

УДК 35.078.3 : 343.451 : 044 (477) (075.8)
ББК Х 9 (4 Укр) 304.4 я 73
С 382

О. В. Синєокий

ІНФОРМАЦІЙНЕ ПРАВО УКРАЇНИ ТА ЕЛЕКТРОННЕ ПРАВО ВИСОКИХ ТЕХНОЛОГІЙ

Електронний курс лекцій

3 01 квітня 2010 р. розміщено на сайті Національної бібліотеки України ім. В.І. Вернадського

Електронна адреса: <http://www.nbuv.gov.ua/>

Електронний курс лекцій розроблено на підставі Робочої програми з навчальної дисципліни «Інформаційне право», затвердженої науково-методичною радою юридичного факультету (Протокол №1 від 1.09.2009 р.), ґрунтуючись на матеріали навчальних посібників:

- 1. Синєокий О.В. Інформаційне право (2008),*
- 2. Синєокий О.В. Інформаційне право України: інформаційно-телекомунікаційні технології в прокурорській діяльності (2009),*
- 3. Синєокий О.В. Високотехнологічне інформаційне право (2010),*
рекомендованих до друку Вченою радою Запорізького національного університету (Протоколи №10 від 26.06.2008 р. та №5 від 25.12.2009 р.)

Рецензенти:

Завідуюча кафедрою адміністративного та господарського права
Запорізького національного університету,
доктор юридичних наук, професор, Заслужений юрист України
Г. О. Коломоєць

Завідуючий кафедрою мікро- та наноелектроніки
Запорізького національного технічного університету, доктор фізико-математичних наук, професор
В. В. Погосов

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

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

Синєокий, О. В.

С382 Інформаційне право України та електронне право високих технологій : [електронний ресурс] (електронний курс лекцій українською мовою) / Автор – доцент кафедри кримінального права та правосуддя ЗНУ, кандидат юридичних наук, доцент **Олег Володимирович Синєокий** ; Запорізький національний університет ; Національна бібліотека України ім. В. І. Вернадського [цифрова мікроформа *e-text*]. – Запоріжжя : ЗНУ, 2010. – 215 ел. с. = 15 ум. друк. арк. : іл. ; сх. // [http: www.nbuv.gov.ua/](http://www.nbuv.gov.ua/).

25.03.2010

Синеокий, О. В.

С382 Информационное право Украины и электронное право высоких технологий : [электронный ресурс] (електронний курс лекцій на українському мові) / Автор – доцент кафедри кримінального права і правосуддя ЗНУ, кандидат юридических наук, доцент **Олег Владимирович Синеокий** ; Запорожский національний університет ; Національна бібліотека України ім. В. И. Вернадського [цифрова мікроформа *e-text*]. – Запорожжє : ЗНУ, 2010. – 211 эл. с. = 15 усл. печ. с. : илл. ; сх. // [http: www.nbuv.gov.ua/](http://www.nbuv.gov.ua/).

Розкриваються основи правового регулювання високих технологій, що використовуються у інформаційно- телекомунікаційних та інших електронних системах.

Окрему увагу приділено системному дослідженню організаційно-правових особливостей високих технологій, наноіндустрії та нових обчислювальних електронних систем інтелектуальної обробки інформації у діяльності правоохоронних органів. Вперше у вітчизняній літературі досліджено правові проблеми розвитку нанотехнологій та застосування високих технологій щодо стримування нових видів злочинності. Визначено та обґрунтовано перспективи розвитку електронного права високих технологій як новітньої підгалузі інформаційного права.

Розраховано для поглибленого вивчення навчальних дисциплін «Інформаційне право» та «Правове регулювання інформаційної безпеки».

УДК 35.078.3 : 343.451 : 044 (477) (075.8)
ББК Х 9 (4 Укр) 304.4 я 73

© Синеокий О.В., 2010
© ЗНУ, 2010

ПРОГРАМНИЙ ПЛАН «ІНФОРМАЦІЙНЕ ПРАВО УКРАЇНИ»

МОДУЛЬ 1. ІНФОРМАЦІЙНЕ ПРАВО В СИСТЕМІ ПРАВА УКРАЇНИ ТА ОСНОВИ ЗАКОНОДАВСТВА В СФЕРІ ВИСОКИХ ТЕХНОЛОГІЙ

ЛЕКЦІЯ 1

ПОНЯТТЯ ІНФОРМАЦІЙНОГО ПРАВА УКРАЇНИ ТА ЙОГО ОСНОВНИХ ГАЛУЗЕВИХ ІНСТИТУТІВ

1. *Право, інформаційні відносини та інформаційне законодавство.*
2. *Теорія правової інформатики.*
3. *Наука інформаційного права.*
4. *Поняття технології та види високих технологій.*
5. *Електронне право високих технологій як галузевий інститут інформаційного права.*
6. *Методи інформаційного права та методологія електронного права високих технологій.*
7. *Основні принципи, об'єкти і суб'єкти високотехнологічного інформаційного права.*
8. *Синергетична концепція інноваційного розвитку інформаційного права.*
9. *Перспективи розвитку інноваційного законодавства у сфері високих технологій.*
10. *Розробка проекту Інформаційного кодексу України.*

ЛЕКЦІЯ 2

ДЕРЖАВНА ПОЛІТИКА РОЗВИТКУ ВИСОКИХ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ІНФОРМАЦІЇ

1. *Поняття, основні види та властивості інформації.*
2. *Феномен інформатизації.*
3. *Інформаційне електронне суспільство та глобальний інформаційний простір.*
4. *Програмоване суспільство та високотехнологічна цивілізація.*
5. *Модернізація технологічної діяльності суспільства та формування технологічного світогляду у цифрову епоху.*
6. *Сутність інформаційної політики.*

25.03.2010

7. Національна програма інформатизації.
8. Основні завдання національної системи науково-технічної інформації.
9. Правовий режим інноваційної діяльності технопарків та спеціальних економічних зон.
10. Реформування національної інформаційної політики.

ЛЕКЦІЯ 3

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЇЇ ОКРЕМИХ ВИДІВ В ЕЛЕКТРОННОМУ ФОРМАТІ

1. Поняття інформаційної діяльності, її основні напрями та електронні види.
2. Правові основи редакційно-видавничої та інформаційної діяльності преси в електронному форматі.
3. Правовий статус інформаційних агентств та електронної пошти.
4. Організація бібліотечної діяльності та правові проблеми електронних бібліотек.
5. Правові особливості організації архівної діяльності та системи електронних архівів.
6. Цифрове телебачення, національне радіомовлення і кінематографія України.
7. Організаційно-правові засади здійснення видавничої справи та види електронних видань.
8. Законодавство у сфері рекламної діяльності та правова регуляція електронної реклами в Інтернеті.
9. Правове регулювання державної статистики та електронний облік статистичної інформації.
10. Правові проблеми використання інсайдерської інформації.

ЛЕКЦІЯ 4

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА ТА ВИДИ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

1. Основні дефініції, поняття та функції електронної комунікації.
2. Цифрові права людини та мультимедіа-технології як наукові категорії.
3. Сфера застосування та класифікація телекомунікацій.
4. Поняття та види телекомунікаційних послуг.
5. Суб'єкти ринку телекомунікаційних послуг.
6. Поняття електронного документообігу та правові ознаки електронних документів.
7. Інформаційні ресурси та інформаційні продукти.
8. Інформаційні моделі та компоненти інформаційної системи.
9. Інформаційні процеси та новітні інформаційні технології.
10. Глобальна система Інтернет як вид електронної комунікації та проблеми правового регулювання Інтернет-простору.

МОДУЛЬ 2. ПРАВОЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ВИСОКОТЕХНОЛОГІЧНИХ ІННОВАЦІЙ

ЛЕКЦІЯ 5

КРИМІНАЛЬНО-ПРАВОВІ ТА КРИМІНОЛОГІЧНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ВИСОКИХ ТЕХНОЛОГІЙ

1. Інформаційна сфера і політика у сфері боротьби зі злочинністю.
2. Політика інформатизації правоохоронних органів.
3. Поняття кримінально-правової політики.
4. Інформаційні правопорушення і злочини у сфері високих технологій.
5. Злочинність у сфері високих технологій.
6. Інформаційна та міжнародна злочинність.
7. Проблеми інтелектуалізації високотехнологічної злочинності.
8. Кримінальне право і електронне право високих технологій.

9. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
10. Специфічні риси злочинів у сфері нанотехнологій і прогнози розвитку нанозлочинності.

ЛЕКЦІЯ 6

ЕЛЕКТРОННЕ ПРАВО ВИСОКИХ ТЕХНОЛОГІЙ І КРИМІНАЛІСТИЧНА МОДЕРНІЗАЦІЯ

1. *Методи інформаційної безпеки та електронні системи захисту інформації.*
2. *Інформаційна надійність оптоволоконних телекомунікацій та проблеми правової регуляції.*
3. *Методологія, принципи та функції Інтернет-моніторингу.*
4. *Мета та завдання правового моніторингу цифрових інформаційних мереж.*
5. *Криміналістична інформатика та високі технології.*
6. *Проблеми досудового слідства у сфері високих технологій та криміналістична модернізація.*
7. *Електронні види інформаційних та експертно-криміналістичних систем.*
8. *Характеристика інформаційних та експертно-криміналістичних систем.*
9. *Автоматизоване робоче місце слідчого.*
10. *Проект «Оптико-електронний кабінет криміналістики».*

ЛЕКЦІЯ 7

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ

1. *Інформаційне забезпечення органів прокуратури.*
2. *Інфраструктура прокурорських телекомунікацій.*
3. *Електронний документообіг в органах прокуратури.*
4. *Інформаційно-аналітична підсистема «Статистика».*
5. *Електронна система «Нагляд».*
6. *АРМ «Прокурор-кримінолог-аналітик».*
7. *Розбудова інформаційних технологій нового покоління.*
8. *Основні завдання інформатизації прокурорської діяльності.*
9. *Концептуальні засади інформатизації органів прокуратури.*
10. *Стратегії розвитку інформатизації органів прокуратури України.*

ЛЕКЦІЯ 8

НАНОТЕХНОЛОГІЯ ЯК СПЕЦІАЛЬНИЙ ОБ'ЄКТ ЕЛЕКТРОННОГО ПРАВА ВИСОКИХ ТЕХНОЛОГІЙ

1. *Поняття та правові ознаки нанотехнології.*
2. *Правове забезпечення наноіндустрії.*
3. *Нанотехніка, види наноматеріалів та організаційно-правові проблеми нанотехнологій.*
4. *Концепція розвитку нанотехнологій.*
5. *Інформаційно-правові проблеми штучного інтелекту і нанороботи.*
6. *Перспективи інноваційних розробок антикримінальних наносистем.*
7. *Інформатизація Збройних Сил та військові нанотехнології.*
8. *Інформаційне забезпечення судово-експертних досліджень і нанонаукові можливості.*
9. *Судова медицина, судова хімія і нанохімія.*
10. *Судова (криміналістична) фізика і криміналістична нанотехніка.*

**ПІДСУМКОВІ ТЕСТИ РІЗНИХ РІВНЕЙ СКЛАДНОСТІ
ІНДИВІДУАЛЬНІ ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ
СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ**

ЛЕКЦІЯ 1. ПОНЯТТЯ ІНФОРМАЦІЙНОГО ПРАВА УКРАЇНИ ТА ЙОГО ОСНОВНИХ ГАЛУЗЕВИХ ІНСТИТУТІВ

© Синєокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синєокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. *Право, інформаційні відносини та інформаційне законодавство.*
2. *Теорія правової інформатики.*
3. *Наука інформаційного права.*
4. *Поняття технології та види високих технологій.*
5. *Електронне право високих технологій як галузевий інститут інформаційного права.*
6. *Методи інформаційного права та методологія електронного права високих технологій.*
7. *Основні принципи, об'єкти і суб'єкти високотехнологічного інформаційного права.*
8. *Синергетична концепція інноваційного розвитку інформаційного права.*
9. *Перспективи розвитку інноваційного законодавства у сфері високих технологій.*
10. *Розробка проекту Інформаційного кодексу України.*

1. Право, інформаційні відносини та інформаційне законодавство

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

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

Таким чином, право є закономірним результатом внутрішнього розвитку регулятивної системи, відповідь 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.

Однією з найважливіших властивостей права є його здатність виступати в ролі

регулятора суспільних відносин. Саме в цьому полягає соціальне призначення права.

Правове регулювання відбувається в результаті впливу норм права на свідомість людей, а через неї – на їх поведінку, її одноманітність і повторюваність, відповідність вимогам права становить зміст правового регулювання [63].

Отже, *право* – це система норм (правил) поведінки, що встановлюються або санкціонуються державою (компетентними державними органами, іншими суб'єктами, які наділені такими повноваженнями, або населенням у результаті референдуму), гарантуються нею, містяться в нормативно-правових актах і регулюють найважливі сфери суспільних відносин.

Соціальні норми покликані забезпечити врегулювання взаємовідносин, 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 у залежності від своєї значимості розташовані у прийнятому в юриспруденції порядку й утворюють систематику певного правового явища. Грунтуючись на тому, що правовідносинами називають суспільні відносини, змістом яких є суб'єктивні права та юридичні обов'язки осіб, що охороняються державою, право в сфері інформаційних відносин слід розуміти як вид інформованості суб'єктів та міру інформатизації суспільства, що відображає інформаційні потреби суспільного розвитку, яка у своїй основі склалася в процесі повторюваних суспільних відносин і визнається й охороняється державою.

З цього приводу виникає питання: оскільки інформаційні відносини виникають у різних сферах суспільного життя і є у тій чи іншій мірі предметом регулювання багатьох галузей права, то які ж критерії розмежування.

Отже, *інформаційні відносини* – це суспільні відносини, які виникають при збиранні, одержанні, зберіганні, використанні, поширенні, охороні та захисту інформації.

Не може викликати особливих заперечень той факт, що першим критерієм для класифікації права на інформацію є зв'язок останнього із предметом правового регулювання різних галузей права.

Звідси за цим критерієм виділяємо права на інформацію, які 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.

Останнім часом окрему увагу приділяється дослідженню системних зв'язків інформаційного права з авторським правом, що знаходить втілення у розвитку законодавства про інтелектуальну власність, оскільки інформація є об'єктом права

власності громадян, організацій (юридичних осіб) і держави.

Під терміном «законодавство» прийнято розуміти сукупність законів та інших нормативно-правових актів, що забезпечують правове регулювання суспільних відносин на всій території держави. Отже, основною формою стандартизації норм соціотехнологічних правовідносин є *інформаційне законодавство*.

Звідси, основними джерелами 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.

Разом із тим, проблеми інформаційного суспільства, що виникають в контексті недосконалого нормативно-правового регулювання інформаційних та інформаційно-інфраструктурних відносин, потребують вирішення на законодавчому рівні.

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

2. Теорія правової інформатики

Дослідження щодо застосування здобутків інформатики в юридичній діяльності в Україні свідчать, що в нашій країні окреслилися ознаки активного формування в юридичній науці вітчизняної наукової школи – правової інформатики – комплексних досліджень на межі правознавства і прикладної інформатики [237].

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. Беляков,

В. Павловський, В. Голубєв, М. Гуцалюк, Ю. Жаріков, О. Крупчан, А. Марущак, І. Рогатюк, Г. Серєда, О. Шинальський, Ю. Ящуринський та багато інших.

Особливо слід підкреслити внесок у розробку проблеми інформаційного забезпечення державного управління таких провідних вчених 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. Корєнєв, В. Д. Малков, В. Г. Машликін, Дж. Міллер, В. А. Мінаєв, В. С. Михалєвич, А. М. Омаров, В. Ф. Опришко, Г. І. Петров, Н. С. Полевой, 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. Цветков, Л. П. Юзьков та інших.

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

Як складові особливої частини правової інформатики або на рівні спеціальних комплексних міжгалузєвих інститутів зазначеними дослідниками активно формуються: криміналістична, кримінологічна, оперативно-розшукова, фінансово-правова, податкова, адміністративно-правова інформатики.

Таким чином, права інформація визначається як 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 (І) з інформаційним правом (2).

До предмету правової інформатики відносяться питання інформаційного забезпечення (Із) правових процесів (Ід).

Разом із тим, предметом інформаційного права виступають, навпаки, питання правового забезпечення та

регулювання (Із) інформаційної діяльності, відносин та процесів (Ід), що можна представити формулою: $1 = \frac{Iz}{Id} \neq \frac{Lz}{Id} = 2$.

Таким чином, теоретичні основи правової інформатики складаються з двох основних компонентів: інформатики та права, про що далі ще відбудеться докладна розмова.

3. Наука інформаційного права

Поняття інформаційного права з'явилося відносно нещодавно – на межі 80-90-х рр. ХХ ст. [39]. Хоча це не є вичерпним доказом того, що позначуваного ним явища не існувало раніше. Втім, такий підхід є цілком справедливий в природних науках, але може опинитися невірним в соціальних.

Інтеграція наукових знань – це процес «з'язування» окремих диференційованих ідей, методів, частин та функцій взаємодіючих наук у єдине ціле. Синтезовані у будь-якій предметній галузі пізнання, вони разом утворюють вже нову галузь знань, нову науку. Особливо гостро це відчувається у формуванні суспільних відносин нового типу – інформаційних процесів, обумовлених високотехнологічною революцією. У правовій сфері саме це може стати основними передумовами високотехнологічного інформаційного прориву, тобто принципово нового вирішення проблем нетрадиційним шляхом.

Інформаційне право слід розуміти у трьох значеннях: як галузь права, як науку і як самостійну навчальну дисципліну.

Кожна наука має свій предмет. Інформаційне право предметно охоплює правову регуляцію достатньо широкого спектру суспільних відносин, що виникли 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, яка сьогодні динамічно

розвивається [19]. Виникають нові правові терміни, набувають додаткового значення фундаментальні юридичні поняття [217, с. 3]. Так, наприклад, поряд із визначенням терміну «інформаційне право» сучасні юридичні енциклопедії містять визначення терміну 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. Вживаються також такі термінологічні конструкції як «інформаційно-комп'ютерне право», «електронне право», «кібернетичне право» та «правова кібернетика» [102, с. 13].

Інформаційне право постійно удосконалюється, оскільки є сукупністю правових норм, що регулюють соціальні відносини, які так чи інакше взаємодіють або пов'язані з інформацією, де високі технології посідають на особливе місце.

Таким чином, 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 вимагає здійснення ланцюгової реакції «мета – теорія – практика – суспільний результат».

Наука інформаційного права, а звідси й відповідна навчальна дисципліна, ще знаходяться на стадії формування. Проведений 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 є підгалуззю 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 в деяких моментах навіть різняться з раніше прийнятими у вітчизняній юридичній науці. Втім, сподіваємося, що систематизація раніше здобутих і нових унікальних даних, сприятиме становленню високотехнологічної теорії інформаційного права.

Викладення матеріалу не охопило всього кола 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. Названа концепція є новою в теорії права. Вона ще не набула глибокого наукового обґрунтування, проте активно впливає на формування своїх методологічних основ і поглибленні 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 носять загальний характер, а займаються ними фахівці різних галузей права, що стримує розвиток високотехнологічних інновацій.

4. Поняття технології та види високих технологій

Термін «технологія» походить від базового терміну «техніка», який означає загальну назву різноманітних пристроїв, механізмів та устроїв, не існуючих в природі, а виготовлених людиною. Універсальної класифікації технічних засобів ще не створено. Тенденція зростання ролі науки в житті сучасного суспільства сьогодні обумовлює використання високотехнологічних рекомендацій в правоохоронній практиці. При цьому

дослідниками акценти наголошуються на проблемах, що лежать на стиках різних галузей знань, оскільки тільки тісна взаємодія між ними сьогодні забезпечує пріоритети на всіх напрямках науки та техніки [117, с. 139].

Загальноприйнято поняття «технологія» розуміти як сукупність методів, процесів та матеріалів, що використовуються в певній галузі діяльності, а також науковий опис засобів виробництва. Так, у сценічному мистецтві технологія виконання спектаклів, п'єс, зйомки кінофільмів і т.п., описується сценарієм.

У розгляді загального змісту поняття та видів технологій можна також звернути окрему увагу і на те, що загальне коло політичних технологій може бути представлене такими видами як технології політичного консультування, технології політичної реклами, де особливе місце займає такий підвид як антирекламні технології, виборчі технології, де, наприклад, потрібно звернути увагу на інформаційний прийом пресупозиції як ілюзії вибору у ситуації невизначеності («Ми повинні відбросити усі сумніви й коливання...», «Народ зробив свій вибор...» і т.п.), нейролінгвістичне програмування (індивідуальні та масові NLP-технології), технологія іміджмейкінгу, PR-технології (*від англ. PR – Public Relations – зв'язок із широкою громадськістю*), де спеціальна роль відводиться менеджменту новин та інформаційних повідомлень.

Сьогодні термін Пі-Ар застосовується при інформаційному впливі для зміни суспільної думки, який найчастіше неправильно сприймається громадськістю як рекламна/інформаційна акція. Стрижнем політичного Пі-Ару розглядається технологія спін-мастеру (*англ. spin-master*) як інструмента роботи із інформаційним світом новин та символів у випадках, коли інформаційний розвиток подій приймає несприятливий характер.

Технологіями морального плану називаються закони предків (чого робити не можна або якщо робити, то що і як), правила поведінки людини в суспільстві, кодекс честі, конституція (у цивілізованому суспільстві), поняття (у кримінальному світі) і т.п.

Разом із тим технологія як об'єкт правового регулювання і один з ключових термінів інформаційного законодавства залишається фактично не визначеною. У найбільш загальному випадку під поняттям технологія розуміють сукупність взаємозв'язаних способів обробки матеріалів, виготовлення виробів та процесів, що супроводжують ці види робіт.

Процес представляє певну сукупність дій, що спрямовані на досягнення поставленої мети. Він повинен визначатися вибраною людиною стратегією і реалізовуватися за допомогою сукупності різних засобів і методів.

Тому технологічний процес є послідовністю технологічних операцій, що необхідно для виконання певного виду робіт або діяльності. Технологічна операція як основна розрахункова одиниця для визначення продуктивності науково-технічної діяльності є частиною технологічного процесу.

Окреме місце у технологічному процесі відведено технологічним картам, тобто технологічним документам, в яких фіксується повний цикл операційного процесу обробки виробу, матеріалів, виробничого обладнання, технологічних режимів, час та кваліфікація працівників.

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.

Ми бачимо, що багато явищ соціального життя все більшою мірою знаходять відображення 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. Адже сьогодні інформаційна сфера неможлива без застосування автоматизованих інформаційних систем та банків даних, програмного забезпечення операційних систем, прикладного та сервісного програмного забезпечення, інших інформаційних технологій, що засновані на використанні засобів обчислювальної техніки

і зв'язку. Подальше удосконалення середовища накопичення інформації на різних носіях, глобальне охоплення населення засобами зв'язку, що дозволяють передавати інформацію в будь-яку точку планети, автоматизована обробка інформації задалегідь розробленими алгоритмами – це три технічних досягнення, на яких базуються сучасні інформаційні технології і які можуть бути використані для проведення оперативнотехнічних заходів.

Таким чином, нові інформаційні технології пропонують визначати як цілісну систему операцій щодо збирання, зберігання, обробки та передавання інформації, що здійснюється з використанням комп'ютерної техніки та телекомунікаційних каналів зв'язку.

П. І. Орлов акцентує увагу на тому, що нові інформаційні технології засновані на впровадженні обчислювальної техніки, засобів зв'язку, систем телекомунікації. Таким чином, за думкою цього автора нові інформаційні технології визначаються як цілісна система операцій щодо збирання, зберігання, обробки 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 електронна обробка інформації (з метою її збереження, передачі, копіювання, переробки, знищення, кодування тощо) та використання мереж зв'язку, в більшості своїй глобальних.

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

Тому з точки зору політики технологічного розвитку існують підстави щодо окремого визначення найбільш міцного зв'язку техніки з наукою, що може бути визначено так: $\sum T + L = Tl$, де T – техніка (*technika*), L – наука (*logos*), Tl – технологія (*technology*).

Отже, технологія – це комплекс організаційних заходів, операцій та приймів, що спрямовані на виготовлення,

обслуговування, ремонт та/або експлуатацію виробу з номінальною якістю та оптимальними витратами.

Інформаційна технологія є більш емним поняттям, що відображає сучасне уявлення про процеси перетворення інформації в інформаційному суспільстві.

Метою нових технологій у галузі передачі інформації є отримання інформації для аналізу й прийняття на його основі рішення на виконання будь-якої дії. Звідси визначимо інформаційну технологію як процес, що використовує сукупність засобів і методів збирання, обробки і передачі даних (первинної інформації) для одержання інформації нової якості про стан об'єкта, процесу або явища (інформаційного продукту).

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

Тож, ми наблизилися до розуміння високотехнологічної теорії як окремої підгалузі інформаційного права. На ці питання відповіді далі спробуємо надати ґрунтовну відповідь, після визначення правового змісту поняття «висока технологія» як основного елемента.

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

Під інтелектуальними технологіями розуміють високі наукоємні технології, що відтворюють елементи інтелекту людини [41, с. 29]. Складні за розробкою вони досить прості в експлуатації, навіть, для непрофесійного користувача.

Інноваційні технології – це набори методів і засобів, що підтримують етапи реалізації нововведення, серед яких розрізняють такі основні види як впровадження, тренінг, консалтинг, трансферт, аудіт, інжиніринг.

Термін висока технологія («*high-tech*») є більш емним, ніж критична, а за часом створення може включати в себе нові

технології, що були розроблені останніми роками ХХІ ст. Високі технології – це технології, які стануть визначальними у постіндустріальному суспільстві [54, с. 646].

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

Звідси постає проблема відсутності нормативно-правового регулювання суспільних відносин, що виникають в цій галузі. «Нова технологія» і «новітня технологія» також є двома різними термінами. При цьому новітні технології в інформаційній сфері випереджають нові приблизно на 5 років. Отже, високі технології з одного боку є вищими, ніж «звичайні», утім 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 перейти структурно вже на інший уніфікований рівень.

З метою систематизації понять, ми пропонуємо для єдиного позначення сукупності таких технологій вживати єдиний термін прогресивні технології або прог-технології («*prog-tech*»).

З метою розвитку Основ політики РФ в галузі розвитку науки й технологій на період до 2010 р. розроблені Правила формування, коректування й реалізації пріоритетних напрямів розвитку науки, технологій й техніки в РФ і переліку критичних технологій.

Перелік критичних технологій, що підпадають під чинність Закону РФ «Про порядок здійснення іноземних інвестицій у стратегічні галузі», 25.08.2009 р. було затверджено [136]. До переліку включено 35 технологій, що мають важливе соціально-економічне значення або важливе значення для оборони країни й безпеки держави. У

списку критичних технологій – клітинні технології, нанотехнології, технології біоінженерії, водневої енергетики, нових і поновлюваних джерел енергії.

До цього списку включено також технології обробки, зберігання, передачі й захисту інформації, створення інтелектуальних систем навігації, обробки композиційних, керамічних матеріалів, кристалічних матеріалів, полімерів і еластомірів.

Крім цього, визначені галузі, що мають стратегічне значення для забезпечення оборони країни й безпеки держави. Так, до стратегічних галузей віднесені 42 виду діяльності [146]. Нажаль, в Україні до цього часу у цьому напрямку заходів не здійснено.

Наведемо основні визначення:

Інформаційні технології (англ. *information technology*) – широкий клас галузей діяльності, що відносяться до технологій управління, та комплекс взаємопов'язаних наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці з використанням обчислювальної техніки, комп'ютерів та програмного забезпечення для зберігання, перетворення, обробки, передачі та одержання інформації.

Інноваційні інформаційні технології – цілеспрямовано організована сукупність інформаційних процесів та реалізація інформаційних нововведень з використанням вперше створених та вдосконалених технологічних засобів передачі даних, до пошуку, одержання, обробки яких пристосована інформація або інформаційний продукт.

Інтелектуальні інформаційні технології (англ. *intellectual information technology*) – інформаційна концепція підвищення ефективності прийняття інноваційних рішень в умовах, що пов'язані з виникненням проблемних ситуацій, а також технології прискорення аналізу політичної, економічної, соціальної та технічної ситуації, при цьому методи, що використовуються при синтезі управлінських рішень, не обов'язково повинні копіювати процеси людського мислення.

Інформаційно-комунікаційні технології
– технології, пов’язані зі створенням, збереженням, передачею, обробкою і управлінням інформацією.

Спробуємо систематизувати за термінологічними ознаками види критичних технологій і схематично наведемо їх у схемі:

	<i>Перша група</i>	<i>Друга група</i>	<i>Третя група</i>
1	Критичні технології	Екстремальні технології	Високі технології
2	Електронні технології	Прогресивні технології	Нові технології
3	Ефективні технології	Максимальні технології	Новітні технології
4	Передові технології	Револьюційні технології	Супертехнології
5	Креативні технології	Модернізаційні технології	Метатехнології
6	Цифрові технології	Високопродуктивні технології	Інноваційні технології

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

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

5. Електронне право високих технологій як галузевий інститут інформаційного права

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 розробки 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, вони створюються з

урахуванням соціотехнологічного досвіду та інформаційних інтересів людей.

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

Сьогодні фактично виникає нова підгалузь інформаційного права, яку можна визначити як *електронне право високих технологій*.

Електронне право – це комплексна галузь права, яка регулює суспільні відносини у сфері інформатики, створення і використання електронно-обчислювальних машин, електронних засобів і програмних продуктів.

Ці відносини частково регулюються нормами адміністративного, цивільного, трудового, кримінального та інших галузей права. Структура ж електронного права високих технологій дає змогу забезпечити комплексний підхід до регулювання зазначених відносин.

Звідси бачимо, що електронне право високих технологій можна розуміти як в об’єктивному, так і в суб’єктивному змістах. Так, електронне право високих технологій в об’єктивному змісті – це суспільні відносини

у сфері високих технологій, які набувають втілення у нормах, врегульованих на публічно-правовому та приватно-правовому рівні. Електронне 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 соціо-технологічних відносин.

Таким чином, електронне право високих технологій є сукупністю правових норм, які регулюють електронні інноваційні розробки в інформаційній сфері.

Це може забезпечити правове впорядкування процесу високотехнологічного розвитку інформаційного суспільства на основі електронних засобів обробки, передачі та розповсюдження інформації.

Високотехнологічне інформаційне право як наука – це система наукових знань про електронне право високих технологій як підгалузь інформаційного права, його предметі, методах, принципах правового регулювання інформаційних відносин у сфері високих технологій, історії розвитку суспільних відносин в інформаційній сфері й порівняльно-правовому аналізі норм високотехнологічного права закордонних країн.

У цілому електронне право високих технологій як підгалузь інформаційного права ще перебуває на початковому етапі свого формування.

Високотехнологічні правовідносини є соціальними відносинами найвищого (критичного) рівня, які виникають у сфері технологій нового покоління, і перш за все з використання електронних засобів комунікації, а звідси мають особливий правовий зміст, оскільки регулюють правила поведінки у сфері розробки та застосування високих технологій.

Отже, пропонуємо далі розглядати електронне право високих технологій як систему правового регулювання соціотехнічних відносин, що складаються у сфері високих технологій.

Дальший розвиток методу електронного права високих технологій пов'язаний зі створенням нових поколінь «інтелектуальних» комп'ютерів та

вдосконаленням комп'ютерно-інформаційних технологій, появою нових суб'єктів суспільних відносин, зокрема нанотехнологій, та нових специфічних видів юридичних фактів.

6. Методи інформаційного права та методологія електронного права високих технологій

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

Метод правового регулювання – це сукупність прийомів і засобів, за допомогою яких упорядковуються суспільні відносини визначеного виду.

Головними регулятивними засобами є: а) характер співвідношення обов'язків і заборон; б) зміст і обсяг прав і обов'язків правових відносин; в) механізм реалізації цих прав і обов'язків.

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. 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.

Правове регулювання суспільних відносин в інформаційній сфері регулюється також за допомогою таких загальнотеоретичних методів як формально-юридичного аналізу, прикладний системний аналіз, правового моделювання, статистичний, конкретно-соціологічний, формально-логічний, порівняльно-правовий, документальний аналіз, граматичний розгляд і

тлумачення правових норм, діалектичний та ін.

Потрібно відзначити окремі спеціальні методи інформаційного права, зокрема такі як рівність суб'єктів інформаційних відносин, диспозитивність тобто надання учасникам інформаційних відносин в певних межах права інформаційного вибору варіанта поведінки у випадках, що передбачені законом, неприпустимість необгрунтованого втручання в інформацію приватного характеру, обмеження інформаційного доступу до особистого життя, матеріальна компенсація заподіяного будь-кому, у тому числі морального збитку в інформаційній сфері тощо. Адже останнє пояснюється тим, що інформаційне право не може обійтися у певних випадках без застосування від імперативного методу, що передбачає виконання інформаційних заборон та обмежень певними суб'єктами інформаційних правовідносин, забезпечених можливістю застосування до порушників заходів правового примусу.

Отже, метод електронного права високих технологій є комплексним. Застосування норм електронного права високих технологій забезпечується як власними методами, так і методами інших галузей і підгалузей права. Сукупність зазначених методів дозволило запровадити методологічно уніфікований системно-інформаційний підхід на всіх рівнях управлінської системи до збирання та опрацювання інформації і визначення її релевантності (цінності).

7. Основні принципи, об'єкти і суб'єкти високотехнологічного інформаційного права

Принципи інформаційного права – це розроблені наукою інформаційного права на основі аналізу інформаційно-правових норм і виявлення закономірностей, що притаманні цій галузі, основні ідеї, керівні положення, які визначають стратегію та напрями розвитку окремих інститутів і норм цієї нової галузі права, забезпечують системність правового регулювання соціотехнологічних відносин, що виникають в інформаційній сфері.

Принципи інформаційного права поділяються на загальноправові, галузеві, міжгалузеві та специфічні, тобто притаманні тільки інформаційному праву.

Принципи в інформаційному праві є теоретично обгрунтованими основними положеннями, обумовленими об'єктивними закономірностями реалізації інформаційних потреб особи, окремих груп осіб та суспільства у цілому.

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 – це 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 й навчальної дисципліни «Інформаційне право» визначається відповідно до суті 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 тощо. Зокрема безпосереднім предметом в нашій роботі є політика розвитку високих технологій передачі інформації у сфері боротьби зі злочинністю.

З цього приводу далі визначимо об'єктів 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, що закріплені діючими правовими нормами. Об'єкт права – це конкретні майнові та немайнові блага та інтереси, з приводу яких відносини регламентовані законом.

Об'єкт правового регулювання, як правило, уявляє собою умовне виділення окремо визначеного відособленого 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 щодо 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 вважаються документована або публічно оголошена 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, що пов'язана з інформацією.

Таким чином, визначимо, що об'єктом інформаційного права є суспільні відносини, що пов'язані із створенням, формуванням, зберіганням обробкою, розповсюдженням, використанням інформаційних продуктів, управлінням процесом формування та використання інформаційного продукту та надання інформаційних послуг, розвитком та застосуванням нових технологій роботи інформації та її передачі в системах і мережах комунікацій, посиленні 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 включають питання використання 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.

Таким чином, основними об'єктами високотехнологічних інформаційних відносин виступають високотехнологічна інформація, а також високі технології, що застосовуються в інформаційній сфері.

За наслідками аналізу правового регулювання високотехнологічних інформаційних відносин в Україні та в міжнародній практиці існує сенс визначити, що основним предметом цих суспільних відносин, як і власне інформаційних відносин залишається інформація (відомості, дані, знання, технології, тайна й т.п.).

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, розробки 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 та юридичні обов'язки (тобто правосуб'єктністю).

Суб'єкти права є необхідним елементом правовідносин у всіх галузях права, утім в кожній з них стан суб'єктів мають 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, незалежно від їх форми власності та організаційно-правової форми, що наділені законодавством України інформаційними права і обов'язками, а також державу Україна та іноземні держави.

Іноземні держави можуть бути суб'єктами інформаційних відносин у відповідності до діючого законодавства України, а також на основі міжнародних договорів, ратифікованих Україною.

У цьому контексті важливим елементом виступає *інформаційна дієздатність* – тобто визначена інформаційним законодавством юридична можливість суб'єкта інформаційних правовідносин здійснювати свої інформаційні права й обов'язки, реалізуючи що він здатний бути активним учасником інформаційних відносин [217, с. 69]

Таким чином, визначимо, що суб'єкти інформаційного права – це учасники інформаційних відносин, які володіють інформаційними права та обов'язками, організаційно здійснюючі їх на нормативно-правовій основі, що у 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 є 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 та обов'язки, які складають зміст інформаційних правовідносин [217, с. 72]. Адже відомо, що правовий статус є встановлений нормами права стан його суб'єктів, сукупність їхніх прав та обов'язків.

Враховуючи 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 їхні посадові особи, засоби масової інформації та їхні штатні працівники, інші інформаційно-телекомунікаційні засоби. Тобто, як ми бачимо, вищезазначені учасники є *суб'єктами високотехнологічного інформаційного права України*.

8. Синергетична концепція інноваційного розвитку інформаційного права

Останнім часом вчені 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 напрям. Синергетика вивчає загальні закономірності самоорганізації, становлення структур, які утворюються в складних, відкритих системах в 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 самі різні системи, від атома до людини.

Слово «синергетика» (від грец. συν – «спільно» і грец. εργος – «діючий») і означає «спільна дія», підкреслюючи узгодженість поведінки часток, що відображається в функціонуванні системи як цілого. Тобто пропонуються базові моделі, нові поняття й методи, які можуть бути застосовані в даній ситуації, які можуть 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 самоорганізації систем, що складаються з підсистем.

Таким чином, синергетика – це наука, що займається вивченням процесів

самоорганізації й виникнення, підтримки, стабільності й розпаду структур всілякої 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 інновацій подібно тому, як інколи кібернетика визначалася, як «універсальна теорія управління», однаково придатна для опису будь-яких операцій регулювання й оптимізації: у природі, у техніці, у суспільстві й т.п. Час показав, що загальний кібернетичний підхід виправдав далеко не всі надії, що покладались на його.

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

Зрозуміло, у соціальній і медійній системі 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 мікроепливів являє собою «режим із загостренням», здатний породити з будь-якої мікрофлуктуації макроструктуру.

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

Інформаційний синергізм або синергетичний ефект – це ефект взаємозв'язку й взаємодії, підвищення результативності за рахунок використання взаємозв'язку й взаємопосилена соціо-технологічного впливу інформаційної діяльності.

У системному підході аналіз ведеться, як правило, на якісному рівні. На відміну від системного підходу, де основна

увага акцентується на зв'язках частин у цілому, синергетика досліджує причини властивостей системи [250].

Таким чином, синергетика є науковою дисципліною, що розглядає закономірності процесів системної інтеграції й самоорганізації в різних системах.

Підхід – це комплекс механізмів пізнання або практики, що характеризує конкуруючі між собою стратегії і програми в науці, політиці, філософії або в 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 їхнього опису повинен бути придатний загальний математичний апарат.

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

Стосовно до 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 і їхнє саморегулювання.

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

Хоча, як зазначають автори, 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].

Потрібно зазначити, що існує зв'язок високотехнологічної теорії інформаційного права з іншими юридичними науками – адміністративним, конституційним, цивільним, фінансовим, інвестиційним, авторським правом та ін.

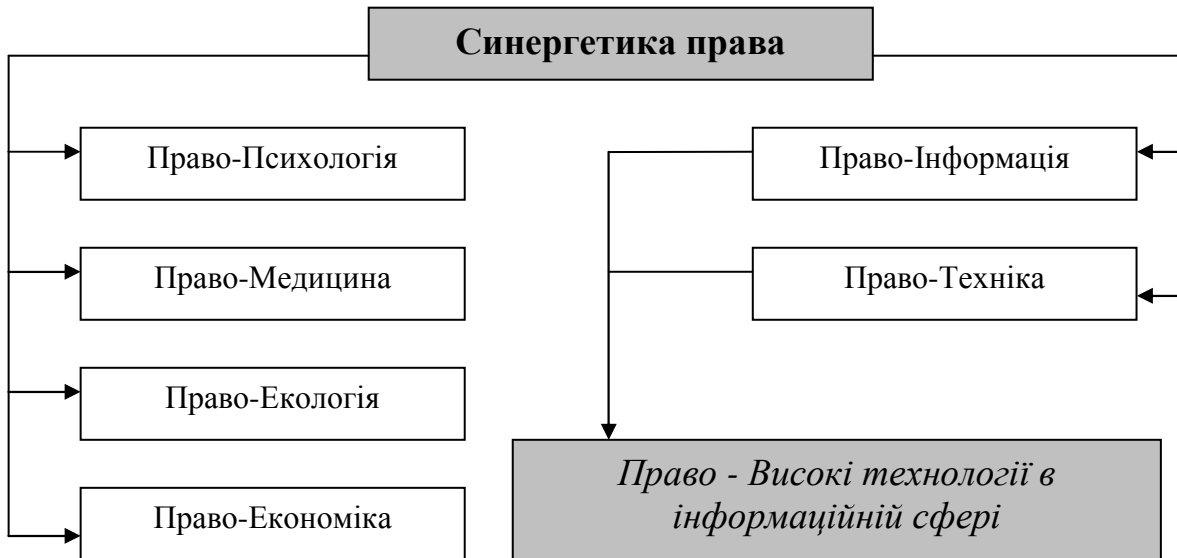
Окремо потрібно зазначити дисципліни кримінально-правового циклу як-то кримінальне право, кримінальний процес, кримінологія, криміналістика, судова експертиза та окремі підгалузеві інститути. Далі про кожний з них чекає докладний аналіз системних зв'язків.

Отже, існує сенс визначити метод у високотехнологічному інформаційному праві як єдиний узагальнений правовий спосіб

вирішення інформаційних задач високотехнологічного класу, одними з особливостей чого є кібернетичне та комп'ютерне моделювання, формування високотехнологічних гіперсистем, а також організаційно-правове обмеження інформаційного доступу до технологічної карти і самого технологічного процесу в дії.

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

Важливим аспектом високотехнологічної теорії інформаційного права є проблематика його підсистем, що показано на схемі:



У високотехнологічному інформаційному праві використовується вся сукупність способів регулюючого впливу на інформаційні правовідносини, що виникають у сфері високих технологій, тобто як диспозитивне регулювання (воля вибору, рівність сторін, децентралізація, координація), так і імперативне регулювання (централізоване здійснення владних повноважень, стругаючи субординація).

Залучення різних методів у систему високотехнологічного інформаційного права не означає їхнього довільного зіткнення або конкуренції.

Дискусії з питань значущості тих або інших методів для високотехнологічного інформаційного права можна примирити, тільки виробивши самостійну правову систему для вирішення проблем, що виникають у інформаційних відносинах з приводу розробки та використання високих технологій.

Безумовно, правові заборони певною мірою обмежують інформаційну самостійність та ініціативу учасників високотехнологічних відносин. Але такі інформаційні обмеження встановлюються як в інтересах окремих груп, так і у загальних суспільних інтересах.

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 й концептуальному розвитку високотехнологічного інформаційного права.

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

$$I = \frac{I \xrightarrow{2} HT}{L} \Rightarrow T+ \uparrow$$
, де I – інформація, $I 2$ – інформатизація, HT – високі технології, L – правова регуляція, $T+$ – технологічний прорив.

Отже, з позицій синергетичного підходу зазначений новий феномен може розглядатися як динамічна система інформаційних взаємодій суб'єкта з техносвітом, у процесі чого відбувається створення особливої правової конструкції, втілення її в об'єкті правового регулювання, здійснення й перетворення інформаційних

правовідносин суб'єктів у сфері високотехнологічної діяльності.

Оскільки електронне право високих технологій є окремою підгалуззю (науковою теорією), що формується у рамках науки інформаційного права, правова регуляція високих технологій є новою категорією, зміст якої може бути визначений за допомогою теорії синергетичного підходу.

9. *Перспективи розвитку інноваційного законодавства у сфері високих технологій*

Невиправдане виключення теоретико-правових засад високих технологій з інформаційного права обмежує сферу правового регулювання останнього і, фактично, залишає його на тупиковій гілці розвитку.

Отже, як ми бачимо, інші інститути права агрегуються з інформаційним правом. Окремі з них 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 на схемі:



До функцій електронного права високих технологій мають бути віднесеними правове регулювання нанотехнологій, правове регулювання технологій обробки, зберігання, передачі й захисту інформації, правове регулювання інтелектуальних систем навігації, правове регулювання ядерного виробництва та нових джерел енергії, правове регулювання космічної діяльності тощо.

Потрібно зазначити, що в нашій країні поки що немає спеціального систематизованого законодавства щодо

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 у рівній мірі використовуються обидва із зазначених термінів. До докладного розгляду правових

аспектів нанотехнології ми далі ще повернемося.

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.

У цілому, загальноєвропейські вимоги по захисту авторських прав зафіксовані в шести Директивах Єврокомісії. Зокрема, у 1998 р. в США був прийнятий Закон про захист авторських прав у цифрову епоху (*Digital Millennium Copyright Act*), в якому було узагальнено накопичений досвід правового регулювання авторських прав в інформаційному просторі, чим було створено передумови для приєднання США до нових міжнародних угод, а в 2001 році була прийнята Директива ЄС «Про гармонізацію деяких аспектів авторського права й суміжних прав в інформаційному суспільстві» № 2001/29/ЄС. Зазначені вимоги охоплюють охорону комп'ютерних програм; право прокату й надання в користування творчих виробів і режим суміжних прав; строк охорони; ефірне віщання через супутник і кабельну ретрансляцію; охорону баз даних; комплексне правове регулювання в інформаційному суспільстві [84, с. 4].

У цьому зв'язку, захист авторських прав на зроблену інформацію є одним із пріоритетних напрямків законодавчого забезпечення формування й розвитку глобального інформаційного простору й інформаційного законодавства в цифрову епоху.

З розвитком інформаційно-цифрових технологій виникла необхідність у розробці нових правових конструкцій, застосування яких забезпечило б належний рівень захисту авторських прав у глобальному інформаційному просторі, оскільки інформаційно-цифрові технології забезпечують вільне й неконтрольоване переміщення добутоків і виконань у рамках

глобального інформаційного простору [84, с. 23].

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 розробки та застосування високих технологій.

Досягнення науки інформаційного права має стати важливим чинником, здатним вплинути на удосконалення 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.

Таким чином, високотехнологічне інформаційне право охоплює пізнання нормативно-правових основ інформаційних правовідносин, що виникають у сфері високих технологій. Ґрунтуючись на аналізі викладеного, існує сенс резюмувати, що високотехнологічне право є основним нормативним регулятором інформаційних відносин найвищого (критичного) рівня, які виникають у сфері технологій нового покоління, де під останньою потрібно розуміти сукупність критичних технологій усіх видів.

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

спосіб: $\frac{A}{B} \Leftrightarrow \frac{C}{D}$, де правове забезпечення

інформаційного діяльності (*A*) виступає основним фактором 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: $\frac{X}{Y} \leq \frac{W}{Z}$, де інформаційне право (*X*)

співвідноситься з електронним 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 звідси додатково потребують удосконалення особливості механізму правової регуляції. Таким чином, обгрунтовано, що правове регулювання високих технологій є предметом високотехнологічного інформаційного права як окремої підгалузі інформаційного права.

10. Розробка проекту Інформаційного кодексу України

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», Постанова Кабінету Міністрів України від 4 січня 2002 р. № 3 «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади», Постанова Кабінету Міністрів України від 11.02.2004 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 [46; 67-72; 128-129; 163-167; 173-174].

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» 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 всіх форм власності, за навмисне 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 15.08.2003 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 надаватись з використанням електронної інформаційної системи «Електронний Уряд», визначені 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 послугі [35].

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 учасниками круглого столу виділено підготовку й прийняття Інформаційного кодексу України, який би відповідав рівню розвитку інформаційних відносин та адекватно врегульовував питання функціонування інформаційної сфери.

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

Так, О.А. Баранов пропонує за архітектонікою типово для національної юридичної доктрини розділити цей акт кодифікації на загальну (книга перша) та особливу (книга друга) частини.

При цьому першу традиційно почати із Загальних положень, де відобразити основи інформаційного законодавства, гарантії і захист прав та інтересів в інформаційній сфері, об'єкти та суб'єкти інформаційного законодавства, функції держави та її органів в інформаційній сфері, основні положення про інформацію, основні положення про інформаційну інфраструктуру.

У другу ж книгу пропонується внести такі окремі частини: інформаційні відносини, загальні положення обігу та створення інформації, питання щодо поширення, використання, зберігання та знищення (утилізація) інформації. Завершити кодекс обґрунтовується розділом, де визначити правовий режим інформації, як-то відкрита

інформація, інформація з обмеженим доступом, інформація обмеженого використання, право власності на інформацію [18, с. 214-268].

Висловлюючись з цього приводу потрібно зазначити, що подібна конструкція є застарілою і недосконалою, оскільки вже не відповідає сучасним вимогам. Ми ж, у свою чергу, вважаємо зручнішим укладати кодекс з трьох основних частин: Загальної (основні інститути інформаційного 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 учасників круглого столу 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 й 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, Європейської конвенції про захист прав людини та основних свобод й інших загальноприйнятих міждержавних нормативних актах, які сьогодні виступають у ролі стандартів, що визначають цивілізованість світового співтовариства у цілому.

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

Основні положення, що були викладені вище, зокрема відносно питань поняття та видів інформації, правового регулювання інноваційних процесів розроблення, модернізації, впровадження та використання нових технологій в інформаційній сфері, пропонується використати при розробці та прийнятті у новій редакції Законів України «Про інформацію» та «Про науково-технічну інформацію». Більш того, у цьому зв'язку існують підстави щодо наголосу на розробці окремого проекту Закону України «Про високі (прогресивні) технології».

