інформації.

22. Зміст суб'єктивного права на інформацію.

23. Інформаційні правопорушення і злочини у сфері високих технологій.

24. Злочинність у сфері високих технологій.

25. Основні положення кримінально-правової політики у сфері високих інформаційних технологій.

26. Кримінальне право і право високих технологій.

27. Телекомунікаційна мережа та види електронних інформаційних ресурсів.

28. Сфера і класифікація телекомунікацій.

29. Поняття та види телекомунікаційних послуг.

30. Суб'єкти ринку телекомунікаційних послуг.

31. Інформаційні ресурси та інформаційні продукти.

32. Інформаційні системи та процеси.

33. Компоненти інформаційної системи.

34. Правове регулювання захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

35. Законодавство України про захист інформації в інформаційно-телекомунікаційних системах.

36. Інформаційно-телекомунікаційні системи. Обробка інформації, несанкціонований доступ, витік інформації.

37. Відносини між суб'єктами в процесі обробки інформації в інформаційно-телекомунікаційній системі.

38. Відповідальність за порушення законодавства про захист інформації в інформаційно-телекомунікаційних системах.

39. Законодавство про Національну систему конфіденційного зв'язку.

40. Порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям.

41. Загальні засади оптоволоконної системи передачі інформації.

42. Організаційно-правові аспекти оптоволоконних телекомунікацій.

43. Волоконно-оптичні лінії зв'язку і телекомунікаційна мережа правоохоронних органів.

44. Проблеми організаційно-правового забезпечення безпеки у високотехнологічних інформаційних системах.

45. Методи інформаційної безпеки та системи захисту інформації.

46. Інформаційна надійність оптоволоконних телекомунікацій.

47. Зміст поняття «технічний захист інформації».

48. Основні нормативні положення щодо технічного захисту інформації.

49. Зміст поняття «інформація з обмеженим доступом», її види та правові особливості обігу.

50. Визначення таємної інформації та правовий статус державної таємниці в Україні.

МОДУЛЬ 2

Основні галузеві інститути високотехнологічного інформаційного права та політика розвитку високих технологій передачі інформації у сфері боротьби зі злочинністю

1. Політика модернізації та освоєння нових технологічних коридорів передачі інформації у сфері боротьби зі злочинністю.

2. Шляхи системної інформатизації правоохоронних органів України.

3. Технологічна модернізація систем передачі інформації у сфері боротьби зі злочинністю.

4. Формування технологічного світогляду, високотехнологічна цивілізація і соціально-правові проблеми програмованого суспільства.

5. Суперкомп'ютери і Грід-мережі — нова комп'ютерна революція.

6. Застосування Грід-технологій в криміналістиці.

7. Цифрові права людини та інформаційна нерівність.

8. Особливості розвитку національної складової глобальної інформаційної мережі Інтернет.

9. Високотехнологічне інформаційне право та Інтернет.

10. Інформаційні функції інтернет-моніторингу та мультимедіатехнології.

11. Правовий моніторинг цифрових інформаційних мереж.

12. Інновації, інноваційна політика та управління інноваційними проектами.

13. Криміналістична інформатика та високі технології.

14. Проблеми досудового слідства у сфері високих технологій та криміналістична модернізація.

15. Нові інформаційні технології та експертні системи.

16. Види інформаційних та експертно-криміналістичних систем.

17. Характеристика інформаційних та експертно-криміналістичних систем.

18. Автоматизоване робоче місце слідчого.

19. Інноваційний проект «Оптико-електронний кабінет криміналістики».

20. Модернізація експертно-пошукових систем у діяльності органів внутрішніх справ.

21. Суб'єкти інформаційного права України у сфері боротьби зі злочинністю.

22. Інформаційне забезпечення органів прокуратури.

23. Інфраструктура прокурорських телекомунікацій.

24. Органи прокуратури як спеціальні суб'єкти високотехнологічного інформаційного права.

25. Інформаційно-телекомунікаційна система органів прокуратури України та шляхи її розвитку.

26. Правові ознаки електронних документів та забезпечення електронного документообігу.

27. Суб'єкти електронного документообігу та електронний документообіг в органах прокуратури.

28. Інформаційна діяльність у сфері державної статистики та інформаційно-аналітична підсистема «Статистика».

29. Електронна система «Нагляд» та Автоматизоване робоче місце «Прокурор-кримінолог-аналітик».

30. Перспективи розбудови електронних наглядових систем та аналітичних систем обробки інформації нового покоління.

31. Основні завдання інформатизації прокурорської діяльності.

32. Стратегії розвитку інформатизації органів прокуратури України.

33. Інноваційне законодавство у сфері високих технологій.

34. Поняття нанонауки та нанотехнології.

35. Наноіндустрія як об'єкт права високих технологій.

36. Сучасні теоретико-практичні проблеми нанотехнологій та шляхи розвитку правового забезпечення.

37. Модернізація економіки та концепція розвитку нанотехнологій.

38. Нанонаукові засади експертних досліджень об'єктів надмалих розмірів.

39. Судова експертиза та високі експертні технології.

40. Нанотехнології в судово-експертній практиці.

41. Види наноматеріалів і криміналістична нанотехніка.

42. Судова медицина і нанотехнології.

43. Судова хімія і нанохімія.

44. Судова (криміналістична) фізика і нанотехнології.

45. Інформаційне забезпечення розвитку експертних стандартів нанотехнологій.

46. Інформаційна і міжнародна злочинність як особлива суспільна загроза XXI століття та проблеми стримування її рівня інтелектуалізації.

47. Злочини у сфері нанотехнологій та нанозлочинність.

48. Штучний інтелект та нанороботи.

49. Інформаційний тероризм і перспективи інноваційних розробок антикримінальних наносистем.

50. Інформатизація Збройних Сил та військові нанотехнології.

Термінологічний словник

Запропонований термінологічний словник відноситься до класу систематизованих визначень допоміжного характеру, де використані такі основні атрибути: а) обумовлене слово або термінологічне словосполучення, де має використовуватися слово, якому дається визначення в називному відмінку; б) суть визначення як офіційно закріплений текст, що пояснює фактичну суть обумовленого слова; в) сфера дії визначення указує наскільки широко законодавець припускає використовувати дане визначення.

■ **Автоматизована інформаційна система** — інформаційна система, що реалізована на базі обчислювальної техніки та інших організаційно-технічних засобів.

■ **Автоматизована система (в інформаційних технологіях)** — організаційно-технічна система, що реалізує інформаційну технологію виконання встановлених функцій за допомогою персоналу і комплексу засобів обчислювальної техніки й зв'язку, методи й процедури, програмне забезпечення, фізичне середовище і інформацію, яка обробляється.

■ **Автоматизована система оброблення інформації** — сукупність технічних та програмних засобів, методів оброблення інформації й дій персоналу, що забезпечують виконання автоматизованого оброблення інформації.

■ **Автоматизоване оброблення даних** — оброблення даних технічними та програмними засобами з участю людини.

■ **Адміністратор безпеки —** посадова особа, відповідальна за виконання заходів щодо забезпечення захисту локальної обчислювальної мережі від несанкціонованого втручання.

■ **Адміністратор системи** — особа або група осіб, що мають повне уявлення про функціональну та програмно-апаратну структуру інформаційної системи і контролюють її проектування та використання.

■ **Асиметрична інформація** (англ. *asymmetric(al) information*) — термін, який використовується в економіці наряду з термінами «недосконала інформація» та «неповна інформація», коли одна сторона угоди чи операції володіє більшою інформацією, ніж інша.

■ **Багатоканальна телемережа (ефірна або кабельна)** — телекомунікаційна мережа загального користування, призначена для передавання телерадіопрограм, а також надання інших телекомунікаційних і мультимедійних послуг, здатна забезпечити одночасно трансляцію більше, ніж однієї телерадіопрограми і може інтегруватися з іншими телекомунікаційними мережами загального користування.

■ **База знань** — сукупність набору даних та евристичних прийомів (емпіричних правил) певної галузі.

■ **Банк даних** — система програмно-апаратних, мовних і організаційних засобів, призначених для централізованого накопичення і колективного використання даних, а також самі дані, які зберігаються в базах даних.

■ **Безпека даних автоматизованої системи** — властивість організації доступу до даних, що забезпечує їх захист від несанкціонованого використання, навмисного чи ненавмисного спотворення або руйнування.

■ **Безпека мережі** — організаційно-технічні заходи, які забезпечують захист локальної обчислювальної мережі від несанкціонованого втручання в її роботу чи спроб порушення нормальної роботи її елементів.

■ **Безпроводовий доступ до телекомунікаційної мережі** — електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися зі збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які приєднані до одного комутаційного центру.

■ **Блокування інформації** — 1) дії, наслідком яких є припинення доступу до інформації; 2) унеможливлення санкціонованого доступу до інформації.

■ **Взаємоз'єднання телекомунікаційних мереж** — встановлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватись інформацією.

■ **Витік інформації** — 1) результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї; 2) неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

■ **Глобальні мережі передачі даних** — іноземні та міжнародні мережі передачі даних, у тому числі мережа Інтернет.

■ **Грід-технології** — об'єднання ресурсів шляхом створення комп'ютерної інфраструктури нового типу, що забезпечує глобальну інтеграцію інформаційних і обчислювальних ресурсів на основі мережевих технологій і спеціального програмного забезпечення проміжного рівня (між базовими й прикладним програмним забезпеченням), а також набору стандартизованих служб для забезпечення надійного спільного доступу до географічно розподілених інформаційних і обчислювальних ресурсів (окремим комп'ютерам, кластерам, сховищам інформації й мережам).

■ **Дезінформація** — передача будь-яких відомостей, що не відповідають дійсності, із антисоціальною або злочинною метою.

■ **Державна інформаційна політика** — сукупність основних напрямів і способів діяльності держави для створення, зміцнення та сприяння нормативно-правового, методичного, науково-технічного, організаційного, фінансового та матеріально-технічного, захисного (охоронного) забезпечення реалізації права на інформацію.

■ **Дистанційне оброблення даних** — оброблення даних, за якими деякі функції введення-виведення виконуються пристроями, зв'язаними з комп'ютерною системою за допомогою засобів пересилання даних.

■ **Драйвер** — додаткова до операційної системи програма, що виконує функцію зв'язку операційної системи з зовнішнім пристроєм.

■ **Електрозв'язок** — будь-яке передавання, випромінювання або приймання знаків, сигналів, письмового тексту, зображення та звуків чи повідомлень будь-якого роду провідною, радіо, оптичною чи іншою електромагнітною системою.

■ **Електронні засоби захисту** — програмно-технічні засоби, які забезпечують захист електронних документів від несанкціонованого доступу на етапі передавання цих документів електронною поштою.

■ **Ендаумент** (англ. *endowment*) — цільовий фонд, що створюється за рахунок інвестування благодійних внесків, основним призначенням якого є використання з некомерційною метою для фінансування організацій науки, освіти, медицини, культури.

■ **Засоби комунікаційні (мережа)** — сукупність ліній пересилання даних та комунікаційних пристроїв, що дозволяє здійснювати взаємне сполучення прикінцевого обладнання.

■ **Злочини у сфері комп'ютерної інформації** — кримінально каране діяння, предметом посягання якого є комп'ютерна інформація.