КЛЮЧОВІ СЛОВА: *Право, інформатика, високі технології, інновації, законодавство.*

ЛЕКЦІЯ 2. ДЕРЖАВНА ПОЛІТИКА РОЗВИТКУ ВИСОКИХ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ІНФОРМАЦІЇ

© Синьокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синьокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. *Поняття, основні види та властивості інформації.*
2. *Феномен інформатизації.*
3. *Інформаційне електронне суспільство та глобальний інформаційний простір.*
4. *Програмоване суспільство та високотехнологічна цивілізація.*
5. *Модернізація технологічної діяльності суспільства та формування технологічного світогляду у цифрову епоху.*
6. *Сутність інформаційної політики.*
7. *Національна програма інформатизації.*
8. *Основні завдання національної системи науково-технічної інформації.*
9. *Правовий режим інноваційної діяльності технопарків та спеціальних економічних зон.*
10. *Реформування національної інформаційної політики.*

1. *Поняття, основні види та властивості інформації*

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. Беляєва, 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 інші автори.

Інформація є одним із найбільш загальних понять науки, що означає деякі відомості, сукупність певних даних та/або знань.

Інформація – це відомості, що передаються усним, письмовим або іншим способом, зокрема за допомогою умовних сигналів, технічних засобів і т.п.

Найбільш повна характеристика поняття «інформація» подається у визначеннях, закріплених у багатьох законодавчих та підзаконних нормативно-правових актах [66; 67; 70; 71; 128; 164; 225;

226; 227]. Так, під інформацією у ст. 1 Закону України «Про інформацію» розуміється документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі [67].

У Законі України «Про захист економічної конкуренції» інформація визначена як відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості.

Закон України «Про науково-технічну інформацію» визначає науково-технічну інформацію як документовані або публічно оголошені відомості про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської,

проектно-технологічної, виробничої та громадської діяльності [71].

Останніми роками ретельно обговорюються різні варіанти розроблених законопроектів з різними назвами «Про інформацію», «Про доступ до інформації», «Про захист інформації в автоматизованих системах», «Про систему науково-технічної інформації» та ін.

Так, згідно з проектом Закону України «Про інформацію» (2007) інформація визначається як відомості або/та дані у будь-якій формі та вигляді, на будь-яких носіях чи оголошені усно або у будь-який інший спосіб чи отримані у вигляді знань, що поширюються у просторі і часі, які відображають стан, властивості, якості, ознаки суб'єктів і об'єктів (предметів, технологій, засобів, ресурсів тощо), фактів, подій, дій, явищ, процесів, тощо у навколишньому світі, державі, суспільстві, тощо та які є об'єктами збирання, зберігання, використання та поширення [169].

За порушення законодавства про інформацію законопроект передбачає санкції – від дисциплінарних до кримінальних.

Під час доробки зазначеного законопроекту були враховані пропозиції та зауваження експертів Ради Європи, що стосувалися термінології.

Зокрема, із проекту вилучено терміни «інформаційні відносини», «інформаційний суверенітет», «національний інформаційний простір» тощо.

Чи правильна така думка? Адже інформаційні відносини як суспільні відносини, які виникають при збиранні, одержанні, зберіганні, використанні, поширенні та захисту (охороні) інформації, мають ключове значення в інформаційному праві, до аргументації з цього приводу ми повернемося у наступному параграфі.

Проблеми інформації досліджуються у різних наукових галузях, основою чого є інформатика як наука про способи одержання, накопичення, зберігання, перетворення і передачі інформації, а також її використання в обчислювальних машинах та обчислювальних мережах.

Утім, на сьогодні не існує єдиного нормативного визначення поняття

«інформація», яке б цілком відповідало соціотехнологічним 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.

Потоки різних видів соціально-економічної інформації, що використовуються в органах виконавчої влади, класифікуються за: періодичністю виникнення і передачі (п'ятирічна, річна, піврічна тощо); ступенем взаємозв'язку (характеризується кількістю усіх 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, у ході дослідження всіх масивів інформації, що надходить по даному питанню, аналізу стану справ у різних сферах громадського життя); закріпленням та втіленням в матеріальні форми (візуальна, документальна, звукова) та за багатьма іншими ознаками [116].

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.

Взагалі 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 [169].

Особиста інформація – це інформація про особу (в тому числі дитину), її особисте життя. Особиста інформація являється особистою 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 внутрішньої службової діяльності установи, її посадових, службових осіб та кореспонденцію (довідні 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.

Асиметрична інформація (англ. *asymmetric(al) information*) є терміном, який використовується в економіці наряду з термінами «недосконала інформація» та «неповна інформація», коли одна сторона угоди чи операції володіє більшою інформацією, ніж інша.

Отже, пропонуємо загальний спектр усіх видів та рівнів інформації схематично систематизувати у 14 спеціальних інформаційних груп:

№	ГРУПИ	ВИДИ ІНФОРМАЦІЇ
1	<i>За призначенням</i>	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, 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.
2	<i>За режимом</i>	Загального розповсюдження, статусна, індивідуальна, особиста, взаємна, офіційна, публічна, державна, статистична, колективна, групова, корпоративна, фахова, ділова, службова, неслужбова, архівна, бібліографічна, документальна, банківська, фінансова, інвестиційна,

	<i>користування</i>	страхова, фондова, трейдерська, журналістська, літературна, публіцистична, видавнича, поліграфічна, редакційна, рекламна, кінематографічна, музейна, патентна, інсайдерська, енергетична, елітна, презентаційна, аматорська, навчальна, курсова, тестова, залікова, виховна, молодіжна, статеві та ін.
3	<i>За режимом доступу</i>	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	<i>За рівнем якості та достовірності</i>	Понятійна, термінологічна, кількісна, якісна, низькоякісна, неякісна, нова, застаріла, достовірна, недостовірна, сертифікована, корисна, фіктивна, дезінформація, компрометуюча, тенденційна, ґрунтова, необґрунтована, перекручена, контрафактна, чорнова, механічна, уточнена та ін.
5	<i>За рівнем системності</i>	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	<i>За рівнем технологічності</i>	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.
7	<i>За структурою та обсягом</i>	Стандартна, єдина, фізична, матеріальна, атомна, молекулярна, хімічна, нульова, наноінформація, мікроінформація ... мегаінформація, гігаінформація, тераінформація, множинна, регіональна, локальна, фіксована, суперінформація, метаінформація, моноінформація та ін.
8	<i>За походженням та природою впливу</i>	Цивілізаційна, первинна, вихідна, відправна, інтелектуальна, психологічна, суб'єктивна, об'єктивна, конструктивна, креативна, категорична, свідомі, несвідомі, безсвідомі, підсвідомі, правдиві, помилкові, сумлінні, сумнівні, перманентні, необхідні, критичні, резонансні, рекомендовані, контактні, аддитивні, асоціативні, агресивні, позитивні, негативні, нейтральні, обов'язкові, консультативні, ситуаційні, пріоритетні, марні, безглузді, паразитичні, порочні, зворотні, діалогічні, націоналістичні, вікові, расові, PR-інформація та ін.
9	<i>За формою представлення</i>	Текстова, числова, графічна, звукова, візуальна, лінійна, циклічна, схематична, модульна, кольорова та ін.
10	<i>За засобами передачі</i>	Усна, письмова, вербальна, невербальна, сигнальна, телевізійна, телеграфна, телеметрична, квантова, математична, аеронавігаційна, генетична, багатоканальна та ін.
		Правова, нормативна, законодавча, підзаконна, відомча, міжвідомча, процесуальна, дисциплінарна, правозахисна, захисна, правоохоронна,

11	За юридичним характером	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, загрозна, 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.

Пропонуємо останнє розуміти як інформаційний цикл – будь-яку багаторазову інформаційну послідовність, що організована за допомогою умовних виходів, переходів,

завершення та продовження інформаційних груп.

Під поняттям «інформаційний об'єкт» розуміється опис деякої сутності (реального об'єкта, явища, процесу, події тощо) у вигляді сукупності логічно зв'язаних *реквізитів* (інформаційних елементів). Інформаційний об'єкт певного реквізитного складу та структури складає клас (тип), якому має надаватися унікальне ім'я (символьне позначення) [262].

Важливими властивостями інформації є *цілісність інформації* як властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення, *якість інформації* як сукупність властивостей, що відображають ступінь придатності конкретної інформації про об'єкти та їхній взаємозв'язок для досягнення цілей, що стоять перед користувачем, та наявність *особливої інформаційної мови* – тобто формалізованої мови, що призначена для характеристики даних певних видів та рівнів інформації чи змісту документів з метою забезпечення їх зберігання та пошуку.

2. Феномен інформатизації

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.

Інформатизація – це політика й процеси, які спрямовані на побудову й розвиток телекомунікаційної інфраструктури, що поєднує територіально розподілені інформаційні ресурси.

Процес інформатизації є наслідком розвитку інформаційних технологій і трансформації технологічного, продукт-орієнтованого способу виробництва в постіндустріальний. В основі інформатизації покладені кібернетичні методи і засоби управління, а також інструментарій інформаційних і комунікаційних технологій.

Інформатизація є не стільки технологічним, скільки соціальним і, навіть, культурологічним процесом, який міцно зв'язаний зі значними змінами у способі життя населення. Такі процеси вимагають суттєвих зусиль не тільки влади, але й усього співтовариства користувачів інформаційно-комунікаційних технологій на багатьох

напрямах, включаючи ліквідацію комп'ютерної неграмотності, формування культури використання нових інформаційних технологій та ін.

Ціллю інформатизації є трансформація рушійних сил суспільства, що повинне бути перенацілене на виробництво послуг, формування виробництва інформаційного, а не матеріального продукту. У ході інформатизації вирішуються завдання зміни підходів до виробництва, модернізується уклад життя, система цінностей. Особливу цінність знаходить вільний час, відтворюються й споживаються інтелект, знання, що приводить до пріоритетності розумової праці. Звідси від громадян інформаційного суспільства потрібна здатність до творчості, зростає попит на креативні знання.

Таким чином, «інформатизація» означає динамічний процес, а «інформаційне забезпечення» – вищий інформатизаційний рівень усіх соціальних процесів, що може бути схематично представлено формулою:



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

У цифрову епоху 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 в діяльності фізичних та 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.

Окремо наголосимо актуальність правового вирішення проблеми *інформаційного вакууму* як нестабільного стану потенційно вільного (відкритого) інформаційного поля, що уявляє собою особливе локальне середовище, в якому існує загроза неконтрольованого інформаційного

проникнення і наповнення інформаційної пустоти небажаною або суперечливою інформацією.

У цьому зв'язку є важливим визначення *дезінформації* як передачі будь-яких відомостей, що не відповідають дійсності, із антисоціальною або злочинною метою.

Отже, феномен інформатизації полягає в тому, що є одночасно і політикою, і процесами, які у сукупності спрямовані на побудову та розвиток телекомунікаційної інфраструктури, що об'єднує територіально розподілені інформаційні ресурси.

3. Інформаційне електронне суспільство та глобальний інформаційний простір

Одним із основних соціальних феноменів є громадянське суспільство як сукупність соціальних утворень (груп, колективів), які внутрішньо упорядковані та об'єднані специфічними інтересами, що реалізуються поза сферою діяльності держави, тобто абсолютно вільно або з мінімізованим рівнем безпосереднього впливу з боку посадовців.

Разом із тим інформаційна сфера життєдіяльності індивідів не може бути повністю незалежною від взаємодії з державою, звідси однією з тенденцій розвитку сучасної глобальної цивілізації є формування інформаційного суспільства як громадянського суспільства нового рівня, в якому формується різноманіття форм інформаційних відносин.

Цим можна пояснити соціотехнологічне втілення інформатизації суспільства як цивілізаційної мети, тобто створення такого суспільного устрою, за якого будь-яка предметна діяльність людей здійснюється за допомогою нових електронних та інформаційно-телекомунікаційних технологій.

Власне поняття «інформаційне суспільство» почало використовуватись у другій половині ХХ 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 [67-69].

На початковій стадії електронна технологія (космічний зв'язок, портативний відеозапис) виконувала роль соціальної терапії. Вона створила новий етап соціального спілкування, у якому вирівнюються перекручування й диспропорції, викликані географією й економікою, сприяючи росту взаєморозуміння між різними верствами суспільства й народами.

На більше високих стадіях електронна революція виступила як першопричина великих соціальних змін (ЗМІ диктують культуру).

Інформаційна технологія, з'єднана з аудіовізуальними засобами створює цілий мир поведінкових моделей, які постійно, щодня, на роботі й у побуті, оточують людини й програмують його діяльність в усі зростаючому масштабі.

Другий етап комунікаційної революції пов'язаний із трьома великими інноваціями: супутниковий зв'язок, створення оптоволоконних кабелів і кабельних мереж, цифрових електронних пристроїв, із застосуванням мікропроцесорів і інтегральних схем для швидкісного прийому й передачі інформації. Це відкриває доступ будь-якій людині, у будь-якій крапці Землі до баз даних і знань, якщо він має термінальний пристрій (комп'ютер) для одержання інформації.

Подібні інтелектуально-технологічні системи ведуть до принципово нового стану цивілізації й культури - до глобального гіперінтелекту (індустрії даних і знань).

Таким чином, повсюдне впровадження й широке використання інформаційно-комунікативних технологій розглядають як вирішальний крок від індустріального до постіндустріального (інформаційному) суспільству.

Поняття «інформаційно-комунікативний простір» слідом за привнесеним у науковий оберт на початку 90-х років ХХ ст. поняттям «інформаційний простір» є невід'ємним чинником розвитку теорії інформаційного суспільства й

спостережуваних кожним членом соціуму процесів глобалізації.

У цьому зв'язку можна погодитися з тим, що інформація є станом простору. Більше того, інформація як продукт передачі різноманітних форм життєвого простору людини породжує систему більше складного порядку - інформаційний простір.

Щоб інформаційно-комунікативний простір, що автоматично виникає навколо будь-якого виду діяльності, працювало не проти, а в благо, було конструктивним, важливо створити підконтрольну модель, де з максимальною ефективністю здійснюються контакти між різними суб'єктами інформації та комунікації.

Концептуальна модель глобального інформаційного простору перебуває в стадії становлення, у зв'язку із чим встає питання про формування єдиного теоретичного поняття *глобального інформаційного простору*.

Однієї з найважливіших тенденцій становлення інформаційного суспільства є стрімкий інноваційний розвиток, що в умовах глобалізації приведе до створення й використання нових об'єктів інтелектуальної власності, що бідують у правовому захисті. Крім того, що спостерігається в останні роки активне формування й розвиток мережевого інформаційного простору (Інтернет) обумовило необхідність модифікації й систематизації всіх нормативних положень, що діють у сфері авторських і суміжних прав у глобальному інформаційному просторі.

Інформаційний простір є простором тільки тоді, коли воно відбивається у свідомості окремої особи, що визначає широту й зміст інформаційного простору. Глобальний інформаційний простір формується на основі всієї інформації, що людина може одержати в інформаційному суспільстві. Межами глобального інформаційного простору є ті межі, у яких здійснюється передача й поширення інформації в інформаційному суспільстві.

Така концептуальна модель глобального інформаційного простору зв'язує інформаційне суспільство, інформаційний простір і інформаційне право. У юридичній літературі існують і інші концепції

інформаційного простору, що засновані на територіальному, технологічному або функціональному підходах, які в принципі не суперечать концепції глобального інформаційного простору [84, с. 8].

Розробка ж правових конструкцій, застосованих до породжених технічним прогресом і збільшенням можливостей щодо поширення та використання інформації відносинам, є вимогою часу, і в цьому зв'язку застосування авторсько-правових моделей є найбільш прийнятним в умовах формування інформаційного суспільства.

Виходячи з об'єктивних законів інформаційного обміну в інформаційному суспільстві можна виділити додаткову категорію інформаційного простору – мережеве.

Мережевим простором є частина глобального інформаційного простору, обмежена рамками комунікаційних (цифрових інтерактивних) мереж, що передбачає право на доведення до загальної відомості інформації в інтерактивному режимі. Прикладом мережного простору може служити цифрова інтерактивна мережа Інтернет.

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, зовнішньо-формальною стороною якої виступає її комп'ютеризація, а внутрішньо-змістовною – імперативна орієнтація на модернізаційні пріоритети

інтелектуалізму і відповідне профілювання [168].

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

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

Електронне суспільство уявляє собою використання інформаційно-комунікаційних технологій для перетворення органів влади з метою зробити їх більш доступним для громадян, більш ефективним та більш підзвітним.

Зміст електронного суспільства полягає у використанні інформаційних технологій для розширення можливостей кожного члена громадянина. Тому електронне суспільство характеризується використанням ІКТ як основного засобу для колективних розумових та адміністративних процесів (інформатизація, прийняття спільних рішень, контролювання виконання рішень і т.п.) на усіх рівнях: починаючи з рівня місцевого самоуправління і закінчуючи міжнародним.

Таким чином, можна визначити головні складові поняття «інформаційне електронне суспільство»: 1) модернізацію інформаційної економіки на інноваційну модель; 2) електронну індустрію інформаційних послуг; 3) сучасні інтелектуальні інформаційні технології та прогресивні технології волоконно-оптичного зв'язку; 4) значний потенціал науки; 5) розвиток нанотехнологій; 6) комп'ютеризацію суспільно-політичних,

економічних та інших процесів; 7) інформаційне та матеріально-технічне забезпечення різноманітних електронних послуг.

Ось самим така соціальна природа детермінує створення високотехнологічних умов для розвитку інформаційно-правових відносин.

4. Програмоване суспільство та високотехнологічна цивілізація

Інформаційна сфера уявляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, розповсюдження та використання інформації, а також системи регулювання суспільних відносин, що виникають при цьому. Саме в інформаційній сфері при виконанні інформаційних процесів виникають соціотехнічні відносини, що підлягають правовому регулюванню. Нагадаємо, що саме ці суспільні відносини складають 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 (мейнфреймів), 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 розповсюдженої в західних країнах теорії постіндустріального суспільства.

У цьому зв'язку однією з нових форм управління суспільством, визначають *нетократію*, у рамках якої основною цінністю є не матеріальні предмети (гроші, нерухомість і т.п.), а інформація.

Соціальні та науково-технічні процеси високотехнологічної цивілізації вкрай складні, суперечливі та досить складно 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]. Адже у сучасному суспільстві, де основним технічним засобом технології переробки інформації є комп'ютер, пріоритетне місце займає спеціально організована поведінка, що надає можливість знайдення нових алгоритмів і технологій інформаційної діяльності. І це, безумовно, суттєво змінило загальну структуру суспільних відносин в інформаційній сфері, а відтак позначилося на соціотехнологічному рівні життя. За таких умов планомірно відбувається суттєвий вплив як на концепцію побудови й використання технологічних процесів, так і на якість результативної інформації.

Технологічна експансія поступово прирікає людину до штучного 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.

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

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. Суть формування останньої полягає у приєднанні локальних (регіональних) суспільств, держав до сучасної світової комп'ютерної інформаційної культури.

Отже, науково-технічна революція є вирішальним кроком до формування глобальної високотехнологічної цивілізації.

Рівень життя суспільства фактично залежить від технології, звідси перехід на

нову технологічну цивілізаційну ступінь потрібно забезпечити розвитком пріоритетних напрямів модернізації економіки, якими згідно з програмною доктриною Президента РФ Д. А. Медведєва є: 1) енергетика; 2) інформаційні технології (Ай-Ті-технології – від *англ. скор. IT*); 3) біомедичні технології; 4) ядерні технології; 5) телекомунікації.

5. Модернізація технологічної діяльності суспільства та формування технологічного світогляду у цифрову епоху

Модернізація – це удосконалення, поліпшення, відновлення об'єкта, приведення його у відповідність із новими вимогами й нормами, технічними умовами, показниками якості. Модернізуються, у переважній більшості, економічні процеси та технологічне обладнання [77].

Поняття модернізації виникло в 50-60-х рр. ХХ ст. в США для пояснення процесів, що змінюють традиційний суспільний порядок і сприяють перехід цих країн до сучасного (індустріального й 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 терміну. Заперечується, однак, не сам по собі факт модернізації, як він мав місце в історії й продовжує зберігатися до нашого часу, а можливість досягти на цьому шляху в цей час скільки-небудь істотних результатів [123].

Зрештою з'явилися концепції «часткової модернізації», «тупікової модернізації», «кризового синдрому модернізації» та ін.

Тлумачення модернізації як послідовного руху до вибраного стану через ряд проміжних етапів призводить до потреби класифікації різних форм розвитку, серед яких особливе місце займає форма технологічного розвитку, що доганяє.

У підсумку до визначальних факторів модернізації в економіці стали відносити розширення індустріальних технологій, що ґрунтуються на використанні капіталу та наукового знання, широкому освоєнні

природних ресурсів, високотехнологічному розвитку інтелектуального потенціалу, розширенні ринків товарів, капіталу та праці. Утім, як свідчить світовий досвід, для типу перехідного суспільства, до якого поки може бути віднесено Україну, існує ризик застрягти на стадії часткової модернізації, коли формування технологічних інститутів суттєво залежить від економічних, адміністративних, технічних навичок й відповідних організаційних структур.

Існують різні варіанти та шляхи модернізації, але для інформаційної політики держави головним показником є стабільність і технологічність інформаційного простору. Адже зрозуміло, що процес інформатизації є системним перетворенням продукт-орієнтованого способу виробництва у постіндустріальний. В основі інформатизації знаходяться кібернетичні методи й засоби управління, а також інструментарій інформаційно-комунікаційних технологій. У ході інформатизації змінюється матеріально-технологічна основа суспільства, ключове значення починають мати аналітичні інформаційні системи управління, тобто модернізується соціальний уклад життя. Тобто ми бачимо як інформатизація набуває риси іншого феномену – технологізації.

Технологічний світогляд – це система специфічних поглядів на природу, суспільство, людину. Формування технологічного світогляду обумовлено інформаційними особливостями суспільного буття та соціально-технічними умовами. Технологічний світогляд уявляє собою сукупність (систему) стійких поглядів, принципів, оцінок та переконань, що визначають ставлення до технологічних процесів, що відбуваються у навколишньої дійсності, та характеризує бачення світу в цілому й місце людини в сфері високих технологій. Зміна технологічного світогляду детермінує широкі дискусії, у центрі яких знаходиться питання щодо стратегічної основи розвитку техніки, що не вступає в протиріччя з цивілізаційною перспективою. Утім останнім часом висловлюються аргументи на користь так званої «дозованої інформатизації», яка передбачає сукупність нормативних обмежень, що має як позитивне,

так і негативне значення при формуванні єдиноможливої інформаційної концепції високотехнологічного розвитку суспільства.

Звідси, «технологічна діяльність» на сучасному етапі розвитку суспільства має відношення не тільки до техніки або технологій у повсякденному розумінні цих слів.

Отже, разом із відсутністю знайдених кінцевих відповідей на низку невирішених проблем у цій сфері, ми бачимо, що інформатизація поетапно і наступально формує нове соціальне уявлення – системний високотехнологічний світогляд на природу інформаційних процесів.

Як свідчать дослідження модернізації інформаційно-аналітичного забезпечення діяльності органів влади України, у реалізації їх різних стратегій виникають типові проблеми, на які пропонується звернути увагу: 1) усвідомлення актуальності проблем першими керівниками, їхні бажання і воля до вирішення 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.

Технологічна модернізація – це корінні зміни у технологіях, у зв'язку з системним переходом економіки на інноваційній шлях розвитку.

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 обумовленою причиною.

Однією з провідних ознак інформаційної модернізації у цифрову епоху 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.

6. Сутність інформаційної політики

Економічна, політична, інформаційна незалежність відповідає інтересам будь-якої держави, оскільки вона забезпечує свободу й 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.

Далі перейдемо до розгляду сутності та змісту інформаційної політики держави. Як ми вище 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 напрямків її діяльності лежить політика, що відображає принципи, стратегію, основні напрямки і форми досягнення соціальних цілей, які ставлять перед собою суспільство, політичні й владні структури, що його представляють.

Існують різні інтерпретації поняття «політики». Цей термін, як і більшість інших соціального й політичного дискурсу, використовується для позначення певних понять. Досить розповсюдженою, хоча й неповною, залишається найдавніша думка про те, що політика є управлінням. Буквально термін «політика» (від грец. *politike*) означає державну діяльність або державні, суспільні справи, з якими пов'язані загальні засади політичної культури. Тому дефініція «політики» так і не має однозначного тлумачення [157, с. 64-65]. І це пов'язане з тим, що мета політики й способи її досягнення не залишалася незмінною. Як, втім, не залишався незмінним і зміст самого поняття політики.

По-перше, політика розуміється як сфера соціального життя, пов'язана з

діяльністю держави, управлінням суспільними справами й 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 застосований прикметник «політичний».

По-друге, 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 й стосовно до ситуацій, не зв'язаних прямо з діяльністю державних і інших публічних інститутів та організацій.

І нарешті, по-третє термін «політика» використовується в тих випадках, коли мовець прагне підкреслити хитрість, обережність, обачність певного суб'єкта або використання їм маніпуляції, обману й 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 останнім значенні термін «політика» звичайно використовується тільки в повсякденній мові, то перші два поняття є ключовими категоріями політичної науки.

У загальному визначенні соціальна політика є діяльністю держави щодо підтримки стабільного розвитку суспільства за допомогою політики збалансованого добробуту різних соціальних груп і верств населення. Крім того, поняття «політика» може вживатися в значенні ціннісного судження.

Формуючись під впливом різних факторів, політика накладає своєрідний відбиток на інформаційне життя людей. Його необхідно враховувати в інформаційно-правовій діяльності, навіть якщо такий відбиток заслуговує нашого глибокого презирства й зневаги. 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 й 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 їхнє суспільне становище й не піддаються задоволенню без втручання третьої сили, якою 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 обмеження доступу до неї. Інформаційна політика України характеризується монополізацією інформаційного сектору, впровадження нових мультимедійних засобів зв'язку в усі сфери державного управління. Звідси тенденції розвитку законодавства України обумовлюють інтерес до сфери інформаційних відносин і, зокрема, до прав суб'єктів-учасників таких відносин.

Підсумуємо, що *державна інформаційна політика* – це 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.

Отже, державна інформаційна політика є складовою частиною внутрішньої та зовнішньої політики країни, що складається у

регулюванні інформаційних потоків та інформаційної діяльності структур усіх форм власності й підпорядкованості, а також організацій інформаційного профілю.

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

У цьому зв'язку з'явилась нове поняття *«електронна держава»*, що означає спосіб здійснення інформаційних аспектів державної діяльності, що заснований на використанні ІКТ-систем. Разом із тим, електронне суспільство і електронна держава є принципово різними поняттями. Електронна держава має підтримувати за допомогою ІКТ діяльності як виконавчої влади («електронний уряд»), так й парламентських («електронний парламент»), а також судових органів («електронне правосуддя»).

Вектор інформатизації на сучасному етапі має бути зорієнтованим на створення системи «електронного правосуддя», досягнення відкритості, доступності та зручності для учасників процесу за допомогою використання електронних інструментів. Зокрема, планомірний перехід судів до використання новітніх комунікаційних систем та комп'ютерних засобів зв'язку, наприклад таких як системи відеопроколювання судових засідань, значно підвищить якість судових рішень. Впровадження інформаційних електронних технологій дозволить публікувати інформацію щодо руху справ та результатах судового розгляду на Інтернет-сайті відповідних судів.

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

Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр. затверджені Законом України від 9 січня 2007 р. [147]. 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 рр.

Таким чином, *політика безпеки інформаційно-телекомунікаційних технологій* включає правила, директиви та практика, що визначають засоби управління, захисту та розподілення активів, у тому числі критичної інформації, в інформаційних мережах.

7. Національна програма інформатизації

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 в складі Радянського Союзу в рекордний термін створила ядерні, космічні, комп'ютерні технології і зберегла в них лідерство, навіть незважаючи на катаклізми останніх десятиліть.

Широко в світі відома українська школа кібернетики. На початку 90-х рр. минулого століття в УРСР було сформовано концепції та програми інформатизації. Вже у 80-90 рр. ХХ ст. вчені (перш за все фізики-ядерники) для вирішення складних математичних завдань намагалися комбінувати декілька різних робочих станцій, використовуючи вільні обчислювальні ресурси для скорочення часу обробки. Разом із цим потрібно відзначити, що розпад СРСР обумовив глибоку системну технологічну, наукову, освітню, а звідси й інтелектуальну

кризу, наслідки чого ми, нажаль, відчуваємо дотепер, в тому числі у сфері розвитку й впровадження сучасних технологій.

Тенденції повільного відродження науково-технічного потенціалу України з'явилися на початку ХХІ 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 вчених 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 дозволяє одержити 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 компактні, ніж існуючі.

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

Розробка скляних волоконних світловодів з низьким рівнем затухання світла справедливо вважається одним із самих яскравих досягнень науки й техніки ХХ ст. Завдяки використанню волоконних світловодів замість атмосфери було створено оптичні системи зв'язку з надвисокою швидкістю передачі інформації. З іншого боку, дисперсія й нелінійність скла, з якого виготовлені волоконні світловоди, складають передачу інформації на значні відстані. Для того, щоб перебороти ці складнощі, потрібно було провести фундаментальні дослідження з метою розробки правової регламентації волоконно-оптичних інформаційних систем.

Волоконна оптика в цей час одержала широкий розвиток і знаходить застосування в різних галузях науки й 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, які ведуть боротьбу зі злочинністю. Інакше кажучи, високі технології передачі інформації стають однією з науково-технологічних галузей, які надають найбільший вплив на розвиток людського суспільства.

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

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

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

Сьогодні збереглася 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, не порушуючи загального контексту праці, докладно висвітлюються організаційно-правові аспекти розвитку нанотехнологій.

Нанотехнологія – це революційна технологія, яка й визначить профіль ХХІ 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 наукова розробка національної програми розвитку високих технологій постає пріоритетною державною програмою розвитку, оскільки уявляє інтелектуальний прорив. Перехід України до інформаційного суспільства вимагає удосконалення 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 вимагають прискореного

розвитку інформаційного суспільства в Україні.

Разом із тим ступінь розбудови інформаційного суспільства в Україні порівняно із 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, у використанні безготівкових розрахунків 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 розробки конкурентоспроможного програмного забезпечення [121].

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

Глобалізація, інформаційні технології дають абсолютно нові можливості для цивілізацій, культур в плані прояву себе у світі, подальшого розвитку.

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

У цьому зв'язку одним з пріоритетних завдань національної інформаційної політики є розвиток інноваційного проєкту «Укрвікіпедія», який може стати найповнішим джерелом інформації про світ українською мовою. Як відомо, вікіпедія – це унікальний міжнародний інтернет-проєкт енциклопедії, який твориться багатьма (сьогодні їх кількість – 250) мовами світу, який уже зайняв перші позиції серед системно-наукової, довідкової інформації в Інтернеті.

Управління використанням Інтернет охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь всі зацікавлені сторони й відповідні міжурядові й міжнародні організації.

У зв'язку із цим залишаються неврегульованими такі питання: а) політичні повноваження щодо пов'язаних з Інтернетом питань державної політики міжнародного рівня, які мають права й обов'язки стосовно Інтернету; б) приватний сектор відіграє й повинен продовжувати відігравати важливу роль у розвитку Інтернет у технічній та економічній сферах; в) громадянське суспільство також відіграє важливу роль у питаннях, пов'язаних з Інтернет, особливо на

рівні громад, і повинне продовжувати відігравати таку роль; г) міжурядові організації відіграють і повинні продовжувати відігравати роль, що сприяє координації пов'язаних з Інтернет питань державної політики; д) міжнародні організації повинні відігравати важливу роль у розробці технічних стандартів і відповідної політики щодо Інтернет.

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

8. Основні завдання національної системи науково-технічної інформації

Згідно із ст. 9 Закону України «Про науково-технічну інформацію» основними завданнями національної системи науково-технічної інформації є:

1) формування на основі вітчизняних і зарубіжних джерел довідково-інформаційних фондів, включаючи бази і банки даних, та інформаційне забезпечення юридичних та фізичних осіб;

2) одержання, обробка, зберігання, поширення і використання інформації, одержаної в процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності юридичних та фізичних осіб;

3) організація надходження до України, обробка, зберігання і поширення зарубіжної науково-технічної інформації на основі вивчення світового інформаційного ринку;

4) підготовка аналітичних матеріалів, необхідних для прийняття державними органами, органами місцевого і регіонального самоврядування рішень з питань науково-технічного, економічного і соціального розвитку країни;

5) аналітично-синтетична обробка першоджерел, реферування опублікованих і не опублікованих на території України джерел науково-технічної та економічної інформації, створення на цій основі і поширення інформаційної продукції та послуг;

б) розроблення і впровадження сучасних технологій в науково-інформаційну діяльність;

7) організація пропаганди і сприяння широкому використанню досягнень науки і техніки, передового виробничого досвіду;

8) створення загальнодоступної мережі бібліотек, інформаційних центрів громадського користування, як бази для освіти, виробництва та наукових досліджень, системи реалізації прав громадян на культурний та фаховий розвиток [71].

На сучасному етапі 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 високотехнологічними процесами, створенню вітчизняної елементної бази, налагодженню серійного виробництва електронних карток і впровадженню інформаційних систем з їх використанням, широке запровадження цифрового (електронного) підпису.

Таким чином, існує сенс окремо визначити, що у сучасних умовах пріоритетним завданням національної системи науково-технічної інформації стає створення конкурентного середовища для розвитку високих технологій.

9. Правовий режим інноваційної діяльності технопарків та спеціальних економічних зон.

У світовій економічній літературі «інновація» трактується як перетворення потенційного наукового процесу на реальний, що втілюється у нових продуктах і технологіях. У зарубіжній і вітчизняній літературі науково-технічний прогрес пов'язується із інноваційними процесами.

Інноваційний продукт – це результат виконання інноваційного проекту, науково-дослідної і (чи) дослідно-конструкторської

розробки нової технології (у тому числі - інформаційної) чи продукції з виготовленням експериментального зразка чи дослідницької партії і відповідає таким вимогам: є реалізацією (впровадженням) об'єкта інтелектуальної власності, має державні охоронні документи (патенти, свічення), розробка продукту підвищує вітчизняний науково-технічний і технологічний рівень, в Україні цей продукт вироблений (буде вироблений) вперше, чи якщо не вперше, то порівняно з іншим аналогічним продуктом, представленим на ринку, він є більш конкурентоздатним і має істотно вищі техніко-економічні показники.

Формування та розвиток національної інноваційної системи є необхідною умовою реалізації інноваційного сценарію модернізації держави.

Інноваційна економіка є типом економіки, у 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, тому поєднує ряд внутрішніх ознак: комерційну ціль, інтелектуальну основу та отримання прибутку як кінцеву мету.

Одним з основних пріоритетних напрямків 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 зростові.

Такий шлях залишається практично неможливим без вирішення багатьох питань, які пов'язані з правовим регулюванням інноваційної діяльності у сфері високих технологій, що додатково 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 щодо 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 й стабільного розвитку промисловості у сучасних умовах потрібні якісні й органічні модернізаційні зміни у структурі економіки, що неможливо стихійно, без свідомого проведення відповідної державної політики, у тому числі й 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 складають 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 шляхом обробки інформації та установлення 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 факторів.

Ґрунтуючись на цьому потрібно визначити, що соціально-технологічна сфера знаходиться у рамках інвестиційної

діяльності, де особливе місце в модернізації економіці відводиться інвестиційній політиці.

Одним із ефективних варіантів вирішення поставлених проблем є *венчурні компанії* (англ. *venture* – ризиковане підприємство) – тобто інвестиційні компанії, що працюють виключно з інноваційними підприємствами та проектами у сфері високих технологій, діяльність яких спрямована на впровадження новітніх технічних розробок, технологічних нововведень та останніх наукових досягнень, які ще не використовуються на практиці.

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 й технологічного розвитку економіки України є визначення пріоритетних напрямків, форм і методів державного регулювання, у тому числі у сфері високих технологій. Це додатково підкреслює актуальність розробок механізму правової регуляції, оскільки правові норми упорядковують соціальні процеси у сфері високих технологій та інформаційної діяльності, встановлюючи однакові правила поведінки для суб'єктів.

Тому сформульовано п'ять пріоритетів технологічного розвитку країни – це енергетика, у тому числі, енергоефективність, енергозбереження, нові види палива, ядерні технології, інформаційні технології, наземна й космічна інфраструктура передачі інформації, медицина, фармацевтика [16].

Інноваційне підприємство – це підприємство (об'єднання підприємств) будь-якої форми власності, у якого більше 70% обсягу його продукції (у грошовому вираженні) за звітний податковий період є інноваційними продуктами і/чи інноваційною продукцією. Інноваційне підприємство може функціонувати у вигляді інноваційного центру, бізнес-інкубатору, технополісу, технопарку і т.п.

Важливі результати для оздоровлення економіки України може надати впровадження інноваційного проекту, що отримав назву як парк високих технологій. До речі використовуються також інші назви: технопарк, науково-технологічний або регіональний індустріальний парк, що свідчить про існування різних моделей технопарків.

Існує думка, що в сучасних умовах, із розвитком таких засобів комунікацій, як Інтернет, визначення технопарку розширилося. Адаже з'явилася можливість об'єднати територіально розрізнені елементи в одне ціле, тому можна казати про появу «віртуальних» технопарків, тобто технопарків, що не обов'язково розташовані на єдиній компактній території [263].

Однією з нових перспективних моделей може стати *інноград* як територіально відособлений комплекс для розвитку досліджень і розробок, а також комерціалізації їхніх результатів. Інноград не є обмежено технопарком або новим варіантом Академмістечка (наукограду), а стане містом нового типу, що вже є інновацією, в якому існують інноваційні системи ЖКХ, енергетики, самоуправління. Фактично інноград має стати ядром-технопарком, де створюються інновації, мешкають вчені та їхні сім'ї, біля якого створюються поліси з високотехнологічними виробництвами у різних сферах. Таким чином, інноград є прообразом міста майбутнього, іспитовий полігон нової економічної політики, нових технологій, а звідси такий проект не повинен стати містом у традиційному розумінні цього терміну, а центром, де люди мешкають тимчасово.

Інноваційний проект – це проект, згідно якого передбачається розробка, виробництво і реалізація інноваційного продукту і/чи продукції.

Інноваційний проект розробляється відповідно до форми бізнес-плану, стандарт якого відпрацьовується Міністерством науки й освіти України і затверджується Кабінетом міністрів України.

У цілому *правовий режим* (від лат. *regimen* – управління, керівництво) визначається як певна сукупність юридичних

засобів, способів, що застосовуються в певній сфері суспільних відносин та забезпечують дію механізму правового регулювання.

Загальними ознаками правового режиму є: наявність відповідних обмежень, заборон і пільг. Таким чином, фактично правовий режим інноваційної діяльності є особливим порядком, що встановлений для високотехнологічної сфери суспільних відносин.

Згідно зі ст. 1 Закону України «Про спеціальний режим інвестиційної й інноваційної діяльності технологічних парків» *спеціальний режим інноваційної діяльності* є правовим режимом, який передбачає надання державної підтримки щодо стимулювання діяльності технологічних парків, їх учасників та спільних підприємств при реалізації проектів за пріоритетними напрямками діяльності технологічних парків [64].

Звідси правовий режим інноваційної діяльності передбачає особливий порядок регулювання, з використанням різнобічного комплексу правових засобів, що характеризують особливе поєднання взаємодіючих дозволів і заборон та позитивних зобов'язань, що створюють особливу спрямованість регулювання, бажаний соціально-технологічний стан, забезпечують або не забезпечують задоволення інформаційних та інших інтересів суб'єктів права високих технологій.

Спеціальний режим інноваційної діяльності запроваджується для технологічного парку строком на 15 років і діє при виконанні проектів технологічного парку (ст. 3 Закону України «Про спеціальний режим інвестиційної й інноваційної діяльності технологічних парків»).

Особлива, вільна або спеціальна економічна зона визначається як обмежена окремо визначена територія з особливим юридичним статусом по відношенню до іншої території держави та пільговими економічними умовами, включаючи можливість не сплачувати окремі податки або сплачувати їх у меншому розмірі, для національних та іноземних підприємств, однією з головною цілей чого є ефективне рішення стратегічних задач інноваційного

розвитку економіки, що ґрунтується на високих технологіях.

Ціллю проекту є створення в державі сприятливих умов для модернізації індустрії експортно-орієнтованого програмування, розвитку інших експортних виробництв, що ґрунтуються на високих технологіях, а також для концентрації кадрового, науково-виробничого та інвестиційно-фінансового потенціалу. Технопарк представляється 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. Звідси додатково впливає доцільність запровадження особливого правового та податкового режиму техноградів (техномістечек). 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.

Проект визнається інноваційним після визнання вироблених ним продуктів інноваційними (спеціальна процедура підтвердження/кваліфікації) і проходження процедури реєстрації в спеціально уповноваженому для цього органі. Для того, щоб пройти реєстрацію інноваційного проекту, необхідно стати учасником Технопарку.

Метою створення Технопарку, згідно Закону України «Про спеціальний режим інвестиційної й інноваційної діяльності технологічних парків» № 991-XI від 16 липня

1999 р. зі змінами, внесеними Законом України № 3118-III від 07 березня 2002 р. [64], є виконання інноваційних і інвестиційних проектів по розробці і виробництву високотехнологічної наукомісткої продукції.

Технологічний парк (технопарк) – це юридична особа або група юридичних осіб (далі - учасники технологічного парку), що діють відповідно до договору про спільну діяльність без створення юридичної особи та без об'єднання вкладів з метою створення організаційних засад виконання проектів технологічних парків з виробничого впровадження наукоємних розробок, високих технологій та забезпечення промислового випуску конкурентоспроможної на світовому ринку продукції.

Учасниками технологічного парку можуть бути юридичні особи – суб'єкти наукової, науково-технічної, підприємницької діяльності, що уклали між собою договір.

Пріоритетні напрями діяльності технологічного парку – економічно і соціально зумовлені напрями науково-технічної та інноваційної діяльності технологічного парку, що відповідають визначеним законодавством науково-технічним та інноваційним пріоритетам і спрямовані на промислове виробництво конкурентоспроможної високотехнологічної та інноваційної продукції і насичення нею внутрішнього ринку та забезпечення експортного потенціалу держави.

Для фінансової підтримки проектів технологічних парків запроваджується бюджетна програма підтримки діяльності технологічних парків (ст. 6), крім того державою надаються цільові субсидії, окремі види яких визначені Законом (ст. 7).

Відповідальність за нецільове використання ввезених на територію України матеріалів, устаткування, обладнання, комплектуючих та інших товарів, а також коштів цільових субсидій, зарахованих на спеціальні рахунки технологічних парків, їх учасників та спільних підприємств, несуть керівники технологічних парків, їх учасників та спільних підприємств згідно із законом (ст. 12).

Пріоритетними напрямками діяльності Технопарку є: 1) комп'ютерні і

телекомунікаційні технології для навчання, наукових досліджень, мікроелектроніки і нанотехнології; 2) нові і нетрадиційні технології енергозабезпечення і ресурсозбереження, технології ефективного використання низькосортних палив; 3) охорона навколишнього середовища й інженерні та біотехнічні розробки за рішенням екологічних проблем; 4) удосконалення хімічних технологій промислового призначення, одержання матеріалів з новими функціональними можливостями; 5) сучасні технічні комплекси і системи, у тому числі спеціального призначення.

Як правило, технопарк створюється в місті або приміській зоні, частіше за все на території університету, займає невелику площу і має відносно невеликі масштаби діяльності.

В якості пріоритетних напрямів кожного технопарку логічно визначати окремі спеціалізації. У певному сенсі технопарками можливо вважати академістечки. У таких умовах вчені зможуть проводити дослідження у науково-дослідних інститутах, викладати у навчальних закладах та приймати 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, Обнинськ, Санкт-Петербург, Тюмень) досвіду.

З 1994 р. почала практично реалізовуватись ідея створення в Україні наукових, технологічних та інноваційних парків. Згідно з Указом Президента України розпочато проведення економічно-технологічного експерименту на базі агротехнопарку «Броди» на Львівщині. Ця форма організації науки, яка дає змогу включити наукові дослідження до єдиного технологічно-фінансового і підприємницького комплексу, має найбільші перспективи серед інших ринкових форм організації і проведення НДДКР.

Важливе значення інноваційного прориву в Україні стало прийняття Верховною Радою України Закону “Про спеціальний режим інвестиційної й

інноваційної діяльності технологічних парків «Напівпровідникові технології та матеріали, оптоелектроніка і сенсорна техніка», «Інститут електрозварювання імені Е. О. Патона», «Інститут монокристалів»» від 16.07.99 р. Згідно з цим законом передбачаються митні та податкові пільги для технологічних парків при реалізації інвестиційних й інноваційних проектів у пріоритетних напрямках науково-технічної діяльності.

Особливо необхідно виділити Київський, Харківський, Донецький, Дніпропетровський, Запорізький і Львівський регіони, де зосереджено більше 50% наукового потенціалу України. Понад 20% загальної кількості наукових організацій розташовано в м. Києві, 14% — в Харківській, а в Донецькій, Дніпропетровській і Львівській областях — по 6%. У цих областях є всі можливості для створення інноваційної інфраструктури, адже в них переважають наукомісткі і технічно складні галузі.

Зокрема, інноваційне підприємство Технологічний парк «Київська політехніка» - один з восьми Національних Технопарків, зареєстрованих в Україні, створений при найбільшому ВУЗі країни - Національному технічному Університеті «Київський політехнічний інститут».

На території технопарку монокристалів діє науково-технологічний, алмазний концерн «Алкон», який об'єднав науково-технічні, виробничі, фінансові можливості 16 організацій. Основною організацією цього концерну є інститут надтвердих матеріалів ім. В. Бакуля НАН України, а генеральний директор — академік НАН України М. Новіков. В алмазному концерні «Алкон» за рахунок внутрішніх фінансових ресурсів, оптимальної організації циклу «наука-виробництво», використання ряду наукових досягнень інституту експорт мікропорошків кубічного нітриду бору за останні 2 роки збільшений в 5 разів, освоєний випуск нового покоління алмазних і твердосплавних інструментів.

У Львівській області створена і успішно функціонує асоціація «Львів-Технополіс», яка об'єднує більше десяти малих інноваційних підприємств. В

Харківській обласній держадміністрації розроблена регіональна програма інноваційного розвитку виробничої соціально-економічної сфери регіону «Технокрай». Вона передбачає комплексний підхід до технологічного переоснащення виробництва, створення сучасної комунікаційної інфраструктури тощо. Крім того, відпрацьовується модель перетворення міста на територію інноваційного прориву.

Утім, потрібно визнати, що в Україні відбувається подальше відставання в галузі впровадження новітніх технологій (технологічних інновацій) та освоєння на їх базі нових видів наукомісткої продукції. Так, кількість впроваджених прогресивних технологічних процесів на підприємствах машинобудування за останні роки зменшилася більше ніж у 5 разів.

Актуальним завданням є створення в Україні нових форм управління циклом «наука—техніка—виробництво», до яких належать технопарки і технополіси. У сучасному світі технопарки і технополіси відіграють значну роль в реалізації механізму прискорення науково-технічного прогресу в передових галузях промисловості, пов'язаних із реалізацією новітніх досягнень фундаментальної науки.

Створення технопарків, що спеціалізуються на розробці технології нової продукції, є можливим і ефективним за багатьма напрямками залежно від функцій, обсягу і рівня кооперування. Чотирьох технопарків недостатньо для інноваційного прориву української економіки. Але в епоху панування мережі Інтернет та глобальних ринків необхідно створювати і нові, більш потужні віртуальні парки, які забезпечують контакти між численними учасниками інноваційного процесу.

Найпоширенішими можуть бути: технологічні, промислові і дослідно-конструкторські парки. У містах України, які мають потужний науково-технічний потенціал, доцільно створювати технопарки у формі агломерації наукомістких фірм і виробничих підприємств, які групуються навколо наукових центрів. Необхідно створювати технополіси, які будуть не тільки центрами досліджень і освоєння нових типів

наукових розробок і виробництва сучасного обладнання, а й центрами єднання міжнародного співробітництва, виробничої діяльності, налагодження належного сервісу, культурного середовища.

Створення технополісів надасть нового імпульсу для структурних змін у традиційних промислових регіонах. Західні експерти відзначають нагромаджений досвід у великих академічних і вузівських центрах України, що може слугувати основою створення технополісів і вільних економічних зон. Щоправда цей досвід, на жаль, не використовується. Особливо сприятливі умови для технополісів має Київський регіон, де зосереджено висококваліфікований потенціал, а в базових галузях науково-промислового комплексу використовуються технології світового рівня.

Отже, розвиток сучасного виробництва має базуватися на новітніх досягненнях у галузі техніки і технології, передових організаційних формах та принципово нових методах інноваційної діяльності з метою скорочення циклу «наука—виробництво», а венчурний капітал в Україні повинен стати ефективним методом фінансування інновацій та науково-технічного прогресу [219].

Відносини, пов'язані з виконанням проектів технологічних парків за пріоритетними напрямками діяльності технологічних парків, регулюються Законом України «Про спеціальний режим інвестиційної й інноваційної діяльності технологічних парків» [64], а також пов'язаними з ним іншими нормативно-правовими актами.

Держава гарантує стабільність устанавленого спеціального режиму інноваційної діяльності технологічних парків (ст. 13). За більшістю прогнозів інноваційної діяльності технопарків у сфері високих технологій вартість сукупного обсягу виробленої продукції та наданих послуг зможе перевищити 20 млрд. гривень.

10. Реформування національної інформаційної політики

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.

У загальному визначенні реформа є перетворенням, що уводиться законодавчим шляхом. Головною метою реформування національної інформаційної політики є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави [97].

Поряд із позитивними здобутками потрібно визнати певні прорахунки державної політики у сфері розвитку високих інформаційних технологій. Так, потрібно визначити, що *Google* як найбільша пошукова Інтернет-система світу станом на 2009 р. містить 366 600 000 посилань на англійській мові. Утім на російській мові – 366 000, а на українській взагалі – 36 000 посилань.

У Національній програмі інформатизації визначено три основні проблеми державної політики розвитку високих технологій у сфері інформатизації: 1) розроблення і просування універсальних принципів та норм з метою вирішення високотехнологічних 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.

Таким чином, метою національної інформаційної політики України є створення передумов для побудови в державі розвинутого 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 наведені основи державної політики розвитку високих

інформаційних технологій та визначені її стратегічні цілі, що надає підстави для виведення логічної мережі, яку представимо схемою:



Отже, розглянуті основні поняття складають умовну мережу «ІНФОРМАЦІЙНА ПОЛІТИКА (1) – ПРАВО (2) – ВИСОКІ ТЕХНОЛОГІЇ (3)», яка може тлумачитися як «ЦІЛІ-ЗАДАЧІ (1) – ЗАСОБИ ДОСЯГНЕННЯ (2) – РЕЗУЛЬТАТ (3)».