■ **Інкапсульовані наноматеріали** — структури, де наноматеріали замикаються до зовнішньої капсули чи оболонки.

■ **Інноваційні інформаційні технології** — цілеспрямовано організована сукупність інформаційних процесів та реалізація інформаційних нововведень з використанням уперше створених та вдосконалених технологічних засобів передачі даних, до пошуку, одержання, обробки яких пристосована інформація або інформаційний продукт.

■ **Інтерактивний режим** — режим взаємодії користувача з обчислювальною системою, при якому система здійснює приймання, оброблення і видачу повідомлень в реальному масштабі часу.

■ **Інтранет** — внутрішньо корпоративна мережа, яка може бути ізольована від зовнішніх користувачів або функціонувати як автономна мережа, що не має доступу ззовні, використовуючи стандарти, технології і програмне забезпечення Інтернету.

■ **Інформаційна мова** — формалізована мова, призначена для характеристики даних чи змісту документів з метою забезпечення їх зберігання та пошуку.

■ **Інформаційна модель** — сукупність ідентифікаційних сигналів, що подають інформацію про об'єкт керування (контролю), зовнішнє середовище та саму систему управління, що їх використовують у процесі прийняття рішень щодо управління об'єктом.

■ **Інформаційна радіоелектронна система** — радіоелектронна система, яка здійснює збирання, оброблення і видавання інформації визначеного цільового призначення.

■ **Інформаційний злочин** — навмисні дії, спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які вчиняються з корисливих, політичних або хуліганських мотивів.

■ **Інформаційний канал** — маршрут пересилання інформації.

■ **Інформаційний сигнал** — акустичний чи оптичний сигнал, що сповіщає абонента чи оператора про етапи та результати установлення телефонного з'єднання.

■ **Інформаційні відносини** — суспільні відносини, які виникають при збиранні, одержанні, зберіганні, використанні, поширенні та захисту (охороні) інформації.

■ **Інформаційні ресурси** — 1) організована сукупність інформації, інформаційних продуктів і інформаційних технологій, призначених для забезпечення визначених економічних, екологічних, фінансових, інформаційних та інших потреб людини, суспільства і держави; 2) сукупністю інформаційних продуктів одного або декількох тематичних напрямів, що згруповані за змістом в інформаційних системах (бібліотеках, архівах, банках даних і ін.), що мають ретроспективний характер, необхідні для задоволення інформаційних потреб людини, суспільства і держави.

■ **Інформаційно-аналітична система** — суспільна структура, що включає інформаційні технології, інформаційні системи й інформаційні ресурси для здійснення інформаційно-аналітичної діяльності.

■ **Інформаційно-комунікаційні технології** — технології, пов'язані зі створенням, збереженням, передачею, обробкою і управлінням інформацією.

■ **Інформаційно-пошуковий масив** — упорядкована сукупність документів, фактів або відомостей про них, призначених для інформаційного пошуку.

■ **Інформаційно-телекомунікаційна система** — організаційно-технічна сукупність, що складається з автоматизованої системи та мережі передачі даних.

■ **Канал зв'язку** — засоби двостороннього обміну даними як сукупність апаратури закінчення ланки даних та лінії пересилання даних.

■ **Квантова електроніка —** галузь фізики, що вивчає методи посилення та генерації електромагнітного випромінювання на засадах явища вимущеного випромінювання в квантових системах.

■ **Компаратор —** (від англ. *comparare* — порівнювати) — інформаційний пристрій цифрової техніки, що призначений для порівняння будь-чого, в тому числі може бути програмою пошуку та порівняння схожих файлів.

■ **Комп'ютерна мережа** — 1) сукупність територіально розосереджених систем оброблення даних, засобів і (чи) систем зв'язку і пересилання даних, що забезпечує користувачам дистанційний доступ

до її ресурсів і колективне використання цих ресурсів; 2) мережа, в одному або кількох вузлах якої як ресурс оброблення даних містяться комп'ютери.

■ **Комунікаційні послуги** — послуги зв'язку, в тому числі телекомунікаційні, забезпечення телефонного, телексного, телеграфного зв'язку, радіомовлення, електронної пошти, супутникового, факсимільного та телевізійного зв'язку, поштові послуги.

■ **Комутація каналів** — процес з'єднання двох чи більше абонентських станцій, який забезпечує монопольне використання каналу пересилання даних до його роз'єднання.

■ **Кримінаніти** — нанороботи, що активно виконують заборонені (протиправні) дії згідно заданої інформаційної програми.

■ **Локальна обчислювальна мережа** — система, яка забезпечує на обмеженій території один чи декілька каналів зв'язку, наданих приєднаним до неї абонентам для короткочасного монопольного користування.

■ **Мережа інформаційна** — сукупність мережі електронно-обчислювальних машин (ЕОМ) і відділених реальних прикінцевих систем, що взаємодіють через мережу ЕОМ, яка забезпечує доступ прикладних процесів, розташованих в будь-якій із цих систем, до всіх її інформаційних, обчислювальних, комунікаційних ресурсів і колективне їх використання.

■ **Мережа передачі даних** — організаційно-технічна система, яка складається з комплексів телекомунікаційного обладнання (вузлів комутації) та реалізує технологію інформаційного обміну з використанням первинної мережі зв'язку.

■ **Мікроносій інформації** — репрографічна копія у вигляді мікрофільму або мікроафіши, що містить одне чи кілька мікрозображень документа на рулонній або форматній плівці, читання яких можливе тільки за допомогою оптичних приладів.

■ **Моніторинг** — інформаційна система (процес) спостережень, яка складається зі збору, обробки та аналізу інформації про стан об'єкта.

■ **Моніторинг мережі** — збір, обробка, збереження та аналіз інформації про поточний стан мережі без втручання в її функціонування.

■ **Нановиробництво** — виробництво або підготовка наноструктур.

■ **Наноелектроніка** — галузь електроніки, що займається розробкою фізичних і технологічних засад створення інтегральних електронних схем з характерними топологічними розмірами елементів менш 100 нм, основними завданнями якої є розробка фізичних основ роботи активних приладів з нанометровими розмірами, у першу чергу квантових, а також розробка інтегральних схем з нанометровими технологічними розмірами та виробів електроніки на ґрунті наноелектронної елементної бази.

■ **Наноінженерія** — науково-практична діяльність людини щодо конструювання, виготовлення та застосування нанорозмірних об'єктів чи структур, а також об'єктів чи структур, що створені методами нанотехнологій.

■ **Нанопередавачі** — маленькі органічні молекули, які переносять сигнали та інформацію від однієї частини мозку (нейрона) до іншої.

■ **Нанотехнологія** — сукупність наукових знань, способів і засобів, спрямованого, регульованого складання (синтезу) із окремих атомів і молекул різних речовин, матеріалів і виробів із лінійним розміром елементів структури від 0,1 до 100 нанометрів (10^{-9} м).

■ **Обробка інформації** — вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, уключаючи обмін по каналах передавання даних.

■ **Оброблення інформації** — систематичне виконання операцій над інформацією.

■ **Оптичний квантовий генератор** — пристрій, що перетворює енергію накачування (світлову, електричну, теплову, хімічну та ін.) в енергію когерентного, полярізованого та вузькоспрямованого потоку випромінювання.

■ **Послуга електрозв'язку** — продукт (результат) діяльності оператора електрозв'язку, що полягає в передаванні, прийманні та обробці інформації.

■ **Провайдер телекомунікацій** — суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.

■ **Проводовий електрозв'язок** — передавання і приймання інформації із застосуванням проводових ліній з металевими або волоконно-оптичними жилами.

■ **Ресурс мережі** — організаційне, інформаційне, програмне та технічне забезпечення мережі з пакетною комутацією, призначене для використання як окремих так і всіх функцій мережі.

■ **Сервер бази даних** — програмно-апаратний комплекс, який зберігає дані та приймає й обробляє запити, що керують цими даними.

■ **Система операційна** — 1) організована певним чином сукупність керівних та оброблювальних програм, що забезпечують найекономніший розподіл ресурсів обчислювальної системи та виконання програм; 2) сукупність програмних засобів, призначених для автоматизованого керування виконанням програмами та надання користувачам певних послуг.

■ **Система управління базами знань** — інструментальна система, яка забезпечує створення і використання баз знань.

■ **Телеграфія** — вид електрозв'язку для передавання текстової інформації з використанням сигнального коду.

■ **Телемережі** — телекомунікаційні мережі загального користування, що створюються в межах одного населеного пункту і призначаються для передавання абонентам програм радіо та телебачення з використанням штучного спрямовуючого середовища і які можуть інтегруватися в телекомунікаційні мережі загального користування загальнодержавного рівня.

■ **Технічні засоби телекомунікацій** — обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж.

■ **Технологічна модернізація** — корінні зміни у технологіях, у зв'язку з системним переходом економіки на інноваційний шлях розвитку.

■ **Транспортна телекомунікаційна мережа** — мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу.

■ **Фіксований зв'язок** — телекомунікації, що здійснюються із застосуванням стаціонарного (нерухомого) кінцевого обладнання.

■ **Цілісність інформації** — властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення.

■ **Шкідлива програма** — створена або існуюча програма зі спеціально внесеними змінами, яка завідомо призводить до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи електронно-обчислювальної машини (ЕОМ), системи ЕОМ або їх мережі.

■ **Якість інформації** — сукупність властивостей, що відображають ступінь придатності конкретної інформації про об'єкти та їхній взаємозв'язок для досягнення цілей, що стоять перед користувачем.

Список використаної та рекомендованої літератури

1. Абрамчук, Н. С. Нанотехнологии. Азбука для всех [Текст] : [монография] / [Н. С. Абрамчук и др.] ; под ред. Ю. Д. Третьякова. — М. : Физматлит, 2009. — 367 с.

2. Аксенов, Е. Т. Интегральная оптика для систем обработки информации [Текст] : [учебник] / Е. Т. Аксенов ; Санкт-Петербургский гос. политехнический ун-т. — СПб. : Изд-во Политехнического ун-та, 2005. — 81 с.

3. Альтман, Ю. (Jurgen Altmann) Военные нанотехнологии. Возможности применения и превентивного контроля вооружений = Military Nanotechnology: Potential Applications and Preventive Arms Control [Текст] : [монография] / Ю. Альтман ; (пер. с англ.). — М. : Техносфера, 2006. — 421 с.

4. Ананян, М. Опыт преодоления [Текст] / М. Ананян // Вестник инноваций. — № 1 (2). — январь 2005 г. http://www.tpprf.ru/img/uploaded/200 5022114594983.doc

5. Андрианов, С. Н. Волоконно-оптические системы [Текст] / С. Н. Андрианов, С. О. Мирумянц, Л. А. Трофанчук // Оптический журнал. — 1997. — Т. 64. — С. 102.

6. Андрианов, С. Н. Волоконно-оптические системы технического зрения для применения в науке, промышленности и делопроизводстве [Текст] / С. Н. Андрианов, В. А. Зуйков, А. А. Калачев // Известия Российской академии наук. — 2002. — Т. 66. — № 3. — С. 369–372.

7. Арістова, І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади [Текст] : автореф. дис. ... д-ра юрид. наук ; 12.00.07 — адміністративне право і процес, фінансове право, інформаційне право. / І. В. Арістова ; Національний університет внутрішніх справ. — Х. : НУВС, 2002. — 39 с.

8. Аркуша, Л. І. Проблеми взаємодії та інформаційного забезпечення правоохоронних органів у боротьбі з економічною організованою злочинною діяльністю [Текст] / Л. І. Аркуша // Інформаційне забезпечення протидії організованій злочинності / [зб. наук. ст.] ; за ред. М. П. Орзіха, В. М. Дрьоміна. — Бібліотека журналу «Юридичний вісник». — Одеса : ФЕНИКС, 2003. — С. 109 –117.

9. Аршинов, В. И. Синергетика как феномен постнеоклассической науки [Текст] : автореф. дис. … д-ра философ. наук: 09.00.08 — философия

науки и техники. / В. И. Аршинов ; Рос. акад. наук. Ин-т философии. — М. : ИФ РАН, 1999. — 48 с.

10. Аушев, В. Н. Волоконно-оптические системы передачи информации [Текст]: [конспект лекций] / В. Н. Аушев, П. Р. Смекалов; Ленингр. ин-т точ. механики и оптики. — Л. : ЛИТМО, 1988. — 41, [1] с.

11. Ахтирська, Н. Комп'ютерна злочинність в Україні через призму судової практики [Текст] / Н. Ахтирська, В. Антощук // Вісник прокуратури. — 2008. — № 3. — С. 84–94.

12. Ашурбеков, Т. Правовой мониторинг угроз национальным интересам [Текст] / Т. Ашурбеков // Законность. — 2007. — № 5. — С. 47–50.

13. Бабаев, Д. Ю. Акмеологический мониторинг как средство обеспечения качества подготовки кадров управления [Текст] : автореф. дис. ... канд. психолог. наук : 19.00.13 — психология развития, акмеология. / Д. Ю. Бабаев ; [Рос. акад. гос. службы при Президенте РФ]. — М., 2007. — 27 с.

14. Бавижев, А. Д. Защита файлов от несанкционированного доступа в ОС ЕС [Текст] / А. Д. Бавижев, В. В. Кореньков // Сообщения объединенного института ядерных исследований. — Дубна, 1988. — С. 1.

15. Баган, В. А. Наноструктурные волоконные темперы для активных и нелинейных применений [Текст] / В. А. Баган, Ю. К. Чаморовский, С. А. Никитов и др. // newrusnano.explosion.ru/sadm_files/disk/Docs/3/2/2%20(4).pdf

16. Балабанов, В. Нанотехнологии. Наука будущего: [фантастические возможности ближайшего будущего] [Текст] / В. Балабанов. — М. : Эксмо, 2009. — 246, [1] с.

17. Бандурин, С. Г. АРМ руководителя следственного подразделения. АРМ следователя [Текст] : [метод. пособие] / С. Г. Бандурин, Я. С. Шатило, И. Ю. Шорин. — Саратов : СЮИ МВД России, 2009. — 55 с.

18. Баранов, О. А. Інформаційне право України: стан, проблеми, перспективи [Текст] : [навч. посіб.] / О. А. Баранов. — К. : Видавничий дім «СофтПрес», 2005. — 316 с.

19. Бачило, И. Л. Информационное право [Текст] : [учебник для вузов] : (специальный курс) / И. Л. Бачило ; Ин-т государства и права Российской акад. наук, Академический правовой ун-т (ин-т). — М. : Юрайт ; Высш. образование, 2009. — 454 с.

20. Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження [Текст] : [монографія] / М. С. Вертузаєв, В. О. Голубєв,

О. І. Котляревський та ін. / під ред. О. П. Снігерьова. — Запоріжжя : ПВКФ «Павло», 1998. — 316 с.

21. Бірюков, В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів [Текст] : монографія / В. В. Бірюков ; Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2009. – 664 с.

22. Бєляков, К. І. Питання визначення правопорушень, що вчинюються з використанням інформаційних технологій: аксіоматичний підхід [Текст] / К. І. Бєляков // http://mndc.naiau.kiev.ua/Gurnal/9text/g9_20.htm

23. Богуш, В. М. Інформаційна безпека держави [Текст] : [навч. посіб.] / В. М. Богуш, О. К. Юдін. — М. : «МК-Прес», 2005. — 432 с.

24. Богуцький, О. Щодо проблем правового визначення суб'єктів телекомунікаційних послуг [Текст] / О. Богуцький // Право України. — 2006. — № 6. — С. 72–76.

25. Бутузов, В. М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [Текст] : [наук.-практ. коментар] / В. М. Бутузов, С. Л. Остапець, В. П. Шеломенцев ; [Департамент державної служби боротьби з економічною злочинністю МВС України]. — К. : Міністерство внутрішніх справ України, 2005. — 87, [1] с.

26. Бутузов, В. М. Планування заходів щодо запобігання та протидії комп'ютерній злочинності [Текст] / В. М. Бутузов, В. Д. Гавловський // Науковий вісник Дніпропетровського державного університету внутрішніх справ : [зб. наук. праць]. — 2007. — Спеціальний випуск № 1 (36) «Актуальні питання протидії злочинності». — С. 319–328.

27. Ващинець, І. І. Цивільно-правова охорона авторських прав в умовах розвитку інформаційних технологій [Текст] : дис. ... канд. юрид. наук: 12.00.03 — цивільне право і цивільний процес; сімейне право; міжнародне приватне право. / І. І. Ващинець ; НАН України; Інститут держави і права ім. В. М. Корецького. — К., 2006. — 179 с.

28. Вейнберг, В. Б. Волоконная оптика [Текст] / В. Б. Вейнберг // Оптико-механическая промышленность. — 1967. — № 11. — С. 48–51.

29. Вертузаев, М. С. Внимание, вас слушают..: обзор рынка приборов, выявляюших прослушивание телефонных переговоров [Текст] / М. С. Вертузаев, А. М. Вертузаев // Бизнес и безопасность. — 2002. — № 4. — С. 50–51.

30. Вертузаев, М. С. Реальности виртуального терроризма: Нью-Йорк, Киев, Одесса ... далее везде? [Текст] / М. С. Вертузаев //Бизнес и безопасность. — 2002. — № 2. — С. 19–22.

31. Власов, А. А. Актуальные проблемы прокурорского реагирования на нарушения прав личности в сети Интернет [Текст] / А. А. Власов, Т. П. Кесарева // Российский следователь. — 2000. — № 5. — С. 2–4.

32. Военные нанотехнологии : возможности применения и превентивного контроля вооружений [Текст] : [учеб. пособие] / Ю. Альтман ; [пер. с англ. А. В. Хачояна]. — М. : Техносфера, 2006. — 421 с.

33. Волков, С. В. Нанохімія. Наносистеми. Наноматеріали [Текст] : [монографія] / [С. В. Волков, Є. П. Ковальчук, В. М. Огенко та ін.] ; НАН України; Інститут загальної та неорганічної хімії ім. В. І. Вернадського; Львівський національний ун- т ім. Івана Франка. — К. : Наукова думка, 2008. — 423 с.

34. Воронов, І. О. Інтеграційний метод в теорії та практиці організації оперативно-розшукової діяльності [Текст] / І. О. Воронов // Роль та місце ОВС у розбудові демократичної правової держави : [матеріали Міжнародної науково-практичної конференції] (м. Одеса, 10 квітня 2009 р.). — Одеса : ОДУВС, 2009. — С. 270–271.

35. Гаман, Т. В. Вдосконалення організаційно-правового механізму інформаційної діяльності місцевих державних адміністрацій [Текст] : дис. ... канд. наук з держ. упр. : 25.00.02 — механізми державного управління. / Т. В. Гаман ; Львівський регіональний ін-т держ. управління Національної академії держ. управління при Президентові України. — Л., 2006. — 246 с.

36. Герасименко, К. С. Сучасні ознаки загроз «інформаційного тероризму» [Текст] / К. С. Герасименко // Форум права. — 2009. — № 3. — С. 162–166 [Електронний ресурс]. — Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09covcpk.pdf

37. Годунов, И. В. Транснациональная организованная преступность в России: Пути и формы противодействия [Текст] : дис. ... д-ра юрид. наук : 12.00.08 — уголовное право и криминология; уголовно-исполнительное право, 12.00.11 — судебная власть, прокурорский надзор, организация правоохранительной деятельности, адвокатура. / И. В. Годунов. — Рязань, 2002. — 604 с.

38. Головин, Ю. И. Введение в нанотехнику [Текст] : [учебник] / Ю. И. Головин. — М. : Машиностроение, 2007. — 493 с.

39. Городов, О. А. Информационное право [Текст] : [учебник] / О. А. Городов. — М. : Проспект, 2009. — 242 с.

40. Горшенков, Г. Н. К понятию «информационная преступность» [Текст] / Г. Н. Горшенков // Российский криминологический взгляд. — 2005. — № 4. — С. 93–96.

41. Гриценко, В. Суспільство в інформаційну епоху: реалії і перспективи розвитку [Текст] / В. Гриценко // Вісник Національної академії наук України. — 2005. — № 6. — С. 28–32.

42. Гуляев, Ю. В. Стандарты информационных и нанотехнологий: проблемы и решения [Текст] / Ю. В. Гуляев // Проблемы теории и практики управления. — 2008. — № 10. — С. 8–16.

43. Гуцалюк, М. Протидія правопорушенням у мережі Інтернет [Текст] / М. Гуцалюк // Вісник прокуратури. — 2002. — № 6. — С. 98–101.

44. Денісова, О. О. Інформаційні системи і технології в юридичній діяльності [Текст] : [навч.-метод. посіб.] / О. О. Денісова ; Київський національний економічний ун-т — К. : КНЕУ, 2005. — 256 с.

45. Державна програма інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю [Текст] / Затверджена Постановою Кабінету Міністрів 9 квітня 2009 р. № 321 // Офіційний вісник України. — № 27 — 2009 (21.04.09) [http://www.ovu.com.ua/articles/922-pro-zatverdzhennya-derzhavnoyi-programi-informatsi]

46. Державна інноваційна політика в умовах соціально орієнтованої ринкової економіки [Текст] : автореф. дис. ... канд. наук з держ. упр. : 25.00.02 / Катерина Андріївна Алексеєва; НАН України; Рада по вивченню продуктивних сил України. – К., 2009. – 20 с.

47. Державна політика у сфері запобігання тероризму: міжнародний досвід і його актуальність для України [Текст] : [матеріали наук.-практ. конф.] ; 31 жовтня 2008 р., м. Київ / Національна академія СБУ / І. Л. Серікова (упоряд.) — К. : Інтертехнологія, 2008. — 184 с.

48. Державні наукові і науково-технічні програми [Текст] / http://www.mon.gov.ua/ development/programs.doc

49. Джавадов, Ф. М. Экспертная деятельность и развитие науки судебной экспертизы [Текст] / Ф. М. Джавадов. — Баку : Элм, 1998. — 187 с.

50. Дианов, Е. М. Волоконно-оптическая связь и ее роль в современном обществе [Текст] / Е. М. Дианов, А. М. Прохоров // Вестник Российской академии наук. — 2002. — Т. 72. — № 6. — С. 483–486.