З цього випливає, що інформаційна політика визначає стратегічні цілі-задачі, оптимальним регулятором процесу досягнення яких виступає право в цілому та його окремі галузеві інститути. Звідси, результатом як кінцевою крапкою цілей-задач постають високі технології. При цьому їхня сукупність, у свою чергу, також є новим соціотехнічним процесом інформаційного змісту.

Нарешті, потрібно резюмувати, 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 вирішальним є економічний інтерес, що визначає необхідність правового регулювання

суспільних відносин в галузі інформаційної індустрії.

Переорієнтація інтересів і цілей національної політики з модернізації на глобальний розвиток нових інформаційних технологій – це єдиний послідовний напрямок, що відповідає реаліям сьогодення. Виконання комплексу визначених заходів має призвести до модернізації й технологічному розвитку інноваційної економіки в цілому. Саме в цьому напрямку варто шукати систему цінностей, здатну стимулювати економічний ріст і соціальний розвиток. Лише ввімкнувшись у вирішення проблем високотехнологічної цивілізації глобального порядку, Україна одержить суттєвий імпульс розвитку, зможе перебороти кризу, заявити про себе як про спроможну країну XXI ст. Не повторювати й копіювати те, що вже пройдено іншими, а разом із міжнародним товариством брати участь у створенні нового світу – тільки так можна й надолужити упущене, і створити нову Україну як високотехнологічну державу.

КЛЮЧОВІ СЛОВА: *Інформація, інформатизація, інформаційне суспільство, політика модернізації, технопарки.*

ЛЕКЦІЯ 3. ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЇЇ ОКРЕМИХ ВИДІВ В ЕЛЕКТРОННОМУ ФОРМАТІ

© Синєокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синєокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. *Поняття інформаційної діяльності, її основні напрями та електронні види.*
2. *Правові основи редакційно-видавничої та інформаційної діяльності преси в електронному форматі.*
3. *Правовий статус інформаційних агентств та електронної пошти.*
4. *Організація бібліотечної діяльності та правові проблеми електронних бібліотек.*
5. *Правові особливості організації архівної діяльності та системи електронних архівів.*
6. *Цифрове телебачення, національне радіомовлення і кінематографія України.*
7. *Організаційно-правові засади здійснення видавничої справи та види електронних видань.*
8. *Законодавство у сфері рекламної діяльності та правова регуляція електронної реклами в Інтернеті.*
9. *Правове регулювання державної статистики та електронний облік статистичної інформації.*
10. *Правові проблеми використання інсайдерської інформації.*

1. Поняття інформаційної діяльності, її основні напрями та електронні види

Поняття «діяльність» відіграє ключову роль і виконує ряд найважливіших функцій. Взагалі діяльність визначається як суто людський спосіб відношення до світу, сутністю якого є перетворення й підпорядкування матеріального світу людським цілям, спонуканням і волі, тобто всьому тому, що становить духовну сторону людського буття і є істинно творчим відношенням до навколишнього середовища, створенням нового, неповторного, того, що не зроблене природою.

Тобто фактично діяльність можна розуміти як активність особи, що спрямована на пізнання й перетворення соціуму в цілях задоволення власних потреб. Цей процес за своєю сутністю соціальний, містить у собі такі складові: сам процес діяльності, мета, засоби і результат діяльності.

Отже, діяльність є специфічною інформаційною формою відношення до навколишнього світу, що за змістом становить доцільну його зміну в інтересах людей, умову існування суспільства.

Науковцями висловлюються думки відносно того, що діяльність включає певні елементи: мету, засіб і результат, або мету, засіб, результат і сам процес діяльності, або мету, засіб, результат і форму самого процесу діяльності, або об'єкт, суб'єкт, мету й очікуваний результат, а також засоби, методи та способи діяльності, або суб'єктів, учасників, юридичні дії й операції, засоби і способи їх здійснення, результати дій, або мету, завдання, цілі, суб'єктів і об'єктів, принципи, функції та напрями. Висловлюється також думка, що структуру діяльності утворюють такі елементи, як стадії, етапи, дії, операції.

Потрібно розуміти, що будь-яка діяльність визначально ґрунтується на

використанні інформації різних видів. Утім не будь-яка діяльність може бути інформаційною. Певна інформаційна дія, – це, поперед за усе, оголошення про намір. А реальна дія є свого роду вже реалізацією цього інформаційного наміру.

Тобто інформаційна дія є реалізацією моделей перетворення соціального середовища для досягнення мети у вигляді інформаційного акту. Звідси інформаційною визнається виключно така діяльність, що спрямована на задоволення інформаційних потреб різноманітних суб'єктів, головний зміст якої полягає у збиранні, зберіганні, використанні та поширенні інформації.

Ось тепер зрозуміло, що інформаційна діяльність – це головна продукуюча діяльність в умовах інформаційного суспільства.

Інформаційними визнаються відносини, що виникають з приводу задоволення інформаційних потреб громадян.

Наступна проблема полягає в тому, що 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 ст. 6 Закону України «Про науково-технічну інформацію» визначено, що науково-технічна інформація є об'єктом права власності [71].

Закон України «Про інформацію» регламентує правові основи інформаційної діяльності (ст. 12-16) [67]. Закон 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» визначає, що аналітично-синтетична обробка науково-технічної інформації – це процес обробки інформації за методом аналізу і синтезу змісту документів з метою одержання

необхідних відомостей, а також шляхом їх класифікації, оцінки, співставлення і узагальнення [71].

Основними напрямками 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, обробки і використання наукових знань (інформаційних ресурсів як раціональної форми їх зберігання) для подолання матеріально-енергетичної та екологічної кризи і забезпечення подальшого розвитку суспільства у всіх сферах життєдіяльності.

Ефективність інформаційної діяльності забезпечується через застосування здобутків інформатики, послуг з використанням комп'ютерних інформаційних технологій, у тому числі нових технологій електронної телекомунікації. Засобами реалізації інформаційної діяльності є електронно-обчислювана техніка, цифрові засоби телекомунікації, волоконно-оптичні системи зв'язку та передачі інформації, нанотехнології, суперкомп'ютерні та Грід-технології, розвиток яких постійно стимулюється технологічним прогресом інформаційних відносин.

Особливе місце має бути відведено доцільності як відповідності інформаційного явища певному високотехнологічному процесу, матеріальна або ідеальна високотехнологічна модель якого виступає метою інформаційної діяльності.

Діяльність щодо оприлюднення офіційних нормативно-правових актів також визнається як інформаційна. Таким чином, будь-яка діяльність щодо збирання, зберігання, використання і поширення інформації, спрямована на задоволення інформаційних потреб різноманітних суб'єктів, визнається інформаційною.

Звідси можна визначити інформаційну діяльність як сукупність інформаційних дій, технічних засобів,

організаційних умов і модернізаційних заходів, що ґрунтуються на ефективному використанні високих технологій, метою чого є оптимальне задоволення інформаційних потреб громадян і юридичних осіб, а також реалізація інформаційних функцій і завдань держави.

Основними напрямками інформаційної діяльності є: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Держава зобов'язана постійно дбати про своєчасне створення, належне функціонування і розвиток інформаційних систем, мереж, банків і баз даних у всіх напрямках інформаційної діяльності. Держава гарантує свободу інформаційної діяльності в цих напрямках всім громадянам та юридичним особам в межах їх прав і свобод, функцій і повноважень.

Основними видами інформаційної діяльності є одержання, використання, поширення та зберігання інформації.

Одержання інформації — це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошеної інформації громадянами, юридичними особами або державою.

Використання інформації — це задоволення інформаційних потреб громадян, юридичних осіб і держави.

Поширення інформації — це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошеної інформації.

Зберігання інформації — це забезпечення належного стану інформації та її матеріальних носіїв.

Обробка інформації — це вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних.

Оброблення інформації — це систематичне виконання операцій над інформацією.

Фізична або юридична особа, якій належить право власності на інформацію, вважається *власником інформації*.

В Україні створюються умови для здобуття професійної освіти в галузі інформаційної діяльності через систему її навчальних закладів.

Порядок створення навчальних закладів інформаційного напрямку (журналістики, статистики, бібліотечної та архівної справи, науково-інформаційної діяльності, інформатики, обчислювальної техніки тощо) та принципи їх діяльності визначаються Законом України «Про освіту» та іншими законодавчими актами.

Окремими видами інформаційної діяльності законодавство України визначає: діяльність друкованих засобів масової інформації, діяльність інформаційних агентств, науково-інформаційна діяльність, статистична діяльність, рекламна діяльність, бібліотечна справа, архівна справа, надання телекомунікаційних послуг тощо.

Держава також встановлює обов'язкові для виконання норми, які передбачають наповнення національного інформаційного фонду України, тобто сукупності інформаційних фондів (інформаційних ресурсів) держави: архівного, бібліотечного, стандартів, архіву друку, фонду фільмів, патентного та інших фондів.

Інформаційну діяльність органів державної влади можна умовно розділити на два види: сукупність дій, пов'язаних із задоволенням інформаційних потреб громадян, юридичних осіб приватного права та інших суб'єктів, а також сукупність дій, пов'язаних із задоволенням власних інформаційних потреб.

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.

Працівників розумового труда, чия професійна діяльність ґрунтується на обробці інформації та отриманні нової, в тому числі тих, хто має високий рівень освіти або пов'язаний з освітою (зокрема, технічна інтелігенція, вчені, викладачі, студенти тощо), можна вважати *інформаційними працівниками*.

Особливу інформаційну дієздатність мають співробітники суду, правоохоронних, контрольно-ревізійних та податкових органів, які виконують службові завдання.

Закон України «Про доступ до судових рішень» передбачає, що судді мають право на доступ до усіх інформаційних ресурсів Реєстру, в тому числі до відомостей, що дають можливість ідентифікувати фізичну особу. Доступ суддів до державної таємниці, що міститься в судових рішеннях, забезпечується відповідно до Закону України «Про державну таємницю». Право на доступ до інформаційних ресурсів Реєстру мають посадові чи службові особи, визначені порядком ведення Реєстру.

Повний доступ до судових рішень мають: судді, працівники апарату судів, працівники Державної судової адміністрації, працівники інформаційно-технічного адміністратора Реєстру у разі надання їм на один рік дозволу на такий доступ з урахуванням службових обов'язків і здійснюється шляхом автентифікації користувача.

Особливий правовий статус має і такий представник правоохоронного органу прокуратури як прокурор. Так, Законом України «Про прокуратуру» встановлено, що статистична та інша інформація або їх копії, необхідні для здійснення прокурорського нагляду чи розслідування, видаються на вимогу прокурора або слідчого безкоштовно. При здійсненні прокурорського нагляду за додержанням і застосуванням законів прокурор має право доступу до документів і матеріалів, необхідних для проведення перевірки, в тому числі за письмовою вимогою, і таких, що містять комерційну таємницю або конфіденційну інформацію.

Співробітникам органів міліції для виконання покладених на неї обов'язків

надається право одержувати безперешкодно і безплатно від підприємств, установ і організацій незалежно від форм власності та об'єднань громадян на письмовий запит відомості (в тому числі й ті, що становлять комерційну та банківську таємницю), необхідні у справах про злочини, що знаходяться у провадженні міліції.

Важливим засобом виконання обов'язку органів державної влади та місцевого самоврядування оприлюднювати інформації про свою діяльність є існування їх офіційних видань.

Одним із основних напрямів інформаційної діяльності у сучасних умовах стають електронні новини, електронна статистика, Інтернет-журналістика, цифрові видання, електронні архіви, реклама в Інтернеті та інші види, що дозволяє зробити висновок щодо поступового перетворення інформаційної діяльності преси в новий формат – електронний.

2. Правові основи редакційно-видавничої та інформаційної діяльності преси в електронному форматі

Преса – це частина ЗМІ, сукупність масових періодичних друкованих видань, що призначені для масового читача: газет, журналів, збірників, альманахів тощо.

Діяльність друкованих засобів масової інформації законом України «Про друковані засоби масової інформації (пресу) в Україні» визначається як збирання, творення, редагування, підготовка інформації до друку та видання друкованих засобів масової інформації з метою її поширення серед читачів.

Закон України «Про інформацію» визначає, що *друкованими засобами масової інформації* є періодичні друковані видання (преса) — газети, журнали, бюлетені тощо і разові видання з визначеним тиражем.

Закон України «Про друковані засоби масової інформації (пресу) в Україні» визначає пресу як періодичні і такі, що продовжуються, видання, які виходять під постійною назвою, з періодичністю один і більше номерів (випусків) протягом року на підставі свідоцтва про державну реєстрацію.

Додатки до друкованих засобів масової інформації у вигляді видань газетного та журнального типу є окремими періодичними і такими, що продовжуються, друкованими виданнями і підлягають реєстрації на загальних підставах. Зазначені вище друковані видання можуть включати до свого складу інші носії інформації (платівки, дискети, магнітофонні та відеокасети тощо), розповсюдження яких не заборонено чинним законодавством України.

Друкований засіб масової інформації вважається виданим, якщо він підписаний до виходу в світ і видрукований будь-яким тиражем. Сфера розповсюдження друкованого засобу масової інформації не обмежується.

Свобода слова і вільне вираження у друкованій формі своїх поглядів і переконань гарантуються Конституцією України означають право кожного громадянина вільно і незалежно шукати, одержувати, фіксувати, зберігати, використовувати та поширювати будь-яку відкриту за режимом доступу інформацію за допомогою друкованих засобів масової інформації.

Держава гарантує економічну самостійність та забезпечує економічну підтримку діяльності друкованих засобів масової інформації, запобігає зловживанню монопольним становищем на ринку з боку видавців і розповсюджувачів друкованої продукції.

Друковані засоби масової інформації в Україні видаються державною мовою, а також іншими мовами. Стиль і лексика друкованих засобів масової інформації мусять відповідати загально визнаним етично-моральним нормам. Вживання лайливих і брутальних слів не допускається.

Реєстрація друкованих засобів масової інформації в Україні здійснюється відповідно до Закону України «Про друковані засоби масової інформації (пресу) в Україні», постанови Кабінету Міністрів України від 17.11.97 р. № 1287 «Про державну реєстрацію друкованих засобів масової інформації, інформаційних агентств та розміри реєстраційних зборів» та Положення про державну реєстрацію друкованих засобів масової інформації,

затвердженого Наказом Міністерства юстиції України від 21.02.2006 р. № 12/5 (у редакції наказу Міністерства юстиції України від 23.04.2007 р. N 194/5).

Діяльність друкованих засобів масової інформації, спрямована на отримання прибутку, є підприємницькою діяльністю у цій сфері.

Особа, яка заснувала друкований засіб масової інформації, є його засновником. Особи, які об'єдналися з метою спільного заснування видання, вважаються його співзасновниками.

Підготовку та випуск у світ друкованого засобу масової інформації за дорученням засновника (співзасновників) здійснює редакція або інша установа, що виконує її функції. Редакція діє на підставі свого статуту та реалізує програму друкованого засобу масової інформації, затверджену засновником (співзасновниками).

Редакція друкованого засобу масової інформації набуває статусу юридичної особи з дня державної реєстрації, яка здійснюється відповідно до чинного законодавства України.

Редактор (головний редактор) друкованого засобу масової інформації є керівником редакції, уповноваженим на те засновником (співзасновниками). Редактор (головний редактор) призначається (обирається) на посаду і звільняється з посади в порядку, встановленому засновником (співзасновниками) у статуті редакції відповідно до чинного законодавства України про працю.

Редактор (головний редактор), обраний на посаду трудовим колективом редакції, не може бути звільнений з посади без згоди трудового колективу редакції. Редактор (головний редактор) керує діяльністю редакції в межах повноважень, визначених її статутом, представляє редакцію у відносинах із засновником (співзасновниками), видавцем, авторами, державними органами, об'єднаннями громадян і окремими громадянами, а також у суді і третейському суді та несе відповідальність за виконання вимог, що ставляться до діяльності друкованого засобу

масової інформації, його редакції відповідно до Закону «Про друковані засоби масової інформації (пресу) в Україні» та інших актів законодавства України.

Редакційна колегія — дорадчий орган управління діяльністю редакції друкованого засобу масової інформації — створюється, діє та припиняє свою діяльність відповідно до статуту редакції і очолюється її редактором (головним редактором). Рішення редакційної колегії набирає чинності після його затвердження редактором (головним редактором).

Редакція зобов'язана використовувати авторські матеріали, твори літератури, науки і мистецтва з дотриманням законодавства з питань інтелектуальної власності. Громадяни, юридичні особи і державні органи, а також їх законні представники мають право вимагати від редакції друкованого засобу масової інформації опублікування ним спростування поширених про них відомостей, що не відповідають дійсності або принижують їх честь та гідність.

Якщо редакція не має доказів того, що опубліковані нею відомості відповідають дійсності, вона зобов'язана на вимогу заявника опублікувати спростування їх у запланованому найближчому випуску друкованого засобу масової інформації або опублікувати його за власною ініціативою.

Спростування повинно бути набрано тим же шрифтом і поміщено під заголовком «Спростування» на тому ж місці шпальти, де містилося повідомлення, яке спростовується. Обсяг спростування не може більше ніж удвічі перевищувати обсяг спростовуваного фрагменту опублікованого повідомлення або матеріалу. Забороняється вимагати, щоб спростування було меншим, ніж половина стандартної сторінки машинописного тексту.

Спростування може бути підготовленим у формі відповіді, обсяг якої не перевищує спростовуваного матеріалу. Скорочення чи інші зміни в тексті спростування заявника без його згоди не допускаються.

Журналістом редакції друкованого засобу масової інформації відповідно до Закону «Про друковані засоби масової

інформації (пресу) в Україні» є творчий працівник, який професійно збирає, одержує, створює і займається підготовкою інформації для друкованого засобу масової інформації та діє на підставі трудових чи інших договірних відносин з його редакцією або займається такою діяльністю за її уповноваженням.

У кожному випуску друкованого засобу масової інформації повинні міститися такі вихідні дані: 1) назва видання; 2) засновник (співзасновники); 3) прізвище та ініціали редактора (головного редактора); 4) порядковий номер випуску і дата його виходу в світ; 5) індекс видання, розповсюджуваного за передплатою; 6) тираж; 7) ціна або помітка «Безкоштовно»; 8) адреси редакції, видавця, друкарні; 9) серія, номер і дата видачі свідоцтва про державну реєстрацію; 10) видавець (співвидавець).

Розповсюдження продукції друкованого засобу масової інформації без вихідних даних забороняється. Контрольні примірники періодичних і таких, що продовжуються, видань відразу після надрукування безоплатно надсилаються редакцією засновникові (співзасновникам) і реєструючому органу.

Правові, економічні, організаційні засади державної підтримки засобів масової інформації та соціального захисту журналістів визначає Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів». Зазначений закон розповсюджується не лише на пресу та її журналістів, а і на інші засоби масової інформації (на теле- і радіомовні організації, інформаційні агентства).

Професійні назви службових посад (роботи) журналістів включаються до державного класифікатора професій України, тарифно-кваліфікаційні характеристики цих посад (роботи) — до нормативного акта, який призначається для державного регулювання оплати та охорони праці. Стаж роботи журналіста в державних та комунальних засобах масової інформації зараховується до стажу державної служби, а стаж державної служби зараховується до

стажу роботи журналіста в державному або комунальному засобі масової інформації.

Журналісти державних та комунальних засобів масової інформації отримують надбавки, користуються пільгами, передбаченими для державних службовців відповідних категорій посад [121].

Наприкінці ХХ ст. у зв'язку з розповсюдженням Інтернету з'явився новий різновид журналістики – електронна або Інтернет-журналістика.

Журналістів, що працюють на Інтернет-видання називають *Інтернет-журналістами*, специфіка роботи яких дозволяє не стикатися з багатьма атрибутами традиційної журналістики, зокрема спеціалізованою апаратурою для телезйомки та звукозапису, поліграфією та ін. Разом із тим важливою прогалиною залишається правовий аспект діяльності відповідальності журналіста інформацію, що він опублікував в Інтернеті. Інтернет-видання керуються загальними принципами журналістики. Звідси у структурі Інтернет-видань можуть бути створені *Інтернет-редакції*, де здійснюється електронне редагування інформаційних матеріалів, утім сьогодні це не є обов'язковою умовою.

3. Правовий статус інформаційних агентств та електронної пошти

Поняття «агентство» має декілька визначень. У загальному розумінні пропонуємо вважати агентство як установу, що виконує певну державну, суспільну або соціальну функцію.

Закон України «Про інформаційні агентства» визначає діяльність інформаційних агентств — це збирання, обробка, творення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції.

Інформаційними агентствами є зареєстровані як юридичні особи суб'єкти інформаційної діяльності, що діють з метою надання інформаційних послуг.

Під представництвом інформаційного агентства в Україні слід розуміти зареєстровану в Україні відповідно до чинного законодавства як суб'єкт

інформаційної діяльності будь-яку установу (бюро, представництво, корпункт тощо), що представляє в Україні державне або недержавне інформаційне агентство, зареєстроване як юридична особа згідно з чинним законодавством відповідної країни, і яке здійснює свою діяльність в Україні у сфері інформації відповідно до Закону України «Про інформацію», Закону України «Про інформаційні агентства».

Інформаційні агентства не мають права у своїх матеріалах розголошувати дані, що становлять державну таємницю, або іншу інформацію, яка охороняється законодавством, закликати до насильницької зміни або повалення існуючого конституційного ладу, порушення територіальної цілісності України, підриву її безпеки, вести пропаганду війни, насильства і жорстокості, розпалювати расову, національну, релігійну ворожнечу, розповсюджувати порнографію або іншу інформацію, яка підриває суспільну мораль або підбурює до правопорушень, принижує честь і гідність людини, а також інформацію, яка ущемляє законні права й інтереси громадян, давати оцінку щодо винуватості осіб у здійсненні злочину, вказувати на особу, яка ніби скоїла злочин до рішення суду, публікувати матеріали, які розкривають тактику і методику розслідування.

Державна реєстрація інформаційних агентств, заснованих за участю громадян та/або юридичних осіб інших держав, здійснюється відповідно до порядку, встановленого законодавством для державної реєстрації спільних (за участю іноземного капіталу) підприємств.

Журналіст інформаційного агентства — це творчий працівник, який збирає, одержує, створює та готує інформацію для інформаційного агентства і діє від його імені на підставі трудових чи інших договірних відносин з ним або за його уповноваженням. Належність журналіста до інформаційного агентства підтверджується службовим посвідченням цього агентства чи іншим документом, виданим йому цим агентством.

Журналіст інформаційного агентства має права та виконує обов'язки, визначені чинним законодавством України про пресу, телебачення і радіомовлення. Акредитація журналіста інформаційного агентства при державних органах та органах управління об'єднань громадян проводиться на підставах і в порядку, встановлених чинним законодавством України.

Спеціалістом у галузі засобів комунікації є працівник інформаційного агентства, який на професійних засадах здійснює розповсюдження інформаційної продукції через засоби комунікації та несе відповідальність за використання цих засобів виключно на підставі чинного законодавства України.

Видавцем (виробником) продукції інформаційного агентства може бути як саме агентство, так і суб'єкт підприємництва, який здійснює випуск (тиражування або виробництво) інформаційної продукції на підставі угоди, укладеної між ним та інформаційним агентством.

Розповсюджувачем продукції інформаційного агентства може бути як саме агентство, так і суб'єкт підприємництва — власник (користувач) засобу комунікації, через який він розповсюджує продукцію інформаційного агентства в порядку і на умовах, визначених чинним законодавством України та укладеною між ними угодою.

Споживачами продукції інформаційних агентств є громадяни, юридичні особи, державні органи України та інших держав, які на підставі відповідної угоди з інформаційними агентствами одержують їх інформаційну продукцію.

Продукція інформаційного агентства — це матеріалізований результат його діяльності, призначений для розповсюдження з метою задоволення інформаційних потреб громадян, юридичних осіб, держави. Продукція інформаційного агентства є його власністю, якщо інше не передбачено законодавством. Право власності на неї охороняється чинним законодавством України.

Інформаційні агентства згідно з чинним законодавством України поширюють свою продукцію державною, а

також іншими мовами, дотримуючи загальновизнаних етично-моральних норм слововживання.

Основними видами продукції інформаційних агентств є: електронна, друкована, фото-, кіно-, аудіо- та відеопродукція.

Кожен випуск продукції інформаційних агентств повинен містити такі вихідні дані: 1) назву інформаційного агентства; 2) прізвище чергового редактора чи відповідального за випуск та їх реквізити; 3) порядковий номер випуску і дату його виходу у світ; 4) адресу агентства.

Засобами комунікації є засоби розповсюдження продукції інформаційних агентств, такі як: друковані та екранні видання, радіо, телебачення (кабельне, супутникове, глобальне), електричний та електронний зв'язок (телеграф, телефон, телекс, телефакс), комп'ютерні мережі та інші телекомунікації [121].

Мережеву службу, що дозволяє користувачам обмінюватися повідомленнями або документами без застосування паперових носіїв, називають *електронною поштою (Electronic mail, e-Mail)*.

4. Організація бібліотечної діяльності та правові проблеми електронних бібліотек

Бібліотека – це установа, де зібрані та зберігаються друковані твори та інші писемності для суспільного користування. Також бібліотека здійснює довідково-бібліографічну роботу.

Закон України «Про бібліотеки і бібліотечну справу» визначає, що *бібліотека* — це інформаційний, культурний, освітній заклад, що має упорядкований фонд документів і надає їх у тимчасове користування фізичним та юридичним особам.

Закон України «Про бібліотеки і бібліотечну справу» визначає, що бібліотечна справа є складовою частиною інформаційної, виховної, культурно-освітньої діяльності, що включає комплекс державних, громадських, наукових та практичних заходів, які забезпечують організацію діяльності бібліотек, їх науково-

дослідну і методичну роботу, а також підготовку бібліотечних фахівців.

Закон України «Про бібліотеки і бібліотечну справу» визначає статус бібліотек, правові та організаційні засади діяльності бібліотек і бібліотечної справи в Україні, гарантує право на вільний доступ до інформації, знань, залучення до цінностей національної та світової культури, науки та освіти, що зберігаються в бібліотеках.

Бібліотечна справа — це галузь інформаційної, культурної, освітньої діяльності суспільства, що включає створення і розвиток мережі бібліотек, формування та обробку бібліотечних фондів, організацію бібліотечного, інформаційного та довідково-бібліографічного обслуговування користувачів бібліотек, підготовку бібліотечних кадрів, наукове та методичне забезпечення розвитку бібліотек.

Бібліотечний фонд — це упорядковане зібрання документів, що зберігається в бібліотеці.

Бібліотечна система України — це розгалужена мережа бібліотек різних видів, пов'язаних взаємодією і взаємовикористанням бібліотечних ресурсів.

Бібліотечні ресурси — це упорядковані фонди документів на різних носіях інформації, довідково-пошуковий апарат, матеріально-технічні засоби опрацювання, зберігання і передачі інформації.

За значенням бібліотеки поділяються на: 1) всеукраїнські загальнодержавного значення (національні, державні); 2) республіканські (Автономної Республіки Крим); 3) обласні; 4) міські; 5) районні; 6) селищні; 7) сільські.

За змістом бібліотечних фондів бібліотеки є: 1) універсальні; 2) галузеві; 3) міжгалузеві.

За призначенням бібліотеки поділяються на: 1) публічні (загальнодоступні); 2) спеціальні (академії наук, науково-дослідних інститутів, навчальних закладів, підприємств, установ, організацій); 3) спеціалізовані (для дітей, юнацтва, осіб з фізичними вадами).

Публічні, спеціальні та спеціалізовані бібліотеки можуть об'єднуватися у централізовані бібліотечні системи.

Національна бібліотека України — провідний державний культурний, освітній, науково-інформаційний заклад, що виконує функцію методичного та координаційного центру з питань бібліотекознавства, бібліографознавства, документознавства, бере участь у розробленні державної політики в галузі бібліотечної справи та реалізує її.

Державна бібліотека — це бібліотека загальнодержавного значення, що здійснює бібліотечне, бібліографічне, інформаційне обслуговування користувачів і виконує функцію всеукраїнського науково-дослідного, методичного та організаційного центру бібліотек відповідної галузі або категорій користувачів. Державна бібліотека може бути універсальною, спеціальною, спеціалізованою. Державна бібліотека також має право на одержання обов'язкового безоплатного примірника документів.

Центральні бібліотеки — це головні бібліотеки регіонів, які зобов'язані формувати, зберігати та надавати в користування найбільш повне зібрання документів у межах своєї території, організувати взаємовикористання бібліотечних ресурсів і надавати методичну допомогу бібліотекам різних видів відповідних територій.

Значне місце у бібліотечній системі України займають *бібліотеки закладів освіти*. Так, наприклад, Наказом Міносвіти від 30.04.1998 р. № 155 було затверджено Типове положення про бібліотеку вищого закладу освіти Міністерства освіти України. Відповідно до наказу така бібліотека є навчальним, науковим, інформаційним та культурно-просвітницьким структурним підрозділом вищого навчального закладу.

Обмінні фонди — це фонди бібліотек, які використовуються для обміну, перерозподілу, безкоштовної передачі та реалізації документів. Обмінний фонд відокремлений від основного фонду, на баланс бібліотеки-фондоутримувача не береться та не використовується для обслуговування читачів.

До обмінного фонду приймаються документи всіх видів, з усіх галузей знань, такі, що не втратили наукового, виробничого, історико-культурного значення

та є фізично придатними для подальшого використання. Документи, отримані бібліотекою-фондоутримувачем від інших бібліотек, організацій та приватних осіб, приймаються до обмінного фонду після попереднього перегляду і відбору необхідних видань до основного фонду бібліотеки.

Приймання видань до обмінного фонду здійснюється за супровідними документами (акт і список, накладна, квитанція тощо). У разі їх відсутності необхідні документи складаються самою бібліотекою.

Розповсюдження документів з обмінного фонду здійснюється шляхом:

- 1) обміну документами між бібліотеками та органами науково-технічної інформації, іншими установами України;
- 2) безкоштовної передачі документів бібліотекам, засновникам бібліотек;
- 3) безкоштовної передачі документів центрам української культури в Україні та інших державах;
- 4) обміну документами з вітчизняними та міжнародними благодійними організаціями;
- 5) передачі літератури з благодійною метою громадським організаціям та установам;
- 6) реалізації (продажу) документів бібліотекам і населенню.

Відбір та передача документів з обмінного фонду здійснюється на основі офіційного листа бібліотеки-замовника, з урахуванням профілю та потреб даної бібліотеки, і письмового дозволу директора бібліотеки, яка передає документи, або керівника установи, підприємства чи організації, у підпорядкуванні яких перебувають бібліотеки [121].

У програмуванні під терміном бібліотека розуміють збірник підпрограм або об'єктів, що використовуються для розробки програмного забезпечення.

Останнім часом все більше розповсюджуються електронні документи та входять до фонду бібліотек у вигляді мікроформ (наприклад, мікрофіши, мікрокарти та мікрофільми), аудіо- та відеокасети, діапозитиви, оптичні носії (наприклад, CD-ROM).

Електронна бібліотека – це упорядкована колекція різнорідних електронних документів із засобами навігації та пошуку. Так, електронна бібліотека може бути веб-сайтом, де поступово накопичуються різні тести (від літературних до комп'ютерних програм) та медіа-файли.

Звідси електронні бібліотеки потрібно відмежовувати від суміжних структурних типів сайту, особливо літературного.

Електронні бібліотеки можуть бути універсальними та спеціалізованими. Особливе місце в ряду електронних бібліотек займають Інтернет-бібліотеки, як правило націлені на збирання новітніх типів текстів та творів авторів, що найбільш яскраво заявили про себе саме в Інтернеті. Крім того, існують Інтернет-бібліотеки науково-освітньої тематики, в яких зібрані видання, що необхідні для здійснення навчального процесу [44].

Слід констатувати недостатнє інформаційне забезпечення пріоритетних напрямів інноваційної діяльності в Україні, про що свідчить, наприклад, наявність у фондах вітчизняних бібліотек на порядок меншої кількості наукових видань з даних напрямів, ніж у бібліотеках Росії. Для кардинального покращення ситуації при організації досліджень в інноваційній сфері доцільно започаткувати відповідну державну програму, що передбачала б цільове виділення асигнувань на створення відповідної інформаційної бази.

З кожного напрямку інноваційної діяльності доцільно створити Веб-портал, що інтегруватиме відомості про теоретичні та науково-прикладні досягнення в вибраній сфері, наявні інформаційні ресурси, організації та фахівців, які займаються даною проблематикою тощо. Наявність такого порталу сприятиме досягненню якісно нового рівня повноти й оперативності інформаційного забезпечення розвитку відповідних наукових і прикладних напрямів [183].

Певні електронні бібліотеки публікують літературні твори без попередньої згоди авторів, чим порушується авторське право. Крім того, існує

невирішеною проблема *оцифровки бібліотечних фондів* з використанням новітніх засобів інформаційних технологій, не запитуючи дозволу у авторів, що також вимагає окремого організаційно-правового врегулювання.

5. Правові особливості організації архівної діяльності та системи електронних архівів

Архів – це установа або структурний підрозділ установи, організації або підприємства, що здійснює прийом, комплектування та зберігання архівних документів в інтересах користувачів.

Закон України «Про Національний архівний фонд та архівні установи» від 24 грудня 1993 року регулює відносини, пов'язані із формуванням, обліком, зберіганням і використанням Національного архівного фонду, та інші основні питання архівної справи.

Закон України «Про Національний архівний фонд та архівні установи» визначає, що архівна справа — це 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.

Національний архівний фонд України відповідно до Закону України «Про Національний архівний фонд та архівні установи» — це сукупність архівних документів, що відображають історію духовного і матеріального життя Українського народу та інших народів, мають культурну цінність і є надбанням української нації та складовою частиною вітчизняної і світової історико-культурної спадщини.

До Національного архівного фонду України (НАФ) належать архівні документи (оригінали або копії, що їх заміняють) незалежно від їх виду, видів носіїв інформації, місця і часу створення і місця зберігання, режиму доступу, форми власності на них, що перебувають на території України або за її межами і відповідно до міжнародних

договорів, ратифікованих Верховною Радою України, підлягають поверненню в Україну.

Відповідно до Закону України «Про Національний архівний фонд та архівні установи» *архівний документ* — це документ незалежно від його виду, виду матеріального носія інформації, місця, часу створення і місця зберігання та форми власності на нього, що припинив виконувати функції, для яких був створений, але зберігається або підлягає зберіганню з огляду на значущість для особи, суспільства чи держави або цінність для власника також як об'єкт рухомого майна. На сьогодні розроблено та затверджено національний стандарт ДСТУ 4331.2004 «Правила описування архівних документів».

Документ Національного архівного фонду — це архівний документ, культурна цінність якого визнана відповідною експертизою та який підлягає державному обліку і зберіганню.

Унікальний документ — це документ Національного архівного фонду, що становить виняткову культурну цінність, має важливе значення для формування національної самосвідомості Українського народу і визначає його вклад у всесвітню культурну спадщину. *Експертиза цінності документів* — це всебічне вивчення документів з метою внесення їх до Національного архівного фонду або вилучення з нього та встановлення термінів зберігання.

Архівна установа, архів, архівний підрозділ, архівний відділ — це відповідно установа чи структурний підрозділ, що забезпечує облік і зберігання архівних документів, використання відомостей, що в них містяться, та формування Національного архівного фонду і/або здійснює управління, науково-дослідну та інформаційну діяльність у сфері архівної справи і діловодства.

Державна архівна установа — це архівна установа, що здійснює свою діяльність за рахунок коштів Державного бюджету України. *Приватне архівне зібрання* — зібрання архівних документів, що є власністю однієї або кількох осіб.

Архівні установи можуть засновуватися на будь-якій формі власності. Засновниками архівних установ можуть бути

органи державної влади, органи місцевого самоврядування, юридичні та фізичні особи.

Діяльність архівних установ здійснюється у порядку, визначеному Законом України «Про Національний архівний фонд та архівні установи», правилами, положеннями, інструкціями, затвердженими центральним органом виконавчої влади у сфері архівної справи і діловодства, державними стандартами та іншими нормативно-правовими актами.

Систему архівних установ України становлять: 1) спеціально уповноважений центральний орган виконавчої влади у сфері архівної справи і діловодства; 2) центральні державні архіви України; 3) галузеві державні архіви; 4) державний архів в Автономній Республіці Крим; 5) місцеві державні архівні установи; 6) інші місцеві архівні установи; 7) архівні підрозділи державних наукових установ, музеїв та бібліотек; 8) архівні підрозділи органів державної влади, органів місцевого самоврядування, державних і комунальних підприємств, установ та організацій; 9) архівні підрозділи об'єднань громадян, релігійних організацій, а також підприємств, установ та організацій, заснованих на приватній формі власності; 10) архівні установи, засновані фізичними особами та/або юридичними особами приватного права; 11) науково-дослідні установи, а також підприємства та організації у сфері архівної справи і діловодства.

Центральні державні архіви України створюються за рішенням Кабінету Міністрів України для зберігання документів Національного архівного фонду відповідно до свого профілю, що мають загальнодержавне значення.

Галузеві державні архіви створюються для зберігання геологічних, гідрометеорологічних, картографічних та інших специфічних видів архівних документів, які потребують особливих умов їх зберігання і використання відомостей, що в них містяться. Рішення про створення галузевих державних архівів приймається Кабінетом Міністрів України на підставі спільного подання центрального органу виконавчої влади у сфері архівної справи і

діловодства та центрального органу виконавчої влади, що реалізує державну політику в галузі, де створюється відповідний архів.

Місцеві державні архівні установи створюються у порядку, передбаченому законом, для зберігання документів Національного архівного фонду, що мають місцеве значення, та здійснення управління архівною справою і діловодством на відповідній території. До місцевих державних архівних установ належать державні архіви областей, міст Києва і Севастополя, архівні відділи районних, районних у містах Києві і Севастополі державних адміністрацій.

Державні наукові установи, музеї та бібліотеки мають право створювати архівні підрозділи для зберігання документів Національного архівного фонду, а також поповнювати свої фонди і колекції профільними документами.

Архів зберігає документи НАФ в особливому режимі, що забезпечує їх збереженість і цілісність інформації, що міститься в них, цілісність упорядкованих документальних комплексів (архівних фондів, архівних колекцій, архівних зібрань тощо), доступність їх для користувачів.

Таємні документи організуються в порядку, передбаченому спеціальною інструкцією, з віднесенням їх до відповідних архівних фондів або нефондових комплексів на загальних засадах.

Архіви, архівні підрозділи (далі — архіви) розміщуються в спеціально збудованих або пристосованих для зберігання документів будівлях або окремих приміщеннях будівель. Будівництво й реконструкція будівель архіву проводяться відповідно до спеціальної нормативної та проектної документації.

Придатність території для розташування архіву визначається з урахуванням висновку місцевої санітарно-епідеміологічної станції щодо ступеня забрудненості повітря.

У виключних випадках оригінали цих документів може бути видано лише з письмового дозволу директора архіву. Не видаються для користування і проведення

робіт, пов'язаних зі створенням страхового фонду і фонду користування та поліпшенням фізико-хімічного стану, документи, що не пройшли наукового описування і технічного оформлення. Такі документи може бути видано, як виняток, для проведення невідкладних реставраційно-ремонтних робіт. Не видаються для користування документи під час проведення перевіряння їх наявності та стану, проведення реставраційних та інших спеціальних робіт з ними, а також документи з обмеженим режимом доступу, допуск до яких надається у встановленому законодавством порядку.

Основні правила роботи державних архівів України встановлюють, що основними принципами користування документами архіву є: 1) відкритість ретроспективної документної інформації, 2) законність її пошуку, отримання та використання, 3) рівні права доступу до неї усіх юридичних і фізичних осіб, 4) незавдання шкоди документам під час користування ними. Стаття 15 Закону України «Про Національний архівний фонд та архівні установи» визначає доступ до документів Національного архівного фонду. Документи Національного архівного фонду і довідковий апарат до них надаються у користування в архівних установах з часу їх надходження на зберігання, а в приватних архівних зібраннях — відповідно до рішення їх власників.

Держава заохочує власників приватних архівних зібрань до розширення доступу до документів Національного архівного фонду, сприяє публікації та експонуванню цих документів на виставках. Забороняється відносити до державної або іншої передбаченої законами України таємниці інформацію про місця зберігання документів Національного архівного фонду, що належать державі, територіальним громадам, а також створювати таємні архіви для зберігання таких документів.

Архів забезпечує для громадян України, іноземців та осіб без громадянства, що перебувають в Україні на законних підставах, вільний доступ до документів з відкритою інформацією та архівних довідників і баз даних до них з часу

надходження цих документів на зберігання до архіву чи з часу створення в архіві цих довідників та баз даних.

Архів може обмежити доступ до документів НАФ, що належать державі, територіальним громадам, на строк до одного року в зв'язку з їх науково-технічним опрацюванням, перевіркою наявності та стану або реставрацією. У разі проведення великого обсягу зазначених робіт строк обмеження може бути продовжено з дозволу Держкомархіву України, але не більше, ніж на один рік.

Доступ до документів з конфіденційною інформацією про особу, а також до документів, що можуть створити загрозу для її життя чи недоторканості житла може бути надано з дозволу фізичної особи, права та законні інтереси якої можуть бути порушені (суб'єкта персональних даних), а у разі його смерті — з дозволу її спадкоємців. До таких документів можуть належати особові справи, медичні карти (історії хвороб), первинні документи переписів населення, соціологічних досліджень та інші документи офіційного походження, а також листи, щоденники та інші документи особового походження, що містять окремі відомості чи сукупність відомостей про факти, події і обставини приватного життя фізичної особи.

У разі виявлення особою недостовірних відомостей про себе до документів з персональними даними може бути долучено документи, що спростовують або уточнюють ці дані.

Доступ до документів, що є об'єктами авторського і суміжних прав та права інтелектуальної власності, надається на загальних підставах, якщо інше не передбачено письмовим розпорядженням суб'єкта права (фондоутворювача чи іншої особи) або його спадкоємців.

Доступ до аудіовізуальних та науково-технічних документів, створених як продукт цільової виробничої діяльності, регулюється угодою архіву з юридичними особами — виробниками, які передали документи на зберігання, за погодженням з іншими суб'єктами права відповідно до законодавства. Про відмову в доступі користувачеві повідомляється письмово із

зазначенням вичерпних підстав відмови [121].

Порядок користування документами Національного архівного фонду України, що належать державі, територіальним громадам затверджено Наказом Державного комітету архівів України від 24.11.2005 р. № 139.

Державна програма розвитку архівної справи на 2006-2010 роки, затверджена Постановою Кабінету Міністрів України від 1 лютого 2006 р. № 92, визначає, що архівна справа є важливою складовою інформаційної та культурної сфери життєдіяльності суспільства, що охоплює наукові, організаційні, правові, технологічні, економічні та інші питання, пов'язані з нагромадженням, обліком, зберіганням юридичними і фізичними особами архівних документів та використанням відомостей, що в них містяться.

В інформатиці архів має інше значення і означає файл, що містить в собі інформацію з одного або декількох, іноді стислих (без втрат), інших файлів. Так, архів Інтернету збирає копії веб-сторінок, графічні матеріали, відео- та аудіо записи та програмне забезпечення, чим забезпечується довгострокове архівування зібраного матеріалу та безкоштовний доступ до своїх баз даних для широкої публіки.

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.

Електронний архів – це комплексне рішення по створенню і наповненню електронного архіву документів, забезпеченню їхнього надійного збереження й оперативної доступності, а значить – ефективного використання. 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. Співробітники підрозділів, що володіють відповідними правами, у будь-який момент можуть одержати його електронну копію. Паперовий оригінал при цьому залишається в оперативному архіві централізованої служби, звідки після закінчення визначеного терміну він передається безпосередньо в централізований архів організації. Така форма збереження значно знижує можливість втрати документів і підвищує оперативність роботи за рахунок скорочення часу пошуку потрібного документа.

Визначимо *основні задачі*, що вирішуються при впровадженні електронного архіву: 1) підвищення надійності збереження інформації, зменшення ризику втрати важливої інформації внаслідок недбалості персоналу 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 за умови наявності відповідних прав доступу; 4) інтеграція з іншими інформаційними системами підприємства.

Електронний архів виконує наступні *функції*: 1) організація збереження електронних версій документів і облікової інформації; 2) ведення класифікаторів та рубрикаторів і їх використання для пошуку документів; 3) встановлення і підтримка логічних зв'язків між документами; 4) організація пошуку документів – а) за атрибутами реєстраційних карток; б) повнотекстовий пошук; в) за анотаціями; 5) забезпечення доступу до облікової інформації та електронних документів відповідно до прав доступу; 6) ідентифікація електронних документів за їхніми реквізитами; 7) формування звітів про роботу користувачів з електронним архівом.

Отже, електронний архів є якісно новим рівнем використання документальної

інформації. Його впровадження дає могутній імпульс до розвитку органам державного управління, міністерствам і відомствам, архівам, банкам, промисловим підприємствам і корпораціям, великим комерційним фірмам, установам науки, освіти і культури [259].

Подібними за призначенням з електронними журналами є *архіви електронних препринтів наукових статей*, наприклад ArXiv.org. [254] Подібні електронні архіви забезпечують своєчасне інформування про нові наукові статті з і забезпечення доступу до текстів. Головна різниця полягає в тому, що в електронних журналах статті проходять рецензування, що, як правило, позитивно позначається на їхній якості.

6. Цифрове телебачення, національне радіомовлення і кінематографія України

Технології телебачення не були винайдені однією людиною і за один раз.

Перший етап становлення та кількісного зростання телерадіоорганізацій (надалі — ТРО) України припав на 1993-1999 рр. За цей час їх кількість зросла з 25 (головним чином державні ТРО) до 791 компанії. Паралельно розгортався процес форматування мовлення кожної з телерадіоорганізацій, здебільшого хаотичний.

Другий етап (2000-2004 рр.) ознаменувався якісними змінами в національному телерадіопросторі. Хоча домінуючою тенденцією залишалося кількісне зростання, зокрема кількість ТРО сягнула 1100, а загальний обсяг мовлення — майже 9 тисяч годин щодоби. Після характерного для першого етапу засилля в українському телерадіофері зарубіжної відео- і аудіопродукції почала збільшуватися кількість програм вітчизняного виробництва, спроможних успішніше конкурувати із зарубіжними аналогами. Розпочалося очищення вітчизняного телерадіоферу від пропаганди насильства і розпусти. Мешканці більшості регіонів України стали приймати, крім передач місцевих ТРО, також і прог-

рами 6-8 центральних (київських) теле- і радіокомпаній.

Третій етап, що розпочався в 2004-2005 рр. і триває донині, характеризується передусім масовим переходом ТРО на цифрове мовлення і викликаною цим докорінною перебудовою їхньої діяльності. Оскільки запроваджені технології якісно змінюють ситуацію в телерадіопросторі, Національна рада визначила цей процес як один із своїх пріоритетів, плануючи діяльність таким чином, щоб до 2014 р. в Україні було завершено перехід на *цифрову форму мовлення*.

Суб'єктами інформаційної діяльності у сфері телебачення і радіомовлення визнаються юридичні особи, які здійснюють господарську діяльність у сфері телебачення і радіомовлення (телерадіоорганізації, провайдери програмної послуги тощо).

Телерадіоорганізація — це зареєстрована у встановленому законодавством порядку юридична особа, яка на підставі виданої Національною радою України з питань телебачення і радіомовлення ліцензії на мовлення створює або комплектує та/чи пакує телерадіопрограми і/або передачі та розповсюджує їх за допомогою технічних засобів мовлення.

Структуру національного телебачення і радіомовлення України становлять: 1) державні та комунальні телерадіоорганізації, 2) система Суспільного телебачення і радіомовлення України, 3) приватні, незалежно від способу розповсюдження програм, 4) громадські та інші телерадіоорганізації, засновані відповідно до вимог законодавства України.

Суспільне телебачення і радіомовлення України — це організаційно-правова форма некомерційного телебачення і радіомовлення, засади діяльності якої визначено Законом України «Про систему Суспільного телебачення і радіомовлення України». Право на заснування телерадіоорганізацій як суб'єктів господарювання в Україні належить юридичним особам України та громадянам України, не обмеженим у цивільній дієздатності.

Мовник (теле- чи радіо) — суб'єкт господарювання, який створює (комплектую

та/або пакетує) телевізійні чи радіопрोगрами та передачі і розповсюджує їх у відкритому або кодованому вигляді за допомогою технічних засобів шляхом трансляції та ретрансляції для приймання їх споживачами.

Відповідно до пункту 2 перехідних положень Закону України «Про телебачення і радіомовлення», до загальнонаціональних мовників прирівнюються телерадіоорганізації, які на день набрання чинності зазначеного Закону вели мовлення в областях (з урахуванням Автономної Республіки Крим), де проживає не менше двох третин населення України. Таких телерадіоорганізацій налічується 15: Національна телекомпанія України, ТОВ «ТРК «Ера», ТРК «Студія 1+1» у формі ТОВ, АТЗТ «Українська незалежна ТВ-корпорація» («Інтер»), ТОВ «Міжнародна комерційна ТРК «ІСТУ», ЗАТ «Новий канал», ЗАТ «ТРК «Україна», ЗАТ «Міжнародний Медіа Центр СТБ», «ТК «ТЕТ», ЗАТ «ТелеОдин», ТОВ «ТРО «Мульти Медіа Сервіс», ТОВ «ТРК «НБМ», ТОВ «ТС «Служба інформації», ТОВ «ТРК «Експрес-Інформ», ВАТ «ТК «Тоніс» (надалі — загальнонаціональні канали мовлення). Цей статус закріплено за ними умовами чинних ліцензій відповідно до положень розділу X Закону України «Про телебачення і радіомовлення».

Створено 4 регіональних телемережі — ТОВ «Київтелемонтаж», ТОВ «Гравіс», ЗАТ «ТРК «Люкс», ТОВ «ТС «Астра-ТБ», а також 30 регіональних телекомпаній, що мовлять у межах окремих областей (регіонів).