51. Дианов, Е. М. От тера-эры к пета-эре [Текст] / Е. М. Дианов // Вестник Российской академии наук. — 2000. — № 1. — С. 1010.

52. Дробатухин, В. С. Кибернетическое моделирование при расследовании преступлений [Текст] : автореф. дис. ... канд. юрид. наук : 12.00.09 — уголовный процесс, криминалистика и судебная экспертиза; оперативно-

розыскная деятельность / В. С. Дробатухин ; Академия управления МВД России. — М., 1998. — 27 с.

53. Дунаев, А. В. Приобретение знаний в интеллектуальных системах поддержки принятия решений разработчика вычислительных приложений в среде Грид [Текст] : автореф. дис. ... канд. техн. наук : 05.13.18 — математическое моделирование, численные методы и комплексы программ / А. В. Дунаев ; С.-Петерб. гос. ун-т информац. технологий, механики и оптики. — СПб., 2008. — 18 с.

54. Економіка та організація інноваційної діяльності [Текст] : [підручник] / [О. І. Волков, М. П. Денисенко, А. П. Гречан та ін.] — К. : Центр учбової літератури, 2007. — 662 с.

55. Желтов, В. В. Основы политологии [Текст] : [учебник] / В. В. Желтов. — Ростов н/Д : Феникс, 2004. — 544 с.

56. Жигалов, Е. А. Тактическая операция по собиранию информации о преступлении, связанном с использованием электронной почты [Текст] / Е. А. Жигалов // Известия Алтайського государственного университета. — 2000. — № 2 (16). — С. 35–38.

57. Жигулин, Г. П. Информационная безопасность [Текст] : [учебник] / Г. П. Жигулин, С. Г. Новосадов, А. Д. Яковлев ; С.-Петерб. гос. ун-т информ. технологий, механики и оптики. — СПб. : ИТМО ун-т, 2003. — 339 с.

58. Жиляев, А. И. Криминологические аспекты информационной преступности [Текст] / А. И. Жиляев, С. Н. Данилин // http://www.cir.nnov.ru/pages/issues/vestnik/ 99990195_West_pravo_2003_2(7)/B_3-7.pdf

59. Загородній, А. Грід — нова інформаційно-обчислювальна технологія для науки [Текст] / А. Загородній, Г. Зінов'єв, Є. Мартинов та ін. // Вісник Національної академії наук України. — 2005. — № 6. — С. 17–25.

60. Загородній, В. Застосування сучасних інформаційних технологій у діяльності прокуратури Одеської області [Текст] / В. Загородній, А. Іщенко // Вісник прокуратури. — 2006. — № 6. — С. 116–120.

61. Загоруйко, Н. Г. Информационные технологии в генетике [Текст] / Н. Г. Загоруйко, А. Г. Пичуева, О. А. Кутненко [и др.] // Информационные системы и технологии ИСТ-2003 : Труды Междунар. науч.-техн. конф. (г. Новосибирск, 22–25 апреля 2003 г.). — Новосибирск, 2003. — Т. 3. — С. 136–139.

62. Зайцев, В. А. Тенденции развития волоконно-оптических систем передачи информации [Текст] : [учеб. пособие] / [В. А. Зайцев, О. Г. Мясников, В. Н. Рыжевнин] ; Межотрасл. ин-т повышения квалификации кадров

по новым направлениям развития техники и технологии при Ленингр. ин-те точ. механики и оптики. — Л. : МИПК при ЛИТМО, 1990. — 32 с.

63. Зайчук, О. В. Теорія держави і права. Академічний курс [Текст] : [підручник] / О. В. Зайчук (ред.), А. П. Заєць, В. С. Журавский, О. Л. Копиленко, Н. М. Оніщенко (ред.). — 2-ге вид., переробл. і доп. — К. : Юрінком Інтер, 2008. — 688 с.

64. Закон України «Про внесення змін до Кримінального, Кримінально-процесуального та Виправно-трудового кодексів України» від 22 лютого 2000 р. [Текст] // Відомості Верховної Ради України. — 2000. — № 17. — Ст. 123.

65. Закон України «Про прокуратуру» від 5.11.1991 р. [Текст] // Відомості Верховної Ради України. — 1991. — № 53. — Ст. 793.

66. Закон України «Про захист інформації в автоматизованих системах» від 25.03.1994 р. [Текст] // Відомості Верховної Ради України. — 1994. — № 31. — Ст. 286.

67. Закон України «Про інформацію» від 2 жовтня 1992 р. [Текст] // Відомості Верховної Ради України. — 1992. — №48.

68. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. [Текст] // Відомості Верховної Ради України. — 2003. — № 36. — Ст. 275.

69. Закон України «Про телекомунікації» від 18 листопада 2003 р. [Текст] // Відомості Верховної Ради України. — 2004. — № 12. — Ст. 155.

70. Закон України «Про Національну програму інформатизації» від 04.02.1998 р. [Текст] // Відомості Верховної Ради України. — 1998. — № 27–28. — Ст. 181.

71. Закон України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р. [Текст] // Відомості Верховної Ради України. — 1998. — № 27. — Ст. 182.

72. Закон України «Про електронний цифровий підпис» від 22 травня 2003 р. [Текст] // Відомості Верховної Ради України. — 2003. — № 36. — Ст. 276.

73 Закон України «Про наукову і науково-технічну експертизу» [Текст] // Відомості Верховної Ради України. — 1995. — № 9. — Ст. 56.

74. Закон України «Про судову експертизу» [Текст] // Відомості Верховної Ради України. — 1994. — № 28. — Ст. 232.

75. Захаров, В. П. Вдосконалення організації захисту інформації від несанкціонованого доступу [Текст] / В. П. Захаров // Роль та місце ОВС у

розбудові демократичної правової держави : [матеріали Міжнародної науково-практичної конференції] (м. Одеса, 10 квітня 2009 р.). — Одеса : ОДУВС, 2009. — С. 289–291.

76. Иванов, А. Н. Использование при расследовании преступлений информации, полученной у операторов связи [Текст] : [метод. рек. для следователей и надзирающих прокуроров] / [А. Н. Иванов, И. С. Кошелева ; Прокуратура РФ]. — Саратов : Саратовская гос. акад. права, 2008. — 25, [2] с.

77. Иванова, Е. В. Технологическая модернизация российской экономики : (теоретико-методологические аспекты) [Текст] : [монография] / Е. В. Иванова. — М. : ВЗФЭИ, 2009. — 170 с.

78. Інструкція про порядок функціонування дактилоскопічного обліку експертної служби МВС України [Текст] / затверджена наказом МВС України від 19.09.2001 р. № 785 // [http://licasoft.com.ua/component/lica/?base=1&id=819586]

79. Информатика [Текст] : [учебник] / под ред. проф. Н. В. Макаровой. — М. : Финансы и статистика, 2001. — 768 с.

80. Информационно-аналитическое обеспечение раскрытия и расследования преступлений правоохранительными органами [Текст] : [материалы международной научно-практической конференции, 24–25 мая 2007 г.] / [редкол. : А. Б. Свистильников и др.]. — Белгород : БелЮИ МВД России, 2007. — 154 с.

81. История и синергетика : Методология исследования [Текст] / [отв. ред. : С. Ю. Малков, А. В. Коротаев]. — М. : КомКнига, 2005. — 184 с.

82. Калитич, Г. І. Творчість — стратегічна парадигма інноваційного розвитку [Текст] / Г. І. Калитич, В. Я. Рубан // Науково-технічна інформація. — 2003. — № 2. — С. 29–34.

83. Капани, Н. С. Волоконная оптика: принципы и применения [Текст] : [монография] / Н. С. Капани ; [пер. с англ. под ред. В. Б. Вейнберга и Д. К. Саттарова]. — М. : Мир, 1969. — 464, [2] с.

84. Каркач, П. М. Органи прокуратури України [Текст] : [навч.-метод. посіб.] / П. М. Каркач, С. М. Іванов. — Х. : СПД ФО Вапнярчук Н. М., 2007. — 360 с.

85. Каркач, П. М. Організація роботи прокуратури міста, району [Текст] : [метод. посіб.] / П. М. Каркач. — Х., 2006. — 352 с.

86. Карпенков, С. Х. Современные средства информационных технологий [Текст] : [учеб. пособие] / С. Х. Карпенков. — М. : КноРус, 2009. — 399, [1] с.

87. Карпусь, А. Інформатизація органів прокуратури: стан і перспективи [Текст] / А. Карпусь // Право України. — 2007. — № 6. — С. 89–90.

88. Синеокий, О. В. Високотехнологічна концепція інформаційного права в системі права України [Текст] / О. В. Синєокий // Вісник Донецького національного університету : [серія В. Економіка і право]. — Донецьк, 2010. — № 1. — С. 328–330.

89. Кастельс, М. Информационная эпоха : Экономика, общество и культура [Текст] / М. Кастельс ; пер. с англ. под науч. ред. О. И. Шкаратана ; [Гос. ун-т. Высш. шк. Экономики.] — М., 2000. — 606, [1] с.

90. Клементьев, А. С. Телекоммуникационное обеспечение уголовного процесса [Текст] : автореф. дис. ... канд. юрид. наук : 12.00.09 / А. С. Клементьев ; Владимир. юрид. ин-т Федер. службы исполнения наказаний. — Владимир, 2007. — 21 с.

91. Клименко, Н. І. Судова експертологія [курс лекцій] [Текст] : навч. посіб. / Н. І. Клименко. — К. : Вид. Дім «Ін Юре», 2007. — 528 с.

92. Колдин, В. Я. Информационные процессы и структуры в криминалистике [Текст] / В. Я. Колдин, Н. С. Полевой. — М. : Изд-во МГУ, 1985. — 133 с.

93. Колпаков, С. А. Организационно-правовые вопросы обеспечения информационной безопасности [Текст] : [учеб. пособие] / [С. А. Колпаков, А. Б. Лось, Е. С. Черногузов] ; М-во образования и науки Российской Федерации, Федеральное агентство по образованию, Московский гос. ин-т электроники и математики (технический ун-т). — М. : МГИЭМ, 2007. — 113 с.

94. Конвенція № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No.108 allowing the European Communities to accede), Страсбург, 28.01.1981 р. — Серія «Європейські угоди», № 108 // www.convention.coe.int/ treaty/en/Treaties/Html/108.htm. Офіційний переклад здійснено у ДКЗІ України, засвідчено МЗС України від 01.07.2002 р.

95. Концепція Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010–2014 роки [Текст] // Вісник Національної академії наук України. — 2009. — № 6. — С. 27–31.

96. Копєлєв, І. Ю. Інформаційні загрози: суть і проблеми [Текст] / І. Ю. Копєлєв // Науковий вісник Дніпропетровського державного університету внутрішніх справ : [зб. наук. праць]. — 2008. — № 3. — С. 85–98.

97. Кормич, Б. А. Організаційно-правові основи політики інформаційної безпеки України [Текст] : автореф. дис. ... д-ра юрид. наук: 12.00.07 — адміністративне право і процес, фінансове право, інформаційне право / Б. А. Кормич ; Національний університет внутрішніх справ МВС України. — Х., 2004. — 41 с.

98. Косюта, М. В. Проблеми та шляхи розвитку прокуратури України в умовах побудови демократичної правової держави [Текст] : дис. ... д-ра юрид. наук : 12.00.10 — судоустрій; прокуратура та адвокатура. / М. В. Косюта; Нац. юрид. акад. України ім. Ярослава Мудрого. — Х., 2002. — 467 с.