Модель передачі відео- та аудіо сигналу від транслятору до телевізору, де використовується цифрова модуляція та стиснення для передачі даних складає зміст *цифрового телебачення*. *Цифрове телебачення* (Digital Television) є способом передачі і прийому стислого цифрового відеосигналу, що є сучасною альтернативою традиційному аналоговому телебаченню і забезпечує істотно вищу якість зображення при рівних витратах засобів. Передаванням телевізійним сигналом є послідовність кодових (цифрових) комбінацій електричних імпульсів. Вживання цифрових методів

дозволяє усунути багато недоліків аналогових систем мовлення, у тому числі спотворення сигналів при їх формуванні, обробці і передачі. Що привело до значного поліпшення якості зображення і звуку, збільшення числа програм і сервісу для телеглядачів [260].

Основою сучасного цифрового телебачення є мультимедійний стандарт стиску MPEG. Застосування цифрового телебачення забезпечує певні переваги порівняно з аналоговим телебаченням, головним з яких є вища якість зображення і звуку в порівнянні з аналоговим.

Цифрове мовлення з використанням радіочастотного ресурсу України ліцензується як багатоканальне мовлення. Видача ліцензій на мовлення здійснюється на конкурсних засадах (за результатами відкритих конкурсів) або без конкурсів (за заявковим принципом).

На конкурсних засадах здійснюється видача ліцензій на: 1) ефірне мовлення; 2) багатоканальне мовлення з використанням радіочастотного ресурсу.

Телебачення і радіомовлення пов'язані із розповсюдженням так званої аудіовізуальної інформації – тобто будь-яких сигналів, що сприймаються зоровими і слуховими рецепторами людини та ідентифікуються як повідомлення про події, факти, явища, процеси, відомості про осіб, а також коментарі (думки) про них, що передаються за допомогою зображень та звуків.

Закон України «Про телебачення і радіомовлення» визначає, що *телебачення* – це виробництво і розповсюдження аудіовізуальних передач та програм.

Закон України «Про телебачення і радіомовлення» визначає, що *мовлення (телерадіомовлення)* – це створення (комплектування та/або пакетування) і розповсюдження програм, пакетів програм, передач з використанням технічних засобів телекомунікацій для публічного приймання за допомогою побутових теле- та радіоприймачів у відкритий спосіб чи за абонентну плату на договірних засадах.

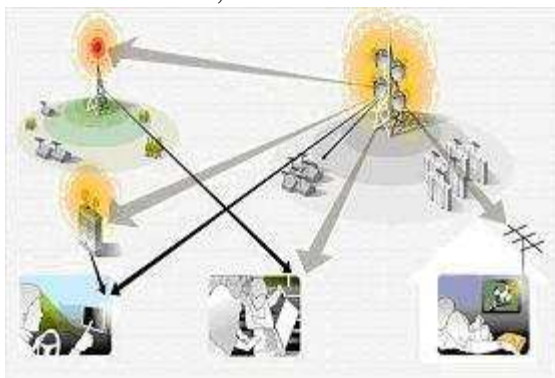
Останнім часом окремо потрібно визначити *Онлайн-телебачення* як новий вид

телебачення, що функціонує тільки при підключенні до Інтернету, широке запровадження чого є черговим кроком у сфері розповсюдження інформації телевізійного формату. Тим більше, що он-лайн телебачення виглядає як передача даних в режимі реального часу. Крім того, останніми роками стали з'являтися канали, які можна подивитися тільки через Інтернет, що вимагає правового регулювання шляхом введення окремих додаткових норм з цього приводу у законодавчі акти.

Послуга платного телебачення, заснована на системі контролю умовного доступу, дозволяє створювати стосунки нового типу між оператором і абонентом,

отримала назву як *інтерактивне цифрове телебачення*. Абонент перестає бути пасивним одержувачем вмісту трансльованих каналів і починає сам вирішувати про те коли, за яку ціну і якими послугами користуватиметься. Умовою введення інтерактивного цифрового телебачення в кабельній мережі є наявність інфраструктури що дозволяє працювати із зворотним зв'язком.

Таким чином, на малюнку 1 схематично показано модель цифрового телебачення як системи зв'язку для трансляції та прийому зображення та звуку, що рухаються на відстані.



Малюнок 1.

Зараз в світі відбувається глобальний перехід на цифрове мовлення телевізійних каналів. Даний перехід зачіпає всі країни світу. І Україна не виключення. Найближчим часом цифрове ефірне телебачення буде впроваджено в окремих областях України, звідси трансляція цифрового мовлення в експериментальному режимі охопить майже третину мешканців країни. 17 липня 2015 р. станеться остаточний перехід на цифрове мовлення телевізійних каналів [260].

Основною перешкодою до функціонування цифрового мовлення у повномасштабному режимі є недосконалість нормативно-правової бази. Її вимоги не враховують особливості сучасних технологій, що не дає змоги реалізувати потужний потенціал і технічну готовність до переходу на «цифру».

Розробку типових проектів систем цифрового телерадіомовлення і його тестове впровадження забезпечує Концерн радіомовлення, радіозв'язку та телебачення (Концерн РРТ).

Сьогодні Державна адміністрація зв'язку працює над розробкою пропозицій з удосконалення законодавчої бази у сфері телекомунікацій та її гармонізації з європейським законодавством. Пропозиції Держзв'язку стосуються, передусім, спрощення системи доступу до вітчизняного ринку телекомунікацій. Ефективна реалізація проектів державної ваги, зокрема й впровадження цифрового мовлення, стане можливою лише за умови прийняття необхідних змін до законодавства [261].

Одним із можливих варіантів одержання цифрового сигналу є *кабельне цифрове телебачення*. Тому першими на собі відчули результати епопеї переходу на «цифру» абоненти кабельних мереж Києва та інших великих міст держави, оскільки з 2009 р. «кабельщики» поступово перевели майже всіх своїх абонентів з аналогового на цифрове телебачення.

На малюнку 2 зображено елементи супутникового телебачення.



Малюнок 2.

Відповідно до законодавства, в Україні існує 3 загальнонаціональні радіомережі, на яких здійснюють мовлення УР-1, УР-2, УР-3 (на цей час не функціонує).

Радіомовлення – це технологія передачі звукової інформації через радіохвилі, проводових мережах або в мережах з пакетною комутацією. Радіомовлення шляхом радіохвиль називають «ефірним радіомовленням» або коротко «ефір». В комп'ютерних мережах застосовується Інтернет-радіо або веб-радіо – група технологій передачі потокових аудіоданих через мережу Інтернет.

Правові засади діяльності Національної ради України з питань телебачення і радіомовлення (далі — Національна рада) як конституційного, постійно діючого, колегіального, наглядового та регулюючого державного органу в галузі телерадіомовлення визначає Закон України «Про Національну раду України з питань телебачення і радіомовлення». Національна рада є юридичною особою, має печатку із своїм найменуванням та зображенням Державного Герба України.

Ліцензування мовлення здійснюється виключно Національною радою України з питань телебачення і радіомовлення. Ліцензування мовлення іноземних телерадіоорганізацій забороняється. Залежно від організаційно-технологічних особливостей розповсюдження програм Національна рада видає ліцензії на такі види мовлення: 1) супутникове; 2) ефірне; 3) кабельне; 4) проводове; 5) багатоканальне.

Залежно від території розповсюдження програм визначається територіальна категорія мовлення та

територіальна категорія каналу мовлення або багатоканальної телемережі: 1) загальнонаціональне мовлення — мовлення не менше ніж на дві третини населення кожної з областей України; 2) регіональне мовлення — мовлення на регіон (область, декілька суміжних областей), але менше ніж на половину областей України; 3) місцеве мовлення — мовлення на один чи кілька суміжних населених пунктів, яке охоплює не більше половини території області; 4) закордонне мовлення — мовлення на територію поза межами державного кордону України.

Провайдер програмної послуги – це суб'єкт господарювання, який на підставі ліцензії, виданої Народою України з питань телебачення та радіомовлення, на договірних засадах надає абонентам можливість перегляду пакетів програм, використовуючи для передавання цих програм ресурси багатоканальних телемереж.

Телерадіоорганізації, їх працівники мають право на одержання від державних органів, підприємств, установ, організацій незалежно від форм власності необхідної інформації для здійснення своєї статутної діяльності. Редакційний статут телерадіоорганізації містить вимоги до створення та поширення інформації. Редакційний статут затверджує власник телерадіоорганізації або уповноважений ним орган.

Власник телерадіоорганізації не має права втручатися у творчу діяльність телерадіоорганізації в інший спосіб, ніж через внесення змін до редакційного статуту телерадіоорганізації.

Телерадіоорганізація зобов'язана: а) дотримуватися законодавства України та

вимог ліцензії; б) виконувати рішення Національної ради та судових органів; в) поширювати об'єктивну інформацію; г) не створювати перешкод у передачі та прийманні програм інших телерадіоорганізацій, функціонуванні засобів телекомунікацій; г) дотримуватися вимог державних стандартів і технічних параметрів телерадіомовлення; д) попереджати телеглядачів про те, що її програми є платними; є) виконувати правила рекламної діяльності і спонсорства, встановлені законодавством; е) з повагою ставитися до національної гідності, національної своєрідності і культури всіх народів; ж) зберігати у таємниці, на підставі документального підтвердження, відомості про особу, яка передала інформацію або інші матеріали за умови нерозголошення її імені; з) не поширювати матеріали, які порушують презумпцію невинуватості підсудного або упереджують рішення суду; і) не розголошувати інформацію про приватне життя громадянина без його згоди, якщо ця інформація не є суспільно необхідною. У разі якщо суд визнає, що поширення інформації про особисте життя громадянина не становить суспільної необхідності, моральна шкода та матеріальні збитки відшкодовуються в порядку, встановленому законодавством України; к) розмістити спростування поширеної інформації, визнаної недостовірною, наклепницькою тощо.

Телерадіоорганізаціям забороняється розповсюджувати, а також анонсувати програми та передачі, які можуть зашкодити фізичному, інтелектуальному і духовному розвитку неповнолітніх та юнацтва, крім як протягом ефірного часу в добовому відрізку з 23.00 до 6.00 та на каналах з обмеженим доступом [121].

Закон України «Про кінематографію» визначає, що *кінематог рафія* – це галузь культури, що об'єднує комплекс видів професійної діяльності, пов'язаної з виробництвом, розповсюдженням, зберіганням та демонструванням фільмів, навчально-науковою роботою у цій галузі.

Виробництво фільму – це діяльність, що поєднує співпрацю авторів і виконавців

фільму та інших суб'єктів кінематографії, спрямовану на втілення твору кінематографії технічними засобами. Демонстрування (публічний показ, публічне сповіщення і публічна демонстрація) фільму – професійна кінематографічна діяльність, що полягає в показі фільму глядачам у призначених для цього приміщеннях (кінотеатрах, інших кіновидовищних закладах), на відеоустановках, а також каналами мовлення телебачення.

7. Організаційно-правові засади здійснення видавничої справи та види електронних видань

Загальні засади видавничої справи в Україні визначає Закон України «Про видавничу справу». Цей закон також регулює порядок організації та провадження видавничої діяльності, розповсюдження видавничої продукції, умови взаємовідносин і функціонування суб'єктів видавничої справи.

Поняття «*видавнича діяльність*» розкривається у законі України «Про видавничу справу» як сукупність організаційних, творчих, виробничих заходів, спрямованих на підготовку і випуск у світ видавничої продукції.

Видавнича справа – це сфера суспільних відносин, що поєднує в собі організаційно-творчу та виробничо-господарську діяльність юридичних і фізичних осіб, зайнятих створенням, виготовленням і розповсюдженням видавничої продукції.

Складовими частинами видавничої справи є: 1) видавнича діяльність – сукупність організаційних, творчих, виробничих заходів, спрямованих на підготовку і випуск у світ видавничої продукції; 2) виготовлення видавничої продукції – виробничо-технологічний процес відтворення визначеним тиражем видавничого оригіналу поліграфічними чи іншими технічними засобами; 3) розповсюдження видавничої продукції – доведення видавничої продукції до споживача як через торговельну мережу, так і іншими способами.

Видавнича справа спрямована на:

- 1) задоволення потреб особи, суспільства, держави у видавничій продукції та отримання прибутку від цього виду діяльності;
- 2) 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;
- 3) забезпечення права на свободу думки і слова, на вільне вираження своїх поглядів і переконань;
- 4) сприяння національно-культурному розвитку українського народу шляхом збільшення загальної кількості тиражів, обсягів та розширення тематичного спрямування українського книговидання;
- 5) забезпечення доступу українського суспільства до загальнолюдських цінностей шляхом перекладу державною мовою кращих здобутків світової літератури, науки тощо, налагодження співпраці з іноземними видавництвами, українською діаспорою, укладення відповідних міжнародних угод;
- 6) здійснення книговидання російською мовою для забезпечення культурних потреб російського населення в Україні з урахуванням імпорту друкованої продукції;
- 7) здійснення книговидання мовами інших національних меншин в Україні;
- 8) збільшення кількості видань іноземними мовами, які поширювали б у світі знання про Україну;
- 9) зміцнення матеріально-технічної бази видавничо-поліграфічного комплексу і мережі розповсюдження видавничої продукції;
- 10) сприяння закордонним українцям у забезпеченні вітчизняними друкованими виданнями.

Кожний примірник видання повинен містити вихідні відомості. *Вихідні відомості видання* – це сукупність даних, які характеризують видання і призначені для його оформлення, інформування споживача, бібліографічного опрацювання і статистичного обліку. Вихідні відомості оформляє видавець. Усі книжкові видання в Україні, незалежно від мови основного тексту, повинні мати обов'язкову анотацію та вихідні бібліографічні відомості державною мовою. Винятком можуть бути тільки

видання іноземними мовами, призначені для розповсюдження за кордоном або серед іноземців. Вихід у світ видання без обов'язкових для нього вихідних відомостей не допускається.

Діяльність у видавничій справі не може бути використана для закликів, спрямованих на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, пропаганду війни, насильства, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини, здоров'я населення.

У видавничій справі забороняється:

- 1) виготовляти чи розповсюджувати продукцію, яка містить інформацію, віднесена до недобросовісної реклами, рекламу з використанням шаржування державних символів України (Державного Герба, Державного Прапора, Державного Гімну) у будь-якому вигляді;
- 2) оприлюднювати інформацію, дані, відомості, рекламувати товари, послуги, які можуть завдати шкоди громадянам, підприємствам, установам, організаціям або державі;
- 3) виготовляти чи розповсюджувати видавничу продукцію порнографічного характеру і таку, що пропагує культ насильства і жорстокості;
- 4) виготовляти чи розповсюджувати видавничу продукцію, що проповідує релігійні віровчення, які загрожують життю, здоров'ю, моралі громадян, порушують їх права і свободи або закликають до порушення громадського порядку;
- 5) реалізовувати видавничу продукцію без дозволу її власника (співвласників), а також з порушенням законодавства України з питань інтелектуальної власності.

Суб'єкти видавничої діяльності не мають права розголошувати дані, що становлять державну або іншу таємницю, яка охороняється законодавством.

Автор — це фізична особа, творчою працею якої створено твір (документ).

Замовник — це фізична чи юридична особа, яка замовляє видавничу продукцію,

беручи на себе фінансові зобов'язання. За-
мовниками будь-якої видавничої продукції
можуть бути: громадяни України, іноземці та
особи без громадянства, що перебувають в
Україні на законних підставах, юридичні
особи України та інших держав.

Замовник визначає мову, обсяг, тираж
видання, самостійно вирішує питання про
його використання чи розповсюдження.

Видавець — це фізична чи юридична
особа, яка здійснює підготовку і випуск
видання. Видавець має право бути
замовником перед виготовлювачем та
розповсюджувачем видавничої продукції.
Основною структурною ланкою у
видавничій справі є видавництва і видавничі
організації різних форм власності.
Видавництво, видавнича організація діють
на підставі своїх статутів (положень), якими
визначаються мета, завдання, функції та
порядок діяльності. *Видавництво* — це
спеціалізоване підприємство, основним
видом діяльності якого є підготовка і випуск
у світ видавничої продукції.

Видавнича організація — це
підприємство, установа або організація,
статутом якої поряд з іншими видами
діяльності передбачено підготовку і випуск у
світ видавничої продукції.

Виготовлювач видавничої продукції
— це фізична чи юридична особа, що
здійснює виготовлення замовленого тиражу
видання. Відповідно до Закону України «Про
обов'язковий примірник документів»
передачу одержувачам обов'язкових
примірників документів здійснює їх
виробник — юридична особа, незалежно від
форми власності або фізична особа, яка
виготовляє (в тому числі публікує) різні види
тиражованих документів. Відповідно до За-
кону України «Про авторське право і
суміжні права» опублікування твору — це
випуск в обіг за згодою автора чи іншого
суб'єкта авторського права виготовлених
поліграфічними чи іншими способами
примірників твору шляхом їх продажу або
передачі права власності на них, чи
володіння ними іншими способами.

Згідно із Законом України «Про
видавничу справу» саме видавець має право
реалізувати свою видавничу продукцію та

іншим чином розпоряджатися нею (ст. 20
Закону), а виготівник не має право без
дозволу замовника, яким може виступати
видавець, передавати будь-кому
виготовлений тираж видання (ч. 5 ст. 21),
крім випадків, передбачених законом.

Розповсюджувач видавничої
продукції — це фізична чи юридична особа,
яка займається розповсюдженням
видавничої продукції. Розповсюдження
видавничої продукції може здійснюватися
шляхом її реалізації (продажу) в роздрібній
та оптовій торгівлі, безоплатного
розповсюдження чи обміну на договірних
засадах. Безоплатне розповсюдження
видавничої продукції може здійснюватися з
науковою, культурно-просвітницькою,
благодійною, рекламною метою тощо.

Споживач видавничої продукції — це
приватні особи, підприємства, установи,
організації. Споживач має право на: заміну
видавничої продукції, в якій виявлено
поліграфічний та інший технологічний брак;
гарантію виконання відповідно оформлених
передплатних зобов'язань.

До суб'єктів видавничої справи в
Україні законодавством відносяться видавці,
виготовлювачі та розповсюджувачі видав-
ничої продукції. Суб'єктами видавничої
справи в Україні можуть бути: громадяни
України, іноземці та особи без громадянства,
що перебувають в Україні на законних
підставах, юридичні особи України та інших
держав.

Останнім часом широко увійшло до
соціального обігу нове поняття «*Електронне
видання*». Такі видання за своєю структурою
включають як Інтернет-видання, так і інші
видання, що зберігаються в електронному
(цифровому) форматі, зокрема у локальних
інформаційних мережах.

Інтернет-видання можна позначити
як Інтернет-сайти, основним завданням яких
є виконання функції засобів масової
інформації в Інтернеті.

Сайт новин — це веб-сайт, який є
окремим випадком Інтернет-видання і може
представляти самостійний Інтернет-проект,
що спеціалізується на розміщенні новин в
Інтернеті. Електронні новини можуть бути
зорієнтованими як на читачів окремої

держави (Росії, України), або на більш широке коло споживачів.

Специфіка Інтернету дозволяє практично будь-кому створювати Інтернет-ЗМІ. Утім такі видання можуть мати офіційний статус ЗМІ, а можуть його і не мати. Юридично до поняття «Інтернет-ЗМІ» можна віднести тільки частину ресурсів новин, оскільки статус Інтернет-ЗМІ набувається тільки після його державної реєстрації. При цьому реєстрації дотепер є добровільною і необов'язковою.

Традиційні друковані та ефірні ЗМІ, як правило, можуть мати власні Інтернет-сторінки, на яких розміщені виключно анонси статей, чим фактично дублюється зміст офлайн-випусків (тобто традиційних випусків, які не спрямовані на розміщення в електронному вигляді в Інтернеті), а іноді – повні тексти минулих номерів. До того Інтернет-видання не відрізняються від офлайн-видач за жанрами – існують сайти новин, літературні, науково-популярні, дитячі, жіночі та інші сайти.

На сьогодні розповсюджено два основних види Інтернет-видань: 1) такі, що виходять з певною періодичністю (наприклад, щоденно, щотижнево, два рази на місяць і т.п.); 2) такі, що за надходженням нових матеріалів постійно обновляються (як правило, сайти новин).

Книжкова палата України — це державна наукова установа у сфері видавничої справи та інформаційної діяльності, що здійснює: 1) державну бібліографічну реєстрацію та централізовану каталогізацію всіх без винятку видів видань, випущених в Україні; 2) збирання та використання адміністративних даних, які характеризують динаміку та тенденції у видавничій справі; 3) аналіз тенденцій розповсюдження видавничої продукції, вивчення книжкового ринку, його регіональних особливостей; 4) комплектування і збереження повного і недоторканного фонду Державного архіву друку — головного сховища всіх видів видань, випущених в Україні; 5) державну стандартизацію видавничої та бібліотечної справи, розроблення і контроль за дотриманням стандартів суб'єктами

видавничої справи, а також сертифікацію баз даних; 6) розробку та обґрунтування короткострокових і довгострокових прогнозів розвитку видавничої та бібліографічної справи в Україні; 7) наукові дослідження в галузі бібліографії, книгознавства, соціології книги та читання, консервації та реставрації документів; 8) наукознавчі дослідження і розробку бібліометричних методів визначення пріоритетних напрямів і рівнів розвитку наукових досліджень; 9) створення і видання поточних, кумулятивних і ретроспективних бібліографічних покажчиків, реферативних журналів і науково-аналітичних оглядів, друкованих карток; 10) розробку та експлуатацію бібліографічних баз даних і мереж бібліографічної інформації; 11) організацію книгообміну.

Книжкова палата України — це установа у сфері видавничої справи та інформаційної діяльності, заснована на державній власності і підпорядкована Державному комітету телебачення і радіомовлення України.

Фонди друкованої продукції і бази даних Книжкової палати України перебувають під охороною держави та є власністю держави. Книжкова палата України одержує безоплатні та платні обов'язкові примірники всіх видань, випуск яких здійснюється суб'єктами видавничої справи в Україні, і надає узагальнену інформацію про це через засоби масової інформації та надсилає її в управління преси та інформації обласних державних адміністрацій.

Одним із видів електронних видань є *електронні наукові фахові видання*, тобто документи, інформація в яких представлена у формі електронних даних, що пройшли редакційно-видавниче опрацювання, призначені для поширення в незмінному вигляді, мають вихідні відомості та включені до затверджених ВАК України переліків наукових фахових видань, у яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора та кандидата наук і на які можна посилатися у наукових статтях та дисертаціях.

Згідно із п. 1.2-1.3 Положення про електронні наукові фахові видання, що затверджено Наказом Міністерства освіти і науки України, Національної академії наук України, Вищої атестаційної комісії України 30.09.2004 № 768/431/547, видання започатковуються з метою досягнення якісно нового рівня повноти й оперативності задоволення інформаційних потреб суспільства в знаннях, одержаних у процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної та виробничої діяльності українських учених і фахівців. Засновник існуючого друкованого наукового фахового видання може здійснювати його випуск в електронній формі.

Національна бібліотека України імені В. І. Вернадського та Національна парламентська бібліотека України створюють зведений електронний каталог статей з усіх Видань, представляють його в Інтернет на своїх веб-сайтах і забезпечують безкоштовний доступ до каталогу та повних текстів статей (п. 4.1 Положення).

Електронний журнал – це періодичне видання, що рецензується у встановленому порядку, яке може бути електронним аналогом друкованого журналу, а може виходити виключно в електронному форматі, що дозволяє його перегляд на комп'ютері. Електронні журнали розповсюджуються через Інтернет або на будь-яких інших високотехнологічних носіях інформації (магнітних, оптичних, цифрових та ін.).

Під *електронними журналами* йдеться про періодику, що містить повні версії публікацій, а не тільки сайти, що забезпечують доступ до змісту та резюме статей.

Електронні наукові журнали визначають як періодичні видання, що містять статті, з якими ознайомила і дала свій коментар редакційна група з метою відповідності матеріалів стандартам якості предметної області. В них концентруються найважливіші наукові результати, фіксуються наукові пріоритети, гарантується авторське право на одержаний результат.

Таким чином, потрібно погодитись із тим, що набирає сили тенденція до

поступового перетворення статті в основну структурну одиницю системи наукових комунікацій в електронному середовищі [110].

У цілому загальне коло електронних журналів можна розділити на три групи: 1) паралельні електронні журнали, тобто електронні версії традиційних друкованих видань, де друкована версія ідентична електронній; 2) інтегровані електронні журнали, що видаються у двох видах, які доповнюють один одного; 3) оригінальні електронні журнали, які видаються виключно в електронному виді.

Видання електронного журналу може бути представлено у вигляді одного або декількох файлів, де містяться статті, що відображають тематику журналу. Доступ до статей відбувається згідно змісту за допомогою системи посилань. За своєю специфікою, електронний журнал, на відміну від друкованих журналів, може містити в собі інтерактивні елементи (гри, тести й т.п.). Із зростанням комп'ютеризації населення та удосконалення засобів зв'язку, а також завдяки доступності, електронні журнали як засіб для одержання необхідної інформації в структурованому виді останнім часом набувають усе більш важливої ролі у житті суспільства.

Отже, як слушно наголошують провідні фахівці з бібліотечної справи, модель «відкритого доступу» видається найліпшою у справі організації вітчизняних наукових періодичних видань [184].

Термін «*Електронна книга*» (*e-book*) використовується як загальна назва групи вузькоспеціалізованих компактних пристроїв, що призначені для відображення текстової інформації, яка представляється в електронному виді. Фактично електронна книга є версією книги в електронному (цифровому) виді. Даний термін застосовується як для праць, які представлені у цифровій формі, так і відносно засобів, що використовуються для їхнього прочитання [254].

Існує кілька груп форматів електронних книг. У цьому зв'язку важливим процесом перекладу паперових книг в електронну (цифрову) форму є *оцифровка*.

Електронні копії книг можуть утворювати електронні бібліотеки й поширюватися в Інтернет-Мережі.

До електронних текстів (*e-text*) відносяться також навчальні електронні посібники, до складу яких, крім тексту, включаються растрові зображення, приклади даних, вправи, спеціально написані коментарі й відповіді на можливі питання. Безсумнівною перевагою електронного формату текстів є можливість зберігання на електронних, оптичних і т.п. носіях десятків і сотень тисяч книг, одним із прикладів, що підтверджують висловлене положення, може стати даний електронний курс лекцій.

Інтерактивна книга – це електронна книга, що платно або безкоштовно доступна онлайн через Інтернет. Вона відрізняється від електронної книги, тому що більшість електронних книг випущені у таких форматах як компакт-диски або DVD.

З метою обліку суб'єктів видавничої справи ведеться Державний реєстр України видавців, виготовлювачів і розповсюджувачів видавничої продукції (далі — Державний реєстр). Положення про Державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції затверджене постановою Кабінету Міністрів України від 28 вересня 1998 р. № 1540.

Без внесення до Державного реєстру діяльність у видавничій справі здійснюється: 1) органами законодавчої, виконавчої, судової влади — для випуску у світ офіційних видань з матеріалами законодавчого та іншого нормативно-правового характеру, бюлетенів судової практики; 2) підприємствами, організаціями, навчальними закладами, науковими установами, творчими спілками, іншими юридичними особами — для випуску у світ і безоплатного розповсюдження інформаційних, бібліографічних, реферативних, рекламних видань, видань, що містять нормативні акти з виробничо-практичних питань, службових та методичних матеріалів, документації для потреб статутної діяльності їх видавця, а також матеріалів на правах рукопису, що

розмножені за допомогою технічних засобів [121].

8. Законодавство у сфері рекламної діяльності та правова регуляція електронної реклами в Інтернеті

Інформація, що розповсюджена будь-яким способом та у будь-якій формі, у тому числі з використанням будь-яких засобів, яка адресована для невизначеного кола осіб та спрямована на залучення уваги до об'єкту рекламування, формування або підтримка інтересу до нього та його просування на ринку складає сутність поняття «реклама».

Відносини, пов'язані з виробництвом, розповсюдженням та споживанням реклами на території України регулює Закон України «Про рекламу».

Фактично зміст реклами означає оплачену, неперсоналізовану комунікацію, що здійснюється ідентифікованим спонсором, що використовує ЗМІ з метою впливу на аудиторію.

Також рекламу можна визначити як процес повідомлення інформації від рекламодавця до цільової аудиторії шляхом медіа-каналів або іншими способами. Часом у визначення реклами включають таку ознаку як комерційні інтереси.

Отже, *реклама* — це інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару.

Рекламна діяльність — це відносини з виробництва, розміщення та розповсюдження реклами. Закон України «Про рекламу» закріплює визначення реклами — інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару.

Даний Закон не поширюється на відносини, пов'язані з розповсюдженням інформації, обов'язковість розміщення та оприлюднення якої визначено іншими законами України (наприклад, законами України «Про інформацію», «Про порядок висвітлення діяльності органів державної

влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про систему суспільного телебачення і радіомовлення України» тощо), а також не поширюється на оголошення фізичних осіб, не пов'язані з підприємницькою діяльністю.

Відповідно до Закону України «Про рекламу» розрізняються внутрішня і зовнішня реклами, реклама на транспорті, соціальна реклама тощо.

Внутрішня реклама — це реклама, що розміщується всередині будинків і споруд. Розміщення внутрішньої реклами погоджується з власником місця її розташування або уповноваженою ним особою. При погодженні розміщення внутрішньої реклами втручання у форму та зміст реклами забороняється.

Забороняється розміщення внутрішньої реклами у приміщеннях органів державної влади та органів місцевого самоврядування, дошкільних навчальних закладах, середніх загальноосвітніх школах та спеціалізованих загальноосвітніх закладах освіти. Однак ця заборона не поширюється на соціальну рекламу.

Зовнішня реклама — це реклама, що розміщується на спеціальних тимчасових і стаціонарних конструкціях, розташованих на відкритій місцевості, а також на зовнішніх поверхнях будинків, споруд, на елементах вуличного обладнання, над проїжджою частиною вулиць і доріг. Розміщення зовнішньої реклами у населених пунктах провадиться на підставі дозволів, що надаються виконавчими органами сільських, селищних, міських рад, та в порядку, встановленому цими органами на підставі типових правил розміщення зовнішньої реклами, що затверджені постановою Кабінету Міністрів України від 29 грудня 2003 р. № 2067. При видачі дозволів на розміщення зовнішньої реклами втручання у форму та зміст зовнішньої реклами забороняється.

Зовнішня реклама на територіях, будинках та спорудах розміщується за згодою їх власників або уповноважених ними органів (осіб). Розміщення зовнішньої реклами на територіях та об'єктах поза населеними пунктами провадиться лише за

згодою їх власників або уповноважених ними органів (осіб). Стягнення плати за видачу дозволів забороняється.

Зовнішня реклама повинна відповідати таким вимогам: 1) розміщуватись із дотриманням вимог техніки безпеки та із забезпеченням видимості дорожніх знаків, світлофорів, перехресть, пішохідних переходів, зупинок транспорту загального користування та не відтворювати зображення дорожніх знаків; 2) освітлення зовнішньої реклами не повинно засліплювати учасників дорожнього руху, а також не повинно освітлювати квартири житлових будинків; 3) фундаменти наземної зовнішньої реклами, що виступають над поверхнею землі, можуть бути декоративно оформлені; 4) опори наземної зовнішньої реклами, що розташована вздовж проїжджої частини вулиць і доріг, повинні мати вертикальну порожню розмітку, нанесену світлоповертаючими матеріалами, заввишки до 2 метрів від поверхні землі; 5) нижній край зовнішньої реклами, що розміщується над проїжджою частиною, у тому числі на мостах, естакадах тощо, повинен розташовуватися на висоті не менше ніж 5 метрів від поверхні дорожнього покриття; 6) у місцях, де проїжджа частина вулиці межує з цоколями будівель або огорожами, зовнішня реклама може розміщуватися в одну з фасадів будівель або огорожами лінію.

Забороняється розташовувати засоби зовнішньої реклами: 1) на пішохідних доріжках та алеях; 2) у населених пунктах на висоті менш ніж 5 метрів від поверхні дорожнього покриття, якщо їх рекламна поверхня виступає за межі краю проїжджої частини; 3) поза населеними пунктами на відстані менш ніж 5 метрів від краю проїжджої частини.

Розміщення зовнішньої реклами на пам'ятках та в межах зон охорони пам'яток національного або місцевого значення, в межах об'єктів природно-заповідного фонду дозволяється за погодженням з центральними або місцевими органами виконавчої влади у сфері охорони культурної спадщини. Зазначений перелік

обмежень та заборон щодо розміщення зовнішньої реклами є вичерпним.

Реклама на транспорті — це реклама, що розміщується на території підприємств транспорту загального користування, метрополітену, зовнішній та внутрішній поверхнях транспортних засобів та споруд підприємств транспорту загального користування і метрополітену. Розміщення реклами на транспорті погоджується лише з власниками об'єктів транспорту або уповноваженими ними органами (особами). При погодженні розміщення реклами на транспорті втручання у форму та зміст реклами забороняється. Розміщення реклами на транспорті повинно відповідати вимогам безпеки та правил дорожнього руху. За умови розміщення реклами на транспорті з дотриманням вимог безпеки і правил дорожнього руху забороняється вимагати від власників транспортних засобів отримання дозволів, погоджень, інших документів щодо розміщення реклами. Забороняється розміщення на транспортних засобах: 1) реклами, яка повторює чи імітує кольорографічні схеми спеціальних та оперативних транспортних засобів; 2) реклами із нанесенням світлоповертаючих матеріалів; 3) реклами, яка супроводжується звуковими чи світловими сигналами.

Забороняється розміщувати рекламу на скляних (прозорих) поверхнях транспортних засобів, за винятком випадків, коли для цього використовуються матеріали, які забезпечують безперешкодний огляд з салону транспортного засобу. Забороняється розповсюдження реклами через радіотрансляційні або інші звукові мережі сповіщення пасажирів у транспортних засобах громадського користування, на станціях метрополітену, вокзалах, в портах та аеропортах, за винятком розповсюдження соціальної реклами.

Соціальна реклама — це інформація будь-якого виду, розповсюджена в будь-якій формі, яка спрямована на досягнення суспільно корисних цілей, популяризацію загальнолюдських цінностей і розповсюдження якої не має на меті отримання прибутку. Рекламодавцем

соціальної реклами може бути будь-яка особа. Соціальна реклама не повинна містити посилань на конкретний товар та/або його виробника, на рекламодавця, на об'єкти права інтелектуальної власності, що належать виробнику товару або рекламодавцю соціальної реклами.

На осіб, які безоплатно виробляють і розповсюджують соціальну рекламу, та на осіб, які передають свої майно і кошти іншим особам для виробництва і розповсюдження соціальної реклами, поширюються пільги, передбачені Законом України «Про благодійництво та благодійні організації».

Засоби масової інформації — розповсюджені реклами, діяльність яких повністю або частково фінансується з державного або місцевих бюджетів, зобов'язані розміщувати соціальну рекламу органів державної влади та органів місцевого самоврядування, громадських організацій безкоштовно в обсязі не менше 5 відсотків ефірного часу, друкованої площі, відведених для реклами. Засоби масової інформації — розповсюджені реклами, що повністю або частково фінансуються з державного або місцевих бюджетів, зобов'язані надавати пільги при розміщенні соціальної реклами, замовником якої є заклади освіти, культури, охорони здоров'я, які утримуються за рахунок державного або місцевих бюджетів, а також благодійні організації.

Недобросовісна реклама — це реклама, яка вводить або може ввести в оману споживачів реклами, завдати шкоди особам, державі чи суспільству внаслідок неточності, недостовірності, двозначності, перебільшення, замовчування, порушення вимог щодо часу, місця і способу розповсюдження. Недобросовісна реклама забороняється. Рішення щодо визнання реклами недобросовісною можуть приймати такі органи державної влади: 1) спеціально уповноважений центральний орган виконавчої влади у сфері захисту прав споживачів; 2) Антимонопольний комітет України; 3) Національна рада України з питань телебачення і радіомовлення; 4) Міністерство фінансів України; 5) Державна комісія з цінних паперів та фондового ринку.

Прихована реклама — це інформація про особу чи товар у програмі, передачі, публікації, якщо така інформація слугує рекламним цілям і може вводити в оману осіб щодо дійсної мети таких програм, передач, публікацій. В Україні прихована реклама забороняється.

Час мовлення, відведений на рекламу, не може перевищувати 15 відсотків, а впродовж виборчого процесу — 20 відсотків фактичного обсягу мовлення протягом астрономічної доби телерадіоорганізацією будь-якої форми власності. Це положення не поширюється на спеціалізовані рекламні канали мовлення. Час, відведений на політичну рекламу впродовж виборчого процесу на спеціалізованих рекламних каналах, не може перевищувати 20 відсотків фактичного обсягу мовлення протягом кожної години мовлення. Частка реклами протягом кожної астрономічної години фактичного мовлення не повинна перевищувати 20 відсотків, а впродовж виборчого процесу — 25 відсотків.

Реклама повинна розміщуватися у перервах між програмами, передачами. Забороняється переривати з метою розміщення реклами трансляції сесій Верховної Ради України, сесій Верховної Ради Автономної Республіки Крим, офіційних державних заходів і церемоній, виступів Президента України, Голови Верховної Ради України, Прем'єр-міністра України, Голови Конституційного Суду України, Голови Верховного Суду України, народних депутатів України, членів Уряду України, а також трансляції релігійних служб, програм, передач для дітей та програм, передач новин.

Трансляція концертно-видовищних програм, передач може перериватися рекламою за умови, що між рекламними вставками програма, передача триває не менше 30 хвилин. Реклама під час трансляції спортивних програм, передач розміщується в перервах між їх частинами. Під час трансляції кіно- і телефільмів реклама розміщується перед початком фільму та/або після закінчення фільму.

Трансляція кіно- і телефільмів, за умови їх тривалості до 42 хвилин, не може

перериватися рекламою або будь-яким редакційним, авторським чи інформаційним матеріалом (включаючи анонси програм, передач). Трансляція кіно- і телефільмів, за умови їх тривалості від 42 до 70 хвилин, може перериватися рекламою або будь-яким редакційним, авторським чи інформаційним матеріалом (включаючи анонси програм, передач) один раз, за умови їх тривалості від 70 до 90 хвилин — два рази. Трансляція кіно- і телефільмів тривалістю понад 90 хвилин може перериватися рекламою або будь-яким редакційним, авторським чи інформаційним матеріалом (включаючи анонси програм, передач) кожні 30 хвилин за умови, що після останньої перерви фільм продовжується не менше 20 хвилин включно.

Обсяг реклами у друкованих засобах масової інформації визначається ними самостійно. Друковані засоби масової інформації, що розповсюджуються за передплатою, зобов'язані в умовах передплати зазначити кількість реклами в загальному обсязі видання. Друкована площа, відведена на політичну рекламу впродовж виборчого процесу в друкованих засобах масової інформації, у тому числі рекламних, не може перевищувати 20 відсотків обсягу друкованої площі кожного номера видання чи додатка до нього. Це обмеження не поширюється на друковані засоби масової інформації, засновниками яких є політичні партії.

Забороняється реклама: 1) з використанням зображень дітей, які споживають або використовують продукцію, призначену тільки для дорослих чи заборонену законом для придбання або споживання неповнолітніми; 2) з інформацією, яка може підірвати авторитет батьків, опікунів, піклувальників, педагогів та довіру до них дітей; 3) з вміщенням закликів до дітей придбати продукцію або звернутися до третіх осіб з проханням зробити покупку; 4) з використанням зображень справжньої або іграшкової зброї, вибухових пристроїв.

Реклама не повинна містити зображення дітей у небезпечних ситуаціях чи за обставин, що у разі їх імітації можуть

завдати шкоди дітям або іншим особам, а також інформації, здатної викликати зневажливе ставлення дітей до небезпечних для здоров'я і життя ситуацій. Реклама не повинна завдавати дітям моральної чи фізичної шкоди, викликати у них відчуття неповноцінності. Реклама не повинна вказувати на можливість придбання рекламованого товару, розрахованого переважно на дітей, кожною сім'єю без урахування можливостей її бюджету. Реклама не повинна створювати у дітей враження, що володіння рекламованою продукцією дає їм перевагу над іншими дітьми.

Законодавство України встановлює вимоги і обмеження стосовно реклами окремих видів товарів та послуг. Зокрема, наприклад, стосовно лікарських засобів дозволяється реклама: 1) лише таких лікарських засобів, медичної техніки, методів профілактики, діагностики, лікування і реабілітації, що в установленому порядку дозволені Міністерством охорони здоров'я до застосування в Україні; 2) лише таких лікарських засобів, які відпускаються без припису (рецепту) лікаря, та лише таких медичної техніки, методів профілактики, діагностики, лікування і реабілітації, застосування яких не потребує спеціальних знань та підготовки.

Забороняється реклама лікарських засобів, які вживаються та розповсюджуються тільки за приписом (рецептом) лікаря. Забороняється реклама допінгових речовин та/або методів для їх використання у спорті. Реклама лікарських засобів, медичної техніки, методів профілактики, діагностики, лікування і реабілітації не може містити посилянь на терапевтичні ефекти стосовно захворювань, які не піддаються або важко піддаються лікуванню.

Забороняється реклама проведення цілительства на масову аудиторію.

Забороняється реклама нових методів профілактики, діагностики, реабілітації та лікарських засобів, які знаходяться на розгляді в установленому порядку, але ще не допущені до застосування. Реклама послуг народної медицини (цілительства) та осіб, які їх надають, дозволяється лише за на-

явності відповідного спеціального дозволу на заняття народною медициною (цілительством), виданого Міністерством охорони здоров'я України або уповноваженим ним органом, і повинна містити номер, дату видачі зазначеного дозволу та назву органу, який його видав.

Реклама тютюнових виробів, знаків для товарів і послуг, інших об'єктів права інтелектуальної власності, під якими випускаються тютюнові вироби, забороняється: на радіо та телебаченні, на перших і останніх сторінках газет, перших і останніх сторінках обкладинок журналів та інших видань, засобами внутрішньої реклами, реклами на транспорті, за допомогою заходів рекламного характеру (крім спеціальних виставкових заходів).

Реклама алкогольних напоїв та тютюнових виробів, знаків для товарів і послуг, інших об'єктів права інтелектуальної власності, під якими випускаються алкогольні напої та тютюнові вироби: 1) забороняється на товарах та у друкованих виданнях, призначених переважно для осіб віком до 18 років, або у розрахованих на зазначених осіб частинах інших друкованих видань; 2) забороняється з використанням осіб віком до 18 років як фотомоделей; 3) не повинна містити зображення процесу паління тютюнових виробів або споживання алкогольних напоїв; 4) не може розташовуватися ближче ніж за 300 метрів прямої видимості від території дитячих дошкільних закладів, середніх загальноосвітніх шкіл та інших навчальних закладів, в яких навчаються діти віком до 18 років; 5) не може формувати думку, що паління або вживання алкоголю є важливим фактором досягнення успіху в спортивній, соціальній, сексуальній або інших сферах життя; 6) не повинна створювати враження, що вживання алкогольних напоїв чи паління тютюнових виробів сприятиме розв'язанню особистих проблем; 7) не може формувати думку, що алкоголь чи тютюнові вироби мають лікувальні якості або що вони є стимулюючими чи заспокійливими засобами; 8) не повинна заохочувати до вживання алкогольних напоїв чи тютюнопаління або негативно розцінювати

факт утримування від вживання тютюнових виробів та алкогольних напоїв; 9) не може містити зображень лікарів та інших професійних медичних працівників, а також осіб, зовнішній вигляд яких імітує зовнішній вигляд лікарів; 10) не повинна включати зображення популярних осіб або пряме чи опосередковане схвалення популярними особами паління чи вживання алкоголю; 11) не повинна створювати враження, що більшість людей палить або вживає алкогольні напої.

Забороною такі види діяльності з рекламування алкогольних напоїв та тютюнових виробів, знаків для товарів і послуг, інших об'єктів права інтелектуальної власності, під якими випускаються алкогольні напої та тютюнові вироби: 1) спонсорування заходів, призначених переважно для осіб віком до 18 років, з використанням знаків для товарів та послуг, інших об'єктів права інтелектуальної власності, під якими випускаються тютюнові вироби та алкогольні напої; 2) розповсюдження та продаж будь-яких товарів з використанням знаків для товарів та послуг, інших об'єктів права інтелектуальної власності, під якими випускаються тютюнові вироби та алкогольні напої, особам віком до 18 років.

Реклама зброї може здійснюватися тільки у відповідних спеціалізованих виданнях щодо зброї, або безпосередньо у приміщеннях торговельних закладів (підприємств), які реалізують зброю, або на відповідних виставках (заходах).

Реклама послуг (банківських, страхових, інвестиційних тощо), пов'язаних із залученням коштів населення, або осіб, які їх ліцензії, що підтверджує право на здійснення такого виду діяльності. Така реклама повинна містити номер дозволу, ліцензії, дату їх видачі та найменування органу, який видав цей дозвіл, ліцензію. Це положення не застосовується у випадках, коли дається тільки реклама знака для товарів і послуг, назви особи (без реклами послуг).

Крім того, заборонено рекламу адвокатської діяльності. У цій сфері адвокатам дозволяється виключно

інформаційні повідомлення з певними обмеженнями [185, с. 300].

Контроль за дотриманням законодавства України про рекламу здійснюють у межах своїх повноважень: 1) спеціально уповноважений центральний орган виконавчої влади у сфері захисту прав споживачів — щодо захисту прав споживачів; 2) Антимонопольний комітет України — щодо дотримання законодавства про захист економічної конкуренції; 3) Національна рада України з питань телебачення і радіомовлення — щодо телерадіоорганізацій усіх форм власності; 4) Міністерство фінансів України — щодо реклами державних цінних паперів; 5) Державна комісія з цінних паперів та фондового ринку — щодо реклами на фондовому ринку.

Органи державної влади зобов'язані повідомляти рекламодавців, виробників та розповсюджувачів реклами про розгляд справ про порушення ними законодавства про рекламу не пізніше як за три дні до такого розгляду, а у невідкладних випадках — не пізніше як за один день [121]. Постановою Кабінету Міністрів України від 28 березня 2007 р. № 555 затверджено Положення про Національну координаційну раду з питань захисту прав споживачів. Національна координаційна рада з питань захисту прав споживачів є постійно діючим консультативно-дорадчим органом при Кабінеті Міністрів України. До основних завдань Ради віднесено окрім іншого створення умов для розвитку механізму саморегулювання рекламної діяльності, формування норм і правил поведінки на рекламному ринку тощо.

Електронна реклама – це розміщення рекламних оголошень в Інтернет, які з'являються на екрані під час перегляду сторінок відповідних оперативно-інформаційних служб або Веб-вузлів [98].

Віртуальна реклама є рекламою, яка розміщується в телеєфірі без переривання трансляції. Такий вид реклами ґрунтується на цифрових технологіях, використання яких дозволяє інтегрувати аудіовізуальне повідомлення, що фізично відсутнє в студії, в програмний телеєфір. Все це дозволяє

визначити цифрову рекламу як інноваційний вид реклами.

Часом до змісту терміну «віртуальна реклама» включають Інтернет-рекламу, ґрунтуючись на тому, що Інтернет називають віртуальним простором. Утім таке ототождження не буде вірним, оскільки віртуальність припускає покращену ідентичність реальності, тоді як Інтернет-реклама, як правило, нескладно візуально ідентифікується як такава.

Тому Інтернет-реклама є іншим особливим видом електронної реклами з використанням різних Інтернет-засобів. Основними видами Інтернет-реклами можна назвати *медійну рекламу* – розміщення матеріалів на сайтах, що представляють собою рекламну площадку й *контекстну рекламу* – розміщення матеріалів на сайтах, що пропонують користувачеві функцію пошуку. Інші види реклами в Інтернеті, як правило, сполучають ознаки зазначених видів електронної реклами.

Варто помітити, що традиційні правові норми про рекламу не завжди можуть ефективно регулювати Інтернет-рекламу, оскільки: 1) ці норми не враховують технічні особливості Інтернет-Мережі; 2) утруднене визначення юрисдикції (законодавство якої території застосовувати); 3) недосконала організація контролю й порядок залучення до відповідальності порушників.

Прикладом одного з негативних типів *електронної реклами* може бути *спам* – масове розсилання комерційної, політичної й іншої реклами, що носить нав'язливий характер. Поширення реклами завдяки мережам електров'язку, у тому числі за допомогою використання телефонного, факсимільного, мобільного радіотелефонного зв'язку, допускається тільки за умови попередньої згоди абонента або адресата на одержання реклами [254]. На жаль, на законодавчому рівні непросто визначити, яка розсилання є законною, а яка немає. Тому в цей час подібні правові положення залишаються малоефективними.

9. Правове регулювання державної статистики та електронний облік статистичної інформації

У загальному визначенні галузь знань, предметом якої є вивчення питань щодо збору, виміру та аналізу масових статистичних (кількісних та якісних) даних (інформації) розуміється як статистика.

Державна статистика — це централізована система збирання, опрацювання, аналізу, поширення, збереження, захисту та використання статистичної інформації. Статистична інформація (дані) — офіційна державна інформація, яка характеризує масові явища та процеси, що відбуваються в економічній, соціальній та інших сферах життя України та її регіонів.

Закон України «Про державну статистику» визначає, що *державна статистична діяльність* — це 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.

З метою складання статистичної інформації органи державної статистики можуть використовувати такі джерела інформації: 1) первинні та статистичні дані щодо респондентів, які підлягають статистичним спостереженням; 2) адміністративні дані органів державної влади (за винятком органів державної статистики), органів місцевого самоврядування, інших юридичних осіб; 3) дані банківської і фінансової статистики, статистики платіжного балансу тощо; 4) статистичну інформацію міжнародних організацій та статистичних служб інших країн тощо; 5) оцінки та розрахунки, що здійснюються на основі зазначених вище даних.

Рішення щодо вибору джерела статистичної інформації приймається органами державної статистики самостійно, з урахуванням якості і своєчасності подання інформації, витрат, а також обов'язків, які виникають у зв'язку з цим у респондентів.