99. Котляр, В. В. Нанофотоника — манипулирование светом с помощью наноструктур [Текст] / В. В. Котляр // Компьютерная оптика. — 2008. — Т. 32. — № 2. — С. 119–135.

100. Кохановська, О. Галузеві розробки проблем інформації як передумова правового регулювання інформаційних відносин [Текст] / О. Кохановська // Підприємництво, господарство і право. — 2004. — № 12. — С. 144–147.

101. Кохановська, О. В. Форми захисту інформаційних прав у доктрині і законодавстві України [Текст] / О. В. Кохановська // Бюлетень Мін'юсту України. — 2006. — № 3. — С. 70–77.

102. Красноступ, Г. М. Організаційні та правові засади регулювання суспільних відносин щодо комп'ютерних програм [Текст] : автореф. дис. ... канд. юрид. наук / 12.00.07 — адміністративне право і процес, фінансове право, інформаційне право. — Ірпінь : НУДПС України, 2009. — 19 с.

103. Крылов, Э. И. Анализ эффективности инвестиционной и инновационной деятельности предприятия [Текст] / Э. И. Крылов, В. М. Власова, И. В. Журавкова. — М. : Финансы и статистика, 2003. — 608 с.

104. Кримінальний кодекс України від 05.04.2001 р. (набрав чинності з 01.09.2001 р.) [Текст] // Відомості Верховної Ради України. — 2001. — № 25–26. — Ст. 131.

105. Криминология [Текст] : [учебник для студентов высших учебных заведений, обучающихся по специальности «Юриспруденция»] / [С. В. Ванюшкин, Ю. В. Ващенко, А. Я. Гришко и др.] ; под общ. ред. А. И. Долговой. — М. : Норма, 2008. — 899 с.

106. Кузенко, Л. В. Правове регулювання права громадян на інформацію в сфері державного управління [Текст] : автореф. дис. ... канд. юрид. наук: 12.00.07 — адміністративне право і процес, фінансове право, інформаційне право / Л. В. Кузенко ; Національний університет внутрішніх справ. — Х., 2003. — 20 с.

107. Куліш, А. М. Напрямки вдосконалення інформаційного забезпечення діяльності органів прокуратури України [Текст] / А. М. Куліш // Форум права : [електронне наукове фахове видання]. — 2006. — № 3. — С. 72–76. — Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2006-3/06sovsez.pdf

108. Курочка, М. Й. Прокурорський нагляд в Україні [Текст] : [підручник] / М. Й. Курочка, П. М. Каркач ; за заг. ред. Е. О. Дідоренка. — К. : Центр навчальної літератури, 2005. — 424 с.

109. Куршев, М. Новая методика выявления педофилов [Текст] / М. Куршев // Уголовное право. — 2003. — № 4. — С. 124–126.

110. Лазарев, В. В. Основы права. Структура юридического процесса [Текст] / В. В. Лазарев // http://society.polbu.ru/lazarev_pravo/ch64_i.html

111. Лебедев, О. Волоконно-оптические компьютерные сети доступа [Текст] / О. Лебедев, В. Варгаузин // ТелеМультиМедиа. — 2002. — № 3. — С. 15–19.

112. Лебеденко, В. І. Методика інформаційно-аналітичного забезпечення планування оперативно-розшукових заходів по оперативно-розшуковій справі «Захист» [Текст] / В. І. Лебеденко // Науковий вісник Національної академії внутрішніх справ України : [Науково-теоретичний журнал. Ч. 2.] — К. : НАВСУ, 2000. — № 1. — С. 46–56.

113. Леонтьева, Л. С. Синергетический контекст масс-медийного становления [Текст] / Л. С. Леонтьева // Электронный журнал «Знание. Понимание. Умение». — 2009. — № 1 — Философия. Политология. http://www.zpu-journal.ru/e-zpu/2009/1/Leontieva/

114. Лисенко, В. В. Використання у доказовому процесі інформації, що міститься в електронному вигляді на магнітних, оптичних чи інших носіях (на матеріалах діяльності податкової міліції) [Текст] / В. В. Лисенко // Взаємодія оперативних та слідчих підрозділів при розслідуванні злочинів у сфері господарської діяльності : [матеріали Міжнародного постійно діючого науково-практичного семінару] (Ірпінь, 13 листопада 2008 р.). — Ірпінь : Національний університет ДПС України, 2009. — С. 185–198.

115. Лисенко, Г. Л. Аналіз і моделювання роботи оптичних комутаторів для високопродуктивних волоконно-оптичних мереж [Текст] / Г. Л. Лисенко, С. Є. Тужанський, Осама Ф. Ф. Абудайя // Вісник Вінницького політехнічного інституту. — 2005. — № 2. — С. 69–76.

116. Логінов, О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади [Текст] : автореф. дис. ... канд. юрид.

наук : 12.00.07 — адміністративне право і процес, фінансове право, інформаційне право. / О. В. Логінов ; Національна академія внутрішніх справ України. — К., 2005. — 22 с.

117. Лукашевич, В. Г. Криміналістика як інтегрована наукова дисципліна [Текст] / В. Г. Лукашевич // Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах : матеріали Всеукраїнської науково-практичної конференції / Запорізький юридичний інститут ДДУВС (м. Запоріжжя, 30 жовтня 2009 р.) : [у 2 ч.] — Запоріжжя : ЗЮІ ДДУВС, 2009. — Ч. І. — С. 139–141.

118. Мазур, И. И. Управление проектами [Текст] : [справочное пособие] / И. И. Мазур, В. Д. Шапира. — М. : Высшая школа, 2001. — 875 с.

119. Макиенко, А. В. Разведывательно-поисковая работа в информационной сфере: тактика и возможности [Текст] / А. В. Макиенко, А. В. Борбат // Российский следователь. — 2004. — № 12. — С. 29–35.

120. Мартинес-Дуарт, Дж. М. Нанотехнологии для микро- и оптоэлектроники [Текст] / Дж. М. Мартинес-Дуарт, Р. Дж. Мартин-Палма, Ф. Агулло-Руеда ; пер. с англ. А. В. Хачояна ; под ред. Е. Б. Якимова. — М. : Техносфера, 2007. — 367 с.

121. Марущак, А. І. Інформаційне право : регулювання інформаційної діяльності [Текст] : [навч. посіб.] / А. І. Марущак. — К. : Видавничий дім «Скіф», КНТ, 2008. — 344 с.

122. Марущак, А. І. Правові основи захисту інформації з обмеженим доступом [Текст] : [курс лекцій] / А. І. Марущак. — К. : КНТ, 2007. — 208 с.

123. Межуев, В. М. Ценности современности в контексте модернизации и глобализации [Текст] / В. М. Межуев // Знание. Понимание. Умения : [электронный журнал]. — 2009. — № 1. [http://www.zpu-journal.ru/e-zpu/2009/1/Mezhuev]

124. Мірошниченко, М. Системно-інформаційний підхід у контексті методологічного забезпечення наукового аналізу проблем теорії правової системи України [Текст] / М. Мірошниченко // Право України. — 2007. — № 6. — С. 22–25.

125. Михальчук, Т. В. Напрямки використання телекомунікаційних технологій у правоохоронній сфері [Текст] / Т. В. Михальчук // Теорія та практика судової експертизи і криміналістики : зб. наук.-практ. матеріалів ; [ред. кол. М. Л. Цимбал, В. Ю. Шепітько, Л. М. Головченко та ін.] — Х. : Право, 2006. — Вип. 6. — С. 76–82.

126. Митин, Н. А. Нанобиология и синергетика. Проблемы и идеи [Текст] / Н. А. Митин, Г. Г. Малинецкий, С. А. Науменко. — М. : Ин-т прикладной математики им. М. В. Келдыша РАН, 2005. — 31 с.

127. Мотлях, О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій [Текст] : автореф. дис. ... канд. юрид. наук : 12.00.09 — кримінальний процес та криміналістика; судова експертиза / О. І. Мотлях ; Академія адвокатури України. — К., 2005. — 20 с.

128. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 24.04.2007 р. № 72 «Про затвердження Порядку формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» [Текст] // Офіційний вісник України. — 2007. — № 35. — Ст. 1400.

129. Наказ Державного комітет України з питань регуляторної політики та підприємництва «Про розмір плати за послуги Депозитарію примірників дисків для лазерних систем зчитування» від 07.07.2003 р. № 75.

130. Наказ МВС України № 786 від 17 липня 2003 р. «Про створення Інтегрованої інформаційно-пошукової системи ОВС України» // [http://licasoft.com.ua/component/lica/?base=1&id=819586]

131. Нанотехнологии и информационные технологии — технологии XXI века [Текст] : [материалы Международной научно-практической конференции] / [редсовет : Назаров Ю. Ф. (пред.) и др.] — М. : Изд-во МГОУ, 2006. — 247 с.

132. Настольная книга следователя. Книга 3 : Расследование преступлений против личности (убийство, торговля людьми) [Текст] : [науч.-метод. пособие] / [Р. А. Адельханян, В. Н. Исаенко, Ю. М. Самойлов и др. ; под ред. А. И. Дворкина и А. Б. Соловьева]. — М. : Экзамен, 2007. — 589 с.

133. Невлюдов, І. Ш. Інформаційні оптоволоконні мережі зв'язку банківських систем [Текст] : [навч. посібник] / І. Ш. Невлюдов, Б. О. Малик, М. А. Омаров та ін. ; Науково-методичний центр вищої освіти; Харківський національний ун-т радіоелектроніки. — Х. : ХНУРЕ, 2004. — 232 с.

134. Ніндипова, В. Нагляд за додержанням законів органами, які проводять оперативно-розшукову діяльність: Конституційно-правовий аспект [Текст] / В. Ніндипова // Вісник прокуратури. — 2007. — № 2. — С. 52–60.

135. Новая криминальная ситуация : оценка и реагирование [Текст] / Общероссийская общественная орг. «Российская криминологическая ассоц.», Акад. Генеральной прокуратуры Российской Федерации ; [редкол. : А. И. Долгова (отв. ред.) и др.]. — М. : Российская криминологическая ассоциация, 2009. — 356 с.

136. Об утверждении Правил формирования, корректировки и реализации приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации [Текст] // Постановление Правительства РФ от 22.04.2009 г. № 30. http://www.russianpeople.ru/en/old/135629

137. Овчинский, В. С. XXI век против мафии : Криминальная глобализация и Конвенция ООН против транснациональной организованной преступности [Текст] / В. С. Овчинский. — М. : Инфра-М, 2001. — 146, [1] с.

138. Овчинский, А. С. Информация и оперативно-розыскная деятельность [Текст] : [монография] / А. С. Овчинский ; Моск. ин-т МВД России. — М. : Инфра-М, 2002. — 95, [2] с.

139. Овчинский, А. С. Правоохранительные инфотехнологии [Текст] : [науч. доклад] / А. С. Овчинский. — М. : Норма, 2009 (Казань : ПИК Идел-Пресс). — 142 с.

140. Одрін, В. Технологія наукової і технічної творчості : нова наука та високоінтелектуальна інформаційна метатехнологія [Текст] / В. Одрін // Вісник Національної академії наук України. — 2005. — № 6. — С. 43–64.

141. Оліфіренко, М. М. Новітні інформаційні технології як інструмент міжнародного тероризму [Текст] : [аналіт. нотатки] / М. М. Оліфіренко. — К. : МаНІ, 2004. — 75 с.

142. Оптическая связь [Текст] : [пер. с яп. И. А. Фомичева / под ред. И. И. Теумина]. — М. : Радио и связь, 1984. — 384 с.

143. Організаційно-правові основи захисту інформації з обмеженим доступом [Текст] : [навч. посіб.] / А. Б. Стоцький, А. М. Гуз, А. І. Марущак та ін.; за заг. ред. Сідака В. С. — К. : Вид-во Європейського ун-ту, 2006. — 232 с.

144. Орлов, П. І. Інформація та інформатизація : Нормативно-правове забезпечення [Текст] : [наук.-практ. посіб.] / П. І. Орлов . — Х. : Вид-во ун-ту внутрішніх справ, 2000. — 576 с.

145. Орлов, С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах [Текст] : автореф.

дис. ... канд. юрид. наук ; 12.00.08 — кримінальне право та кримінологія; кримінально-виконавче право. / С. О. Орлов ; Національний університет внутрішніх справ. — Х. : НУВС, 2004. — 20 с.

146. Оружие России : Федеральный электронный справочник вооружения и военнной техники — 24.11.2009 г. http://www.arms-expo.ru/site.xp/049057054050124051053057050. html

147. Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки, затверджені Законом України від 9 січня 2007 р. № 537 [Текст] // Відомості Верховної Ради України — 2007. — № 12. — Ст. 102.

148. Основи інформаційного права України [Текст] : [навч. посіб.] / [В. С. Цимбалюк, В. Д. Гавловський, В. В. Гриценко та ін. ; за ред. М. Я. Швеця, Р. А. Калюжного та П. В. Мельника]. — К. : Знання, 2004. — 274 с.

149. Павлютенков, А. А. Модель и метод логического контроля использования стандартов информационной безопасности в критически важных системах информационно-телекоммуникационной инфраструктуры [Текст] : автореф. дис. ... канд. техн. наук : 05.13.19 — методы и системы защиты информации, информационная безопасность. / А. А. Павлютенков ; С.-Петерб. гос. ун-т информац. технологий, механики и оптики. — СПб., 2008. — 20 с.

150. Пастухов, О. М. Авторське право у сфері функціонування всесвітньої інформаційної мережі Інтернет [Текст] : дис. ... канд. юрид. наук: 12.00.03 — цивільне право і цивільний процес; сімейне право; міжнародне приватне право. / О. М. Пастухов ; Національний педагогічний ун-т ім. М. П. Драгоманова. — К., 2002. — 173 с.

151. Патон, Б. Нанонаука і нанотехнології: технічний, медичний та соціальний аспекти [Текст] / Б. Патон, В. Москаленко, І. Чекман та ін. // Вісник Національної академії наук України. — 2009. — № 6. — С. 18–26.

152. Петров, Є. В. Інформація як об'єкт правовідносин [Текст] / Є. В. Петров // Вісник Національного університету внутрішніх справ; Спецвипуск. — Х., 2001. — С. 249–252.

153. Пиявский, С. Информатизация сферы культуры и молодежной политики [Текст] / С. Пиявский // Проблемы теории и практики управления. — 2008. — № 10. — С. 65–73.

154. Погорецький, М. А. Судовий контроль та прокурорський нагляд за використанням протоколів оперативно-розшукової діяльності в кримінальному процесі [Текст] / М. А. Погорецький // Вісник Верховного Суду України. — 2003. — № 2. — С. 36–39.

155. Погорецький, М. А. Щодо визначення поняття матеріали оперативно-розшукової діяльності [Текст] / М. А. Погорецький // Вісник прокуратури. — 2007. — № 12. — С. 49.

156. Погосов, В. В. Введение в физику зарядовых и размерных эффектов. Поверхность, кластеры, низкоразмерные системы [Текст] : [учеб. пособие]. — М. : Физматлит, 2006. — 328 с.

157. Покутний, С. И. Оптика наносистем [Текст] : [монография] / С. И. Покутний, В. А. Сминтина, А. П. Шпак та ін. — Одесса : Астропринт, 2007. — 304 с.

158. Политология [Текст] : [учебник] / под ред. В. И. Буренко, В. В. Журавлева. — М. : Экзамен, 2004. — 320 с.

159. Полотнянко, Л. И. Современные высокие технологии и автоматизированные системы в лабораторной службе [Текст] : [учеб. пособие] / Л. И. Полотнянко. — М. : ВУНМЦ Росздрава, 2008. — 361 с.

160. Полякова, М. В. Шляхи вирішення проблеми пошуку графічної інформації на персональному комп'ютері [Текст] / М. В. Полякова, В. С. Рукавішніков // Теорія та практика судової експертизи і криміналістики : зб. наук.-практ. матеріалів ; [ред. кол. М. Л. Цимбал, В. Ю. Шепітько, Л. М. Головченко та ін.] — Х. : Право, 2006. — Вип. 6. — С. 238–243.

161. Попов, А. М. Вычислительные нанотехнологии [Текст] : [учеб. пособие] / А. М. Попов ; Московский гос. ун-т им. М. В. Ломоносова. — М. : МАКС Пресс, 2009. — 279, [1] с.

162. Попов, В. Д. Государственная информационная политика: состояние и проблемы формирования [Текст] / В. Д. Попов // Массовые информационные процессы в современной России. — М. : РАГС, 2002. — С. 18.

163. Постанова Верховної Ради України № 1786-IV від 16.06.2004 р. «Про дотримання законодавства щодо розвитку науково-технічного потенціалу та інноваційної діяльності в Україні» [Текст] // Інтелектуальна власність. 2004. — № 8. — С. 68–72.

164. Постанова Кабінету Міністрів України від 12.04.2000 р. № 644 «Про затвердження Порядку формування та виконання регіональної програми і проекту інформатизації» [Текст] // Офіційний вісник України. — 2000. — № 16. — Ст. 669.

165. Постанова Кабінету Міністрів України від 24.01.2005 р. № 91 «Про генерального державного замовника і керівника Національної програми інформатизації» [Текст] // Офіційний вісник України. — 2005. — № 4. — Ст. 224.

166. Постанова Кабінету Міністрів України від 3 серпня 2005 р. № 688 «Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» [Текст] // Офіційний вісник України. — 2005. — № 31. — Т. 2. — Ст. 1869.

167. Постанова Кабінету Міністрів України від 9 серпня 2005 р. № 720 «Про затвердження Правил надання та отримання телекомунікаційних послуг» [Текст] // Офіційний вісник України. — 2005. — № 32. — Ст. 1935.

168. Постиндустриальная цивилизация и культура управления [Текст] : [монография] / [В. Е. Амелин и др.; под общ. ред. Г. Я. Узилевского]. — Орел : Изд-во ОРАГС, 2005. — 247 с.

169. Проекти нормативно-правових документів та пропозицій з питань формування і реалізації державної політики у сфері євроатлантичної інтеграції України [Текст] : [наук.-інформ. зб.] / В. П. Горбулін (заг. ред.), Ю. М. Романов (підгот.) / Національний центр з питань євроатлантичної інтеграції України. — К. : ДП «НВЦ “Євроатлантикінформ”», 2006. — 336 с.

170. Про кібернетичну злочинність : Конвенція Ради Європи ; [офіційний переклад українською мовою] [Текст] // Лист МЗС України від 24 травня 2004 р. № 91/14-761/1-1161 // http://zakon.nau.ua/doc/?code=994_575

171. Прокопенко, А. Н. Правовая защита информации (информационное право) [Текст] : [учеб. пособие] / А. Н. Прокопенко, А. А. Кривоухов. — Белгород : Изд-во БелГУ, 2007. — 220, [1] с.

172. Прокуратура України : Академічний курс [Текст] : [підручник] / В. В. Сухонос, В. П. Лакизюк, Л. Р. Грицаєнко та ін. ; за заг. ред. В. В. Сухоноса. — Суми : ВТД «Університетська книга», 2005. — 566 с.

173. Прослушивание телефонов в международном праве и законодательстве одиннадцати европейских стран [Текст] / Харьковская правозащитная группа ; сост. Є. Є. Захаров. — Харьков, 1999. — 92 с.

174. Про схвалення Концепції Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов’язана з боротьбою із злочинністю [Текст] / Розпорядження Кабінету Міністрів України від 19 вересня 2007 р. № 754-р // Офіційний вісник України. — № 71. — 2007 [http://www.ovu.com.ua]

175. Про схвалення Концепції Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010–2014 рр. [Текст] / Розпорядження Кабінету Міністрів України від 3 квітня 2009 р. № 331-р // Офіційний вісник України. — № 26. — 2009 (17.04.2009).

176. Ратнер, М. Нанотехнология : простое объяснение очередной гениальной идеи = Nanotechnology : A Gentle Introduction To The Next Big Idea [Текст] : пер. с англ. / Марк Ратнер, Даниэль Ратнер ; [пер. и ред. А. В. Назаренко]. — М. : Издательский дом «Вильямс», 2004 ; Москва — Санкт-Петербург — Киев, 2007. — 240 с.

177. Розенфельд, Н. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів) [Текст] / Н. Розенфельд // Вісник прокуратури. — 2002. — № 4. — С. 23–27.

178. Романюк, Б. Прокурорський нагляд, «судовий» та відомчий контроль за діяльністю слідчого [Текст] / Б. Романюк // Прокуратура. Людина. Держава. — 2004. — № 6. — С. 51–59.

179. Рудейчук, В. Суть прокурорського нагляду [Текст] / В. Рудейчук // Вісник прокуратури. — 2003. — № 4. — С. 49–52.

180. Санакоєв, Д. Б. Взаємодія правоохоронних органів МВС при розслідуванні організованої діяльності у сфері торгівлі людьми [Текст] / Д. Б. Санакоєв // Вісник Запорізького юридичного інституту ДДУВС : [зб. наук. праць]. — Запоріжжя, 2008. — № 2. — С. 192–201.

181. Свирина, М. В. Управление информационно-аналитическим обеспечением органов внутренних дел в сфере борьбы с экономическими преступлениями [Текст] : автореф. дис. ... канд. эконом. наук : 08.00.05 — экономика и управление народным хозяйством. / М. В. Свирина ; Место защиты: Акад. экон. безопасности МВД РФ. — М., 2007. — 24 с.

182. Сегай, М. Я. Сучасна парадигма інформатизації судочинства і питання захисту прав і законних інтересів учасників кримінального процесу [Текст] / М. Я. Сегай // Вісник Академії правових наук України. — 2001. — № 4. — С. 191.

183. Синеокий, О. В. Адвокатура как институт правовой помощи и защиты: проблемы становления и перспективы развития [Текст] : [монография] / О. В. Синеокий : [передм. д-ра юрид. наук Т. О. Коломоєць]. — Запорожье : ЗНУ, 2007. — 429, [2] с.