Закон України «Про державну статистику» регулює правові відносини в галузі державної статистики, визначає права і функції органів державної статистики, організаційні засади здійснення державної статистичної діяльності з метою отримання всебічної та об'єктивної статистичної інформації щодо економічної, соціальної, демографічної та екологічної ситуації в Україні та її регіонах і забезпечення нею держави та суспільства.

Державна статистична діяльність проводиться органами державної статистики згідно з Законом України «Про державну статистику» та відповідно до завдань, віднесених до їх компетенції, на засадах професійної незалежності та самостійності. Втручання будь-яких органів державної влади та органів місцевого самоврядування, інших юридичних осіб, об'єднань громадян, посадових та інших осіб у державну статистичну діяльність, зокрема, з питань змісту статистичної інформації, вибору джерел її отримання, статистичної методології, форм і термінів збирання та поширення даних статистичних спостережень тощо, забороняється.

Статистичне спостереження — це планомірний, науково організований процес збирання даних щодо масових явищ та процесів, які відбуваються в економічній, соціальній та інших сферах життя України та її регіонів, шляхом їх реєстрації за спеціальною програмою, розробленою на основі статистичної методології. Статистичні спостереження проводяться органами державної статистики через збирання статистичної звітності, здійснення одноразових обліків, переписів (опитувань), вибіркових та інших обстежень.

За видами статистичні спостереження розподіляються на суцільні та несучільні. *Суцільне статистичне спостереження* — спостереження щодо всіх без винятку одиниць сукупності, яка вивчається. *Несучільне статистичне спостереження* — спостереження за окремими одиницями сукупності, яка вивчається.

Статистичні спостереження розподіляються також на державні та інші статистичні спостереження. Державні

статистичні спостереження проводяться органами державної статистики відповідно до затвердженого Кабінетом Міністрів України плану державних статистичних спостережень або за окремими рішеннями Кабінету Міністрів України. Державні статистичні спостереження, які проводяться органами державної статистики із залученням тимчасових працівників, здійснюються за рішеннями Кабінету Міністрів України на визначених цими рішеннями умовах.

Статистична методологія — це сукупність науково обґрунтованих способів, правил і методів статистичного вивчення масових соціально-економічних явищ та процесів, які встановлюють порядок збирання, опрацювання і аналізу статистичної інформації.

Усі працівники органів державної статистики зобов'язані дотримуватися вимоги захисту конфіденційної інформації і за порушення цієї вимоги несуть відповідальність згідно із законами.

Статистична інформація, отримана на підставі проведених органами державної статистики статистичних спостережень, існує у вигляді первинних даних щодо респондентів, статистичних даних, що пройшли одну чи декілька стадій опрацювання та накопичені на паперових, магнітних, оптичних та інших носіях або в електронному вигляді, а також аналітичних матеріалів, підготовлених на підставі цих даних.

Первинні дані — це інформація щодо кількісної та якісної характеристики явищ і процесів, яка подана респондентами під час статистичних спостережень.

Статистичні дані — це інформація, отримана на підставі проведених статистичних спостережень, що опрацьована і подана у формалізованому вигляді відповідно до загальноприйнятих принципів та методології. Статистичні дані, що є результатом зведення та угруповання первинних даних, за умови забезпечення їх знеособленості являють собою зведену знеособлену статистичну інформацію (дані).

Статистичною інформацією є також дані банківської і фінансової статистики,

статистики платіжного балансу тощо, які складаються на підставі адміністративних даних, отриманих Національним банком України та спеціально уповноваженими органами державної влади (крім органів державної статистики) відповідно до їх компетенції. Відповідні повноваження зазначених органів, а також засади щодо організації збирання, опрацювання, аналізу, поширення, збереження, захисту та використання такої статистичної інформації визначаються окремими законами.

Первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов'язаною із збиранням та використанням адміністративних даних, є конфіденційною інформацією, яка охороняється Законом використовується виключно для статистичних цілей у зведеному знеособленому вигляді.

Поширення статистичної інформації, на підставі якої можна визначити конфіденційну статистичну інформацію щодо конкретного респондента, забороняється. Статистична інформація, отримана органами державної статистики у процесі статистичних спостережень, не може вимагатися органами державної влади, органами місцевого самоврядування, іншими юридичними особами, об'єднаннями громадян, посадовими та іншими особами з метою використання для прийняття рішень до конкретного респондента.

Статистична інформація, яка дозволяє прямо чи опосередковано встановити конкретного респондента або визначити первинні дані щодо нього, може бути поширена за згодою цього респондента і відповідно до погоджених з ним умов, або якщо вона отримана із загальнодоступних джерел.

Заборона стосовно поширення статистичної інформації не розповсюджується на: 1) знеособлену статистичну інформацію у незведеному вигляді, яка не дозволяє визначити конфіденційну статистичну інформацію щодо конкретного респондента; 2)

інформацію щодо назв, адрес, номерів телефонів і видів діяльності підприємств, установ і організацій, якщо інше не передбачено законодавством.

Статистична інформація, отримана у процесі державних статистичних спостережень, а також первинні дані, отримані у процесі проведення інших статистичних спостережень, є державною власністю, що знаходиться в оперативному управлінні органів державної статистики, які володіють, використовують і розпоряджаються цією статистичною інформацією, визначають правила її збирання, опрацювання, поширення, збереження, захисту та використання.

Право власності на зведену знеособлену статистичну інформацію, отриману органами державної статистики у процесі статистичних спостережень, що проведені за рахунок коштів замовника, визначається договорами на створення цієї інформації, які також передбачають умови поширення органами державної статистики вказаної інформації. Для забезпечення потреб органів державної влади, органів місцевого самоврядування, інших юридичних, а також фізичних осіб у статистичній інформації та доступу до неї, в органах державної статистики створюються спеціальні інформаційні служби.

Статистична інформація (роботи, послуги) на безоплатній основі може бути надана студентам, аспірантам, науковцям (для підготовки курсових, дипломних робіт, кандидатських та докторських дисертацій, наукових монографій тощо) на загальних підставах шляхом виписування даних — у разі офіційного звернення навчального закладу, наукової установи до відповідного органу державної статистики або зі знижками на підставі окремого рішення керівника цього органу в разі копіювання статистичних матеріалів чи тоді, коли для підготовки статистичної інформації потрібні додаткові витрати часу та матеріальні витрати.

Надання статистичної інформації (робіт, послуг) здійснюється із суворим дотриманням державної та комерційної таємниці, а також зі збереженням

конфіденційності й знеособленості даних щодо юридичних і фізичних осіб, за винятком випадків, коли надання відповідним державним органам таємної чи конфіденційної інформації прямо встановлене чинним законодавством.

Запити на отримання статистичної інформації (робіт, послуг) виконуються протягом місяця з дня їх надходження або з дня публікації органом державної статистики відповідного статистичного видання, якщо на день запиту воно не було опубліковане. Відмова в наданні статистичної інформації (робіт, послуг) повинна ґрунтуватися на підставах, передбачених чинним законодавством України, про що користувачу повідомляється письмово із зазначенням підстав відмови в десятиденний термін від дня надходження запиту [121].

10. Правові проблеми використання інсайдерської інформації

І на завершення вважаємо логічним стисло з'ясувати основні правові особливості одного з нових видів інформації, яким є *інсайдерська інформація* (англ. *insider information*).

Інсайдерська інформація – це закрита для прилюдного користування службова інформація щодо нових стратегій відносно підготовки до випуску нового продукту, у першу чергу з використанням високих технологій, яка у випадку її розкриття та оприлюднення здатна вплинути на ринкову вартість цінних бумаг компанії. Також до інсайдерської інформації відносять матеріали фінансової звітності юридичної особи, прогнози відносно корпоративних складнощів, відомості про успішні переговори щодо злиття компаній та ін.

Власне термін «інсайдер» використовується у зв'язку із секретною,

прихованою або закритою інформацією або знаннями. Адаже 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, що недоступна широкій публіці. Окремо наголосимо, що у цілому 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]. Звідси у більш 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 несанкціонована передача інсайдерської інформації щодо притягнення до юридичної відповідальності, адже в інформаційному законодавстві України таке поняття до цього часу відсутнє. Звідси потрібно підготувати проект закону щодо внесення змін до КК України, що передбачають кримінальну відповідальність за використання інсайдерської інформації та маніпулювання цінами на фінансовому ринку.

Таким чином, правові аспекти протидії щодо використання інсайдерської інформації остаточно не вирішені. Тим більше потрібно звернути увагу на те, що окремі заходи правової відповідальності, які головним чином застосовуються безсистемно, в сучасних умовах не сприяють зупиненню протиправної діяльності інсайдерів.

КЛЮЧОВІ СЛОВА: Інформаційна діяльність, преса, інформаційні агентства, бібліотеки, архіви, телебачення, радіомовлення, видавництво, статистика, реклама, інсайдер.

ЛЕКЦІЯ 4. ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА ТА ВИДИ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

© Синьокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синьокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. Основні дефініції, поняття та функції електронної комунікації.
2. Цифрові права людини та мультимедіа-технології як наукові категорії.
3. Сфера застосування та класифікація телекомунікацій.
4. Поняття та види телекомунікаційних послуг.
5. Суб'єкти ринку телекомунікаційних послуг.
6. Поняття електронного документообігу та правові ознаки електронних документів.
7. Інформаційні ресурси та інформаційні продукти.
8. Інформаційні моделі та компоненти інформаційної системи.
9. Інформаційні процеси та новітні інформаційні технології.
10. Глобальна система Інтернет як вид електронної комунікації та проблеми правового регулювання Інтернет-простору.

1. Основні дефініції, поняття та функції електронної комунікації

Масова комунікація (англ. – *mass communications*) – це діяльність щодо трансляції, перенесенню у практичну (масову) свідомість духовно-практичних цінностей у формі оцінок тих або інших соціальних груп суспільно значимих 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 факторів, які впливають на формування інформаційного суспільства.

Отже, масові комунікації здійснюються за допомогою технічних засобів і приймають вигляд публічного процесу виробництва інформації, її передачі засобами преси, радіо, телебачення та міжособистісного спілкування. Зокрема електронна комунікація ґрунтується на

космічному радіозв'язку, мікроелектронній та комп'ютерній техніці та оптичних приладах запису.

Перед початком викладення основного матеріалу відносно піднятої проблематики вважаємо за необхідне навести основні дефініції.

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 обчислюваної 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.

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 інформаційного масиву 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.

Безпроводовий доступ до телекомунікаційної мережі – електровз'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які приєднані до одного комутаційного центру.

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.

Глобальні мережі передачі даних – іноземні та міжнародні мережі передачі інформації, у тому числі мережа Інтернет.

Голографія – набір технологій для точного запису інформації шляхом відтворення та переформатування хвильового поля, де голографічна пам'ять є потенційно-можливою заміною технології підвищеної ємності даних, що широко використовується в магнітних та оптичних носіях, оскільки дозволяє використовувати мільйони одночасних потоків запису інформації.

Грид-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).

Дистанційне оброблення даних – оброблення інформації, за якими деякі функції введення-виведення виконуються пристроями, зв'язаними з комп'ютерною системою за допомогою засобів пересилання даних.

Доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі.

Драйвер – додаткова до операційної системи програма, що виконує функцію зв'язку операційної системи з зовнішнім пристроєм.

Електровз'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.

Інтерактивний режим – режим взаємодії користувача з обчислюваною системою, при якому система здійснює приймання, оброблення і видачу повідомлень в реальному масштабі часу.

Інформаційна радіоелектронна система – радіоелектронна система, яка здійснює збирання, оброблення і видавання інформації визначеного цільового призначення.

Інформаційно-аналітична система – суспільна структура, що включає інформаційні технології, інформаційні системи й інформаційні ресурси для здійснення інформаційно-аналітичної діяльності.

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, які у процесі обробки інформації діють як єдине ціле;

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 одного або кількох вузлах якої як ресурс оброблення даних містяться комп'ютери.

Комунікаційні засоби комунікаційної (мережа) – це сукупність ліній пересилання даних та комунікаційних пристроїв, що дозволяє здійснювати взаємне сполучення прикінцевого обладнання.

Комутація каналів – процес з'єднання двох чи більше абонентських станцій, який забезпечує монопольне використання каналу пересилання даних до його роз'єднання.

Користувач інформації в системі – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі.

Мікроносії інформації – репрографічна копія у вигляді мікрофільму або мікрофіши, що містить одне чи кілька мікро зображень документа на рулонній або форматній плівці, читання яких можливе тільки за допомогою оптичних приладів.

Об'ємна оптична пам'ять – різновид комп'ютерної пам'яті, де інформація може бути записана та зчитана у тривимірному просторі.

Обробка інформації в системі – 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.

Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї 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 провідних 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 обчислюваної 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.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

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.

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.

Послуга електрозв'язку є продуктом (результатом) діяльності оператора електрозв'язку, що полягає в передаванні, прийманні та обробці інформації. Послуги зв'язку, у тому числі забезпечення телефонного, телексного, телеграфного зв'язку, радіомовлення, електронної пошти, супутникового, факсимільного та телевізійного зв'язку, поштові послуги, мають назву *комунікаційних послуг*.

До телекомунікаційних систем належать: телеграф, телефон (у тому числі радіотелефон), радіо, супутниковий зв'язок, телекс, телебачення (у тому числі кабельне), комп'ютерні мережі тощо. Зокрема, телеграфія є видом електрозв'язку для передавання текстової інформації з використанням сигнального коду.

У сфері передачі інформації для позначення телекомунікаційних засобів найчастіше використовуються такі терміни як «система», «мережа», «лінія», «магістраль», «коридор» та деякі інші.

Канал зв'язку – засоби двостороннього обміну даними як сукупність апаратури закінчення ланки даних та лінії пересилання інформації.

Інформаційний канал – це маршрут пересилання інформації.

Інформаційний сигнал – це акустичний чи оптичний сигнал, що сповіщає абонента чи оператора про етапи та результати установалення з'єднання.

Фіксований зв'язок – це телекомунікації, що здійснюються із застосуванням стаціонарного (нерухомого) кінцевого обладнання.

З метою розв'язання 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.

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 приймають участь у даній діяльності або користуються телекомунікаційними послугами.

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

Тобто, *телекомунікації* – це процес дистанційного передавання даних на засадах інформаційних технологій.

2. Цифрові права людини та мультимедіа-технології як наукові категорії

У загальному розумінні, *формат інформації* – це специфікація (однозначний опис) структури даних.

Сьогодні розрізняють декілька видів інформаційних форматів: а) відкритий формат як загальнодоступна специфікація зберігання цифрових даних; б) тестовий формат як формат зберігання текстової інформації; г) графічні формати як формати зберігання графічної інформації – фотографій і малюнків; д) цифрові звукові формати як формати запису звуку. Крім цього, також існують інші формати зберігання інформації. Зокрема, RAW-формат даних, який не має чіткої специфікації і містить неопрацьовані або

опрацьовані у мінімальному ступеню дані, що дозволяє уникнути втрат інформації.

Інформаційно - медійна, комунікативна система є «мережа 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 є типом сигналів і форматів даних в електроніці, що використовують дискретний стан (на відміну від аналогового сигналу, що змінюється безперервно).

Цифровий зв'язок є галуззю техніки, яка пов'язана з передачею 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 і для передачі аналогових сигналів (наприклад, таких безперервних як мова та зображення). Останні з цієї мети 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 призвело перехід різних технічних пристроїв відеоспостереження в цифровий формат.

Мультимедіа-технології є технологіями одночасного використання різних форм представлення інформації та її обробки 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 випадку 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.

Компаратор – (від англ. *comparare* – порівнювати) – це інформаційний пристрій цифрової техніки, що призначений для порівняння будь-чого, в тому числі може бути програмою пошуку та порівняння схожих файлів.

У сучасних цифрових системах інформаційних технологій застосовуються кабельні (волоконно-оптичні), супутникові, радіорелейні та інші лінії й 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, передачі 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 й мережі. Також потрібно 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), коннективність (постійний контакт із затребуваними інформаційними потоками), мультимедійність. Утім з іншого боку у цьому зв'язку окремо виникає проблема цифрових прав людини.

Сьогодні 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 й застосування універсальних

прав людини до потреб суспільства, що засноване на інформації.

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

У глобальному контексті термін «цифрову нерівність» став активно вживатися при аналізі нерівності між країнами у сфері нових технологічних розробок. Цифрові права передбачають подолання або зниження інформаційної нерівності, тобто доступу 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, визначимо, що базові цифрові права людини включають право інформаційного доступу до електронної мережі, право вільно спілкуватися й висловлювати думки у телекомунікаційній системі, і право на інформаційну обмеженість приватної сфери.

3. Сфера застосування та класифікація телекомунікацій

Телекомунікаційна передача інформації є новим кроком у мультимедійних технологіях зв'язку.

Держава гарантує універсальне обслуговування, тобто забезпечення універсального доступу споживачів до телекомунікаційних мереж загального користування та надання загальнодоступних телекомунікаційних послуг нормованої якості за регульованими державою тарифами.

Висока якість зв'язку і повне екранне відеозображення, широкі можливості для роботи над різними проектами, оперативним обміном даними, документами і т. ін. роблять телекомунікаційну передачу інформації потужним інструментом з широким спектром використання.

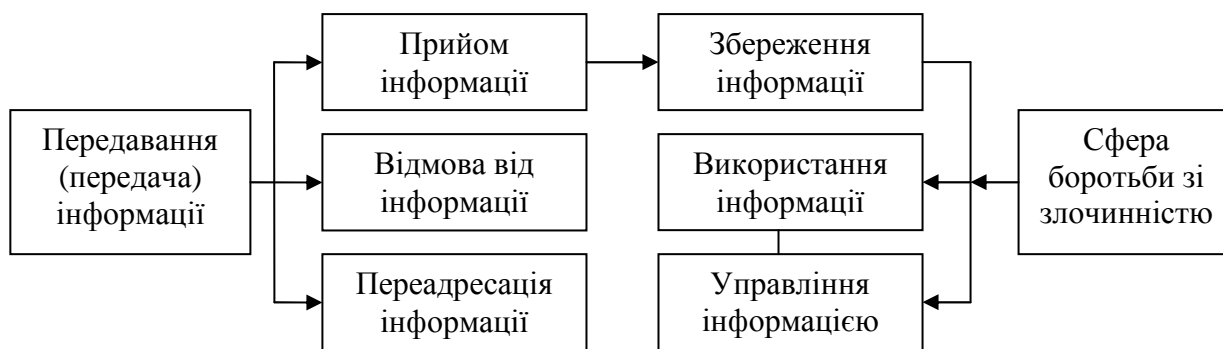
У цілому, сфера телекомунікацій є складовою частиною галузі зв'язку України. Телекомунікації є невід'ємною частиною виробничої та соціальної інфраструктури України і призначені для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах.

На сьогодні 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 техніці під зв'язком розуміється передача 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 передачі інформації.

Закінчення такого циклу може також бути негативним у випадку «*Відмови від інформації*». Крім цього, зустрічається третій нейтральний варіант – «*Переадресація інформації*».

Схематично процес передачі інформації у сфері боротьби зі злочинністю може бути представлений схематично наступним чином:



4. *Поняття та види телекомунікаційних послуг*

Потрібно звернути увагу на те, що з використанням сучасних електронних засобів передачі інформації виникають нові соціальні та психологічні феномени і, відповідно, нові можливості у галузі розвитку комунікації.

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 розвідки 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].

5. 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, що пов'язані з Інтернетом.

З юридичної точки зору Інтернет-провайдер або просто провайдер – це оператор зв'язку, що має ліцензію щодо виділення та надання каналів зв'язку та передачі 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, які 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 електров'язку.

6. Поняття електронного документообігу та правові ознаки електронних документів

Основні організаційно-правові засади електронного документообігу та використання електронних документів визначає Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. [68].

Згідно зі ст. 4 цього Закону Державне регулювання у сфері електронного документообігу спрямовано на:

- 1) реалізацію єдиної державної політики електронного документообігу;
- 2) забезпечення прав і законних інтересів суб'єктів електронного документообігу;
- 3) нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення електронних документів.

Електронний документообіг (обіг електронних документів) – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів (ст. 9).

Електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи

обов'язкові реквізити документа (ст. 5). Обов'язковий реквізит електронного документа – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили.

Законом України «Про електронні документи та електронний документообіг» встановлено правовий статус електронного документа та його копії. Зокрема, юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Разом із тим, згідно зі ст. 8 зазначеного Закону електронний документ не може бути застосовано як оригінал: 1) свідоцтва про право на спадщину; 2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів; 3) в інших випадках, передбачених законом [68].

Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу (ст. 6).

Електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані. Накладанням електронного підпису завершується створення електронного документа. Цифровий підпис призначений для аутентифікації особи, що підписала електронний документ.

Одним з видів електронного підпису є електронний цифровий підпис.

Відносини, пов'язані з використанням електронних цифрових підписів, регулюються Законом України «Про електронний цифровий підпис». Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Закон України «Про електронний цифровий підпис» визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису. Дія даного Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису. Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені Законом «Про електронний цифровий підпис», застосовуються правила міжнародного договору.

Електронний цифровий підпис – це реквізит електронного документа, що дозволяє встановити відсутність перекручування інформації в електронному документі з моменту формування ЕЦП та перевірити приналежність підпису власникові сертифікату ключа ЕЦП.

Значення реквізиту здійснюється за наслідками криптографічного перетворення набору електронної інформації з використанням закритого ключа ЕЦП.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Засіб електронного цифрового підпису – це програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису.

Особистий ключ – це параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ – це параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Сертифікат відкритого ключа (далі – сертифікат ключа) – це документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть

розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача.

Посилений сертифікат відкритого ключа (або посилений сертифікат ключа) – це сертифікат ключа, який відповідає вимогам Закону України «Про електронний цифровий підпис», виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Відповідальність за організацію застосування електронного цифрового підпису в установі несе її керівник, якщо інше не встановлено законодавством. Застосування електронного цифрового підпису в установі забезпечує підрозділ інформаційних технологій, а у разі відсутності такого – підрозділ, що виконує відповідні функції (далі – відповідальний підрозділ), або працівник, спеціально визначений наказом керівника цієї установи.

Суб'єктами електронного документообігу є автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу.

Автор електронного документу – це фізична або юридична особа, яка створила електронний документ.

Послуги електронного цифрового підпису – це надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України «Про електронні документи та електронний документообіг».

Надійний засіб електронного цифрового підпису – це засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Суб'єкти електронного документообігу, які здійснюють його на договірних засадах, самостійно визначають режим доступу до електронних документів, що містять конфіденційну інформацію, та встановлюють для них систему (способи) захисту. В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять інформацію, яка є власністю держави, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства.

Суб'єкти електронного документообігу користуються правами та мають обов'язки, які встановлено для них законодавством. Якщо в процесі організації електронного документообігу виникає необхідність у визначенні додаткових прав та обов'язків суб'єктів електронного документообігу, що не визначені законодавством, такі права та обов'язки можуть встановлюватися цими суб'єктами на договірних засадах.

Формат списку відкликаних сертифікатів визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП. Управління статусом сертифіката та розповсюдження інформації про статус сертифіката повинні бути вільнодоступні цілодобово.

Звернення щодо скасування сертифікатів фіксуються та зберігаються в акредитованому центрі. Акредитований центр повинен забезпечити цілісність та автентичність інформації щодо статусу сертифікатів.

Порядок обов'язкової передачі документованої інформації, затверджений постановою Кабінету Міністрів України від 28 жовтня 2004 р. № 1454 визначає механізм обов'язкової передачі на зберігання центральному засвідчувальному органу або засвідчувальному центру посиленних сертифікатів відкритих ключів (далі – сертифікати), документованої інформації акредитованим центром сертифікації ключів (далі – акредитований центр) у разі

припинення його діяльності. Метою зазначеної передачі є забезпечення можливості перевірки електронного цифрового підпису, накладеного на електронний документ підписувачем, відкритий ключ якого засвідчений в акредитованому центрі, що припиняє діяльність.

Акредитований центр, що засвідчив свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі, здійснює передачу центральному засвідчувальному органу або засвідчувальному центру такої документованої інформації:

1) *електронні документи* – сертифікати, що були сформовані акредитованим центром, електронний реєстр сертифікатів, електронні документи, на підставі яких були сформовані, скасовані, блоковані та поновлені сертифікати підписувачів (якщо такий спосіб передбачений регламентом роботи акредитованого центру), список відкликаних сертифікатів;

2) *документи на папері* – договори, на підставі яких підписувачам надавалися послуги електронного цифрового підпису, оригінали документів, що посвідчують фізичних та юридичних осіб – підписувачів, оригінали документів, на підставі яких були сформовані, скасовані, блоковані та поновлені сертифікати підписувачів, або засвідчені в установленому порядку їх копії, а також засвідчені в установленому порядку копії рішень (ухвал) судів щодо відшкодування збитків, понесених внаслідок неналежного виконання акредитованим центром своїх обов'язків.

За місяць до припинення своєї діяльності акредитований центр разом із заявою, в якій зазначаються підстави та дата припинення його діяльності, подає до центрального засвідчувального органу або засвідчувального центру – акт приймання-передачі та документовану інформацію. Акт приймання-передачі, у якому зазначаються дата передачі, номери та назви документів, кількість аркушів у документі, типи та номери носіїв інформації, складається у трьох примірниках. Документована інформація передається до центрального

засвідчувального органу або засвідчувального центру нарочним чи рекомендованим поштовим відправленням [121; 122].

7. Інформаційні ресурси та інформаційні продукти

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

Інформаційні ресурси – 1) організованою сукупністю 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 напрямків, 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.

Глибока комунікація означає щільний інформаційний обмін, до чого залучаються практично усі інформаційні ресурси, і відтак виникає тісне переплетення «силових ліній» інформаційних полей.

Поверхнева комунікація відбувається при неповному (частковому) залученні до обміну інформаційних ресурсів. Звідси щільність інформаційного потоку виявляється набагато менше порівняно з першим випадком.

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

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

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

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

Зокрема, Закон України «Про науково-технічну інформацію» надає визначення інформаційних ресурсів науково-технічної інформації як систематизованого зібрання науково-технічної літератури і документації (книги, брошури, періодичних видань, патентної документації, нормативно-технічної документації, промислових каталогів, конструкторської документації, звітної науково-технічної документації з науково-дослідних і дослідно-конструкторських робіт, депонованих рукописів, перекладів науково-технічної літератури і документації), зафіксованих на паперових чи інших носіях [71].

Інформаційні ресурси національної системи науково-технічної інформації становлять сукупність довідково-інформаційних фондів з необхідним довідково-пошуковим апаратом і відповідними технічними засобами зберігання, обробки і передачі, що є у володінні, розпорядженні, користуванні державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, комерційних центрів, підприємств, установ і організацій [71].

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

Включення інформаційних продуктів до складу національних інформаційних ресурсів здійснюють 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, що інформаційні ресурси – це сукупність інформаційних продуктів одного або декількох тематичних напрямків, 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.

Окремо потрібно відзначити, що національні інформаційні ресурси не здатні конкурувати із глобальними Інтернет-ресурсами – вони приречені на поразку, особливо в міру інформаційного впливу, особливо на молоде покоління, оскільки відбувається підміна моральних основ якимсь універсальним віртуальним сурогатом. Це додатково підтверджує потребу удосконалення правового механізму Інтернет-регуляції.

Інформаційний продукт – це: а) документована інформація, що підготовлена і призначається для задоволення потреб користувача; б) інформаційний продукт – це об'єктивно закріплена на носії інформація, підготовлена для споживання, автоматизованої обробки і поширення за допомогою мереж передачі даних; в) інформаційний продукт – це результат інформаційної діяльності, процес матеріалізації створю продукцію.

До складу національних інформаційних ресурсів включають: а) в обов'язковому порядку – інформаційні продукти, створені органами державної влади й 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 рахунок позабюджетних коштів їх власників або виробників.

Включення цих продуктів до складу національних інформаційних ресурсів не призводить до зміни їх власника, якщо інше не передбачене законом або умовами угоди; д) на основі відповідних міждержавних або міжнародних угод – міждержавні та міжнародні інформаційні продукти.

Інформаційні продукти, що 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 випадку, 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, що розміщені в електронних базах або банках даних, у комп'ютерних системах, системах автоматизованої обробки і передачі даних. Якщо ці ресурси одержують або передають за допомогою Інтернет, то їх називають веб-

ресурсами (від поняття – WWW – «всесвітня павутина комунікації»).

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

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

Інформаційні ресурси можуть бути власністю громадян України, іноземних громадян і осіб без громадянства, органів державної влади й 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 відповідних міжнародних договорів України.

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

Власник або власник ресурсу, в разі завдання йому моральної або 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 здійснює реєстрацію засобу 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, встановленого Кабінетом Міністрів України для друкованих засобів масової інформації.

Отже, враховуючи викладене, 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 потрібно наголосити, що інформаційні ресурси мають свою специфіку: 1) вони не споживані й піддаються не фізичному, а моральному зносу; вони не матеріальні й не залежать від носія інформації; 2) оптимізація структури їхнього використання дозволяє набагато знизити витрати інших видів ресурсів, що веде до великої економії коштів; 3) процес їх створення та використання здійснюється особливим способом – за допомогою комп'ютерної техніки.

8. Інформаційні моделі та компоненти інформаційної системи

Інформаційна модель – це 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.

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

Інформаційна система – це взаємозв'язана сукупність засобів, методів і персоналу, що використовуються для зберігання, обробки й видавання інформації в інтересах досягнення поставленої мети.

На рівні сучасної інформаційної системи в цілому нестійкість пов'язана з інформаційно-комунікативною революцією, що створює нову технологічну базу

цивілізації. Конвергенція засобів обчислювальної техніки з засобами інформаційної комунікації породжує ефект соціально-технологічної інтегрованості системи [89].

Сучасне розуміння інформаційної системи передбачає використання як основного технічного засобу переробки інформації комп'ютерної техніки.

Телекомунікаційна революція замінює єдинолінійність комунікаційного акту багатофункціональним, діалоговим зв'язком, здійснює «стиск» простору й часу, породжуючи нові ступені волі для індивіда й соціуму (і нові проблеми).

Крім того, технічне втілення інформаційної системи саме по собі нічого не буде значити, якщо не врахована роль людини, для якої призначена вироблена інформація і без якої неможливе її одержання й подання [23, с. 34].

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

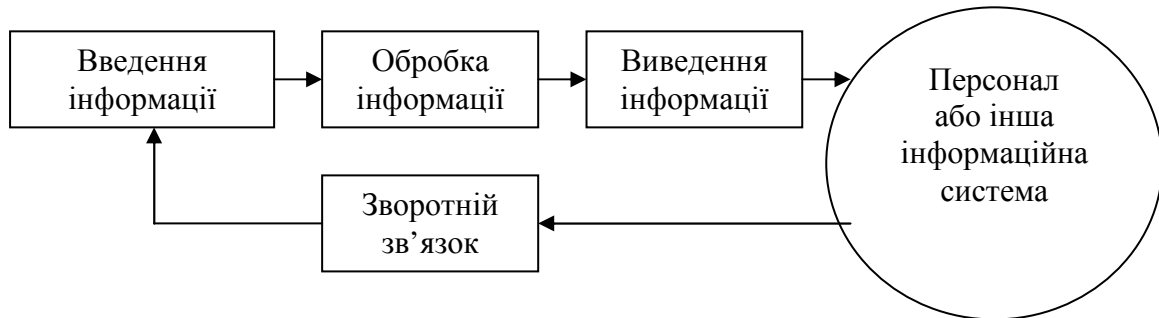
Робота інформаційної системи полягає в обслуговуванні двох зустрічних потоків інформації: введення нової інформації і видавання поточної інформації на запит.

Процеси, що забезпечують роботу інформаційної системи будь-якого призначення, умовно можна представити у вигляді схеми, що складається з блоків: 1) введення інформації із зовнішніх або внутрішніх джерел; 2) обробка вхідної інформації й подання її у зручному вигляді; 3) виведення інформації для представлення її у зручному вигляді; 4) зворотній зв'язок —

інформація перероблена людьми даної організації для корекції вхідної інформації.

Процес інформаційного пошуку включає послідовність операцій, що

спрямовані на збір, обробку та надання необхідної інформації, що показано нижче на схемі:



Структуру інформаційної системи складає сукупність окремих її компонентів, що називаються 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 випадку говорять про структурну ознаку класифікації, а підсистеми називають забезпечуючими.

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

Інформаційні підсистеми як головні складники інформаційного забезпечення призначені для збирання, накопичення, зберігання, обробки та передавання ін-

формації певних напрямів правової діяльності і орієнтовані на загальне використання галузевими службами, мають загальновідомчий характер і належать до службових інформаційних підсистем.

Інформаційна мережа створюється за територіальним принципом і має трьохрівневу 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 нижче показані у схематичному вигляді:



Оскільки головне завдання інформаційної системи – обслуговування клієнтів, то вона побудована таким чином,

щоб відповідь на будь-яке питання видавалася швидко і була достатньо повною. Це забезпечується наявністю стандартних

процедур пошуку інформації і тим, що дані системи розташовані в певному порядку [23, с. 187].

Універсальний доступ до інформаційної системи повинен 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 й одержання зононих, міжміських, міжнародних дзвінків), факсимільний зв'язок, передачу 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.

Систему організаційних структур, підсистем, що забезпечують функціонування та розвиток інформаційного простору країни й засобів інформаційної взаємодії можна визначити як *інформаційну інфраструктуру*.

У загальному сенсі під терміном «*інфраструктура*» розуміють комплекс взаємопов'язаних допоміжних структур або об'єктів, що складають та/або забезпечують основу функціонування системи.

Інформаційна інфраструктура включає сукупність інформаційних центрів, підсистем, банків даних і знань, систем зв'язку, центрів управління, апаратно-програмних засобів та технологій для забезпечення збору, зберігання, обробки й передачі інформації, а також забезпечує доступ споживачів до інформаційних ресурсів.

Глобальна інформаційна інфраструктура є новим інформаційним утворенням, що розробляється як загальносвітова інформаційна мережа масового обслуговування населення планети на основі інтеграції глобальних та регіональних інформаційно-телекомунікаційних систем, а також систем

цифрового телебачення й радіомовлення, супутникових систем і мобільного зв'язку.

Отже, системне співвідношення основних складових компонентів визначимо

таким чином: $\frac{1(a + b...)}{2(c + d...)} < 3 \mapsto 4$. Це означає,

що інформаційні продукти (2) є складовою частиною інформаційних ресурсів (1), а останні, у свою чергу, створюють інформаційні системи (3) для функціонального забезпечення інформаційних процесів (4).

Потрібно наголосити, що інформаційні системи і технології знаходять широке впровадження в юридичній діяльності [45].

9. Інформаційні процеси та новітні інформаційні технології

У загальному розумінні процес є послідовною зміною станів об'єкта у часі. Відомо, що галузей матеріального права існує набагато більше, ніж процесуальних.

Сьогодні ще не існує юридичної науки інформаційного процесу у значенні, наприклад, кримінального чи цивільного процесів. Тому інформаційно-правова діяльність у випадку відсутності «власного» процесуального права неминує здійснюється за процедурами одного з існуючих юридичних процесів.

Юридичний процес – це врегульований процесуальними нормами порядок діяльності компетентних державних органів, що складається у підготовці, 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.

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 уявляє правовий механізм вирішення інформаційних питань; 2) *соціотехнологічний аспект* – модернізація процесів програмного забезпечення та технологічного обміну інформацією (точка зору інформатики), тобто фактично уявляє інформатизацію; 3) *комунікативний аспект* – процеси та механізми міжособистісного та міжгрупового спілкування (точка зору соціальної психології).

Отже, *інформаційний процес* – це процес одержання, створення, збору, обробки, накопичення, зберігання, пошуку, поширення та використання інформації.

Таким чином, у структурі інформаційного процесу реалізуються норми інформаційного права. При цьому динаміка та розвиток інформаційного процесу регулюється процесуальними нормами інших галузей права.

Інформаційні технології – це цілеспрямовано організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечує продуктивні обробку 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].

Потрібно зазначити, що терміни «технологія зв'язку», «сучасна технологія зв'язку» не зовсім чітко передають зміст тієї предметної галузі, яку вони покликані позначати. У поняття нової інформаційної технології включені також комунікаційні технології, які забезпечують передачу інформації різними засобами.

Тому, дослідники пропонують вживати термін «телекомунікаційна технологія» [239, с. 103-108].

За класами реалізованих технологічних операцій інформаційні технології розглядають у програмному аспекті і включають: обробку текстів, електронні таблиці, автоматизовані бази (банки) даних,

обробку графічної та звукової інформації, мультимедійні та інші системи [86].

Програмно-технічна організація обміну з комп'ютером текстовою, графічною, аудіо- та відеоінформацією одержала назву *мультимедіа-технології*. 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 із спеціалістом на його рідній мові. Здатність комп'ютера з голосу сприймати нескладні команди керування програмами, відкриванням файлів, виведенням інформації на друк та іншими операціями створює сприятливі умови для взаємодії з ними в процесі професійної діяльності [23, с. 201].

Як один з яскравих прикладів новітніх телекомунікаційних технологій можна зазначити російську супутникову систему навігації, що має назву Глобальна навігаційна супутникова система (ГЛОНАСС), яка включає серію космічних апаратів третього покоління.

Іншим прикладом є мобільний зв'язок третього покоління, що ґрунтується на пакетній передачі інформації. Потрібно визначити, що технології мобільного зв'язку 3G (від англ. *third generation* — «третє покоління») представляють 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 передачі даних. На теперішній час найбільшого поширення одержали два стандарти, що дозволяє організувати відеотелефонний зв'язок, дивитися на мобільному телефоні фільми й телепрограми й т.п. Крім того, мережі 3G

відрізняються підвищеною екологічною безпекою [255].

Останнім часом пропонується для використання нова глобальна/регіональна інформаційна мережа Теланнет (не плутати зі службою Telnet існуючого Інтернету). Істотною перевагою Теланнета в порівнянні з Інтернетом є забезпечення в ньому повної інформаційної безпеки, тобто захисту від хакерів, комп'ютерних вірусів, шпигунських програм (якими зараз уражені 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, у майбутньому здатні вирішувати окремі завдання.

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

Таким чином, визначимо нову інформаційну технологію як технологію, яка засновується на застосуванні комп'ютерів, активній участі користувачів (непрофесіоналів в 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 передачі інформації.

Магістральна мережа зв'язку – це транспортна телекомунікаційна інфраструктура для надання послуг зв'язку, що, як правило, вибудовується на ВОЛЗ із

використанням високошвидкісного каналного обладнання зв'язку.

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

Основним напрямком оптичного зв'язку залишається волоконно-оптичний, оскільки вже впроваджені в практичну діяльність волоконні світловоди мають чудові характеристики передачі інформації.

Поряд із цим волоконно-оптичні деталі знаходять застосування в електронно-оптичних, вимірювальних приладах, телевізійних і акустичних пристроях, у фототелеграфних, телеметричних, голографічних та оптико-механічних, кібернетичних, лазерних системах і при ядерних дослідженнях.

Отже, ґрунтуючись на аналізі викладеного, спробуємо вивести окрему закономірність: $\frac{T}{E} \cong \frac{F}{I}$, де T –

телекомунікаційна мережа, E – електронні інформаційні ресурси, F – волоконно-оптична мережа, I – оптоволоконна система передачі інформації.

Таке співвідношення свідчить про те, що волоконно-оптична мережа майже завжди виступає складовою сучасної телекомунікаційної мережі відповідно як носій до предмету переміщення – електронних інформаційних ресурсів.

10. Глобальна система Інтернет як вид електронної комунікації та проблеми правового регулювання Інтернет-простору

Із впровадженням нових інформаційних технологій відбувається формування нової структури суспільства – так званої *мережевої структури*.

Особливим видом електронної комунікації є Інтернет (*англ. скороч.* від *Interconnected Networks* – об'єднані мережі) – тобто 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 в сфері інформатизації, задоволення конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства, забезпечення авторського права у сфері функціонування Інтернету [150].

У країнах Європи з 90-х рр. ХХ 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 напрямком 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 зв'язана глобальним адресним простором та базується на

інтернет-протоколі, визначеному міжнародними стандартами.

Визначимо основні терміни:

Інтранет – це 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.

Локальна обчислювана мережа – це система, яка забезпечує на обмеженій території один чи декілька каналів зв'язку, наданих приєднаним до неї абонентам для короточасного монопольного користування.

Мережа інформаційна – це сукупність мережі електронно-обчислюваних 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, обчислюваних, комунікаційних ресурсів і колективне їх використання.

Мережа передачі даних – це організаційно-технічна система, яка складається з комплексів телекомунікаційного обладнання (вузлів комутації) та реалізує технологію інформаційного обміну з використанням первинної мережі зв'язку.

Як було вище вже з'ясовано, високотехнологічне інформаційне право є системою правового регулювання інформаційних відносин у сфері високих технологій.

Синергетика займається дослідженням інформаційних систем, що складаються з великого числа частин, компонентів або підсистем, інакше кажучи, деталей, складним образом взаємодіючих між собою.

Підкреслимо, що в потрібний момент при виявленні небезпечних проявів можна втрутитися у хід подій і змінити його. Звідси інформаційне майбутнє також, виявляється, має неєдиний варіант розвитку.

Тому відповідь синергетики високотехнологічного права полягає в тому, що в безлічі випадків відбувається

самоорганізація, пов'язана з виділенням так званих параметрів порядку.

Адміністрування адресного простору українського сегмента мережі Інтернет включає комплекс організаційно-технічних заходів, необхідних для забезпечення функціонування технічних засобів підтримки адресування, у тому числі серверів доменних назв українського сегмента мережі Інтернет, реєстру домену.UA 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].

Останнім часом деструктивні сили все більш активно використовують ресурси мережі Інтернет для організації та ведення інформаційно-психологічної обробки громадян, пропаганди своїх ідей, залучення нових членів, пошуків джерел фінансування.

Звідси випливає, що можна з імовірністю близької до одиниці прогнозувати щодо зростання у світовому масштабі інформаційно-захисних тенденцій.

Наприклад, 1 березня 2010 р. у Міністерстві інформатизації та зв'язку Республіки Казахстан створено Департамент з відстеження національних деструктивних Інтернет-ресурсів, тобто не тільки релігійної, але й руйнівної спрямованості іншого характеру, що несуть шкоду родині й суспільству.

Звідси одна з основних причин формування систем контент-фільтрації Інтернету на державному рівні в ряді держав, є розробка та впровадження захисної реакції, що має бути втілена у правові та технологічні механізми захисту.

Так, у Великобританії після 11 вересня 2001 р. фільтрація контенту Інтернет-ресурсів стала прерогативою Національного відділення по боротьбі зі злочинами в області високих технологій. Зокрема, сьогодні вже передбачається введення нового режиму роботи сектору новин Інтернет-ресурсів.

Таким чином, управління використанням Інтернет охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь всі зацікавлені сторони й відповідні міжурядові й міжнародні організації. Варто особливо звернути увагу на висловлення Патріарха Московського й Всієї Русі Кирилу про те, що фактично Інтернет є лабораторією, де людина сама визначає, що є добром, а що – злом.

Таким чином, визначимо, що Інтернет є глобальною соціально-комунікаційною комп'ютерною мережею, що призначена для задоволення особистісних та групових інформаційних та комунікаційних потреб за рахунок використання телекомунікаційних технологій. Тому сьогодні правовий моніторинг інформаційних програм фактично постає як новий інструмент зворотного зв'язку з метою здійснення електронних проєктів, оцінки Інтернет-програм та стратегічного розвитку інформаційної політики.

КЛЮЧОВІ СЛОВА: *Електронна комунікація, телекомунікації, інформаційні ресурси, інформаційні продукти, інформаційні моделі, інформаційні системи, інформаційна безпека.*

ЛЕКЦІЯ 5. КРИМІНАЛЬНО-ПРАВОВІ ТА КРИМІНОЛОГІЧНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ВИСОКИХ ТЕХНОЛОГІЙ

© Синьокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синьокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. Інформаційна сфера і політика у сфері боротьби зі злочинністю.
2. Політика інформатизації правоохоронних органів.
3. Поняття кримінально-правової політики.
4. Інформаційні правопорушення і злочини у сфері високих технологій.
5. Злочинність у сфері високих технологій.
6. Інформаційна та міжнародна злочинність.
7. Проблеми інтелектуалізації високотехнологічної злочинності.
8. Кримінальне право і електронне право високих технологій.
9. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
10. Специфічні риси злочинів у сфері нанотехнологій і прогнози розвитку нанозлочинності.

1. Інформаційна сфера і політика у сфері боротьби зі злочинністю

Дослідженням проблем у сфері боротьби зі злочинністю присвячено велику кількість фундаментальних праць. Власне стосовно до процесів боротьби зі злочинністю вживається безліч термінів, при цьому кожний викликає наукові суперечки й не може оцінюватися однозначно. Тому упорядкування понятійного апарата має не тільки наукове, але й важливе практичне значення щодо розробки концепції боротьби зі злочинністю.

Не заглиблюючись до аналізу різних точок зору з цього приводу, пропонуємо вживати поняття «сфера боротьби із злочинністю».

Потрібно визначити, що сфера боротьби зі злочинністю є складною системною діяльністю, що представляє собою єдність трьох наступних підсистем:

- 1) загальної організації боротьби;
- 2) попередження злочинності;
- 3) правоохоронної діяльності.

Політика у сфері боротьби зі злочинністю – це вироблена державою

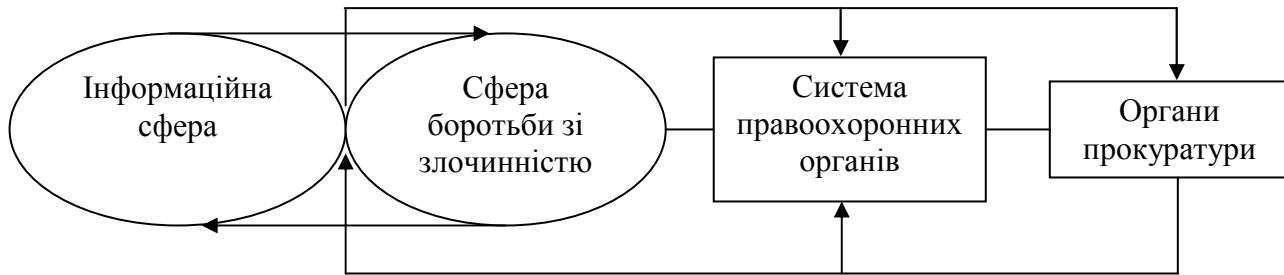
генеральна лінія, що визначає основні напрями, мету й засоби впливу на злочинність шляхом формування кримінального, кримінально-процесуального та кримінально-виконавчого законодавства, регулювання практики їх застосування, а також розробку й реалізацію заходів, спрямованих на запобігання вчиненню злочинів [229].

З першого погляду інформаційна сфера і сфера боротьби зі злочинністю є ніби-то двома абсолютно різними виявами соціального буття. Але ці обидві 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 може бути схематично показано нижче:



Утім також існує і зворотний зв'язок. Так, модернізація соціотехнічних процесів, що відбуваються у сфері боротьби зі злочинністю, детермінує формування та розвиток інформаційних відносин нового виду, в тому числі високотехнологічного змісту.

У загальному вигляді інформаційне забезпечення у сфері кримінальної юстиції складається з шести основних компонентів: 1) інформаційне забезпечення слідчої діяльності; 2) інформаційне забезпечення оперативно-розшукової діяльності; 3) інформаційне забезпечення судово-експертної діяльності; 4) інформаційне забезпечення прокурорської діяльності; 5) інформаційне забезпечення адвокатської діяльності; 6) інформаційне забезпечення судової діяльності.

Зрозуміло, що кожен з названих видів інформаційного забезпечення має окрему структуру, специфіку, організаційно-правову природу, процесуальне походження, матеріальні особливості інформаційних джерел та ін.

2. Політика інформатизації правоохоронних органів

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

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 основні причини 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 напрямку.

Правовою основою інформатизації правоохоронних органів є Указ Президента України «Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю» від 31 січня 2006 р. № 80/2006 та розпорядження КМУ № 146-р «Про утворення міжвідомчої координаційної групи із створення і функціонування Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби із злочинністю» від 15 березня 2006 р.

9 квітня 2009 р. КМУ затверджено Державну програму інформаційно-телекомунікаційного забезпечення правоохоронних органів, де окремо визначено актуальність потреби удосконалення методів боротьби із злочинністю, зокрема за рахунок підвищення ефективності інформаційно-телекомунікаційного забезпечення правоохоронних органів [46; 227].

Метою цієї Програми є забезпечення створення умов для поліпшення координації організаційних, профілактичних, оперативно-розшукових заходів, а також підвищити ефективність 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 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.

3. *Поняття кримінально-правової політики*

Юридична відповідальність є важливим елементом правового регулювання суспільних відносин у сфері обігу інформації з обмеженим доступом, суть якого полягає в цілеспрямованому впливі на поведінку індивідів за допомогою юридичних засобів з метою впорядкування зазначених суспільних відносин, надання їм системності та стабільності, уникнення різких загострень соціальних конфліктів, втілення 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, напрямки діяльності органів, які проводять дізнання,

досудове слідство і оперативно-розшукову діяльність, її основні форми й 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, щоб створити умови для виявлення цих внутрішньо диференційованих інтересів, оцінки й акумуляції їх у єдиний спільний інтерес.

В юридичній і спеціальній літературі проблемам інформаційної безпеки та боротьби зі злочинами у сфері інформаційних технологій приділяється належна 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.

Таким чином, з одного боку складовою частиною державної політики є інформаційна політика, а, у свою чергу, з іншого – 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 терміну «антикримінальна політика».

4. Інформаційні правопорушення і злочини у сфері високих технологій

Логічним бачиться визнати правову категорію правопорушень у сфері суспільних інформаційних відносин, як «правопорушення, що вчинюються 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 обробки – 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 вчинюються 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 розповсюджувати достовірну й повну інформацію.

В юридичній літературі вже висловлювалася точка зору про існування поняття «інформаційні злочини», під якими розуміються суспільно-небезпечні діяння, що заборонені кримінальним законом під погрозою покарання, які вчинені у галузі інформаційних правовідносин, тобто зв'язані зі збором, обробкою, нагромадженням та іншими інформаційними процесами.