184. Синєокий, О. В. Інноваційний проект «Електронний кабінет криміналістики» (концептуальне обґрунтування перспектив впровадження в діяльність прокурорів-криміналістів волоконно-оптичних та Грід-технологій)

[Текст] / О. В. Синєокий // Вісник Запорізького юридичного інституту ДДУВС : [зб. наук. праць]. — Запоріжжя, 2009. — № 4.

185. Синєокий, О. В. Інформаційні технології кримінопереверсологічного моніторингу : інноваційний підхід розвитку [Текст] / О. В. Синєокий // Право на приватність: тенденції і перспективи : [тези Всеукраїнської науково-практичної конференції] / [м. Львів, 14 листопада 2008 р.]. — Львів : Львівський державний університет внутрішніх справ, 2008. — С. 175–178.

186. Синєокий, О. В. Інформаційне право України [Текст] : [навч. посіб.] / О. В. Синєокий. — Запоріжжя : ЗНУ, 2008. — 100 с.

187. Синєокий, О. В. Інформаційне право України : інформаційно-телекомунікаційні технології в прокурорській діяльності [Текст] : [навч. посіб.] / О. В. Синєокий. — Запоріжжя : ЗНУ, 2009. — 191, [3] с.

188. Синєокий, О. В. Курс лекцій з інформаційного права України та основ електронного права високих технологій [Текст] : електронний конспект [e-text CD-R] / О. В. Синєокий ; Запорізький національний університет. – Запоріжжя : ЗНУ, 2010. – 215 ел. с. = 15 ум. друк. арк. : іл. ; сх. – Систем. вимоги : WINDOWS 2000/ NT/XP http://sites.znu.edu.ua/lectory/ ; Донецьк : Донецька обласна універсальна наукова бібліотека ім. Н. К. Крупської – http://www.library.donetsk.ua/; Київ : Національна бібліотека України ім. В. І. Вернадского – http://www.nbuv.gov.ua/

189. Синєокий, О. В. Міждержавні спеціалізовані слідчо-оперативні групи : окремі психолого-організаційні проблеми [Текст] / О. В. Синєокий // Міжнародний постійно діючий науково-практичний семінар «Взаємодія оперативних та слідчих підрозділів при розслідуванні злочинів у сфері господарської діяльності» : [тези доповідей] / Національний університет державної податкової служби України. Кафедра фінансових розслідувань ; (м. Ірпінь, 13 листопада 2008 р.) — К. : НУДПС, 2008. — С. 369–383.

190. Синеокий, О. В. Межгосударственные специализированные следственно-оперативные группы по расследованию транснациональных преступлений, совершенных на сексуальной почве [Текст] / О. В. Синеокий // Уголовное право. — М. : [Академия Генеральной прокуратуры РФ]. — 2009. — № 2. — С. 115–121.

191. Синеокий, О. В. Мониторинг транснациональной педофилии [Текст] / О. В. Синеокий // Психопедагогика в правоохранительных органах. — Омск : [Омская академия МВД России]. — 2009. — № 3. — С. 34–39.

192. Синєокий, О. В. Нанонаука — розвитку судово-експертних технологій [Текст] / О. В. Синєокий // Вісник Запорізького національного універ-

ситету : [зб. наук. стат.] / юридичні науки. — Запоріжжя, 2009. — № 2. — С. 137–142.

193. Синєокий, О. В. Нанотехнологічні методики виявлення латентних слідів та дослідження мікрооб'єктів — криміналістичні інновації майбутнього [Текст] / О. В. Синєокий // «Держава і право : De Lege Praeterita, Instante, Futura» [матеріали Міжнародної науково-практичної конференції «П'яті Прибузькі юридичні читання»] ; (м. Миколаїв, 27–28 листопада 2009 р.) / за заг. ред. О. В. Козаченка ; [Одеська національна юридична академія]. — Миколаїв : Ілліон, 2009. — С. 298–299.

194. Синеокий, О. В. Новые технологии расследования следственно-оперативными группами транснациональной торговли людьми и похищения детей в сексуальное рабство в Содружестве Независимых Государств [Текст] / О. В. Синеокий // Региональный вестник Востока. — Усть-Каменогорск : [Восточно-Казахстанский государственный университет]. — 2008. — № 3. — С. 31–37.

195. Синєокий, О. В. Новые технологические решения специализации межгосударственных следственно-оперативных групп по расследованию многоэпизодных транснациональных преступлений, совершаемых на сексуальной почве [Текст] / О. В. Синєокий // Форум права : електронне наукове фахове видання. — 2009. — № 1. — С. 498–504 [Електронний ресурс]. — Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2009-1/09 sovsez.pdf

196. Синєокий, О. В. Організаційно-правові проблеми нанотехнології [Текст] / О. В. Синєокий // Міжнародна щорічна науково-практична конференція «Запорізькі правові читання» : [тези доповідей] / Запорізький національний університет ; (м. Запоріжжя, 14–15 травня 2010 р.). — Запоріжжя : ЗНУ, 2010. — С. 116–119.

197. Синєокий, О. В. Правоохоронна та правозахисна діяльність в Україні [Текст] / О. В. Синєокий // Правознавство : [навч. посіб.] / [О. Г. Бондарь, О. М. Губрієнко, Г. Ю. Гулєвська та ін. ; за заг. ред. С. М. Тимченка, Т. О. Коломоєць]. — К. : Істина, 2007. — С. 437–472.

198. Синєокий, О. В. Перспективи впровадження волоконно-оптичних технологій в інфокриміналістику прокурорської діяльності [Текст] / О. В. Синєокий // Проблеми удосконалення законодавства і практики протидії злочинності у сфері господарської діяльності : [зб. наук. праць за матеріалами Міжнародного науково-практичного семінару] ; (м. Ірпінь, 10 грудня 2009 р.) / Національний університет ДПС України, НДІ фінансового права. — К. : Вік прінт, 2009. — С. 199–207.

199. Синєокий, О. В. Прокуратура України як контрольно-наглядова інституція у сфері боротьби зі злочинністю. Психологія прокурора-криміналіста [Текст] : [навч. посіб. з психологічним словником прокурора-криміналіста] / О. В. Синєокий. — Запоріжжя : ЗНУ, 2009. — 263, [2] с.

200. Синеокий, О. В. Психолого-акмеологические начала двойственности профессии прокурора-криминалиста [Текст] / О. В. Синеокий // Психопедагогика в правоохранительных органах. — Омск : [Омская академия МВД России]. — 2010. — № 1. — С. 3–7.

201. Синєокий, О. В. Психологічні аспекти прокурорського нагляду за забезпеченням законності слідчо-оперативної діяльності. Досвід прокурора-криміналіста (за матеріалами умисних убивств) [Текст] : [монографія] / О. В. Синєокий ; [передм. — прокурор Запорізької області, державний радник юстиції 3 класу, канд. юрид. наук В. В. Кулаков]. — Запоріжжя : ЗНУ, 2009. — 445, [2] с.

202. Синєокий, О. В. Психолого-правові проблеми кримінальної сексопатології. Вступ до кримінопереверсології [Текст] : [монографія] / О. В. Синєокий ; [передм. д-р юрид. наук О. О. Дудорова]. — Х. : Право, 2009. — 752 с.

203. Синєокий, О. В. Психологічні особливості управління міжвідомчими слідчо-оперативними групами [Текст] / О. В. Синєокий // Вісник прокуратури. — К., 2008. — № 3. — С. 72–80.

204. Синєокий, О. В. Психологічні проблеми прийняття рішень слідчо-оперативною групою [Текст] / О. В. Синєокий // Науковий вісник Дніпропетровського державного університету внутрішніх справ : [зб. наук. ст.]. — Дніпропетровськ, 2008. — № 3. — С. 272–278.

205. Синеокий, О. В. Системные процессы минимизации социально-опасных проявлений педофильного поведения в информационной среде = Sineokyi, O. V. System Tasks Of Minimazation Socially Dangerous Displays Of Paedophilic Conduct In The Informedia [Текст] / О. В. Синеокий = O. V. Sineokyi // Power. Man. Law. : International juridical scientific magazine. — 2009. — № 1. — С. 28–37 = P. 87–95.

206. Синєокий, О. В. Системні медико-психологічні підходи до мінімізації патосексуальних проявів в інтернет-просторі [Текст] / О. В. Синєокий // Психологія і суспільство. — Тернопіль, 2009. — № 2. — С. 122–127.

207. Синєокий, О. В. Системні інформаційно-правові та медико-педагогічні заходи профілактики «фонових» явищ патосексуальної віктимізації молоді [Текст] / О. В. Синєокий // Вісник Запорізького національного

університету : [зб. наук. ст.] / Педагогічні науки. — Запоріжжя, 2009. — № 1. — С. 140–146.

208. Синєокий, О. В. Системні організаційно-інформаційні проблеми діяльності міждержавних змішаних спеціалізованих слідчо-оперативних груп в сучасних умовах [Текст] / О. В. Синєокий // Міжнародна науково-практична конференція «Четверті Прибузькі юридичні читання» : «Сучасний вимір держави та права» [зб. наук. ст.] ; (м. Миколаїв, 29 листопада 2008 р.) / за ред. В. І. Терентьєва та О. В. Козаченка ; [Одеська національна юридична академія]. — Миколаїв : Ілліон, 2008. — С. 137–139.

209. Синєокий, О. В. Стратегії інноваційного проектування волоконно-оптичних технологій в криміналістиці [Текст] / О. В. Синєокий // Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах [Текст] : [матеріали Всеукраїнської науково-практичної конференції] / Запорізький юридичний інститут ДДУВС (м. Запоріжжя, 30 жовтня 2009 р.) : [у 2 ч.] — Запоріжжя : ЗЮІ ДДУВС, 2009. — Ч. І. — С. 162–165.

210. Синєокий, О. В. Теоретичні та практичні проблеми діяльності міждержавних змішаних слідчо-оперативних груп [Текст] / О. В. Синєокий // Криміналістичний вісник / НДЕКЦ МВС України. — 2009. — № 1(11) — С. 44–51.

211. Системна інформатизація законотворчої та правоохоронної діяльності [Текст] : [монографія] / [В. Буржинський, Б. Раціборинський, М. Целуйко та ін.; кер. авт. кол. М. Я. Швець ; за ред. В. В. Дурдинця]. — К. : Навч. книга, 2005. — 639 с.

212. Системна інформатизація правоохоронної діяльності [Текст] : [у 2 кн.] / Кн. 2 : Європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності / М. Швець (ред. та упоряд.), Б. Романюк (ред.) ; Науково-дослідний центр правової інформатики Академії правових наук України ; Департамент інформаційних технологій МВС України. — К. : НДЦПІ АПрН України, 2006 — 510 с.

213. Семенов, Г. В. Расследование преступлений в сфере мобильных телекоммуникаций [Текст] / Г. В. Семенов. — М. : Юрлитинформ, 2008. — 333, [3] с.

214. Сергеев, Г. Б. Нанохимия [Текст] : [учеб. пособие] / Г. Б. Сергеев. — М. : Изд-во МГУ, 2003. — 288 с.

215. Середа, Г. Концептуальні засади наукового забезпечення інформатизації прокуратури [Текст] / Г. Середа, І. Рогатюк, В. Цимбалюк // Вісник прокуратури. — 2006. — № 5. — С. 14–19.

216. Скалозуб, Л. П. Інтелектуалізація злочинності. Варіант стримування [Текст] / [Л. П. Скалозуб, В. М. Бутузов] // Боротьба з організованою злочинністю і корупцією. — 2004. — № 9. — С. 193–198.

217. Словник термінів інформаційного права [Текст] / упоряд. А. І. Марущак ; заг. ред. М. Я. Швеця. — К. : КНТ, 2008. — 184 с.

218. Спирин, В. Варианты реализации широкополосной сети по технологии «волокно в дом» [Текст] / В. Спирин // ТелеМультиМедиа. — 2002. — № 3. — С. 11–14.

219. Стрельбицька, Л. М. Основи безпеки банківської системи України та банківської діяльності [Текст] : [монографія] / Л. М. Стрельбицька, М. П. Стрельбицький ; за ред. М. П. Стрельбицького. — К. : Кондор, 2004. — 600 с.

220. Стрельбицький, М. Нанотехнології в Україні як засіб боротьби з міжнародним тероризмом [Текст] / М. Стрельбицький, М. Вертузаєв, О. Юрченко // Інтелектуальна власність. — 2004. — № 12. — С. 23–29.

221. Суходубов, В. С. Успішне розкриття і розслідування злочинів, пов'язаних з торгівлею людьми [Текст] / В. С. Суходубов // Слідча практика України: із досвіду слідчої роботи органів прокуратури [Східно-регіональний центр гуманітарно-освітніх ініціатив]. — 2003. — № 3. — С. 44–47.

222. Сухонос, В. В. Прокуратура України у схемах, таблицях і діаграмах [Текст] : [навч. посіб.] / В. В. Сухонос, О. Є. Звірко, Л. Р. Грицаєнко ; за заг. ред. В. В. Сухоноса. — Суми : ВТД «Університетська книга», 2006. — 256 с.

223. Требін, М. Інформаційне суспільство. Війни нової епохи [Текст] / М. Требін // Віче. — 2002. — № 4 (121). — С. 64–68.

224. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы [Текст] : автореф. дис. ... канд. юрид. наук : 12.00.08 — уголовное право и криминология; уголовно-исполнительное право / Т. Л. Тропина ; Дальневост. гос. ун-т. — Владивосток, 2005. — 26 с.

225. Указ Президента України від 31.07.2000 р. № 928/2000 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» // http://zakon.nau.ua/doc/?code=928/2000

226. Указ Президента України від 24 вересня 2001 р. № 891/2001 «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» [Текст] // Офіційний Вісник України. — 2001. — № 39. — Ст. 1757.

227. Указ Президента України «Про створення Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю» від 31.01.2006 р., № 80/2006 [Текст] // Офіційний вісник України. — 2006. — № 5. — Ст. 212.

228. Федоров, В. Прокурорский надзор и оперативно-розыскная деятельность [Текст] / В. Федоров // Социалистическая законность. — 1990. — № 6. — С. 35–36.

229. Фостер, Л. Нанотехнологии. Наука, инновации и возможности [Текст] / Л. Фостер ; [пер. с англ. А. Хачояна]. — М. : Техносфера, 2008. — 349 с.

230. Фролков, В. Н. Разработка специальных типов оптических волокон для систем управления [Текст] : автореферат дис. ... канд. техн. наук : 05.11.07 — оптические и оптико-электронные приборы и комплексы / В. Н. Фролков ; С.-Петерб. гос. ун-т информац. технологий, механики и оптики. — СПб., 2007. — 19 с.

231. Хараберюш, І. Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій [Текст]: [монографія] / І. Ф. Хараберюш, В. Я. Мацюк, В. А. Некрасов та ін. — К. : КНТ, 2007. — 196 с.

232. Хлынцов, М. Н. Криминалистическая информация и моделирование при расследовании преступлений [Текст] : [учеб. пособие] / М. Н. Хлынцов ; под ред. В. Г. Власенко. — Саратов : Изд-во Сарат. ун-та, 1982. — 159 с.

233. Хрипко, С. Л. Інформаційне право [Текст] : [навч.-метод. посіб.] / С. Л. Хрипко. — Донецьк: ТОВ «Юго-Восток, Лтд», 2005. — 234 с.

234. Цимбалюк, В. Роль правової інформатики у модернізації прокуратури України [Текст] / В. Цимбалюк // Право України. — 2006. — № 11. — С. 73–77.

235. Цимбалюк, В. Щодо формування стратегії інформатизації прокуратури України в умовах розвитку інформаційного суспільства [Текст] / В. Цимбалюк // Вісник прокуратури. — 2007. — № 5. — С. 92–99.

236. Шарупич, Л. С. Оптоэлектроника [Текст] : [учебник] / Л. С. Шарупич, Н. М. Тугов. — М. : Энергоатомиздат, 1984. — 256 с.

237. Швець, М. Правова інформатика [Текст] : [підручник] / М. Швець, В. Брижко, В. Фурашев та ін. ; В. Дурдинець (ред.) ; Науково-дослідний центр правової інформатики Академії правових наук України. — 2-ге вид., доп. та перероб. — К. : ТОВ «ПанТот», 2007. — 524 с.

238. Шевченко, Є. Концепція інформаційного забезпечення прокурорської діяльності [Текст] / Є. Шевченко, О. Червякова // Вісник прокуратури. — 2003. — № 2. — С. 119–122.

239. Шевчук, Р. Сутність та зміст поняття «інформатизація» в інформаційно-правовій сфері [Текст] / Р. Шевчук // Право України. — 2006. — № 11. — С. 103–108.

240. Шеломенцев, В. П. Фіксація фактичних даних про протиправні діяння у мережі Інтернет [Текст] / В. П. Шеломенцев // Науковий вісник Дніпропетровського державного університету внутрішніх справ : [зб. наук. праць]. — 2007. — Спеціальний випуск № 1 (36) «Актуальні питання протидії злочинності». — С. 342–347.

241. Шинальський, О. Комп'ютерізація органів прокуратури України: сьогодення та перспективи [Текст] / О. Шинальський // Вісник прокуратури. — 2003. — № 4. — С. 3–7.

242. Юрченко, А. М. К вопросу определения терминологии и базовых понятий положения идентификации в теории судебной экспертизы для решения задач предупреждения и раскрытия экономических преступлений [Текст] / А. М. Юрченко // матеріали міжнар. наук.-практ. семін. «Сучасні технології у судовій акустиці» (Україна, Київ, 17–18 жовтня 2002 р.). — К. : Національна академія внутрішніх справ України, 2003. — С. 46–56.

243. Юрченко, А. М. Попередження злочинів у сфері інтелектуальної власності і високих технологій : погляд у майбутнє [Текст] / А. М. Юрченко // Бізнес і безпека. — 2004. — № 5 (43). — С. 4–6.

244. Юрченко, О. М. Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту [Текст] : [монографія] / О. М. Юрченко, В. О. Голубєв; під ред. О. П. Снігерьова, М. С. Вертузаєва. — Запоріжжя: ОЦ «Павло», 1998. — 157 с.

245. Юрченко, О. М. Шахрайства з використанням пластикових платіжних карток // Тіньова економіка та організована економічна злочинність [Текст] : [навч. посіб.] / [Сущенко В. Д. (наук. кер. авт. кол.), Баліна С. Н., Белецький В. О., Юрченко О. М. та ін.] ; під ред. В. А. Предборського. — К. : НАВСУ, 1999. — С. 309–336.

246. Якимчук, М. К. Організаційно-правові основи управління в органах прокуратури України [Текст] : дис. ... д-ра юрид. наук : 12.00.07 — адміністративне право і процес, фінансове право, інформаційне право / М. К. Якимчук ; Ін-т держави і права ім. В. М. Корецького НАН України. — К., 2002. — 396 с.

247. www.chemistry.ru
248. http://www.bioinformatix.ru/grid-superkompyuter-/primenenie-superkomp yuterov.html
249. http://naukainform.kpi.ua/Lists/List4/DispForm.aspx?ID=7
250. http://refu.ru/refs/88/30724/1.html
251. http://www.gridclub.ru/about/. Концепция GRID
252. http://instzak.rada.gov.ua/instzak/doccatalog/document?id=46630
253. http://law.edu.ru/article/article.asp?articleID=1148657
254. http://ru.wikipedia.org/wiki/
255. http://www.gsmrepiter.ru/articles/?id=141
256. http://dic.academic.ru/dic.nsf/lower/17375

АННОТАЦИЯ

На монографическом уровне характеризуются основы политики концептуального развития нанотехнологий и модернизации систем передачи информации в сфере борьбы с преступностью.

Раскрываются основы правового регулирования волоконно-оптических технологий, использующихся в информационно-телекоммуникационных системах. Впервые в отечественной литературе отдельное внимание уделено системному исследованию организационно-правовых особенностей информационных технологий, наноиндустрии и новых электронных систем интеллектуальной обработки информации в области противодействия преступности. Определены инновационные перспективы применения высоких технологий по сдерживанию информационной преступности.

Предназначено для углубленного изучения учебных дисциплин «Информационное право», «Правовое регулирование информационной безопасности» и других соответствующих спецкурсов, которые изучаются студентами юридических факультетов и неюридических специальностей высших учебных заведений. Предлагаемый материал не дублирует ранее опубликованные работы, отсюда эта работа может стать полезной для ученых и практических специалистов защиты информации.

ANNOTATION

At the monographic level the author characterizes the basis of the politic of the nanotechnologies conception development and the modernization of systems of the transmitting the information in the sphere of criminal fighting.

The author opens the basis of the law regulation of the fiber-optical technologies which are used in the information-telecommunication systems activity. For the first time in the national literature the special consideration is given to the systematic investigation of the judicially organized peculiarities of the informatics technology, the nanoindustry and new electronic systems of the intellectual treat of the information in the field of criminal counteractions. In this work it is marked the innovational perspectives of using higher technologies of the determined criminality in the sphere of information.

This work is recommended for deeper studying of such disciplines as «The Informatics Law», «The Law regulation of the informational security» & other proper special courses which are studying by students of law departments and non-juridical specialties of the higher education establishments. This material does not duplicate the ones published earlier. This work may be used by scientists and practical specialists who work in the sphere of protecting information.

Зміст

Розділ 4
Органи прокуратури
як спеціальні суб'єкти
високотехнологічного інформаційного права

Розділ 5
Нанотехнологія як особливий об'єкт
високотехнологічного інформаційного права

Навчальне видання

Синєокий
Олег Володимирович

ВИСОКОТЕХНОЛОГІЧНЕ ІНФОРМАЦІЙНЕ ПРАВО УКРАЇНИ

Навчальний посібник

Редактор *К. К. Гулий*
Коректор *Т. Ф. Зуб*
Комп'ютерна верстка *О. І. Євтєєвої*
Дизайн *В. М. Зеленька*

Підписано до друку з оригінал-макета 07.09.2010.
Формат 60×84 $^{1}/_{16}$. Папір офсетний. Гарнітура Times.
Ум. друк. арк. 20,9. Обл.-вид. арк. 18. Вид. № 491.
Тираж 300 прим.

Видавництво «Право» Академії правових наук України
Україна, 61002, м. Харків, вул. Чернишевська, 80

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції.
Серія ДК № 559 від 09.08.2001 р.

Виготовлено у друкарні ФОП Шевчун О. М.
(057) 719-49-13