Однак таке розуміння інформаційних злочинів є занадто широким, тому що в ряді складів злочинів існує інформаційний спосіб

їхнього вчинення (наприклад, погрози або обман).

А звідси, всі злочини, що вчинені подібним способом, необхідно відносити до інформаційних, що буде перебільшеним спрощенням, а тому невірним.

Визначимо *інформаційний злочин* як навмисні дії, спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які вчиняються з корисливих, політичних або хуліганських мотивів.

Таким чином, нормативні визначення злочинів у сфері високих технологій, а звідси високотехнологічної злочинності відсутні. Утім, подібні терміни мають багатоаспектне застосування, що призвело, з одного боку, до розширення їхнього тлумачення, а з іншого – до не виправданого звуження цієї сфери виключно до комп'ютерних злочинів.

5. Злочинність у сфері високих технологій

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

Злочинність існує у суспільстві відносно самостійно, утім зі своїми закономірностями, кількісними та якісними характеристиками, що не властиві її окремим елементам. і 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 вчинюються з використанням інформаційних технологій, сьогодні іменують по різному – «комп'ютерна злочинність», «кіберзлочинність» [224], «злочинність у сфері високих технологій», «е – злочини» і т.ін. І дійсно, адже з'явилися такі нові форми Інтернет-злочинності як катінг, 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 зазіхань, а також злочинів, які здійснюються за допомогою комп'ютерних засобів [105, с. 673].

Сьогодні 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 обумовлює недостатню науково-теоретичну розробленість інформаційно-правової проблематики, чинної законодавчої бази, та призводить до складностей у практичній діяльності правоохоронних органів.

Високотехнологічна злочинність як системна сукупність двох груп злочинів: 1) у сфері високих технологій та 2) вчинених з використанням високих технологій, може приймати істотно нові властивості та містити специфічні характеристики, оскільки заподіює особливо загрозливі негативні для суспільства та людей наслідки, чого раніше з об'єктивних причин не було.

Звідси потрібно визнати, що людство ще залишається фактично не готовим до стрімкого оновлення злочинності і тому необхідно модернізувати існуючі державні, соціальні та технологічні заходи контролю.

Сьогодні у різних країнах ці питання вирішуються по-різному.

Зокрема, створений у МВС України підрозділ по боротьбі зі злочинами у сфері високих технологій, але єдиними напрямком якого залишається протидія злочинним проявам у переважній більшості у сфері комп'ютерних технологій.

6. Інформаційна та міжнародна злочинність

Стійке функціонування інформаційної інфраструктури, забезпечення інтересів особи, суспільства і держави у цій сфері перетворюється 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 регування на нову кримінальну ситуацію проводяться наукові дослідження та з'являються певні практичні розробки [36; 57; 93; 119; 135; 138; 243].

Термін інформаційна злочинність ще не є загальноприйнятим [40]. Ряд авторів 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 проявляє себе в інформаційній сфері, де інформаційний зв'язок виступає стосовно злочинності як її істотна детерміністська ознака [40, с. 93-96].

Пропонуємо визначати *інформаційну злочинність* як протиправні дії в інформаційній сфері, що порушують установлені законом права особистості, організації або держави, що заподіюють останнім моральну шкоду або матеріальний збиток. Істотною ознакою є те, що *інформаційна злочинність* носить організований і міжнародний (транснаціональний) характер, базується на стрімкому розвитку й використанні телекомунікаційних засобів повідомлень.

Має здійснитися якісний перехід від існуючої системи протидії інформаційній злочинності до нової, більш сучасної, що потребує переосмислення накопиченого досвіду для визначення концепції, загального підходу до зазначеної 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 небезпеку сучасності подає відносно новий вид терористичної діяльності – інформаційний тероризм, розгортання якого обумовлено широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства, що вимагає розробки комплексної системи протидії «інформаційному тероризму» правовими та організаційно-технічними заходами з боку правоохоронних органів з відповідною науковою новизною.

Основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупованнями або окремими особами.

Наслідком такої атаки є проникнення до інформаційно-телекомунікаційної системи, перехоплення управління, пригнічення засобів мережевого інформаційного обміну та здійснення інших деструктивних дій.

Міжнародну злочинність як особливий вид злочинності називають по-різному, найчастіше як злочинність міжнародного характеру або транснаціональна злочинність [37], утім від цього її зміст не змінюється, оскільки міжнародна злочинність являє собою сукупність всіх злочинних діянь, що вчинені в певний період на території більш, ніж однієї держави.

У теорії склався загальноновизнаний розподіл злочинів, що зачіпають інтереси держав і всього міжнародного співтовариства, на декілька груп.

У цьому зв'язку сучасними дослідниками пропонуються 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, яка заснована на праві й 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.

У першому десятилітті ХХІ ст. перед суспільством виникли нові виклики у вигляді не тільки суттєвого зростання злочинності, але й появи таких нових ознак як структуризація, спеціалізація, професіоналізація й інтелектуалізація злочинності. Тобто інформаційна злочинність як соціально-правовий феномен залучив собі на службу досягнення у сфері високих технологій.

7. Проблеми інтелектуалізації високотехнологічної злочинності

Обережно висловлюючись щодо прогнозів розвитку злочинності в Україні на найближчі роки, потрібно визнати основні тенденції як вкрай несприятливі. Головним є те, що характерною прикметою нинішнього дня стала *інтелектуалізація злочинності* [216]. У цілому, ми бачимо, що інтелектуалізація злочинності як відносно новий соціально-правовий феномен постає складною і багатогранною проблемою, що умовно можна відобразити таким чином:

$$\frac{[M + I]c}{I \xleftrightarrow{2} HTc} \uparrow Nc, \text{ де } M - \text{ міжнародна}$$

злочинність, I – інформаційна злочинність, I^2 – інтелектуалізація злочинності, HTc – злочинність у сфері високих технологій, Nc – нанозлочинність. Щодо обґрунтування використання останнього терміну для позначення нового феномену далі ще буде звернено увагу.

Більш того, в Україні варто 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. Слід передбачати також збільшення обсягів залучення до злочинної діяльності наукових співробітників, колишніх офіцерів збройних сил і правоохоронних органів, кваліфікованих юристів. Тобто зросте інтелектуалізація злочинності, за рахунок її озброєння останніми досягненнями високих технологій, у тому числі й військових нанотехнологій [32].

Злочинність терористичної спрямованості можна визначити як сукупність злочинів терористичної спрямованості або тероризм у широкому змісті слова [105, с. 640]. У рамках предмета нашого дослідження поняття «терор» розглядається як метод політичної боротьби й протиставляється всім неекстремістським та іншим насильницьким методам зовнішньополітичної боротьби [135]. При цьому варто помітити, що нерідко такі поняття як «тероризм», «терор», «терористична діяльність» і «терористичний акт», ототожнюються. Ст. 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 самоврядування, 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 прийнято. Характерною ознакою тероризму є його відкритість, коли про мету заподіяння шкоди чи погрози, про вимоги широко розголошується.

Сучасні високоінтелектуальні інформаційні мережі є середовищем для здійснення терористичних планів, розгортання кібертероризму взагалі, що складає реальну загрозу не тільки національній безпеці окремих країн, але 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 було намагання адаптуватися до складної ситуації, змінити форми антикримінального впливу відповідно до нових завдань і нових викликів.

Сучасний стан розвитку інформаційного суспільства та достатньо великий рівень 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 розробка заходів протидії злочинним проявам у глобальній мережі тільки на національному рівні залишається малоефективною. У зв'язку з цим необхідні розробки і прийняття таких норм, що будуть пристосованими до законодавств інших держав.

8. Кримінальне право і електронне право високих технологій

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

З метою кращого розуміння проблеми співвідношення кримінального права з правом високих технологій ключовою категорією потрібно відштовхуватись від змісту та обсягу терміну «високі технології».

Як ми вище з'ясували 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 обмежуються виключно комп'ютерними, а є суттєво розширеним. Звідси буде логічним постає правове уточнення обсягу поняття «високі технології».

У свою чергу право високих технологій регулює соціальні відносини, які виникають під час розробки 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 вважати нормативно закріплені основні принципи дослідження, виробництва, організації та функціонування будь-яких передових технологій.

Тобто обсяг інформаційного права не тотожний обсягу електронного права високих технологій, оскільки останнє є правовим регулятором більш високого рівня. З цього стає зрозумілим співвідношення зазначених правових галузей як частини та цілого.

У цілому прикладів злочинів, що вчиняються із застосуванням високих технологій безліч: банківські системи безготівкових розрахунків, 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 на сторінках спеціальних видань, так і у відкритих засобах масової інформації, зазначали про це [220].

Звідси пропонуємо розділяти термін «злочини у сфері високих технологій» ($C -$) з іншим терміном «злочини, вчинені з використанням високих технологій» ($C +$), яким може бути охоплено суттєво більший спектр злочинів, що надає підстави для такої юридичної комбінації:

$$C - \xleftarrow{1} \frac{A}{HT} \xrightarrow{2} C + \frac{1}{1+2...}$$
, де A – загальна множина злочинів, HT – сфера високих технологій, $1+2 \dots$ – інші види злочинів.

До першої групи «злочини у сфері високих технологій» можуть бути включені: порушення авторського права і суміжних прав (ст. 176 КК, Розділ V), злочини проти безпеки виробництва (ст. 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 (361-363¹ КК, Розділ XIV), розробка, виробництво, придбання, зберігання, збут,

транспортування зброї масового знищення (ст. 440 КК, Розділ XX).

Друга група «злочини, вчинені з використанням високих технологій» 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 вчинення 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 на схемі:



9. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електров'язку

Сучасне інформаційне суспільство характеризується високим динамізмом розвитку інформаційних технологій, їх складністю та безмежною сферою використання. Це обумовлює 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.

Злочини у сфері комп'ютерної інформації – це кримінально каране діяння, предметом посягання якого є комп'ютерна інформація.

Стисло охарактеризуємо злочини, що посягають на відносини у сфері обробки інформації в ЕОМ, автоматизованих системах, комп'ютерних мережах і мережах електров'язку, права власності фізичних та юридичних осіб на інформацію і доступу до неї.

Виходячи зі змісту кримінально-правової характеристики злочинів у сфері інформаційних комп'ютерних технологій, комп'ютер та його програмне забезпечення може бути як предметом злочину, так і засобом, за допомогою якого реалізується задум злочинця [25, с. 5]. Повідомлення електров'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 23.12.2004 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 обробкою інформації в ЕОМ, автоматизованих системах, комп'ютерних

мережах чи мережах електрозв'язку, є: 1) власники інформації чи уповноважені ними особи; 2) власники технічних засобів автоматизованої обробки чи уповноважені ними особи; 3) користувачі інформації; 4) користувачі технічних засобів автоматизованої обробки.

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

Додатковими обов'язковими об'єктами вказаних злочинів є відносини власності на інформацію, яка обробляється 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.

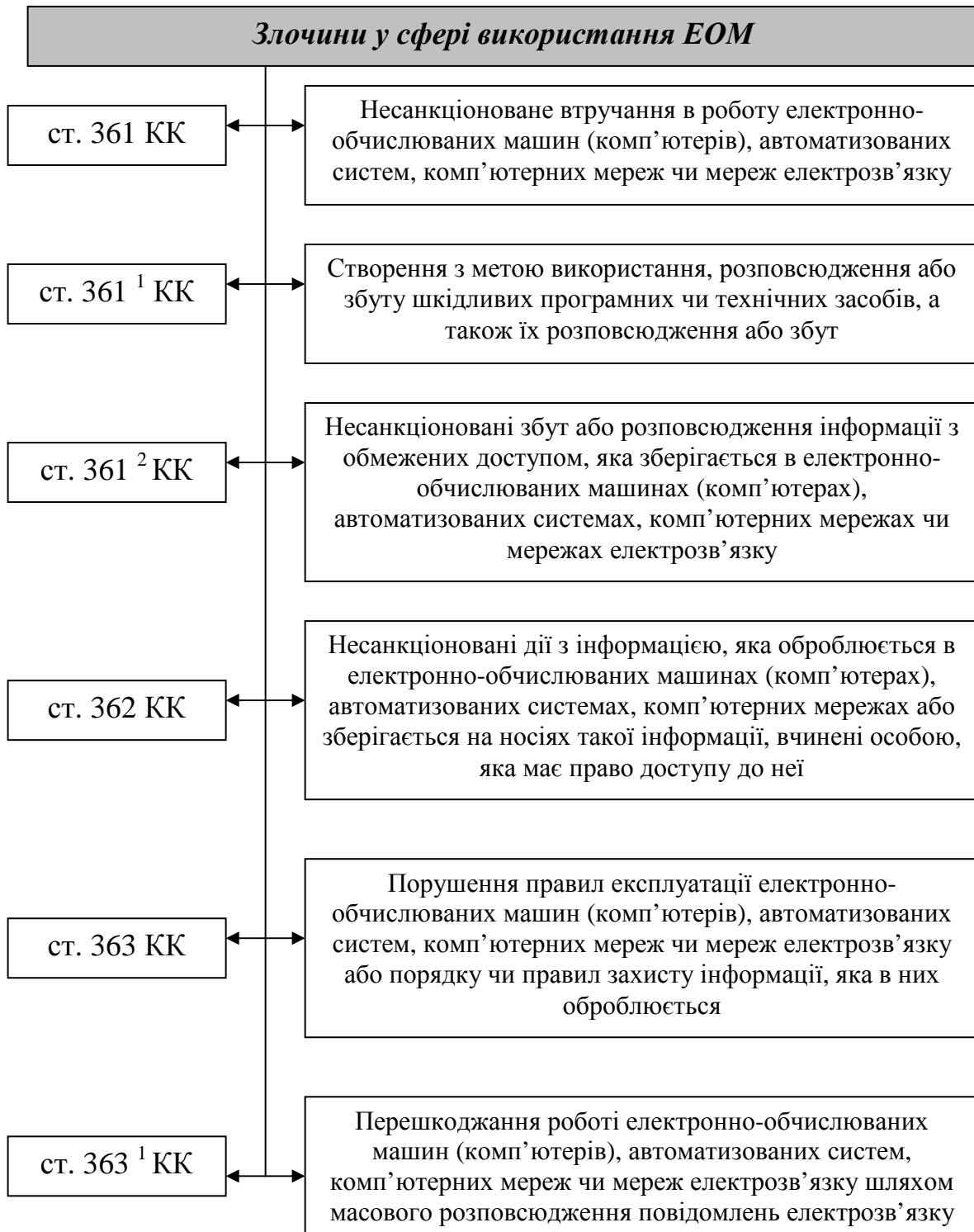
Предметом комп'ютерних злочинів є: 1) інформація, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами зв'язку; 2) технічні засоби автоматизованої обробки та захисту інформації (елементи електронно-обчислювальних 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 тощо), 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 у 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; б) умисному масовому розповсюдженні повідомлень електрозв'язку, що здійснене без попередньої згоди адресатів [88].

Характерною особливістю усіх розглянутих посягань є те, що всі вони вчиняються шляхом активних дій. Порушення 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 може вчинятися шляхом бездіяльності.

У сфері використання ЕОМ в діючому КК України існує шість складів злочинів [104], що може бути схематично представлено на схемі:



Суб'єктом злочинів, передбачених статтями 361-363¹ 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 обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку або до

технічних засобів її автоматизованої обробки (ст. 361); 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); 3) неслужбова особа, яка відноситься 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 визначені для здійснення функцій управління та обслуговування ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363).

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 дотримуватись встановлених правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також порядку та правила 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 оціночною ознакою і потребує вирішення у кожному конкретному випадку з урахуванням всіх обставин справи та розміру матеріальних збитків. Значною шкодою у статтях 361-363¹ КК України, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

10. Специфічні риси злочинів у сфері нанотехнологій і прогнози розвитку нанозлочинності

З одного боку, вже не викликає сумнівів, що нанотехнологічне суспільство є новим виміром соціальної реальності, де перед людиною відкриваються нові позитивні можливості, але з іншого боку – містить високий рівень загрози, що у майбутньому може створити певні проблемні ситуації, чого раніше зовсім не спостерігалось.

Одним із таких способів може стати протиправна діяльність у сфері високих технологій, і в першу чергу з використанням нанопристроїв.

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 зняттям широкого діапазону впливів на техніку й особовий склад, від вказівки на ціль для крилатих ракет до викиду токсинів.

Упродовж наступних років буде винайдено багато малогабаритних пристроїв, здатних накопичувати і передавати інформацію. У Японії і США вже створено зразки «цифрового паперу» – тонких і гнучких, немов паперовий лист, плівкових масивів наноелектронних схем [220]. Нові технології тривимірного друку дозволяють 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, безумовно не є вичерпним, утім 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 ми вище вже зазначали, до злочинів у сфері високих технологій більшість дослідників невинувато обмежено відносить виключно «комп'ютерні злочини». Тому, повертаючись до обґрунтування висловленого раніше зауваження, нарешті зазначимо, що фактично «справжніми» високотехнологічними злочинами потрібно розуміти сукупність інтелектуальних злочинів, які вчиняються з використанням нанотехнологій. Звідси стає зрозумілим необхідність розробки кримінально-правових новацій і внесення відповідних змін до КК України.

Нагадаємо, що злочинність є не тільки особливим соціально-правовим явищем, але й сукупністю злочинів. Фактично з часом можуть з'явитися підстави щодо введення терміну «нанозлочинність». Тому для з'ясування її спочатку пропонуємо завчасно знайти правове визначення цих злочинів.

Вважаємо, що злочини у сфері нанотехнологій потрібно розуміти у вузькому та широкому змісті. Так, пропонується такі дві дефініції:

1) *злочини у сфері нанотехнологій у широкому розумінні* – це окремі види злочинів, що вчиняються з використанням нанотехнологічних засобів, методів та пристроїв.

2) *злочини у сфері нанотехнологій у вузькому розумінні* – 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, у 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, які передбачені діючим КК України, що вчиняються з використанням нанотехнологічних засобів, методів та пристроїв; 2) діяльність, що спрямована на свідоме порушення та перебудову молекулярної структури наноматеріалів та інших об'єктів з метою досягнення протиправних намірів; 3) інші види злочинів, в тому числі терористичної спрямованості.

Зрозуміло, що такі протиправні наміри, можливо, буде досить складно довести. Звідси ця системна проблема потребує додаткового вирішення в організаційно-процесуальній та криміналістичній площині. Отже, як бачимо, нанозлочинність як новий негативний соціотехнічно-правовий феномен несе надвисокий рівень суспільної загрози.

Розглянутий матеріал дозволяє спрогнозувати подальше зростання інформаційної злочинності та появу її нових підвидів як в Україні, так і за рубежом, що диктує необхідність розробки невідкладних заходів щодо її попередження у сфері використання нових інтелектуальних технологій, де найбільше помітно наше технологічне відставання від злочинного середовища.

КЛЮЧОВІ СЛОВА: *Правоохоронні органи, кримінально-правова політика, інформаційні правопорушення, комп'ютерні злочини, інформаційна злочинність.*

ЛЕКЦІЯ 6. ЕЛЕКТРОННЕ ПРАВО ВИСОКИХ ТЕХНОЛОГІЙ І КРИМІНАЛІСТИЧНА МОДЕРНІЗАЦІЯ

© Синьокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синьокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. Методи інформаційної безпеки та електронні системи захисту інформації.
2. Інформаційна надійність оптоволоконних телекомунікацій та проблеми правової регуляції.
3. Методологія, принципи та функції Інтернет-моніторингу.
4. Мета та завдання правового моніторингу цифрових інформаційних мереж.
5. Криміналістична інформатика та високі технології.
6. Проблеми досудового слідства у сфері високих технологій та криміналістична модернізація.
7. Електронні види інформаційних та експертно-криміналістичних систем.
8. Характеристика інформаційних та експертно-криміналістичних систем.
9. Автоматизоване робоче місце слідчого.
10. Проект «Оптико-електронний кабінет криміналістики».

1. Методи інформаційної безпеки та електронні системи захисту інформації

Політика інформаційної безпеки означає сукупність документованих правил, процедур, організаційно-правових засобів, практичних прийомів або керівних принципів у сфері безпеки інформації.

Розглядаючи інформацію як товар, потрібно визнати, що інформаційна безпека у цілому може призвести до значної економії коштів, в той же час як збитки, що нанесені завдяки недосконалій побудові інформаційної безпеки, завдати матеріальних витрат.

У цьому зв'язку особливого значення набуває вирішення проблеми електронних війн як цілеспрямованих дій з метою досягнення інформаційно-технологічної переваги шляхом нанесення збитків інформації, інформаційним процесам та електронним інформаційним системам супротивника при одночасному захисту власних інформаційних ресурсів, що зберігаються на електронних носіях,

інформаційно-технологічних процесів та інформаційних систем.

Безпека даних автоматизованої системи включає властивість організації доступу до даних, що забезпечує їх захист від несанкціонованого використання, навмисного чи ненавмисного спотворення або руйнування.

Оскільки інформаційна безпека – це стан захищеності інформаційного середовища, зміст поняття «інформаційна безпека» розуміється як стан захищеності життєво важливих інтересів людини, суспільства і держави. При цьому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Захист інформації можна визначити як діяльність, яка спрямована на запобігання

втрати та витоків охоронюваної інформації від несанкціонованих впливів. Звідси захист інформації є процесом, який спрямовується на досягнення стану інформаційної безпеки.

Таким чином, захищеність інформації та підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, і складає зміст інформаційної безпеки.

Наведемо інші важливі дефініції:

Безпека інформації – стан захищеності інформації, при якому забезпечується конфіденційність, доступність та цілісність даних.

Безпека мережі – організаційно-технічні заходи, які забезпечують захист локальної обчислюваної мережі від несанкціонованого втручання в її роботу чи спроб порушення нормальної роботи її елементів.

Блокування інформації – 1) дії, наслідком яких є припинення доступу до інформації; 2) унеможливлення санкціонованого доступу до інформації.

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.

Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Знищення інформації в системі – дії, внаслідок яких інформація в системі зникає.

Електронні засоби захисту – програмно-технічні засоби, які забезпечують захист електронних документів від несанкціонованого доступу на етапі передавання цих документів електронною поштою.

Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Криптографічний захист інформації – вид захисту інформації, що реалізується

шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування / відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.

Шкідлива програма – створена або існуюча програма зі спеціально внесеними змінами, яка завідомо призводить до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи електронно-обчислюваної машини (ЕОМ), системи ЕОМ або їх мережі.

Поняття «захист інформації» закріплено у Законі України «Про захист інформації в автоматизованих системах» як «сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння 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. Усі закони з зазначеною назвою забезпечують захист персональних даних. Для комплексного захисту даних на міжнародному рівні використовується термін «забезпечення безпеки даних», тобто в даному випадку мова йде про інформаційну безпеку.

Для виключення термінологічної плутанини поняття «захист даних» варто тлумачити лише у тому змісті, що встановлений статтею 1 Конвенції № 108 Ради Європи по захисту осіб у зв'язку з автоматизованою обробкою персональних даних (м. Страсбург, 28.01.81 р.) [94]. Конвенція № 108 зобов'язала країн-учасниць здійснити коригування національних законодавств в частині втілення встановлених

нею основних принципів захисту персональних даних.

Сьогодні критична маса науково-практичних знань щодо розвитку суспільних інформаційних відносин дає змогу сформулювати 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 їхніх ресурсів. У той час як інформаційна безпека – це стан захищеності інформаційного середовища, захист інформації уявляє собою діяльність щодо запобігання витоку інформації, що захищається, попередження несанкціонованих та ненавмисних впливів на інформацію, що захищається, тобто є процесом, який спрямований на досягнення стану цього стану. Також існують інші визначення [57; 93; 171]. Зокрема, як діяльність, що 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 ст. 50 Конституції України: кожному гарантується право вільного доступу до інформації про стан довкілля, про 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 яких передбачений законодавством України, які визнані такими відповідно до встановлених юридичних процедур і право на обмеження доступу до яких надано власнику таких відомостей.

Отже, прийемо запропоноване визначення захисту інформації з обмеженим доступом як сукупність організаційно-правових, інженерно-технічних та криптографічних заходів, які вживаються власником інформації з обмеженим доступом

або іншими особами за його замовленням, з метою запобігання заподіяння 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 низка розробок [122]. Так, потрібно мати на увазі, що застосування заходів вилучення інформації з каналів зв'язку, контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією, відповідно до чинного законодавства, здійснюється виключно з метою запобігання тяжкому чи особливо тяжкому злочині 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 [178, 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 як на захист безпосередньо комп'ютерної інформації, так і на захист її носіїв. Дослідники свого часу указували про те, що файлова система повинна забезпечувати захист файлів від несанкціонованого доступу [14, с. 1].

Виділяють наступні 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 вказаних напрямів існує достатня кількість якісних, розроблених

професіональними організаціями програмних продуктів, представлених на інформаційному ринку.

Так, в РФ згідно Положення про методи й способи захисту інформації в інформаційних системах персональних даних [158], що вступило в дію з березня 2010 р. до методів і способів захисту інформації в інформаційних системах ставляться: 1) методи й способи захисту інформації, оброблюваної технічними коштами інформаційної системи, від несанкціонованого, у тому числі, випадкового, доступу до персональним даних, результатом якого може стати знищення, зміна, блокування, копіювання, поширення персональних даних, а також інших несанкціонованих дій; 2) методи й способи захисту мовної інформації, а також інформації, представленої у вигляді інформативних електричних сигналів, фізичних полів, від несанкціонованого доступу до персональним даних, результатом якого може стати копіювання, поширення персональних даних, а також інших несанкціонованих дій.

Зазначене Положення регламентує методи й способи забезпечення безпеки персональних даних; використовувані засоби захисту інформації, застосовувані в інформаційних системах; класифікації інформаційних систем; обробки персональних даних і необхідних заходів для забезпечення безпеки й конфіденційності їхнього використання, а також проведення контрольних тематичних досліджень на відповідність нормам безпеки при роботі з персональними даними.

Безпека персональних даних досягається шляхом виключення несанкціонованого, у тому числі випадкового, доступу до персональним даних, результатом якого може стати знищення, зміна, блокування, копіювання, поширення персональних даних, а також інших несанкціонованих дій [258].

Для забезпечення безпеки персональних даних при міжмережевій взаємодії окремих інформаційних систем через інформаційно-телекомунікаційну мережу міжнародного інформаційного обміну (мережа зв'язку загального користування)

додатково застосовуються наступні основні методи й способи захисту інформації від несанкціонованого доступу: 1) створення довіреного каналу між взаємодіючими інформаційними системами через інформаційно-телекомунікаційну мережу міжнародного інформаційного обміну (мережа зв'язку загального користування); 2) здійснення аутентифікації взаємодіючих інформаційних систем і перевірка дійсності користувачів і цілісності переданих даних (п. 2.8 Положення).

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).

Визначимо основні внутрішні загрози щодо модернізації процесів та технологій інформатизації правоохоронних органів: 1) порушення встановленого регламенту збору, обробки, зберігання і передавання інформації, що міститься в картотеках і автоматизованих банках даних і, що використовується для розслідування злочинів; 2) недостатність законодавчого та нормативного регулювання інформаційного обміну в правоохоронній і судовій сферах; 3) відсутність єдиної методології збору, обробки та зберігання оперативно-розшукової, довідкової, криміналістичної та статистичної інформації; 4) відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах; 5) навмисні 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, у 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 системи або конструкції забезпечити необхідні інформаційні ресурси для підтримки їхнього стійкого функціонування в будь-яких складних умовах існування й розвитку. Крім цього, до поняття інформаційної безпеки слід віднести здатність зазначених суб'єктів ефективно протидіяти відносно загроз інформаційних ресурсів, технічних систем і джерел передачі та обміну інформації.

2. Інформаційна надійність оптоволоконних телекомунікацій та проблеми правової регуляції

Ми бачимо, що оптоволоконний зв'язок знаходить усе більше широке застосування у всіх областях – від комп'ютерів і бортових авіакосмічних та корабельних систем, до систем передачі інформації на значні відстані, в тому числі в правоохоронній діяльності.

Організація захисту комп'ютерних інформаційних систем та волоконно-оптичних мереж визначає порядок і схему функціонування основних їхніх підсистем,

використання пристроїв та ресурсів, взаємовідносини користувачів між собою 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 витік інформації найчастіше зумовлені зловмисними діями, недбалістю користувачів або персоналу. Ці фактори 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, мають за мету виключити, зменшити або повністю усунути збитки при дії різноманітних деструктивних факторів.

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

$$A \geq \frac{Bt}{Bl} \geq C, \text{ в якій } A - \text{ інформаційна безпека,}$$

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 не можливе 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, Закон України «Про основи національної безпеки України», Закони 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 [46; 67-72].

Питання захисту інформації в інформаційно-телекомунікаційних системах окрім Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та інших законів регулюються також низкою підзаконних нормативно-правових актів [163-167].

Постановою КМУ від 13 березня 2002 р. № 281 уповноважив Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 р. 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 обумовлюються розробки заходів, що адекватні 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. Головними такими вимоги згідно норм міжнародних стандартів є: 1) заборона на об'єднання веб-сайту персональних даних з веб-сайтами будь-яких інших даних загального інформаційного

змісту без письмової згоди власника персональних даних; 2) заборона обробки 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 додаткову обробку персональних даних, що необхідна 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 й органах місцевого самоврядування, організаціях, установах і підприємствах усіх форм власності [211, с. 438-439].

З метою оцінки 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 в 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 передачі лініями зв'язку в локальних і глобальних мережах; 5) забезпечувати режим спеціально захищеної електронної пошти для обміну секретною інформацією з високою швидкістю і достовірністю передачі 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 може бути визначено 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 в 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, повинен забезпечуватися захист цієї інформації відповідно до законодавства. У цьому аспекті варто згадати позитивний досвід найпотужнішого в Україні пошукового правового серверу LIGA ONLINE [121-122].

Світові темпи розвитку волоконно-оптичних систем передачі інформації набагато випереджають темпи розвитку систем обробки й зберігання інформації. Експериментальним шляхом підтверджено

підвищення контрасту зображення пристроями більш ніж у два рази в порівнянні із прототипом при масштабуванні малококонтрастних зображень, що особливо істотно для криміналістики. Це розширює межі застосування вже відомих дактилоскопічних і спектрометричних систем, нічних телевізійних камер, створює передумови для побудови на їхній основі детекторів брехні, дозволить підвищити надійність використання кредитних карток і т.п.

Прогрес у різних галузях науки і техніки сприяв створенню компактних та високоефективних ВОЛЗ, за допомогою яких можна легко підключатись до ліній телекомунікацій, та різноманітних технічних засобів обробки інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу 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 витоку 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».

Неможна залишати поза увагою такі важливі напрямки 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 оптоволоконної передачі інформації потребує додаткового організаційно-правового регулювання. У відповідності 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 відкриває новий технологічний коридор передачі інформації у цій сфері.

3. 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 визначеними 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 їх системному адміністраторові. 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 систематичний або безперервний збір інформації про параметри складного об'єкта або дії.

З методологічної точки зору моніторинг інформаційних програм можна розглядати як процедуру щодо оцінки, метою чого є виявлення та (або) фіксація ефектів триваючих загрозливих дій без з'ясування причин. Такий вид моніторингу виступає як внутрішня процедура, що заснована на індикаторах та результатах, а також як інструмент збору інформації й звітності й спрямована на збір інформації про основні ресурси й продукти інформаційної програми.

Особливою рисою моніторингу такого виду як інформаційного процесу є систематичність збору та обробки 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 оцінка та прогноз стану соціального сприйняття у визначений період часу, тобто оприлюднення результатів втручання і правового реагування щодо виявлених порушень закону в інформаційній сфері. Тобто, перш за все, починати таке дослідження потрібно з статистичного спостереження, а саме – зі збирання інформації.

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

Система інформаційно-правового спостереження в Інтернет-просторі ще не дістала ґрунтовного впровадження в практичну діяльність, тому сьогодні фактично виступає інноваційним проектом. Звідси фактично 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 принципах кількох вирішальних припущень, що покладені в основу будь-якої системи відстеження й контролю [200].

Необхідно відзначити, що, до якої би галузі права не було віднесене порушення прав особистості в Інтернеті, організація своєчасного реагування є однією з найбільш ефективних форм їхнього правового захисту. Разом із тим можливість анонімної присутності в Мережі часто дозволяє сховати справжні імена авторів, джерел та осіб, що розмістили незаконну інформацію або вчинили інші правопорушення в Інтернеті, що

представляє певну складність при вирішенні питань про притягнення до відповідальності.

Отже, моніторинг мережі – це інформаційна система (процес) спостережень, яка є процесом збору, обробки, збереження та аналізу інформації про поточний стан мережі без втручання в її функціонування і складається зі збору, обробки та аналізу інформації про стан об'єкту.

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.

4. Мета та завдання правового моніторингу цифрових інформаційних мереж

Процес спостереження, збору 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, які ведуть боротьбу зі злочинністю, та запобігання реалізації цих загроз.

Важливим етапом модернізації і необхідною умовою освоєння нових технологічних коридорів передачі 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, що подібні заходи сприятимуть підвищенню результативності протидії транснаціональним злочинам і особливо тих, що вчиняються з використанням високих технологій [203-205].

Отже, потрібно погодитись з авторами, які проголошують необхідність вирішення проблеми створення загальнодержавної інформаційної інфраструктури, відповідних організаційних структур, що формуватимуть систему збереження, опрацювання та

поширення інформації, відповідатимуть за розробку, 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 техніко-технологічними 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 й територіальну локалізацію, і характер загроз.

З метою спостереження за тенденціями розвитку інформаційної злочинності, орієнтування в причинах та умовах, що сприяють вчиненню 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 якісної обробки інформації та прийняття рішень [119, с. 29-35].

Для ефективної протидії правопорушенням у сфері інформаційних технологій взаємодія правоохоронних органів має ґрунтуватися на розробці 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 Інтернет; 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) вести інформаційно-психологічний вплив через засоби масової інформації з метою боротьби з організованою злочинністю та упередження негативного впливу кримінальних структур на суспільну свідомість тощо.

З метою відстеження протиправних проявів в Інтернеті, що уявляють підвищену суспільну небезпеку, найбільш результативним може стати новий напрямок «антикримінальне інтернет-патрулювання», що буде діяти на випередження [186; 191; 200].

Важлива своєчасність і, головне, адресність доведення результатів правового інтернет-моніторингу. Порушення законів повинні бути структуровані в підгрупи (система індикаторів), які відображають стан законності в окремих галузях права, а потім, використовуючи традиційні аналітичні схеми, варто групувати їх за сферами життєдіяльності – внутрішньополітична, соціальна, економічна, екологічна, оборонна тощо, а відтак, вибудовувати їх за ступенем небезпеки національним інтересам України, показувати прями й опосередковані їхні взаємозв'язки, визначати «критичні маси» таких показників. Його результати необхідно використати для інформування відповідних правоохоронних структур про стан інформаційної загрози і рівень захищеності національних інтересів, можливе загострення й появу нових загроз національним інтересам, для підготовки пропозицій по вдосконаленню 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 даних – відеозображень, графіків і діаграм, текстової документації в електронному виді тощо. Досвід роботи подібних центрів, а також аналіз закордонних і вітчизняних досягнень у цій сфері свідчить,

що їх створення істотно підвищує якість і оперативність обробки правової інформації.

Враховуючи це, антикримінальний моніторинг є інноваційним процесом у галузі забезпечення законності процесу кримінального переслідування як інформаційної системи спостереження, аналізу статистичної інформації про стан законності, оцінки різномірних мікро- і макросоціальних факторів і прогнозу розвитку інформаційної злочинності.

Таким чином, зростанню ефективності антикримінальної діяльності в Інтернет-просторі може сприяти інноваційний проект правового моніторингу цифрової інформаційної мережі.

5. Криміналістична інформатика та високі технології

Ідея нової інформаційної технології полягає у розгляді системи понять предметної галузі і відповідності між нею та системою формальної моделі як похідної інформації для розв'язання прикладного завдання.

Стрімкий розвиток нових технологій в криміналістичній практиці детерміновано потребами у швидкій переробці величезних масивів криміналістично-значимої інформації [92]. Від традиційної криміналістичної науки криміналістична інформатика відрізняється також характером своїх міждисциплінарних зв'язків та функціями. В рамках цієї наукової теорії розробляються загальні методологічні основи математизації та 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].

Відомо, що 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

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 оцінки 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 обумовлено такими чинниками: 1) зміст заходів та умови їх проведення (об'єкт пошуку – інформація, яка обробляється 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, що є зрозумілою для прийняття слідчим та судом.

Для фіксації факту користування певною особою вищезазначеним обладнанням необхідно створити ситуацію, яка б однозначно свідчила про винність конкретної особи (комбінація, затримання «на гарячому», відеофіксація, дактилоскопія тощо).

Як слушно визначається дослідниками цієї проблематики, багато правопорушень здійснюється вже на рівні надання доменних імен [43, с. 98-101]. Водночас, потрібно погодитися із затвердженням окремих експертів у тім, що довести подібні злочини практично неможливо, оскільки, виготовлена порнопродукція, як правило, зберігається на цифрових носіях, які якщо буде потреба ліквідується 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 інформація. 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.

Отже, спробуємо нижче схематично представити модернізацію технологічних коридорів передачі інформації у сфері боротьби зі злочинністю:



6. Проблеми досудового слідства у сфері високих технологій та криміналістична модернізація

Особливості розслідування злочинів у сфері мобільних телекомунікацій привертає 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 розглядаються російськими дослідниками [90]. Потрібно зазначити, що в ч. 4 ст. 303 КПК України (згідно зі змінами, внесеними у 2000 р.) також закріплена можливість проведення дистанційного допиту (тобто допиту з віддаленою присутністю допитуваної особи). Але КПК України не регламентуються 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. Лебедев, 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, проведення експертиз тощо.

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, виготовляються автентичні копії процесуальних документів [182, с. 191].

Доказова інформація у справах за злочинами 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 й комп'ютерного програмного забезпечення.

Специфіка виявлення та проведення слідчих дій в Інтернет-просторі вимагає розробки 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 збору в електронній формі доказів по комп'ютерним злочинам, 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'язані з визначеною передачею інформації через комп'ютерні системи; 4) перехоплення даних змісту інформації; 5) збирання за допомогою технічних засобів або запис даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі 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 має 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 фахівців.

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'язковим є вилучення програмно-технічних засобів, які використовувались під час вчинення 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 у 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 повідомлення, 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) науково правомірне, 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 очевидна. 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 будуть постійно виникати 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, які вчинені у сфері нових інформаційних технологій, є модернізація системи статистичного обліку, аналізу та оцінки криміналістичної інформації у сфері нових технологій.

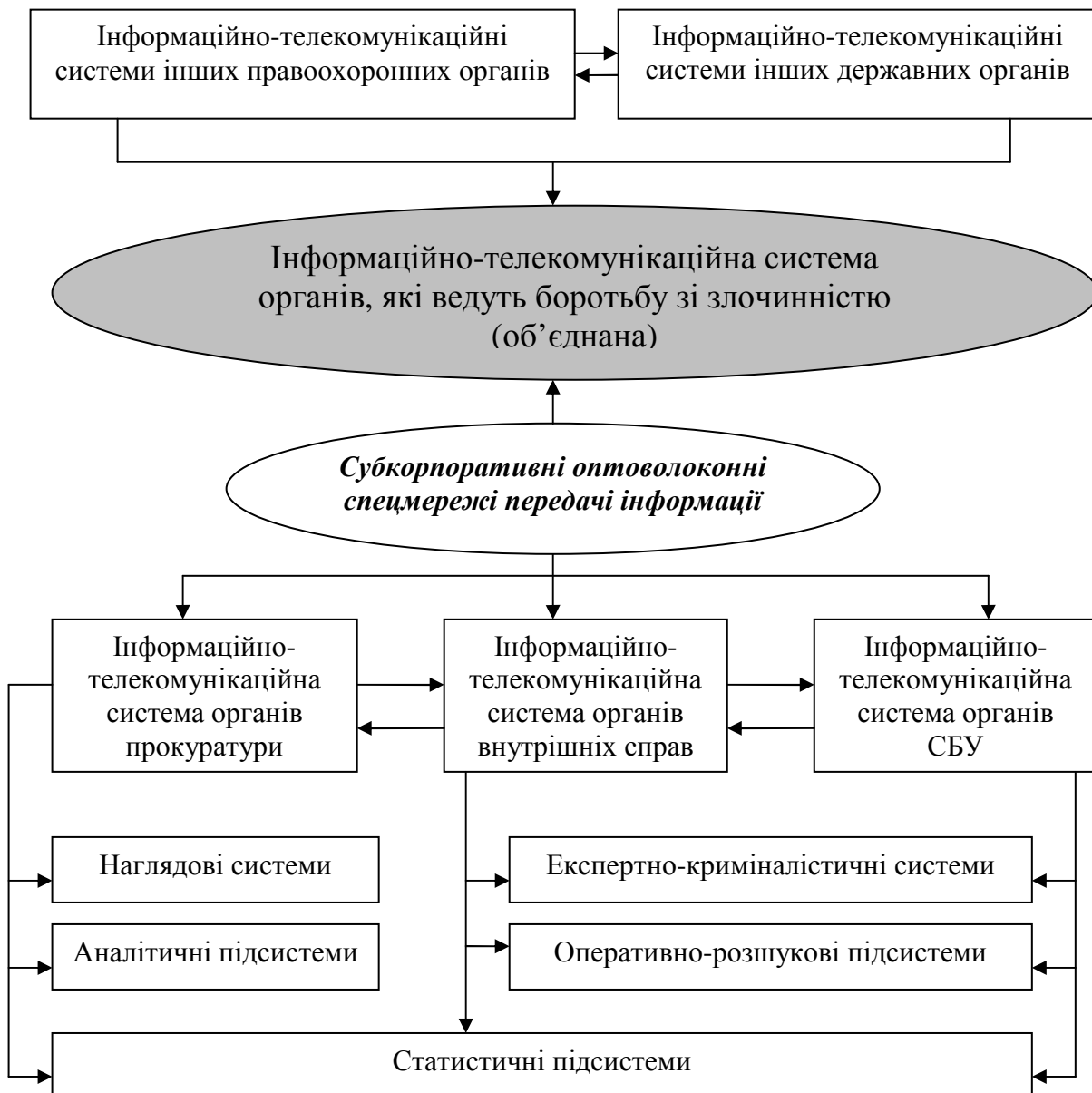
Отже, одним з напрямів щодо вирішення проблеми криміналістичної модернізації є створення інтегрованої інформаційно-аналітичної системи правоохоронних органів, яка передбачена Концепцією національної програми інформатизації України [70] та впроваджується в ОВС України [130; 174].

Технічний аспект пов'язаний, перш за все, з вивченням проблем надійності, швидкості та точності передачі інформації, з методами, технічними засобами побудови

каналів передачі сигналів тощо [100, с. 144-147; 101, с. 70-77].

Потрібно розробити науково обгрунтовані методики програмного забезпечення аналізу оперативної інформації, отриманої оперативно-технічними засобами для моделювання ситуацій, які складаються при проведенні оперативно-розшукових заходів [52; 232].

Модернізаційний проект створення цифрової телекомунікаційної мережі органів, які ведуть боротьбу зі злочинністю, представлений нижче на схемі:



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 варто забувати, що інформаційні системи правоохоронних органів теж можуть піддаватися атакам

хакерів. Тому постійно слід вести кропітку роботу щодо технічного та криптографічного захисту інформаційної інфраструктури [128].

Отже, пріоритетним напрямком криміналістичної модернізації є науково-технічна розробка та впровадження в досудовий кримінальний процес інноваційних проектів експертно-пошукових систем. Особливу актуальність це набуває у сфері розслідування злочинів у сфері високих технологій. Пропонуємо *антикримінальні інформаційні технології* визначити як сукупність криміналістичних, кримінологічних, кримінально-правових та кримінально-процесуальних знань й 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. Тому викладені пропозиції пропонується використати під час розробки проекту Закону України «Про інформаційно-телекомунікаційну систему правоохоронних органів».

7. Електронні види інформаційних та експертно-криміналістичних систем

Поняття *«автоматизована інформаційна система»* означає організаційно-технічну систему, що реалізована на базі обчислюваної техніки та інших організаційно-технічних засобів, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

В інформаційних технологіях зазначений термін має дещо інше значення і визначається як організаційно-технічна система, що реалізує інформаційну технологію виконання встановлених функцій за допомогою персоналу і комплексу засобів обчислюваної техніки й зв'язку, методи й процедури, програмне забезпечення, фізичне середовище і інформацію, яка обробляється.

У системі правоохоронних органів існують інформаційні та експертно-криміналістичні системи різних видів і різного призначення.

Експертні системи (ЕС) започаткували розвиток комплексу методів і технічних прийомів використання штучного інтелекту,

що в цій галузі є одним з найсуттєвіших практичних досягнень.

Експертна система – це обчислювальна система, де зібрані 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.

Експертна система повинна мати такі головні властивості: 1) бути обмеженою певною сферою експертизи; 2) бути компетентною (рівень рішень, які вона пропонує, має бути на рівні експерта-фахівця); 3) здатність до внутрішньої оцінки, якщо дані сумнівні; 4) здатність розв'язувати реальні завдання у межах визначеної предметної галузі та надавати пояснення прийнятим рішенням; 5) факти та механізм виведення чітко розмежовані; 6) відкритість (можливість нарощування системи); 7) бути здатною переформулювати 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, у складі яких неодмінно присутні база знань та певна схема міркувань, що має назву системи (машини) логічного виведення.

Ідеальна електронна експертна система має 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. Сьогодні ЕС вже використовуються для інтерпретації даних, прогнозування подій (за наявності, як правило, неповної інформації); для діагностики; моніторингу, для планування, налагодження, ремонту, для управління та ін.

Отже, системи підтримки прийняття рішень (СППР) призначені для допомоги в отриманні ефективного способу розв'язання експертного завдання.

Інформаційні обліки в системі органів внутрішніх справ створюються для оперативного інформаційного забезпечення службової діяльності всіх підрозділів. На територіальному рівні управління в міськрайліноорганах 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 скоєння злочину, особливостями злочинної поведінки. На жаль, процедура формування похідних даних бази знань на основі стандартних карток обліку злочинів, яка широко використовується, неналежно враховує 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].

Потрібно зазначити, що інформаційні системи в органах, які ведуть боротьбу зі злочинністю, за своїм призначенням умовно можна розділити на *електронні* (автоматизовані системи фінансових підрозділів, кадрів, матеріально-технічного забезпечення, електронного документообігу

тощо) і *функціональні*, які впливають безпосередньо із завдань, покладених на практичні підрозділи.

Ця класифікація не претендує на абсолютну безумовність та повноту, тому надалі вона може бути доповнена й удосконалена. Ми будемо розглядати програми й автоматизовані комплекси, вказуючи клас програми за раніше наведеним розподілом.

8. 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 видачу 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-довідкові 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 перебування 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 23.08.2003 р. № 823/188 [78]. Щоб автоматизувати формування та обробку 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 збір, обробку та аналіз інформації, яка регламентується відповідними наказами МВС України. Автоматизований банк даних призначений 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, автотранспорт, вогнепальну зброю, документи; г) криміналістичні обліки; д) викрадені та вилучені наркотичні речовини; е) об'єкти виготовлення, переробки, зберігання та використання наркотичних речовин; ж) осіб таких категорій: особливо небезпечних рецидивістів; злочинців-«гастролерів»;

злочинців, оголошених у міждержавний розшук; організаторів і членів злочинних угруповань, кілерів; які були засуджені за злочини, пов'язані з наркотиками, торговців та розповсюджувачів наркотичних речовин з міжрегіональними та міжнародними зв'язками; схильних до вчинення злочинів, пов'язаних з посяганнями на інтереси держави; що зникли безвісти; невіданих трупів та невідомих хворих; з) банк оперативно-довідкової інформації, що містить дані алфавітного та дактилоскопічного фондів раніше засуджених осіб; і) банк статистичної інформації про стан злочинності та результати боротьби з нею; к) банк спеціальної інформації, що містить повідомлення спецпарату та іншу оперативну інформацію загальноповідомчого значення; л) банк паспортних даних громадян; м) банк з інформацією про зареєстрований автотранспорт; н) банк з інформацією про зареєстровану вогнепальну зброю; о) банки даних адміністративно-управлінського призначення; п) банки даних спеціалізованого призначення галузевих служб; р) банки даних архівів, спеціальних фондів та інші.

Повнота даних на кожному рівні за категоріями обліку визначається відповідними нормативними документами [112].

Водночас сьогодні активно використовуються телекомунікаційні технології при проведенні оперативно-розшукової діяльності. Зокрема, найбільш поширені 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, які ведуть активний спосіб життя, пересуваючись територією міста і країни. Тому вони можуть допомогти у розкритті злочинів за гарячими слідами.

Інформаційна підсистема «Розшук» призначена для централізованого збирання та обробки інформації від ініціаторів розшуку

про осіб, що розшукуються і встановлюються, які оголошені в регіональній, державній, міждержавній розшук, і надання інформації за запитами працівників органів внутрішніх справ, інших зацікавлених міністерств і відомств.

Технологія обробки інформації передбачає її тиражування каналами електронної пошти в ГУ МВС областей, щоб забезпечити доступ 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, які безвісти зникли; 2) невпізнані трупи; 3) невідомих хворих.

Документом для формування бази даних та обробки запитів є пізнавальна карта, яка надсилається з ГУ МВС в областях до МВС України. Запити на перевірку надсилаються поштою, телетайпом або каналами електронної пошти.

Міжвідомчий банк даних (МБД) «Наркобізнес» використовується для обробки, 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 нарко-бізнесом.

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 з джерел формування і подання 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 спільній співпраці підрозділу комп'ютеризації з підрозділом правового забезпечення з'явилася можливість використання мережної версії інформаційної правової бази «Експерт» для пошуку нормативно-правових актів України. Система «Експерт» є не тільки джерелом повноцінної правової інформації, а й потужним програмним інструментом аналітичної роботи. Інформаційна правова база «Експерт» постійно оновлюється в автоматизованому режимі. Бази даних, як зовнішні, так і внутрішні (відомчі), повинні бути забезпечені надійним і ефективним програмним засобом систематизації й 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 багато користувальницьких розподілених інформаційно-пошукових систем різного призначення й складності.

Інформаційно-пошукові системи, які можуть бути побудовані на основі комплексу «Портрет 4.3», мають архітектуру «клієнт-сервер» і використовують сервери баз даних, завдяки чому забезпечується зберігання й керування інформаційними масивами великого обсягу. «Портрет 4.3» надає слідчому, який може не мати спеціальної технічної кваліфікації, можливості 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].

9. Автоматизоване робоче місце слідчого

«Автоматизоване робоче місце слідчого» – це комплекс індивідуальних технічних і програмних заходів, спрямованих на автоматизацію інформаційної підтримки процесу досудового слідства у кримінальних справах. Комп'ютерна програма «Автоматизоване робоче місце слідчого» призначена 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 використовуватися слідчим як з компакт-диску, так і встановлюватися на комп'ютер слідчого для індивідуального використання. До структури АРМ слідчого входять наступні 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.

Автоматизовані робочі місця слідчого надають можливість користувачам (слідчим) працювати в діалоговому режимі, оперативно вирішувати окремі поточні завдання, викликати необхідну інформацію для обробки, 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. Таким чином, головними завданнями, для розв'язання яких мають використовуватись такі системи, є визначення можливих напрямів розслідування.

10. Проект «Оптико-електронний кабінет криміналістики»

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.

Метою технологій інтелектуального аналізу даних є побудова моделей і виявлення залежностей, прихованих в даних великого об'єму, представлених таблицями (кількість ознак порівняна з кількістю об'єктів), уражених шумами та пропусками, з ознаками, вимірними 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 закладений 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-значимі 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 сформуванню високоякісного масиву бінарної інформації, причому швидкість обробки його за алгоритмом нейронної мережі на кілька 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 покласти виконання таких завдань: 1) аналіз стану протидії організованій злочинності у сфері високих технологій та злочинності транснаціонального характеру; 2) складання стратегічних прогнозів; 3) процесуально закріпити можливість самостійно порушувати кримінальні справи та, за необхідністю, 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 злочинів, що вчиняються з використанням технологічного потенціалу.

Необхідно визначитися, за яких умов, за використання яких методів та засобів інформаційно-комунікаційні та дистанційні технології будуть ефективними при реалізації проекту «ОЕKK». Зокрема, окремі офісні програмні продукти (текстові та графічні редактори планування діяльності СОГ, програми підготовки та призначення судових експертів, 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 для подання слідчим-користувачам такої електронно-комунікаційної мережі результатів перевірки та виконання індивідуальних та групових завдань в електронній формі.

Таким чином, прокурор-криміналіст зможе дистанційно ефективно здійснювати координаційні заходи щодо практичної діяльності слідчого. Удосконалення 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 необхідно забезпечити доступ практично всіх комп'ютерів прокуратури (у тому числі районного рівня) до постійно обновлюваним криміналістично-значимим інформаційним масивам, які повинні 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].

З метою впровадження нових методів пропонуємо використовувати інноваційну модель індивідуального підвищення кваліфікації при кабінеті криміналістики, зміст якої в інтеграції двох форм навчання – стажування і семінарів, що відбуваються з виїздом до прокуратури області, й інформаційно-комунікаційними та дистанційними технологіями навчання з підсумковим автоматизованим тестуванням слідчих. Електронні методичні вказівки можуть стати корисними для обережного постійного керування самостійною роботою слідчих. Аналіз накопиченої в базі дані інформації дозволить слідчим районних прокуратур з бази даних електронного кабінету криміналістики одержувати необхідну інформацію.

Таким чином, регіональні «ОЕKK» мають стати науково-інформаційними центрами органів прокуратури.

КЛЮЧОВІ СЛОВА: Цифрові права, мультимедіа, Інтернет, моніторинг, експертно-криміналістичні системи, криміналістична модернізація.

ЛЕКЦІЯ 7. ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ

© Синьокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синьокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. Інформаційне забезпечення органів прокуратури.
2. Інфраструктура прокурорських телекомунікацій.
3. Електронний документообіг в органах прокуратури.
4. Інформаційно-аналітична підсистема «Статистика».
5. Електронна система «Нагляд».
6. АРМ «Прокурор-кримінолог-аналітик».
7. Розбудова інформаційних технологій нового покоління.
8. Основні завдання інформатизації прокурорської діяльності.
9. Концептуальні засади інформатизації органів прокуратури.
10. Стратегії розвитку інформатизації органів прокуратури України.

1. Інформаційне забезпечення органів прокуратури

У цілому, питання діяльності прокуратури в різних напрямках розглянуті 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. Кожевнікова, І. М. Козьякова, М. В. Косюти, В. В. Кулакова, М. Й. Курочки, А. М. Ларіна, Д. Р. Марочкіна, М. М. Міхеєнка, 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. Фінька та інших учених [85; 108; 134; 154; 172; 179; 199; 201; 222].

Про необхідність, доцільність і перші кроки щодо проблем формування правової інформатики в прокуратурі України свідчать окремі публікації на рівні статей М. Гаврилюка, В. Загороднього, А. Іщенка, А. Карпуся, А. Куліша, О. Черв'якової,

Є. Шевченка та інших [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, яка 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, що 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, які досліджували проблеми правоохоронних органів.

Необхідно зазначити, що, з метою поліпшення координації організаційних,

оперативно-розшукових, правових та інформаційних заходів правоохоронних органів щодо боротьби зі злочинністю, підвищення рівня роботи в цій сфері, Указом Президента України від 31.01.2006 р. № 80/2006 запроваджено створення Єдиної комп'ютерної інформаційної системи правоохоронних органів з питань боротьби зі злочинністю (далі – Єдина комп'ютерна система) [227]. Відповідно даного 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, 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 покращити 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 довгий 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 інших.

20 листопада 1996 р. затверджено Концепцію створення корпоративної інформаційної системи органів прокуратури. Зміст Концепції, а також практика її реалізації, публікації науковців і практиків можна зробити висновок, що впровадження досягнень науково-технічного прогресу у сферу інформатики в органах прокуратури України здійснювалося ситуативним чином. Концепцією не передбачається змін в організаційній структурі, перерозподіл функцій між структурами та змін в системі інформаційного забезпечення при впровадженні комп'ютерної техніки та технологій. І це цілком закономірно, адже теорія комп'ютеризації

таких питань не вирішує. За її науковою концепцією модернізації піддається 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].

Потрібно відзначити, що до цього часу ще спостерігається відставання від потреб практики наукового забезпечення інформатизації органів прокуратури.

Отже, стратегія удосконалення інформаційного забезпечення діяльності прокуратури України має базуватися на алгоритмізації інформатизації.

2. Інфраструктура прокурорських телекомунікацій

На теперішній час спостерігається тенденція до об'єднання різноманітних типів інформаційних технологій в єдиний комп'ютерно-технологічний комплекс, який носить назву інтегрованого. Особливе місце в ньому належить засобам телекомунікації, які забезпечують не тільки надзвичайно широкі технологічні можливості автоматизації управлінської діяльності, але 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 орієнтовані на технологічну взаємодію об'єктів, створених засобами передавання, обробки, нагромадження та зберігання, захисту даних, являють собою інтегровані комп'ютерні системи обробки інформації (даних) великої складності, практично необмежених експлуатаційних можливостей для реалізації управлінських процесів.

Інтегровані комп'ютерні системи обробки 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 спеціалістів в їхній професійній роботі.

Особливе значення в таких системах надається захисту інформації при її передаванні та обробці. Найбільше розповсюдження при захисті інформації одержали апаратно-програмні способи. Зокрема, використання системи зв'язку, обраної за захисними властивостями та якістю обслуговування, гарантує збереження інформації в процесі передавання та доставки її адресату; шифрування та розшифровування даних абонентами мережі загального користування здійснюється при домовленості користувачів про загальні технічні засоби, алгоритми шифрування і т.п.

За типом інтерфейсу користувача можна розглядати інформаційні технології з точки зору можливостей доступу користувача до інформаційних та обчислювальних ресурсів. Так, пакетна інформаційна технологія виключає можливість користувача впливати на обробку інформації, поки вона здійснюється в автоматичному режимі. Це пояснюється організацією обробки, 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 користувачеві 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 користувачеві засоби теледоступу до територіально розподілених інформаційних та обчислювальних ресурсів завдяки розвиненим засобам зв'язку, що робить такі інформаційні технології багатofункціональними та передбачає їхнє широке застосування.

Інформаційно-телекомунікаційна система органів прокуратури України змістовно включена в систему органів

прокуратури України. Органи прокуратури у своїй сукупності складають злагоджену трьохланкову систему [65]. Ми бачимо, що 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 вести мову про систему певних інформаційних процесів.

Інформаційно-телекомунікаційна 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 Генеральної прокуратури України 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 інформаційно-аналітичної системи правоохоронних органів вже частково використовуються новітні інформаційні технології, застосовуються оптоволоконні, провідні та радіоканали передачі 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 невластивих 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 трьохрівневої ієрархічної моделі. Управляють інформаційною мережею центральна та регіональна системи адміністрування, які підпорядковані відповідно інформаційним підрозділам прокуратури.

До цього часу в органах прокуратури України не створено єдиної волоконно-оптичної мережі зв'язку та передачі інформації з можливістю подальшого розширення. Вказана мережа охоплює основні підрозділи апарату прокуратури області і надає можливість створення єдиного інформаційного простору. 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 на сьогодні 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 Генеральної прокуратури України, що розміщені поруч.

Розвиток волоконно-оптичної інформаційної мережі прокуратури характеризується такими етапами.

Перший етап – це використання діючої комп'ютерної мережі на основі електронної пошти Генеральної прокуратури України. 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 INTRANET. 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, яка обробляється. 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 забезпечується первинне накопичення інформації, ведення територіальних банків даних, захист інформації, актуалізація інформаційних фондів та передача інформації до банків даних другого та першого рівнів.

На другому рівні формуються регіональні банки даних, обробляється інформація, забезпечується 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 забезпечується інтеграція та обробка інформації для формування банків даних інформаційних підсистем, міжвідомчий та міжрегіональний інформаційний зв'язок, керування системою інформаційного забезпечення прокуратури та дотримання стратегії її розвитку, розробка нормативно-правової бази впровадження сучасних інформаційних технологій.

Досягнення усього вищезазначеного дасть змогу органам прокуратури України сприяти становленню відкритого демократичного інформаційного суспільства, у якому державою буде гарантовано дотримання конституційних прав громадян, у тому числі щодо участі їх у суспільному житті, прийнятті рішень органами державної влади та органами місцевого самоврядування у межах і в способи, визначені законодавством.

3. Електронний документообіг в органах прокуратури

Провідним напрямом 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 розробка 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 реєстри, 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 впорядкований); 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 неповноти внаслідок відсутності єдиних вимог та умов щодо збирання інформації, що спричинює, з одного боку, одержання випадкових, недостовірних відомостей, а з іншого – надмірні витрати часу на їх опрацювання; д) диспропорційність інформації внаслідок розбіжностей у періодичності та формі отримання даних у різних ланках прокурорської системи, що не дозволяє оперативно та безпомилково зіставити інформацію, провести аналіз відповідних відомостей; є) знецінення інформації через несвоєчасну обробку, що ставить під сумнів її використання у прокурорській діяльності.

Звідси очевидно, що удосконалення прокурорської діяльності тісно пов'язане з реформуванням інформаційного забезпечення, його систематизацією, потребою забезпечення даними, які адекватно відображають процеси, що відбуваються як в самій системі (внутрішнє управління прокурорською системою), так і ззовні (зовнішні, спрямовані на реалізацію функцій прокуратури). Цим зумовлена необхідність розробки 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, які 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 відображає реальний стан справ у відповідних сферах прокурорської діяльності за визначений період; б) об'єктивність даних, які відображають достовірність стану справ; в) повнота відбиття явищ таким чином, що дає можливість визначитися щодо пріоритетних напрямів прокурорської діяльності; г) погодженість та інформаційна єдність показників, завдяки чому первинні дані не суперечать зведеним та похідним; д) можливість виконання таких функцій управлінського процесу, як облік та аналіз, прогнозування та планування, координація та контроль [238, с. 119-122].

Щодо впровадження сучасних інформаційних технологій у 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 Генеральної прокуратури України.

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, Генеральної прокуратури України, у 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 модернізацією галузевої автоматизованої інформаційної системи (ГАІС) «Скарга» в ГАІС «Звернення в прокуратуру».

Важливим аспектом техніко-технологічної структури галузевої інформаційної системи прокуратури України

має стати галузева Інтранет. 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 виникає можливість у керівників та окремих працівників з меншими затратами робочого часу, раціонально планувати та розподіляти навантаження, здійснювати оформлення різних звітів 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, вище показана 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.

4. Інформаційно-аналітична підсистема «Статистика»

Аналіз стану інформаційного забезпечення прокурорської діяльності дозволяє погодитися з висновком, що прокурору необхідно відстежувати дані понад ста форм державної статистичної звітності під час здійснення нагляду за додержанням та застосуванням закону. Проте очевидно, що з часом така інформація потребує певного перегляду та переосмислення. Очевидно, що 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.

Система показників у перелічених обліково-реєстраційних документах побудована на кримінально-правовій основі і спрямована на зміцнення законності під час здійснення обліку злочинів та їх розкриття.

Забороняється вносити в зазначені документи первинного обліку будь-які доповнення та зміни, оскільки вони єдині для всіх органів прокуратури та правоохоронних органів і можуть змінюватися і доповнюватися тільки за узгодженням з Генеральною прокуратурою України.

Під час заповнення документів первинного обліку (статистичних карток, журналів, довідок) належить керуватися правилами реєстрації і обліку злочинів та осіб, які їх вчинили, викладеними в Інструкції про єдиний облік злочинів, та положеннями, які вказані 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 вчинили, а також для подальшого складання статистичної звітності правоохоронними органами про злочинність і заходи боротьби з нею, 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 ж місті, 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 вказується: 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 начальника обліково-реєстраційного підрозділу поштою із супро-

відним листом, у якому вказуються ті самі реквізити, що 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 б) та по закритих кримінальних справах, у разі їх наявності в архівах інформаційних підрозділів. Документи первинного обліку про злочини, по яких справи зупинені за пунктами 1, 3 ст. 206 КПК, не знищуються, а зберігаються у спеціальній картотеці обліково-реєстраційного підрозділу до розкриття злочину або закриття справи на підставі, що виключає кваліфікацію діяння як злочину [211, с. 502-505].

5. 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 термінів 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 термін 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 термінів контролю. Система дала змогу чітко розмежувати обов'язки співробітників секретаріату, рівномірно розподілити їх навантаження.

Заплановано найближчим часом 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 за 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, в 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 виді за допомогою «Корпоративної системи електронної пошти прокуратури області».

Враховуючи актуальність розвитку та впровадження новітніх технологій у діяльності органів прокуратури, вже розроблено та проведено опробування нової версії інформаційної системи електронного обліку документообігу «Нагляд». Нова версія значно поліпшує систему пошуку, зберігання, захищеності інформації, надає можливість керівникам структурних підрозділів

прокуратури самостійно організувати роботу з документами та контроль за строками розгляду скарг, заяв, які надходять до відділів [60, с. 116-120].

6. 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 напрямками;

4) аналізувати стан та прогнозувати можливість застосування додаткових методів та засобів для підвищення ефективності боротьби зі злочинністю з визначених напрямків;

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 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 «КІА3-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, недіючі)); 2) пошуку документів за словами в текстах із урахуванням «відстані» між ними; 3) перегляду текстів знайдених документів, копіюванні 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 «Інформаційної системи розслідування, прокурорського нагляду, попередження кримінальних подій» розроблена на основі СУБД Oracle8i з використанням пакету Oracle Internet Developer Suite і працює в трьохрівневої архітектурі. В рамках наших пропозицій потрібно зауважити, що доступ слідчих районних прокуратур, що знаходяться на значній відстані від системних інформаційних криміналістичних ресурсів може здійснюватися в рамках 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 [246].

Враховуючи 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 у результативну. Це звільнить інших оперативних працівників від технічної роботи, пов'язаної зі збиранням, опрацьовуванням 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 розробку переліку та структури інформаційних масивів відповідно до предмету прокурорської діяльності, створення таблиць регламентуючої інформації, вдосконалення аналітичної роботи, визначення та розрахунок якісних показників ефективності системи інформаційного забезпечення.

7. Розбудова інформаційних технологій нового покоління

Інформаційні технології можуть бути також ефективно використані в організаційно-управлінській діяльності в середині прокурорської системи. Так, фіксування тієї або іншої інформації в електронних службових блокнотах за типом «прокурорського досьє» зможе допомогти розумінню, засвоєнню, аналізу й 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 принципово нові умови в органах прокуратури для протидії злочинам в інформаційній сфері. Ці методи отримання та збереження оперативно-розшукової інформації означені як «аналітична розвідка», «забезпечення інформаційної безпеки», «комп'ютерна розвідка» [137]. Для вирішення проблеми централізованого збирання та накопичення оперативної інформації щодо злочинів у сфері нових інформаційних технологій на сучасному етапі пропонують до автоматизованої інформаційно-пошукової системи «Оріон» залучити підсистему «злочини у сфері нових інформаційних технологій». За аналізом наслідків опитувань необхідність такої системи підтримують 45,7% респондентів [231].

Створення в Україні окремого відомчого або міжвідомчого спеціалізованого

підрозділу, завданням якого має бути вирішення лише цього питання, безумовно, сприятиме підвищенню ефективності протидії злочинності у сфері високих технологій. В якості завдань такого підрозділу пропонується: 1) розробка та проведення конкретних заходів із запобігання та розкриття фактів незаконних дій у сфері інформаційно-телекомунікаційних технологій; 2) проведення заходів з розшуку та затримання осіб, які вчинюють 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 та 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 необхідним є: 1) створення міжвідомчої робочої групи для розробки 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) розробка нормативно-правового забезпечення доступу до інформації про протиправні дії при використанні корпоративних інформаційно-телекомунікаційних технологій; 4) розробка нових програм навчання при кабінетах криміналістики, проведення електронних навчально-методичних семінарів слідчих прокуратури, які спеціалізуються на розслідуванні справ про комп'ютерні злочини;

5) розробка та впровадження ефективних криміналістичних заходів реагування на комп'ютерні інциденти.

Важливого значення набуває 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. У цьому зв'язку загальнодержавний підхід вимагає регулярного доведення до органів прокуратури перспективних планів щодо централізованого впровадження в діяльність програмного забезпечення й технологій збору 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 черзі розгляд питання про можливість створення відомчого (корпоративного) телекомунікаційного середовища, призначеного для об'єднання різних елементів інформаційної системи підрозділів прокуратури й забезпечення стійкого доступу до інформаційних ресурсів.

Отже, наглядово-аналітичні системи обробки інформації є корпоративними інформаційними мережами спеціального призначення і виступають інтегрованими компонентами єдиної телекомунікаційної інфраструктури органів прокуратури.

8. 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 проходитиме поетапно і послідовно з урахуванням трьохрівневої системи органів прокуратури України. Першим етапом є модернізація та розвиток локальної обчислювальної (комп'ютерної) мережі

Генеральної прокуратури України, другим – створення або модернізація і розвиток локальних обчислювальних мереж у прокуратурах обласного рівня і з'єднання їх із локальною системою Генеральної прокуратури, третім – створення автоматизованих робочих місць на базі персональних комп'ютерів у прокуратурах районного рівня і з'єднання їх з локальними системами прокуратур обласного рівня.

Згідно з вимогами розробленої тендерної документації комплексна інформаційна система органів прокуратури України (перша черга) включатиме в себе такі інформаційні модулі: 1) розробку проектно-технологічної документації щодо створення корпоративної телекомунікаційної локальної мережі органів прокуратури України; 2) створення структурованої кабельної мережі Генеральної прокуратури України; 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 розробки, 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, а як наслідок — розширення інформаційної бази. Завдяки впровадженню 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.

Подібні 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 з 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 дорогих паперових носіїв, а також час на відвідування бібліотек.

Результати інвентаризації системного та прикладного програмного забезпечення, яке використовується в Генеральній прокуратурі України, засвідчили, що майже третина його є застарілим, звідси проблеми з придбанням необхідного програмного забезпечення.

Саме з найбільш підготовлених областей потрібно 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 наступним 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 у 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 розробки 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;

б) 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 до загальнодержавних комп'ютерних інформаційних систем у сферах освіти, науки тощо;

7) сприяння застосуванню новітніх Інтернет-технологій у об'єктивному висвітленні діяльності органів прокуратури різними засобами масової інформації, 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 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, нові здобутки правової інформатики відкривають нові можливості підвищення якості інформаційно-аналітичного забезпечення прокурорської діяльності, модернізації організації управління в органах прокуратури з використанням високих технологій.

9. Концептуальні засади інформатизації органів прокуратури

Щодо управління в прокуратурі можна зазначити, що організація системної інформатизації можлива тільки тоді, коли в її необхідності переконані її перші керівники та всі керівники 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 складатися: 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 оцінки 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 наступним чином: 1) технологічна підтримка діяльності органів прокуратури України (наприклад розробка моделей типових управлінських та процесуальних процедур за функціями); 2) типові автоматизовані робочі місця 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) розробка та застосування моделей, а також розрахунків для оперативного і довгострокового прогнозування, планування кримінологічних, соціальних та економічних ситуацій, математичних моделей динаміки зазначених процесів; 4) інформаційне забезпечення прийняття рішень у різних ситуаціях і оцінка наслідків їх реалізації в умовах відповідного масштабу часу; 5) розробка алгоритмів прийняття рішень у типових процедурах; 6) інформаційна безпека функціонування системи, моделювання, прогнозування упередження 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. Варто також пропрацювати ідею акумулювання органами прокуратури у електронному варіанті актів індивідуально-розпорядчого характеру, виданих органами влади, управління та самоврядування всіх рівнів, а також державними підприємствами, установами і організаціями (щось на зразок того, як органи юстиції реєструють нормативні акти, так і органи прокуратури мали б брати до відома індивідуальні розпорядчі акти). Це служило б стримуючим фактором від різного роду порушень закону, а також інформативно сприяло б здійсненню прокуратурою своєї діяльності.

Для проекту Стратегії інформатизації прокуратури України пропонується наступне: 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 прийняття рішень; 5) функціональні автоматизовані робочі місця; 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 і їх аналітичне опрацювання при здійсненні прокурорами функцій щодо нагляду за виконанням законів і проведення профілактичних заходів щодо запобігання порушенням закону; 3) забезпечення документообігу – тобто формування, збереження, пошук, аналіз і видача

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 у 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 більше 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 й т.п.).

Беручи до уваги вищевказане, 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 вказаної 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 з ГПУ у прокуратури на місцях [107, с. 75].

Одним із форвардних сегментів є інформатизація досудового провадження у кримінальних справах, де роль прокуратури є провідною.

Важливим є також і 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 передачі даних в правоохоронних органах, що дозволить продуктивно використовувати існуючі інформаційно-телекомунікаційні мережі, скоротити витрати та терміни на впровадження в телекомунікаційну систему прокуратури нових видів інформаційних послуг.

Побудова ефективної інформаційної системи, організація проходження інформаційних потоків повинні охоплювати всі підрозділи. Для цього в районних прокуратурах необхідно встановити модеми й через мережу Інтернет організувати доступ до поштового сервера електронного кабінету криміналістики прокуратури області, що дозволяє значно оптимізувати інформаційний обмін і скоротити відповідні фінансові витрати. Вважаємо, що при розробці 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 2 складові: 1) можливість доступу 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 іншими) 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, вирішення поточних методологічних, методичних, інформаційно-технологічних проблем передбачає: 1) забезпечення єдності інтерфейсу різних інформаційних систем через стандартизацію; 2) розробка 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) уніфікація та стандартизація робочих процесів при виконанні функцій працівниками органів прокуратури [235, с. 92-99].

На основі узагальнення пропозицій потрібно розробити структуру й вести до експлуатації внутрішній інформаційний сервер органів прокуратури служби, за допомогою якого на основі web-технологій забезпечується доступ користувачів системи до відомостей за напрямками роботи, а саме: статистичної інформації про результати діяльності органів прокуратури; аналітичної інформації із пріоритетних напрямків діяльності; статистичної, аналітичної й текстової інформації про результати діяльності правоохоронних і контролюючих органів, органів державної влади, наукових і навчальних закладів; інформації, яка публікується в ЗМІ, про події й соціально-політичні процеси.

Розглядається можливість створення єдиного банку даних органів прокуратури за рахунок організації уніфікованої системи обліку результатів наглядової діяльності на територіальному рівні з наступним

об'єднанням на загальнодержавному рівні [52; 232].

Визначено, що основним завданням, що розв'язується в рамках цієї програми, є створення Єдиної інформаційно-телекомунікаційної системи (ЄІТС) органів прокуратури України, що повинна об'єднати в інтегрований інформаційний простір розподілені й локальні цифрові (електронні) ресурси – інформаційних, наукові й адміністративних, програмні (алгоритмічні) – територіальних прокуратур і 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 частиною проекту є створення власного інформаційно-телекомунікаційного Web-порталу.

Пропонується процес створення такої програми розбити на чотири послідовних етапи: а) формування цілісної системи цілей і вимог до програми й доведення її до кожного працівника, зокрема, з використанням волоконно-оптичної мережі спеціально розробленого інтернет-порталу; б) збір і систематизація пропозицій щодо включення інноваційних заходів у програму, спільна робота з ініціаторами пропозицій, що сприяє підвищенню вірогідності представленої ними інформації; в) проектування найбільш повного варіанта програми, попередньо розробленої й затвердженої концепції інформатизації, можливостей і перспектив інформатизації прокуратури, аналізу пропозицій, що надійшли, для одержання повноцінного вихідного переліку заходів програми; г) розробка декількох попередніх варіантів програми, що відповідають різним ресурсним обмеженням і цільовим настановам, використанням спеціально розробленого математичного апарата й оптимізаційного комп'ютерного моделювання (управлінської моделі) [153, с. 65-73].

Оптоволоконна інформаційна технологія є комплексом методів, способів і

засобів пошуку, збору (придбання), реєстрації, збереження, поширення (реалізації), захисту і відображення інформації за допомогою високотехнологічних інформаційних систем і волоконно-оптичних мереж передачі даних, що сьогодні набуває особливого значення при впровадженні нових методів передачі інформації в криміналістиці прокурорської діяльності [197; 209].

Першим етапом організаційних заходів 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, установленому законодавством; д) розроблення та запровадження єдиної уніфікованої технології оброблення інформації в системі, а також типових і спільних програмних засобів; є) створення телекомунікаційної складової системи як окремої підсистеми Національної системи конфіденційного зв'язку із забезпеченням можливості інформаційної взаємодії з наявними системами правоохоронних органів; ж) залучення до створення системи вітчизняних науково-дослідних установ; з) створення в органах прокуратури технічної бази для впровадження системи; і) упровадження комплексної системи захисту інформації та підтвердження її відповідності в порядку, установленому законодавством; к) визначення принципів можливої інтеграції системи до міжнародних спеціалізованих інформаційних систем у сфері запобігання злочинності [46].

10. Стратегія розвитку інформатизації органів прокуратури України

Стратегія (від грец. *strategos* – веду військо) – це загальний план дії для

досягнення необхідного результату (на відміну від тактики, що вирішує частки, проміжні завдання). Взагалі, під стратегією розуміють загальний план дій з метою досягнення необхідного результату (на відміну від тактики, що вирішує окремі проміжні задачі). Звідси пропонуємо визначити стратегію розвитку як можливі у відповідності з діючими правилами (правовими нормами) способи дій суб'єктів суспільних відносин.

Серед основних завдань стратегії розвитку 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 [87].

Стратегія 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 зв'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 інформаційної діяльності в екстремальних або надзвичайних умовах.

Стратегія інформатизації прокурорської діяльності на конкретній ділянці нагляду визначається інформаційними особливостями відповідних правовідносин.

Стратегічна позиція інформатизації прокурорської діяльності визначається концептуальною єдністю заходів щодо запобігання інформаційних розривів в телекомунікаційній системі.

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 фоні цього, варто окреслити основні завдання інформатизації органів прокуратури.

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.

Подальший розвиток інформатизації прокуратури України як напряму науково-практичних досліджень має забезпечити формування вітчизняної наукової школи правової інформатики.

Отже, органи прокуратури виступають суб'єктами інформаційного права, що мають особливий статус, тобто фактично є спеціальними суб'єктами, що підтверджує виведене співвідношення:

$$\Pi = \frac{S \xrightarrow{1} C}{S \xrightarrow{2} P} \Leftrightarrow HTI$$
, де Π – інформаційне право, $S 1$ – суб'єкти, C – сфера боротьби зі злочинністю, $S 2$ – спеціальні суб'єкти, P – прокуратура, HTI – право високих технологій.

Слід відзначити такий системний недолік як недостатній рівень надійності правового та організаційно-технічного

захисту інформаційно-телекомунікаційної системи органів прокуратури.

Нарешті, підводячи підсумки з розгляду проблеми високотехнологічної інформатизації прокуратури визначимо системну кореляцію основних категорій: $\frac{O}{T} \neq \frac{E}{I}$, де наглядово-аналітичні системи обробки інформації (O) є спеціальними компонентами телекомунікаційної інфраструктури прокуратури (T); у той же час експертно-пошукові системи (E) складають більш масивну інформаційну систему, що організаційно підпорядковується до інфраструктури органів внутрішніх справ (I).

Подібна конструкція містить у собі приховану загрозу міжвідомчих неузгодженостей, що можуть виникати в інформаційній сфері зазначених відомств.

Для вирішення відзначених проблем вважаємо перспективним створення в органах прокуратури спеціалізованого наукового підрозділу, до завдань якого має бути включено розробка 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.

КЛЮЧОВІ СЛОВА: Прокуратура, нагляд, прокурорські телекомунікації, електронний документообіг, інформатизація, стратегії.

ЛЕКЦІЯ 8. НАНОТЕХНОЛОГІЯ ЯК СПЕЦІАЛЬНИЙ ОБ'ЄКТ ЕЛЕКТРОННОГО ПРАВА ВИСОКИХ ТЕХНОЛОГІЙ

© Синьокий О.В.

Електронний конспект лекції подається в авторській редакції доцента кафедри кримінального права та правосуддя Запорізького національного університету, кандидата юридичних наук Синьокого Олега Володимировича.

Всі права даного електронного видання застережені. Жодна частина лекції не може бути відтворена будь-яким способом та у будь-якій формі без письмового дозволу автора та відповідних посилань.

План лекції

1. *Поняття та правові ознаки нанотехнології.*
2. *Правове забезпечення наоіндустрії.*
3. *Нанотехніка, види наноматеріалів та організаційно-правові проблеми нанотехнології.*
4. *Концепція розвитку нанотехнологій.*
5. *Інформаційно-правові проблеми штучного інтелекту і нанороботи.*
6. *Перспективи інноваційних розробок антикримінальних наносистем.*
7. *Інформатизація Збройних Сил та військові нанотехнології.*
8. *Інформаційне забезпечення судово-експертних досліджень і нанонаукові можливості.*
9. *Судова медицина, судова хімія і нанохімія.*
10. *Судова (криміналістична) фізика і криміналістична нанотехніка.*

1. *Поняття та правові ознаки нанотехнології*

Нанотехнології – це технології роботи з речовиною на рівні окремих атомів.

Нанотехнологіями вважаються міждисциплінарні технології, які розроблені для об'єктів розмірами менш як один мікрон і дають змогу проводити дослідження, маніпуляції та обробку речовин у діапазоні розмірів від 0,1 до 100 нанометрів [95].

Будь-яка технологія, як-то обробка 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 рр. ХХ ст. так звані зонди, що сканують.

Згодом на їхній основі з'явилися перші тунельні мікроскопи.

Нанотехнологія є символом науково-технічного прогресу ХХІ 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; 155; 228].

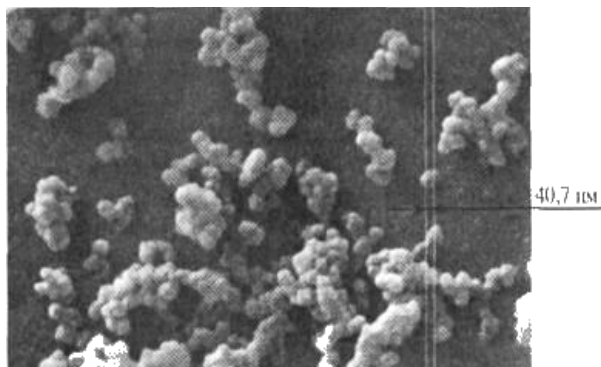
З одного боку нанотехнологія одночасно є наукою і технологію виробництва, орієнтована на одержання унікального обладнання і речовин із задалегідь заданими структурою та властивостями.

Утім нанонауку слід розглядати як один із важливих аспектів цивілізаційного розвитку, що порушує широке коло інформаційно-правових проблем.

Нанонаука включає в себе самі нові 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.

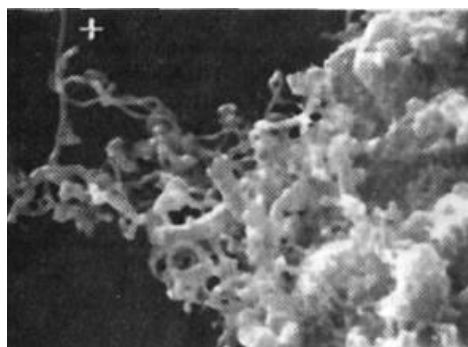
Нижче на малюнку 1 показані сферичні нанорозмірні структури кремнію, де діаметр 84% часток - 44 нм, а 16% - 14 нм.



Малюнок 1.

Нанотехнології вже уражають своїм потенціалом у сфері захисту інформації [161]. Враховуючи це, ми безумовно погоджуємося з твердженням, що ера нанотехнологій вже настала [177, с. 207].

На малюнку 2 представлені нановолокна політетрафторетілену (ПТФЕ), діаметр яких складає 40-60 нм при довжині декілька мікрометрів.



Малюнок 2.

Потрібно визначити, що основними галузями нанотехнології є наноматеріали, наноінструменти, наноелектроніка, мікроелектромеханічні системи і нанобіотехнології [151, с. 18-26].

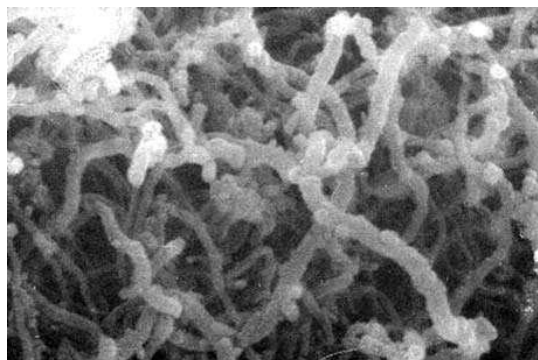
Розвиток наноелектроніки ґрунтується на елементній базі, яка складається з кристалічних структур, розміри яких складають нанометри [120].

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 лакофарбовальні 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), в 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).

На малюнку 3 показано який під мікроскопом мають вигляд нанотрубки, що отримані хімічним осадженням з пару.



Малюнок 3.

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 нанометрів.

Сьогодні у рівній мірі використовуються як термін «нанотехнологія», так і термін «нанотехнології». Утім ми вважаємо, що з юридичної точки зору для визначення поняття цього нового соціально-правового феномену вірніше буде базове вживання в єдиному числі, тобто «нанотехнологія». У свою чергу термін «нанотехнології» є похідним, оскільки означає декілька видів основної технології. Тому з метою мінімізації термінологічної плутанини потрібно визначити основні нормативно-правові джерела, що регулюють соціотехнічні відносини, що пов'язані з нанотехнологією.

Таким чином, 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 від 0,1 до 100 нанометрів (10^{-9} м).

Перш за все, потрібно назвати Концепцію Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010-2014 рр. [95] та

Розпорядження КМУ «Про схвалення Концепції Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010-2014 рр.» від 3 квітня 2009 р. [175].

Отже, право високих технологій не обмежується регулюванням виключно інформаційних правовідносин, а системно регулює усі соціальні відносини, в тому числі які виникають під час розробки 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 повинні 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 потрібно відзначити, що сьогодні існує система відносно обособлених від інших та пов'язаних між собою правових норм щодо нанотехнологій, що регулюють відповідну групу суспільних відносин. Так, до них можна віднести Закони України «Про Національну програму інформатизації» та «Про Концепцію Національної програми інформатизації» [70], «Про науково-технічну інформацію» [71], Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр. [147], Постанову ВРУ «Про дотримання законодавства щодо розвитку науково-технічного потенціалу та інноваційної діяльності в Україні» від 16.06.2004 р. [163], Указ Президента України «Про деякі заходи

щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24 вересня 2001 р. [226], Комплексну програму фундаментальних досліджень НАН України «Наноструктурні системи, наноматеріали, нанотехнології» та деякі інші.

Виникнення численних правових колізій у сфері створення нано технологій та впровадження наноматеріалів свідчить, що існуючий на сьогодні механізм правового регулювання є недостатнім. У зв'язку з тим, що суспільні відносини в цій сфері активно розвиваються, система правового регулювання потребує відповідних змін.

Зокрема, з метою координації діяльності у наносфері, для здобуття передових позицій на світовому ринку високотехнологічної продукції, а також забезпечення конкурентоспроможності та

безпеки країни, захисту і розвитку високих технологій нормативне регулювання нанотехнологій мають виділитися в окремий правовий напрям.

Разом із тим, віднесення нанотехнології до високих технологій передачі інформації потребує додаткової розробки, прийняття та систематизації окремих правових норм у сфері інформаційного права та суміжних галузях.

Нанотехнологія стала найбільш перспективною складовою процесу використання інформаційних ресурсів суспільства. Тому назріла потреба розроблення нормативно-правових документів у сфері нанотехнологій та наноіндустрії, де окремо передбачити норми щодо правового забезпечення нанотехнологій спеціального призначення, що нижче показано в схематичному зображенні:



Таким чином, можна зробити висновок, що сьогодні 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.

2. Правове забезпечення наноіндустрії

Нановиробництво – це виробництво або підготовка наноструктур.

Науково-практична діяльність людини щодо конструювання, виготовлення та застосуванню нанорозмерних об'єктів чи структур, а також об'єктів чи структур, що створені методами нанотехнологій, отримала назву як *наноінженерія*.

Дотепер нерідко термін «індустрія» використовується як синонім терміну «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.

За багатьма прогнозами, ХХІ ст. визначатиме наноіндустрія.

Наноіндустрія – це сфера суспільних відносин та сектор економіки, що включає виробничо-технологічне впровадження інноваційних здобутків науково-дослідної діяльності у пріоритетний сектор економіки відповідно до концепції державної програми створення, виготовлення, впровадження і розповсюдження нанопродукції. При цьому під пріоритетом пропонуємо розуміти першість у відкритті та винаході.

Складовими частинами наноіндустрії є:

1) науково-дослідна діяльність – сукупність інноваційних наукових заходів, спрямованих на розробку досвідних 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 підставах доведення до споживача економічних переваг промислових зразків нанопродукції.

Сьогодні на ринку високих технологій виробляються дослідницькі тунельні й атомно-силові мікроскопи. Проводиться комплекс дуже важливих робіт з лінійного виміру й взагалі з нанометрології.

3 квітня 2007 р. в США надійшли в продаж комп'ютери з ємністю жорсткого диска 1 Тб (10^{12} байт), на якому можна розмістити інформацію, рівнозначну 50 млрд. друкованих сторінок, близько 16 доби відеоматеріалу у форматі DVD, мільйон фотографій у найвищій якості або близько 250 тис. музичних файлів (від півтора до двох років безперервного прослуховування).

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 можна для якихось зовсім інших цілей, включаючи військову техніку.

Не секрет, що у світі ведуться активні роботи з дослідження й розробки нанозброї. Міністерством оборони США створений інститут нанотехнологій для розвитку напрямків військового використання нанотехнологій за лінією Агентства передових оборонних розробок США (DARPA). Наприклад, у цього агентства є програма по наноелектроніці. У ній перераховані, більше 50 напрямків, і за кожним напрямком, принаймні, у відкритій частині, закріплений конкретний американський університет, у деяких випадках окремі фірми. В Україні поки що немає нічого близького.

У зв'язку з цим постають проблеми організаційного та правового забезпечення нанотехнологій: $O + L \Rightarrow Nt$, де організаційне забезпечення нанотехнологій (O) є сукупністю документів, що устанавлюють організаційну структуру процесу розробки, виробництва та впровадження експериментальних, досвідних та промислових зразків нанопродукції, права та обов'язки персоналу та користувачів при експлуатації нанопродукції; правове забезпечення нанотехнологій (L) – сукупність норм, що регламентують правові взаємини при функціонуванні нанопродукції та

юридичний статус результатів їх функціонування.

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 покриттів, що можуть бути використані в судово-експертній практиці.

3. Нанотехніка, види наноматеріалів та організаційно-правові проблеми нанотехнологій

Поняття «нанотехніка» було уведено в обіг в 1974 р. японцем Норіо Танігучи [254]. Зазначений термін є збірним, де досвідним способом реалізовані високотехнологічні можливості нанонауки. Фактично, цим терміном позначається будь-яка фізико-технічна продукція, що виготовлена, як правило малою серією, за допомогою нанотехнологій. Класичними прикладами можуть бути розтворений тунельний мікроскоп (1982), атомний силовий мікроскоп (1986) та нанотрубки (1991). Безумовно, це визначення потребує уточнення, оскільки в ньому залишаються змістовні неясності.

Наноелектроніка – це 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.

Під терміном наноматеріал вважається будь-який матеріал, що має наноскопічні розміри, що вироблений для виконання певної задачі [177, с. 89].

Наноматеріали – це матеріали, які створені з використанням наночасток або завдяки нанотехнологіям, мають унікальні характеристики і властивості, що впливає з мікроскопічних розмірів їхніх складових,

обґрунтованих наявністю цих часток в матеріалі. До наноматеріалів відносяться об'єкти, один з характерних розмірів яких знаходиться в інтервалі від 1 до 100 нм.

Інкапсульовані наноматеріали – це структури, де наноматеріали замикаються до зовнішньої капсули чи оболонки.

Властивості наноматеріалів, 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 дозволяє створювати принципово нові матеріали, криміналістичні технічні прилади та судово-медичні препарати, розробляти нові технологічні процеси з небаченими раніше можливостями.

Існують підстави для твердження, згідно з яким правове регулювання щодо нанотехнологій є правовим феноменом, що формується в інформаційному праві, джерелами якого поряд з інформаційним правом є цивільне, адміністративне, кримінальне право та ряд 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 неоднорічна, але можна визначити три об'єкти, які одночасно постають основними етапами розвитку політики державного регулювання, а саме – нанонаука, нанотехнологія, наноіндустрія.

1 етап) *нанонаука* – це новий особливий вид людської пізнавальної діяльності, що 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 – прогнозувати подальший розвиток нанознань.

2 етап) *нанотехнологія* – це практичні методи дослідження, аналізу і синтезу, а також процес фундаментальної розробки методів виробництва й застосування

продуктів із заданою атомарною структурою шляхом контрольованого маніпулювання окремими атомами та молекулами.

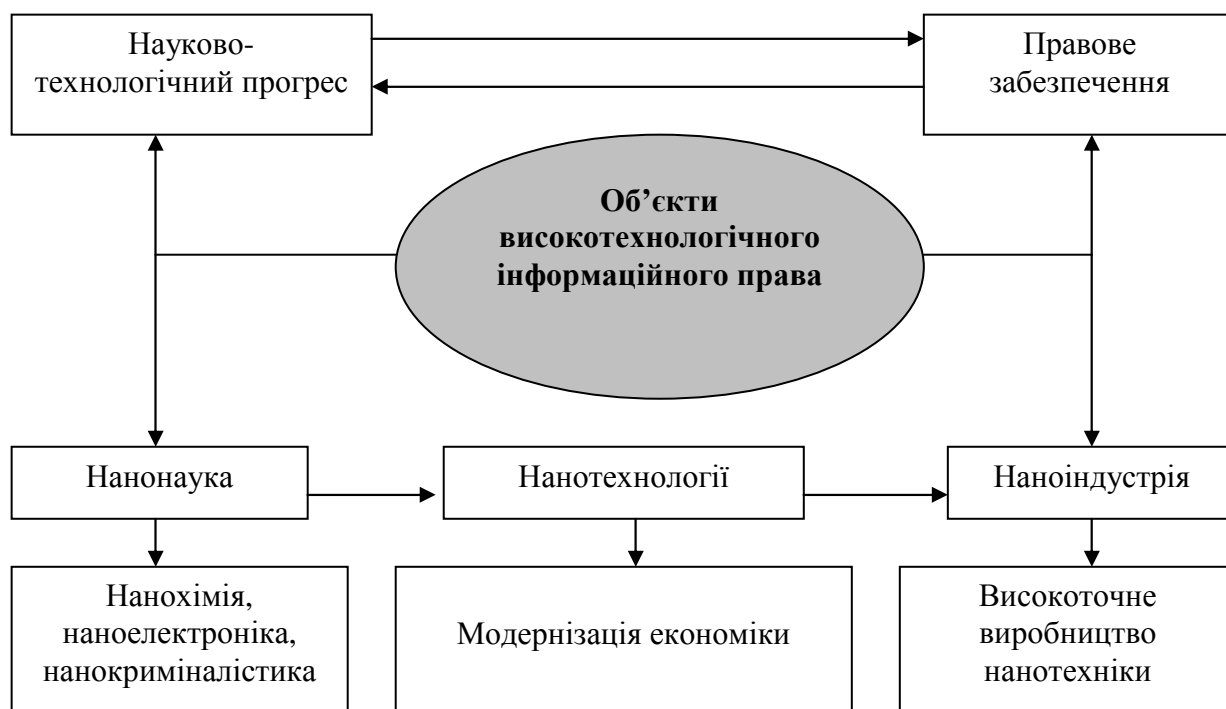
3 етап) *наноіндустрія* – це сфера високотехнологічної діяльності, сектор інноваційної економіки, що включає дослідне та серійне виробництво, промислове впровадження й реалізацію як нанопродукції, так і нанотехнологій, а також допоміжні сектори та споживча аудиторія.

Наведене надають підстави щодо висновку, що наноіндустрія є об'єктами цивільних

правовідносин у інформаційній сфері. Щодо співвідношення наноіндустрії та нанотехнологій останні є складовою частиною цієї комплексної науки майбутнього.

Таким чином, розробка надпотужних інформаційних систем надмалих розмірів є найбільш перспективним напрямком розвитку нанотехнологій.

Спробуємо нижче схематично визначити наноявища та нанопроцеси як об'єкти високотехнологічного інформаційного права:



Нарешті, підсумуємо, що нанотехнологічне суспільство є фактично наступною стадією розвитку інформаційного суспільства, що ґрунтується на розвитку та використанні нанотехнологій.

4. Концепція розвитку нанотехнологій

Зрозуміло, що успішний розвиток нанотехнологій можливий тільки при якісних перетвореннях в економіці й соціальній сфері. Але, незважаючи на розуміння значення нанотехнологій, дослідження у галузі нанометрології, наноелектроніки, біотехнології, точного приладобудування, наноматеріалів, фотоніки тощо в Україні ведуться безсистемно [99, с. 119-135].

Оскільки дотепер не існує центра 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.

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 для

розвитку 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.

За Концепцією Державної цільової науково-технічної програми «Нанотехнології та наноматеріали» на 2010-2014 рр. потрібно визначити такі пріоритетні заходи розвитку нанотехнологій: 1) створення структури управління, безпосередньо підлеглої вищому керівництву держави, яка була б наділена особливими повноваженнями для створення нанотехнологічної наукової школи і промисловості в стислий термін; 2) розгортання нанотехнологічних досліджень і розробок, створення відповідної системи підготовки наукових кадрів, кваліфікованого персоналу, спроможного працювати з нанотехнологічним устаткуванням і об'єктами; 3) розробка стратегії і тактики бойових дій із застосуванням нанотехнологічної зброї, засобів захисту, устаткування і приладів індикації й ідентифікації такої зброї, а також її нейтралізації і знищення; 4) створення у 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, виробництв, складських сховищ для нанооб'єктів і спеціалізованих засобів їх транспортування підвищеної безпеки; 8) широка інформованість населення щодо потенційних загроз нанотехнологій та необхідності мобілізації сил на науково-технічний розвиток; 9) розвиток військово-технічного співробітництва з зарубіжними державами в галузі нанотехнологій; 10) розробка і введення в експлуатацію

системи наносенсорів для антикримінального реження терористичної діяльності.

Згідно з аналітичними даними Американського національного наукового фонду (NSF), уряди і промислові кола розвинених країн очікують в найближчі 10–15 років бурхливого зростання об'ємів ринку нанотехнологічних матеріалів, приладів і іншої продукції з виходом на такі обсяги: наноструктурні матеріали і технологічне обладнання – 340 мільярдів дол./ рік; наноелектроніка – більш 300 мільярдів дол./ рік; фармацевтичні нанопрепарати – більш 180 мільярдів дол./ рік; хімічна продукція на основі нанотехнологій – 100 мільярдів дол./ рік; наноматеріали для аерокосмічної промисловості – 70 мільярдів дол./ рік.

Таким чином, світовий ринок цієї продукції може досягти 1 трильйона доларів до 2015 р.

Широкомасштабні нанотехнологічні розробки почали здійснюватися в більшості розвинених країн з початку 90-х рр. ХХ 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 сконцентрований 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 об'ємами інвестицій в нанотехнології всі останні роки були США і Японія, а в поточному році до них приєдналася РФ, де сконцентровано більше половини світового об'єму інвестицій. У США бюджетне фінансування розвитку нанотехнологій та виготовлення нових наноматеріалів становить більш як 1 млрд. доларів США на рік. В Японії на розроблення у цій галузі у 2005-2008 рр. було виділено 3 млрд. доларів США.

Європейські країни також своєчасно зрозуміли стратегічну важливість розвитку нанотехнологій. В 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. В 7-й Рамковій програмі (2007-2013 рр.) на цей напрям передбачено 3,5 млрд. євро.

У 2007 р. в РФ утворено урядову Раду з нанотехнологій метою ефективної реалізації державної політики 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 Росії до 2015 р. планується виділити 200 млрд. руб., з них 130 млрд. руб. увійде до траншу цього року.

Для 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.

В НАН України протягом багатьох років виконуються фундаментальні і прикладні дослідження, що мають безпосереднє відношення до сьогоденних розробок в галузі нанотехнологій. З метою координації і цілеспрямованої підтримки цих робіт Президією НАН України в 2003 р. було започатковано Комплексну програму фундаментальних досліджень «Наноструктурні системи, наноматеріали, нанотехнології».

За час виконання Програми (2003–06 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 покриттів в 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 наноплівочок для створення датчиків магнітного поля і захисних фільтрів в системах 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 нанокompозитів 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; нанокompозити для світловипромінюючих діодів, матеріали для літєвих акумуляторів високої ємності, систем запису інформації та перетворення сонячної енергії в інші види енергії; наноструктуровані каталізатори для спалювання метану в процесах газової очистки, 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 зносу для інструментів прецизійної обробки матеріалів.

Реалізація таких масштабних завдань в Україні можлива лише за умов суттєвого, не менше ніж десятикратного в порівнянні 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 та 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 щодо нанотехнологій не потрібна, а достатньо окремих розділів, що присвячені нанотехнологіям у загальній великій нацпрограмі за назвою «Національна технологічна база». Але саме в програмі повинна бути позначена якась мета. Такою метою може стати створення в Україні промисловості нового типу –індустрія наносистем і матеріалів.

Формування пріоритетних напрямків і переліку критичних технологій доречно здійснити у два етапи: I етап – підготовка довгострокового прогнозу науково-технологічного розвитку; II етап – підготовка пропозицій по формуванню й корегуванню пріоритетних напрямків і переліку критичних технологій на основі експертизи відповідних пропозицій.

Корегування пріоритетних напрямків і переліку критичних технологій пропонується здійснювати не рідше 1 рази в 4 роки.

Науковий рівень вітчизняних розроблень у галузі розробки нанотехнологій і виготовлення нових наноматеріалів в основному відповідає світовому. Однак на цей час спостерігається недостатня координація робіт, пов'язаних із розробкою нанотехнологій, низька готовність промисловості до широкого впровадження досвідних зразків, істотне заниження потреби 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 сфери, зокрема Законів України «Про наукову і науково-технічну діяльність» і «Про пріоритетні напрями інноваційної діяльності в Україні» [95].

Метою Програми є створення сучасної національної наноіндустрії.

Основними завданнями Програми є: 1) формування інфраструктури для проведення ефективних фундаментальних досліджень у галузі нанотехнологій; 2) координація робіт із розробки та застосування нанотехнологій та наноматеріалів; 3) розроблення нових підходів до підготовки кваліфікованих спеціалістів 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. 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 будуть розвиватися; 2) залучення державних кредитів до закупівлі 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-дослідних і дослідно-конструкторських робіт у рамках державної цільової програми та залучення позабюджетних коштів для реконструкції існуючих та створення нових промислових потужностей 4) введення митних пільг та податкових канікул для інноваційних підприємств, що займаються розробкою та впровадженням нанотехнологій, тобто часткового або повністю звільнити відповідних інвесторів на термін до п'яти років від сплати податків на власність та майно, ПДВ і т.п.

Аналіз викладеного свідчить, що найбільш ефективними є сукупність третього та четвертого варіантів.

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 й технологічного розвитку й оцінки конкурентоспроможності України на світовому ринку; б) виявлення першочергових потреб країни в наукових і технічних досягненнях, виходячи зі стратегічних цілей соціально-економічного й оборонного будівництва, наявності природних, фінансових, матеріальних і кадрових ресурсів, а також науково-технічного й технологічного потенціалу; в) проведення аналізу наукових досліджень, що відбивають публікаційну діяльність, коефіцієнт цитуємості українських учених, а також аналізу патентних документів; г) визначення основних секторів економіки, у яких Україні необхідно забезпечити світове лідерство, а також технологій, що забезпечують рішення завдань національної обороноздатності й безпеки; д) проведення аналізу соціальних, технологічних, економічних, екологічних і політичних аспектів розвитку національної інноваційної системи; е) використання якщо буде потреба інших методів оцінки тенденцій науково-технічного й технологічного розвитку України й закордонних країн.

Для цього у рамках національної програми впровадження моделі розвитку й комерціалізації нанотехнологій повинне бути доручене недержавній структурі [4]. Фінансування Програми планується здійснювати за рахунок коштів державного бюджету та інших джерел. Інвестиційні кошти будуть спрямовані насамперед на закупівлю сучасного імпортного обладнання, організацію та налагодження виробництва нанопродукції [95].

Отже, нанотехнології є не менш важливим для держави напрямком з погляду економічної, соціальної й військової безпеки, що така програма не може бути прирівняна до програми щодо розвитку, наприклад, металургії, нафти або газу. У цьому зв'язку необхідно вжити заходів, які стосувалися б не тільки формування державної програми, але й передбачали відповідні політичні кроки. Перераховані заходи, могли б стати поворотним моментом у розвитку країни, початком загальнонаціонального технологічного прориву.

Нарешті в останній частині цього параграфу існує сенс зауважити, що останнім часом висловлюються певні спрощення, що призвело до впровадження у літературний обіг окремих помилкових тез, спростування яких потребує додаткової аргументації.

Зауваження перше. Інновація розглядається як системне перетворення технологічної модернізації, яке за своїм змістом залишається глибоко соціокультурним явищем. З першого погляду, ця теза не може викликати особливих заперечень. Однак разом із тим, в якості основного двигуна інновацій формується оптимальна комбінація інвестицій великих наукомістких корпорацій, середнього бізнесу переважно малих компаній плюс елемент державної політики. При цьому останній передбачує корінні 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 устоялися та процес їхнього становлення продовжується. Але існуючий різнобій в юридичній термінології стосовно визначення високотехнологічних інновацій не може бути виправданим, оскільки подібний стан вже провокує різні підходи судів у вирішенні типових категорій справ. Ось тому 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 є виключно науково-технологічною сферою, 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 відношення та визначають їхню належність. Утім нанотехнологія як процес уявляє 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 й особливо тактичні задачі розвитку нанотехнологій.

Таким чином, сукупність викладених аргументів додатково обумовлює потребу кодифікації законодавства у сфері високих технологій, а звідси вимагає структурної переробки існуючих проектів Інформаційного кодексу, про що частково йшлося ще у § 1.2.

З цього існують 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:

$$Ol = \frac{Ns + Nt + Ni}{W} \leftarrow_{\text{з}} \rightarrow \{I\},$$

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 окремою главою у відповідному розділі спеціальної частини проекту Інформаційного кодексу України.

Потрібно наголосити, що у найближчі десять років саме розвиток наноіндустрії, а саме – синтез та використання нових наноматеріалів стане одним з 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. Інформаційно-правові проблеми штучного інтелекту 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 розробка інтелектуальних машин та інформаційних систем, особливо інтелектуальних комп'ютерних програм, що спрямовані на те, щоб зрозуміти людський інтелект.

Існування потужного зворотного зв'язка між інформаційними системами й зовнішнім світом, а також розвиток нанонейромереж неминуче призведе до виникнення штучного інтелекту.

Під проблемою комп'ютерного інтелекту ми розуміємо підпроблему штучного інтелекту, необхідного для вирішення завдань з використанням нових інформаційних технологій.

Зазначена проблема стає предметом докладного наукового розгляду [131]. «Впровадження» у живий організм нових комбінацій на рівні атомів може мати всілякі наслідки - від «відновлення» вимерлих видів до створення нових типів живих істот та біороботів. До того ж, інтегрування із робототехнікою можна вважати ще одним напрямком досліджень – створення інтелектуальних нанороботів.

Нанороботи (в англійській літературі також використовуються терміни «наноботи», «наноїди», «наніти», «наногени» і «наномурахи») – це роботи, що створені з наноматеріалів і за розміром можуть бути порівняні з молекулою. Вони повинні мати функції руху, обробки й передачі інформації,

виконання програм. Розміри нанороботів не перевищують декількох нанометрів. Відповідно до сучасних теорій, нанороботи повинні вміти здійснювати двосторонню комунікацію: реагувати на акустичні сигнали й могли підзаряджатися або перепрограмуватися ззовні за допомогою звукових або електричних коливань. Також важливою представляється функція реплікації, тобто самозбірки нових нанітів і програмованого самознищення, коли середовище роботи, наприклад, людське тіло, більше не має потреби щодо присутності в ньому нанороботів. В останньому випадку роботи повинні розпадатися на нешкідливі компоненти, що швидко виводяться.

Нанороботи фактично є нанорозмірними машинами, що здатні рухатися під час енергетичного впливу. Навіть звичайних роботів, які можуть переміщатися з нанорозмірною точністю, можна вважати нанороботами. Вже існують нанороботи, які називаються реплікаторами, що можуть створювати свої копії, тобто здатними до самовідтворення.

Утім вчені-фізики обґрунтовано застерігають, що ці мікромашини можуть стати основою для нових, ще більш жахливих, ніж сучасні, засобів ведення війни.

Таким чином, *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 порівнянні з молекулою (менш 10 нм), що можуть виконувати інформаційні програми, обробляти та передавати інформацію.

Нанороботи можуть виявляти токсичні хімічні речовини у навколишньому середовищі й вимірювати рівень їхньої концентрації. Можливо військового застосування нанороботів як засобів спостереження й шпигунства, а також для використання нанороботів як зброї [146]. Оскільки наноробот може управлятися оператором або працювати по заздалегідь складеній програмі, наймовірно широким може бути використання «кримінальних нанороботів» у протиправних цілях, що не

тільки потенційно несе в собі інформаційну погрозу найвищого рівня, але й взагалі може призвести до переформатування існуючих знань про злочинність та способи боротьби з нею, що впливає із визначеної закономірності: $Nc = \sum \frac{1+2...A+B...}{Nr} \rightarrow \infty$, де

Nc – нанозлочинність, $1+2...$ – окремі види нанозлочинів терористичної спрямованості, $A+B...$ – інші види злочинів, що вчинені з використанням нанотехнологій, нанозасобів та наноприладів, Nr – нанороботи (кримінаніти).

Таким чином, існують усі підстави вважати штучний інтелект спеціалізованим напрямом наукових досліджень, пов'язаний зі створенням нейрокомп'ютерів, здатних навчатися, аналізувати та розуміти.

Нанопередавачі – це маленькі органічні молекули, які переносять сигнали та інформацію від однієї частини мозку (нейрона) до іншої.

Кримінаніти – це нанороботи, що активно виконують заборонені (протиправні) дії згідно заданої інформаційної програми.

Звідси використання можливостей нанотехнологій у найближчій перспективі сприятиме інформатизації за рахунок багаторазового збільшення об'єму пам'яті та продуктивності системи обробки, зберігання і передачі інформації, а також створення нових високоефективних швидкісних пристроїв з наближенням можливостей обчислювальних систем до властивостей, притаманних об'єктам живої природи з елементами інтелекту.

Таким чином, потрібно наголосити, що залишається небезпека не тільки стрімкого розвитку нанотехнологічних озброєнь, але й непередбаченого поведіння наносистем, їхнього виходу з-під контролю людини.

6. Перспективи інноваційних розробок антикримінальних наносистем

Матеріал базується на офіційних джерелах, державних документах західних держав та публікаціях визнаних експертів [29; 32; 96; 135; 138; 220; 223 та ін.].

Місцезнаходження більшості боєприпасів відоме зацікавленим колам. Оскільки вбудовані захисні та сигнальні

системи є перешкодою для наноприладів перших поколінь, терористи можуть зосередитися на атаках засобів доставки 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 доставки – це підводні човни, авіація, підземне та наземне пускове обладнання – можна швидко і раптово ушкодити, якщо не будуть розроблені і встановлені спеціальні засоби протидії нанозброї. Місцезнаходження та маршрути цих засобів доставки, їх детальний технічний опис можуть передаватися терористам іноземними розвідками. Порухення роботи електронних меж і механіки за допомогою малогабаритних роботизованих пристроїв – очевидний варіант такого впливу.

Дуже небезпечною вважається атака на заводи боєприпасів – вони захищені набагато гірше, ніж окремі боєзаряди, і як наслідок – можливі ушкодження унікальних заводських потужностей, а найгірше – це вибух і радіоактивне зараження величезних площ [32].

Психотероризм. Грунтовні дослідження ведуться у галузі нейронних технологій і зчитування нервових імпульсів. Ми звикли вважати подібні речі фантастикою, але два місяці тому у лабораторіях NASA створені 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, що 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 сек., при цьому люди стають

абсолютно безпомічними на великих територіях.

Авіатероризм. Систематичне і вибіркоче ураження найважливіших об'єктів військового й 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 на площу радіусом – тисячі кілометрів на будь-якій відстані від місця запуску.

Програма «*Advanced Standoff Cruise Missile*» передбачає створення снарядів, що застосовуються у ряді систем, від супутникових до лазерних, здатних до перепрограмування у польоті і забезпечених великою кількістю сенсорів для розвідки та наведення на ціль. Наноконструктивні 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 переробки, військової дослідницької лабораторії.

Спеціально запрограмовані або дистанційно керовані пристрої зможуть швидко і таємно доставити вибухівку для підриву сховищ агресивних речовин, а потім розповсюдити їхню 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 напрямки терористичних атак стають усе реальнішими в 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.

Антитерористичні нанотехнології. Активізація антитерористичної діяльності з використанням новітніх досягнень в 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: покладення 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 та надання методичної та практичної допомоги іншим галузевим службам та правоохоронним органам у межах своєї компетенції; 4) накопичення, узагальнення та аналіз інформації про кіберзлочинність.

Необхідно 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 і уміння діяти на випередження.

На розв'язання цієї проблеми спрямовані 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 вибраного курсу.

Пропонуємо кілька 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 або 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, що 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 кілька порядків і вищу ніж стандартні засоби; 5) наноелектронні компоненти і схеми, що здатні цілком витиснути імпорتنі комплектуючі з вітчизняної електроніки й 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, є: 1) розвідувальна діяльність спеціальних служб іноземних держав, міжнародних злочинних угруповань, організацій і груп, пов'язана зі збором 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.

Для детального вивчення сучасної проблематики нанотехнологій та інших критичних технологій, а також захисту інтелектуальної власності в системі правоохоронних органів України створено спеціальні підрозділи, у складі яких в тому числі працюють аналітичні групи, що відслідковують напрацювання сотні світових джерел у сфері нанотехнологій. У той же час, як показує закордонний досвід, спроби подолати інфотероризм винятково силовими засобами в сучасних умовах малоперспективні.

Тому державна політика у сфері запобігання тероризму [47] має містити особливе місце щодо розробки та впровадженню антитерористичних нанотехнологій, чому, на жаль, до цього часу уваги приділяється недостатньо.

7. Інформатизація Збройних Сил та військові нанотехнології

Інформатизація Збройних Сил України є складовою частиною національної програми інформатизації [30, с. 19-22]. Високотехнологічна інформатизація є складовою цього процесу і включає створення, впровадження, застосування і модернізації у 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 є 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 мір, у тому числі в інформаційному протиборстві.

У цьому зв'язку потрібно визначити особливу загрозу такого злочину як диверсія в сфері комп'ютерної інформації, що може бути

пов'язана з інформаційною війною, що планується й ведеться з метою досягнення інформаційної переваги над супротивником у військовій ситуації.

Стратегічні, оперативні й тактичні потреби боротьби з інформаційним ресурсом породили новий клас інформаційної зброї – ракети й 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, що заснована на широкому застосуванні комп'ютерних мереж.

У зв'язку з цим до основних вимог ефективної діяльності систем управління військами потрібно віднести здатність функціонувати в умовах різкого збільшення потоку інформації при одночасному зменшенні часу на її передачу, обробку та використання.

Таким чином, висока ефективність і значимість інформатизації стала одним з найважливіших факторів підвищення бойової готовності Збройних Сил на новому витку їхнього розвитку й удосконалювання. Це обумовлює істотний перегляд військово-політичних, стратегічних та оперативно-тактичних поглядів на зміст і характер військового протистояння у сучасних умовах.

На жаль, певні кола, зацікавлені в підтримці міжнародного тероризму, теж використовують нові технологічні можливості для порушення міжнародної стабільності і створення нових погроз національній безпеці України і 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 інформа-

ційних, спеціальних і повітряно-морських десантних операцій у віддалених регіонах світу, а також операцій в умовах великих міст. Має велике значення розробка нових препаратів, заснованих на досягненнях нанобіотехнології, що дозволять бойовикам не спати тривалий час без утрати боєздатності.

Безсумнівно, рівень загрози модифікованих видів зброї, що можуть бути створені на основі молекулярних нанотехнологій, можна порівняти з ядерною.

Тому окрема загроза в інформаційному протистоянні виходить з військових нанотехнологій. Зокрема, 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, що у найближчі 10–20 років можуть бути створені супермалі комп'ютери, більш легкі та міцні матеріали, нові типи зброї та, навіть, імплантанти, що будуть вводитися в організм військовослужбовців.

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-криміналік» уже проникнув усередину тіла й затаївся чекаючи злочинного наказу.

Нанотехнології потенційно надають можливість для створення системи, яка повинна здійснити автоматичний ядерний залп у випадку виявлення ядерної атаки. Некерований наноробот, який запрограмований винятково 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, которые самовідтворюються, при цьому не мають

структури у великому масштабі. Такі події можуть трапитися завдяки навмисному включенню або від випадкової мутації наноструктурних утворень.

Створення різного роду захисних засобів є одним з перспективних напрямків військових досліджень в газузі нанотехнології. Так, ізраїльська компанія *ApNano Materials* вже випробувала один з найбільш стійких до удару матеріалів, що відомі людству. Такий матеріал може бути застосованим для виготовлення шоломів і бронезилетів, а також обшивання військового транспорту.

На озброєнні США вже незабаром може з'явитися обмундирування нового типу, що за своїми захисними властивостями та ергономічними характеристиками перевершує сучасні кевларові аналоги. Ефект суперзахисту досягається завдяки спеціальному пакету з кевлару, що наповнюється розчином надтвердих наночасток. Як тільки відбувається механічний тиск високої енергії на кевларову оболонку, наночастки збираються в кластери, змінюючи при цьому структуру розчину рідини, що перетворюється у твердий композит. Цей фазовий перехід відбувається менш ніж за мілісекунду, що й дозволяє захистити солдатів не тільки від ножового удару, але й від кулі або осколка. І нещодавно американський холдінг-виробник військового обмундирування й бронезилетів *U. S. Armor Holdings* ліцензував технологію «рідкого бронезилета» і планує почати його масове виробництво [176].

В Інституті прикладних нанотехнологій (Зеленоград, РФ) продемонструвано перші досвідні російські зразки «рідкої» броні, що у перспективі може застосовуватися для бронезилетів і інших засобів індивідуального захисту.

Звідси перспективи *військових нанотехнологій* потрібно розглядати з точки зору міжнародної безпеки та запобігання нової гонки озброєнь. Таким чином, інформатизація Збройних Сил та правоохоронних органів мають відбуватися у рамках єдиного процесу, що відображає відповідний напрямок державної інформаційної політики.

8. Інформаційне забезпечення судово-експертних досліджень і нанонаукові можливості

Інформаційне забезпечення експертного процесу неможна вважати тотожним високотехнологічному забезпеченню, оскільки під останнім пропонується вважати 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.

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 у майбутньому сформуванню «об'єднаний» чи «колективний» експертний інтелект як високотехнологічний інформаційно-експертний центр найвищого рівня.

Останнім часом поступово не викликає сумнівів перспектив 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 напрямку проводяться й інші дослідження [155].

Отже, нанонаука є не тільки кількісним, але й якісним стрибком від теоретичних досліджень речовини до маніпуляції окремими атомами.

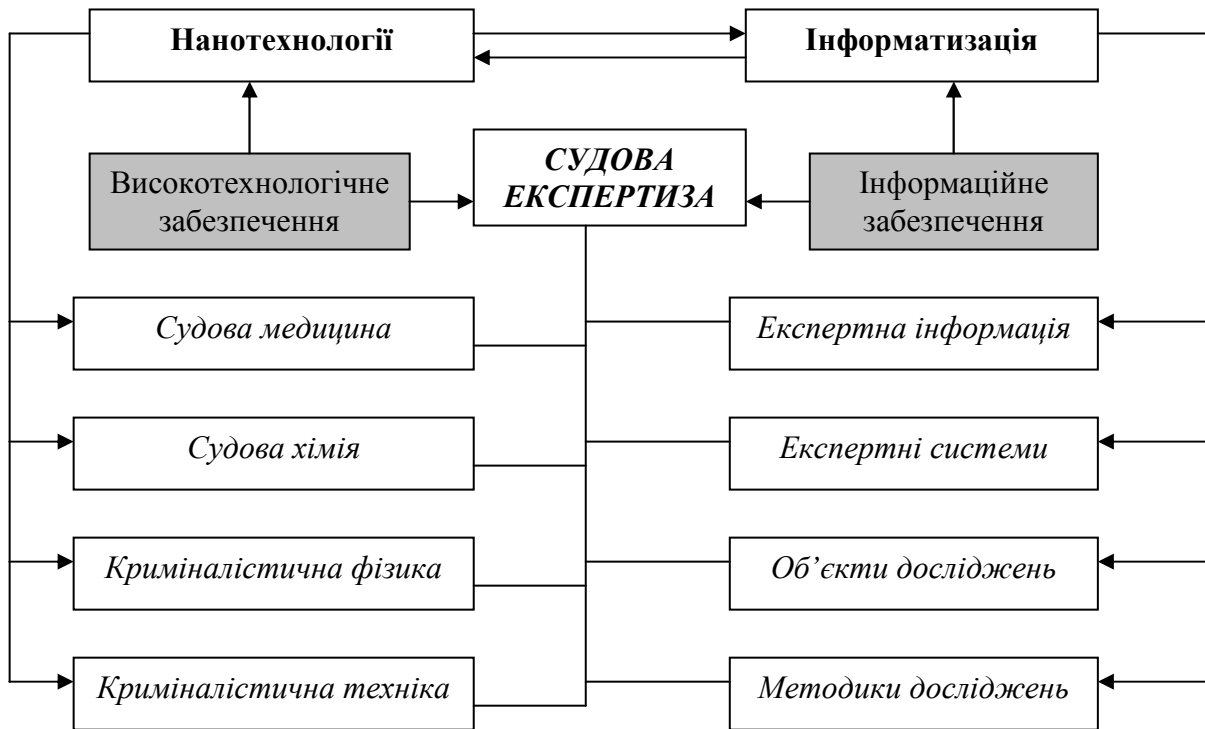
Нанонаука пропонує різні можливості створення магнітних та оптичних запам'ятовуючих пристроїв. Зокрема, для запису інформації та її подальшої зміни можуть бути використані лазери з різним рівнем інтенсивності. Однією з переваг таких наноскопічних оптичних структур є те, що вони можуть існувати у трьох вимірах [177, с.

180]. Найбільш очевидною сферою застосування нанонауки до цього часу залишаються електронні технології.

Як свідчать наслідки досліджень, світлом, яке локалізоване у нанорозмірному обсязі, можна управляти. Застосування лазерів в спектроскопії обумовило бурхливий розвиток нового її напрямку – лазерної

спектроскопії, що відкриває нові перспективи розвитку судово-експертних технологій.

Потрібно відзначити, що високі експертні технології, зокрема нанотехнології, є ефективним способом організації проведення судової експертизи з використанням інноваційних методів та продуктів як це ми маємо побачити з наступної схеми:



У судово-експертній практиці застосовуються два підходи до упровадження 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 складає предмет нанохімії [33].

У судово-експертній практиці сьогодні нанотехнології вже починають знаходити своє впровадження при дослідженні відбитків пальців. Для контрастування жирних слідів пальців використали суспензію золотих наночастинок, що володіють гідрофобними властивостями, тобто здатністю прилипати до поверхонь, покритих жиром. Ці наночастинок, прилипаючи до жирних борозенок відбитків пальців, формували значно більш чіткий малюнок, ніж можна було б одержати за

допомогою традиційної технології. При цьому час процедури не перевищував трьох мінут. У цілому дотепер у криміналістиці нанотехнології обмежено застосовуються при дослідженні прихованих (латентних) відбитків пальців. Зокрема, металеві наночастинок й наноструктуровані частки використовуються для прояву відбитків.

Нанопокриття – це покриття товщиною від 1 до 100 нм, які використовуються в лазерній техніці завдяки здатності якісного відображення. Звідси доцільність використання наноматеріалів, які виготовляються із застосуванням нанотехнологій, зумовлена тим, що у таких розмірах об'єктів речовина має властивості, які не притаманні їй макрокількості. Звідси зрозуміло, що нові напрями судових експертиз свідчать про постійний динамічний

процес розвитку і вдосконалення судово-експертних технологій.

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, 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.

Утім, на наш погляд, перспективним є системне використання наукових методів нанотехнологій, що дозволить виконувати складні експертні дослідження мікрооб'єктів та мікрослідів вже на нанорівні. Звідси відкриваються інноваційні шляхи для розвитку нового класу експертних методик – експертизи нанооб'єктів і нанослідів.

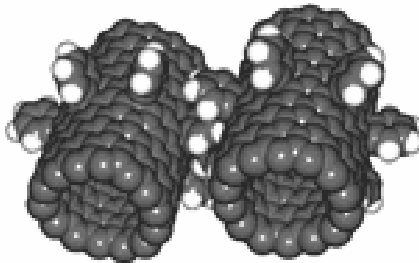
Це може стати новою ерою у розслідуванні практично всіх категорій злочинів, але для реалізації цієї програми організаційно-методичні та процесуально-правові аспекти потребують суттєвого

нормативного удосконалення на законодавчому та відомчих рівнях.

9. Судова медицина, судова хімія і нанохімія

Моделювання і теорія є базисом розуміння та проектування наноструктур, а також, у більш загальному випадку, усього наукового всесвіту. Проектування на молекулярному рівні та молекулярна біологія надають множину нових інтелектуальних матеріалів. Так, моделювання показує, що один з найбільш розповсюджених на сьогоднішній день нанопристроїв – нанотрубки є найбільш міцним синтезованим матеріалом з усіх можливих.

Нанотрубки грають різні ролі: від молекулярних фільтрів, що діють як звичайні сита, і до тривимірних шестірень, без яких важко уявити собі який-небудь механізм. Нанотрубки на малюнку майже цілком складаються з вуглецю, а точніше із замкнутих графітових шарів. Зверніть увагу на виступи з боків трубок: саме вони виконують функції зубів, що перетворюють нанотрубки в шестірні.



Наночастинки починають застосовуватися для наукових розроблень у галузі судової медицини, зокрема, для створення біомаркерів. Магнітні наночастинки, на які нанесені 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 запрограмованим 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 пред-

ставляється можливим. Ця зброя може спрацювати не тільки проти наміченої групи людей, але й за чітко визначеними умовами. Тобто йдеться про відкладене на невизначений термін захворювання. Потрапивши в організм жертви, бактерії спочатку ніяк не будуть себе виявляти. Але як тільки заражена людина, скажімо, занедужавши ангіною, прийме антибіотик, бактерії активуються і починають розмножуватися, викликаючи смертельне захворювання, що не піддається діагностиці. Летальна доза токсину ботулізму для людини складає близько 100 нанограмів. Комплект із десятка пристроїв, здатних здалека розпорошити смертельну дозу над великими містами-«мільйонниками» може уміститися її невеликому кейсі терориста. Медикам складно буде вжити заходів, оскільки спроби лікування лише прискорюватимуть розвиток захворювання.

Дослідники з Каліфорнійського технологічного інституту (США) розробили портативний аналізатор крові, що буде виконувати точний аналіз усього за 2 хвилини. Вони зменшили рахункову машину-аналізатор, що використовується у судово-експертних лабораторіях, і одержали пристрій, що не перевищує розмірами мобільний телефон. У результаті вийшла дійсно портативна лабораторія, де фахівці здатні проводити експертні дослідження по краплі крові.

Судова або інакше криміналістична хімія – це частина прикладної (переважно аналітичної) хімії, яка за обсягом, у широкому сенсі, є практично неосяжною щодо численності та розмаїтості завдань, що нею вирішуються, оскільки будь-яке хімічне дослідження може стати предметом судово-хімічної експертизи, якщо цього вимагають питання, що виникли у правовій (переважно правоохоронній) практиці і розв'язати які можливо виключно за допомогою спеціальних хімічних, токсикологічних або фармацевтичних знань. Таким чином, фактично криміналістична хімія досліджує якісний та кількісний хімічний аналіз об'єктів, що були направлені 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, що 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].

Потрібно зазначити такі напрямки нанохімії як синтез наноструктур у біологічних тканинах, розробку методів складання великих молекул з атомів за допомогою наноманіпуляторів та запровадження нових нанокатализаторів 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 підвищуються при сполученні зовнішнього виду нанокристалів з їхніми оптичними властивостями.

Електрохімія має широке застосування не тільки у виробництві наноструктур, а також може використовуватися для їхнього 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 складає усього одну мільярдну. До того ж, наноскопічні фотосенсиори 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 й компонентного ізотопного складу в будь-яких середовищах для практичного застосування в

криміналістиці, зокрема виявленні фальсифікації продукції й біохімічних досліджень. Так, наприклад, «електронний ніс» вже може забезпечити нові можливості в боротьбі з контрабандним ввозом і поширенням наркотиків, попередити терористичні диверсії. Відчуваючи запах метану, можна швидко виявити й усунути витік із газопроводів. Нанотехнологія сприяє створенню дуже потужних вибухових, запалювальних й отруйних речовин.

Одним з важливих питань, що постають перед нанохімією є проблема пошуку можливостей змусити молекули групуватися певним порядком, щоб у підсумку одержати нові матеріали або пристрої. Цією проблемою і займається нанохімія, що вивчає не скільки окремі молекули, скільки процеси взаємодії між молекулами, які здатні упорядкувати молекули визначеним способом, створюючи нові речовини й матеріали.

Загальновідомий факт, що дрібні частки хімічно активніші через більше співвідношення площі поверхні до об'єму. Дослідження підтверджують, що навіть нешкідливі речовини у вигляді наночастинок стають смертельною отрутою. Тому наночастинок можуть бути використані як потужний каталізатор для широкого діапазону хімічних реакцій — основи надпотужних вибухових запалювальних речовин.

За прогнозами фахівців у цій сфері надалі в судово-хімічній галузі якості та достовірності близько половини досліджень буде залежати від нанотехнологій.

Звідси перспективним напрямком є розробка ряду нових нанокаталізаторів для хімічної промисловості та лабораторної практики, що може бути з успіхом використано в експертно-криміналістичній діяльності.

10. Судова (криміналістична) фізика 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.

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 матеріали.

Разом із тим, можна припустити, що інноваційний розвиток криміналістичної техніки у XXI ст. визначатимуть саме нанотехнології, що викличе істотні зміни у цій галузі криміналістики і стане фундаментом окремого напрямку – криміналістичної нанотехніки.

Останніми роками відбувається значна модернізація криміналістичної техніки, завдяки інтенсивному освоєнню та впровадженню досягнень фізики, 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 її ототожнювати з останньою. За допомогою фізико-технічної експертизи проходить вивчення структурного складу матеріалів. Адже від структури матеріалів залежать майбутні їхні 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 урахуванні фізичних властивостей об'єктів у нерозривному зв'язку розрізняти їхнє зовнішню й внутрішню побудову.

Основними методами криміналістичної фізики є атомно-емісійна спектрометрія, атомно-абсорбційна спектрометрія, рентгеноспектральний аналіз, молекулярний спектральний аналіз, методи виявлення мікродефектів. Так, наприклад, рентгеноструктурний аналіз є типовим методом фізики, тому його розвиток і вдосконалення неможливо поза фізикою.

Використання цього методу для дослідження речових доказів вимагає розробки певних специфічних прийомів, тобто фактично особливого підходу, як відносно техніки, так і відносно оцінки результатів, що не пов'язані із загальною фізикою. Тим не менш, метод залишається фізичним, оскільки зв'язаний, насамперед, з фізикою й тому відноситься до судово-фізичної експертизи. Таким чином, судовий фізик, насамперед, має опиратися на дані фізики, що створює науковий фундамент відповідного виду судово-фізичної експертизи [253].

Для того щоб розглянути й досліджувати мікрочастинки, необхідно вдаватися до допомоги різних фізичних приладів та технологічних інструментів.

Одним з перших таких інструментів судової фізики став 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» [177, с. 49-50].

Комбінації молекулярного розпізнавання та зборки зможе дати нові експертні матеріали, побудова чого можлива виключно в наносвіті. Грунтуючись на цьому мікроскопи, що сканують, дозволяють побачити об'єкти атомного розміру. Першими нанорозмірними структурами, що були побудовані на молекулярному рівні були вуглецеві трубки, які демонструють дійсно унікальні властивості [177, с. 79]. Нанотрубки зможуть вивести експертні технології на новий рівень, але до цього часу їхнє 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.

Впровадження волоконно-оптичного пристрою для одержання контактного зображення відбитку пальця дозволяє 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 їхні майбутні механічні параметри.

До того ж потрібно визначити, що цікавими для криміналістичної фізики можуть стати розробки у галузі нанооптики як розділі оптики та нанотехнології, де використовується світло, що 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 створення мікроскопу, за допомогою якого переборено дифракційну межу в оптиці, яка завдяки розвитку цієї технології може досягти 1 нм.

Усі ці галузі активно розвиваються з використанням нанонауки у сфері електроніки, оптики та магнітних матеріалів. Використовуючи класифікацію видів високих технологій, про що вже вели розмову, це, мабуть, і є «найвищими технологіями» нанонауки, оскільки вони уявляють оптимальну взаємодію нанотехнології з високою інформаційною технологією [177, 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

т.п.). 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 цей час інтенсивно розвиваються напрямки нанофотоніки, до якої можна віднести в першу чергу нанохвилеводи, наноласери, 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, що вище були описані, можуть мати революційні наслідки для формування нових судово-експертних методів, фактичного втілення нанометодик в 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 теоретична розробка системи оцінок ефективності використання нанотехнологій у судово-експертній практиці є важливим напрямком політики розвитку високих технологій у сфері боротьби зі злочинністю [192-193].

Нанотехнології можуть стати для правоохоронних органів тим науково-технічним інструментом, завдяки якому можливо радикально підняти ефективність боротьби зі злочинністю на якісно новий рівень. Зрозуміло, що шляхи використання інформаційних наносистем у сфері протидії інформаційної злочинності та стримуванні рівня її інтелектуалізації потребують ґрунтового осмислення і визначення подальших перспектив розвитку в цій галузі знань. Сьогодні вже не може виникати суперечок щодо доцільності створення антикримінального мега-інформаційного середовища, здатного найбільш повно й оперативно задовольняти інформаційні потреби органів всіх рівнів, які ведуть

боротьбу зі злочинністю, при здійсненні ними своїх функцій і повноважень.

Процес інтеграції інформаційних систем правоохоронних органів повинен бути продовжений і ще глибше охоплювати інформаційні масиви, починаючи з слідчих та закінчуючи експертними установами.

Отже, висловлені аргументи надають нам підстави щодо виведення формули високотехнологічної теорії інформаційного

$$\text{права: } \frac{X}{Y} = \frac{N \xrightarrow{1} N \xrightarrow{2} N \xrightarrow{3}}{W \xrightarrow{1} W \xrightarrow{2}} \Rightarrow HT,$$

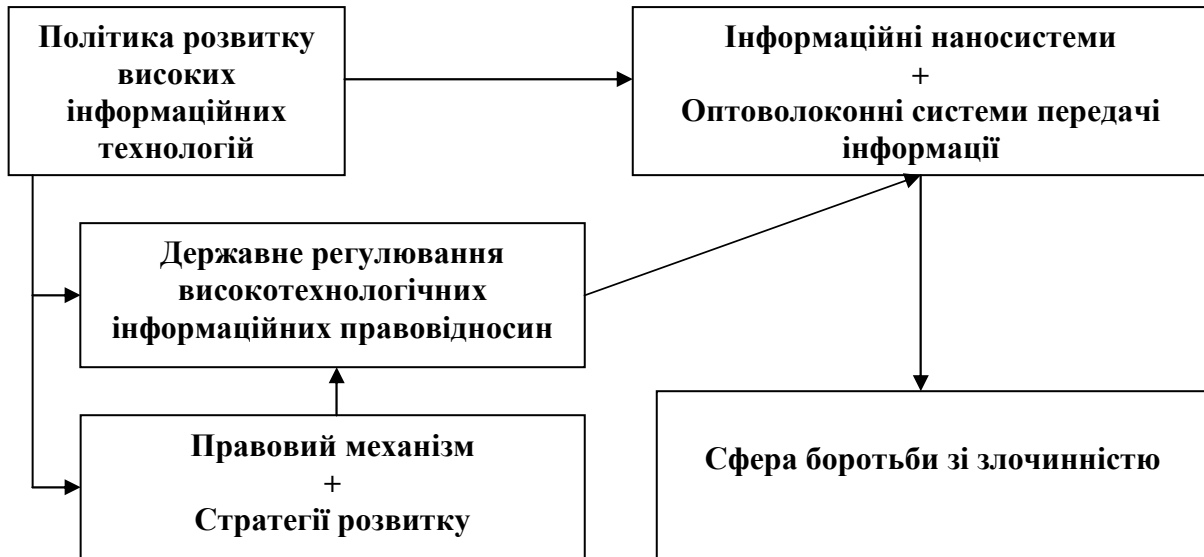
де електронне право високих технологій (X) виступає правовим регулятором суспільних відносин у цій сфері (Y), де новими об'єктами виступають нанонаука (N^1), нанотехнології (N^2) і наноіндустрія (N^3), детермінуючи особливий характер розвитку високотехнологічних інформаційних правовідносин (W^1), а звідси – становлення в рамках інформаційного права (W^2) як окремої теорії електронного права високих технологій (HT).

На завершення потрібно зазначити, що концептуалізація інформаційної політики у сфері боротьби зі злочинністю – це науково обґрунтована системна корінна видозміна об'єкту державного впливу на інноваційний процес програмної інформатизації з метою досягнення кінцевої мети – модернізації засобів антикримінального впливу відповідно з сучасними умовами інтелектуалізації злочинності.

На підставі системного аналізу наслідків дослідження, спробуємо схематично вивести формулу: $P = \frac{D}{L+R} S \sqrt{In + If}$, де P –

політика розвитку високих інформаційних технологій складається з D – державного регулювання високотехнологічних інформаційних правовідносин, L – правового механізму, R – стратегії розвитку, окремим напрямом чого виступає сфера боротьби зі злочинністю (S), модернізувати яку пропонується завдяки високотехнологічному прориву, а саме впровадження інформаційних наносистем (In) та оптоволоконних систем передачі інформації (If).

Логіка цих міркувань впливає із схематичної побудови:



КЛЮЧОВІ СЛОВА: Нанотехнологія, наноіндустрія, наноматеріали, нанороботи, нанохімія, криміналістична нанотехніка, судова експертиза, антикримінальні наносистеми.

ПІДСУМКОВІ ТЕСТИ РІЗНИХ РІВНЕЙ 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 й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості.

◆ **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) наноіндустрію;
- 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 у 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, обробка, творення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції.

◆ **Тест 6.** Архівна справа – це:

- а) збирання, обробка, творення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції;

б) збирання, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні 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 нагромадженням, обліком, зберіганням архівних документів та використанням відомостей, що в них містяться.

◆ **Тест 7.** Державна статистична діяльність – це:

а) як 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) розробку 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, обробки і передачі 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 аналізу її людиною й прийняття на його основі рішення на виконання будь-якої дії;

г) динамічна система інформаційних взаємодій суб'єкта з зовнішнім світом, у процесі чого відбувається створення образу, втілення його в об'єкті, здійснення й 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 правовою регуляцією 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 нанесення шкоди;
- в) стан захищеності приватних інтересів людини, при якому діє правовий механізм щодо запобігання нанесення шкоди;
- г) стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення 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 оголошеної інформації державою та її уповноваженими органами;
- б) набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошеної 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 оголошеної 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) розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошеної інформації;

г) набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошеної 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 визначеним 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 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 дозволу на заняття народною медициною (цілительством), виданого Міністерством охорони здоров'я України або уповноваженим ним органом, і повинна містити номер, дату видачі 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 й 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 є 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, збору даних профілактичних обстежень з метою 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 нових спеціальностей з урахуванням вимог міжнародних стандартів для кадрового забезпечення усіх напрямів інформатизації як 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, які підлягають статистичним спостереженням;
- б) оперативні дані органів, які згідно до законодавства 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 передачі даних;
- б) інформація, яка передається мережею передачі 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 обробки 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, які містять конфіденційну інформацію, що 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 передбачений 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, 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 у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту.

◆ **Тест 9.** Волоконно-оптичний зв'язок – це:

- а) передача інформації на значні відстані з більш високою швидкістю передачі даних, ніж в електронних засобах зв'язку, в тому числі надання широкого доступу в Інтернет;
- б) вид провідного електрозв'язку, що використовує як носій інформаційного сигналу електромагнітне випромінювання оптичного діапазону, а як напрямні системи – волоконно-оптичні кабелі;
- в) високотехнологічний вид системи бездротової передачі інформації;
- г) новий вид зв'язку, при якому інформація передається по оптичних діелектричних хвилеводах, відомим 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, що 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, які 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, установленого 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 заподіяння 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 заподіяння 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 заподіяння 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 заподіяння шкоди інтересам власника інформації та її неконтрольованому поширенню.

◆ **Тест 5.** Блокування інформації в системі – це:

а) дії, внаслідок яких унеможливується доступ до інформації в системі;

б) результат дій, внаслідок 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 обробки персональних даних, а також покладені обов'язки щодо їх захисту;

б) будь-які дії їх власника щодо обробки 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 обробки 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.** Сучасні напрямки розвитку нанотехнологій є:

а) розробка надпотужних інформаційних систем надмалих розмірів та пристроїв оптичного запису інформації;

б) розробка засобів протидії легалізації (відмивання) доходів, одержаних злочинним шляхом;

в) розробка нових психотехнологій гіпно-репродукційного опитування і нейролінгвістичного програмування;

г) розробка 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 є в основному ґрунтується на високих технологіях.

◆ **Тест 10.** Оптиковолоконна інформаційна технологія – це:

а) процес, що використовує сукупність засобів і методів збирання, обробки і передачі 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, схоронності, поширення (реалізації), захисту і відображення інформації за допомогою високотехнологічних інформаційних систем і волоконно-оптичних мереж передачі даних;

в) виробництво інформації для аналізу її людиною й 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 обробки 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.

© Синьокий О.В., 2010



ІНДИВІДУАЛЬНІ ЗАВДАННЯ



Завдання А. Підготуйте доповіді (реферати) з визначених тем:

- Тема 1. Система та джерела інформаційного права України.
- Тема 2. Основні засади розвитку інформаційного суспільства.
- Тема 3. Наука інформаційного права.
- Тема 4. Поняття та види інформаційної діяльності.
- Тема 5. Друковані засоби масової інформації (преса) в Україні.
- Тема 6. Правовий статус інформаційних агентств в Україні.
- Тема 7. Бібліотечна діяльність в Україні.
- Тема 8. Архівна діяльність в Україні.
- Тема 9. Телебачення, радіомовлення і кінематографія в Україні.
- Тема 10. Законодавство у сфері видавничої справи в Україні.
- Тема 11. Правове регулювання державної статистики в Україні.
- Тема 12. Рекламна діяльність в Україні.
- Тема 13. Електронний документообіг та правове регулювання телекомунікацій.
- Тема 14. Національна складова глобальної інформаційної мережі Інтернет.
- Тема 15. Основні засади політики розвитку високих технологій передачі інформації у сфері боротьби зі злочинністю.
- Тема 16. Правове регулювання інформаційних відносин у сфері високих технологій.
- Тема 17. Оптиволоконні інформаційні комунікації в системі правоохоронних органів України.
- Тема 18. Інформаційно-телекомунікаційна система органів прокуратури.
- Тема 19. Модернізація передачі інформації у сфері боротьби зі злочинністю.
- Тема 20. 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, коли 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. Складіть завершений інформаційний цикл за допомогою умовних переходів та продовження трьох спеціальних інформаційних груп: за режимом користування, за рівнем технологічності та за юридичним характером.

Задача 4. 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'єкту.

Задача 5. Визначте тип відношення між поняттями і зобразіть його за допомогою колових схем: а) «несанкціоноване втручання в роботу електронно-обчислюваних 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 6. 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-обчислюваних 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 інфраструктура.
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.

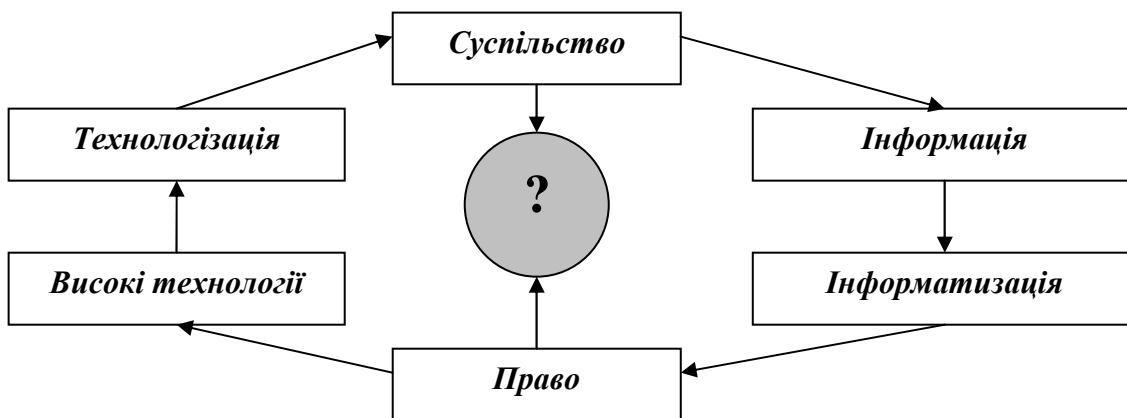
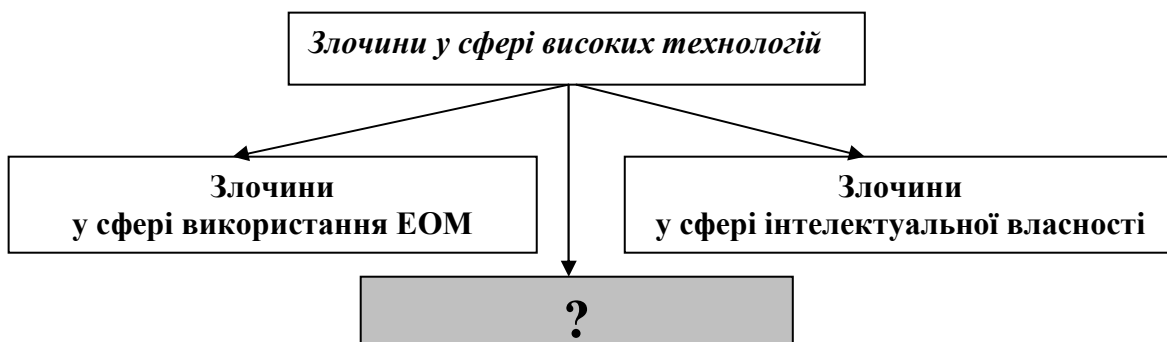


Схема 2.



 **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, зберігання, 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'єкту, 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 електров'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 права 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 інформаційній 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. В 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 обробки 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 у 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 Національній системі 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.



Контрольна група запитань № 1

1. Високотехнологічне інформаційне право як наука та навчальна дисципліна.
2. Місце інформаційного права в системі права України та його основні принципи.
3. Поняття, предмет і методи високотехнологічного інформаційного права.
4. Мета, завдання та функції високотехнологічного інформаційного права.
5. Поняття та основні напрями інформаційної діяльності.
6. Визначити різницю 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 рр.
10. Державна програма інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю.
11. Правовий зміст категорій «інформація», «інформатизація», «технологія» та «інформаційна технологія».
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 показники високотехнологічної злочинності.
19. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
20. Перспективи розвитку правових засад високих технологій в інформаційній галузі.



Контрольна група запитань № 2

1. Поняття, функції та види телекомунікацій.
2. Суб'єкти ринку телекомунікаційних послуг.
3. Національні інформаційні ресурси як основа для забезпечення суверенітету й інформаційної безпеки держави.
4. Інформаційні продукти у структура інформаційних ресурсів.
5. Поняття інформаційної системи, її види та компоненти.
6. Інформаційні процеси у сфері високих технологій.
7. Організаційно-правові засади використання електронних документів.
8. Оптичне волокно та оптоволоконно.
9. Правовий зміст поняття «оптоволоконна інформаційна технологія».
10. Поняття та види волоконно-оптичних мереж.
11. Визначити різницю поміж 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 в правоохоронній практиці.
14. Оптоволоконні системи передачі інформації як новий крок у мультимедійних технологіях зв'язку.

15. Правовий механізм волоконно-оптичних комунікацій.
16. Застосування волоконно-оптичних технологій передачі 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.



Контрольна група запитань №3

1. Визначити зміст поняття «модернізація».
2. Проблеми теорії інновацій та зміст інноватики у сфері діяльності органів, які ведуть боротьбу зі злочинністю.
3. Інновація інформаційної діяльності як процес та 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. Особливості використання в практиці розслідування злочинів нових інформаційних технологій з використанням поліграфу.
15. Програмне забезпечення експертно-криміналістичної діяльності.
16. Інформаційно-пошукові системи «Оперативно-довідкова картотека» і «Автоматизований банк даних».
17. Міжвідомчий банк даних «Наркобізнес» та інформаційні підсистеми «Арсенал», «Розшук» і «Пізнання».
18. Інформаційна правова база «Експерт» та АРМ слідчого.
19. Універсальна інтегрована інформаційна система «Портрет 4.3».
20. Оптико-електронний кабінет криміналістики.



Контрольна група запитань №4

1. Поняття системної інформатизації прокуратури, основні завдання та функції.
2. Органи прокуратури як спеціальні суб'єкти інформаційного права.
3. Архітектура 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».



Контрольна група запитань №5

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, інформаційні проблеми енергетичної безпеки 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 тунельних 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 та кібертероризмом.
20. Шляхи інноваційного розвитку нанотехнологій як антикримінальних метатехнологій XXI століття.

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 інформатики.
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 мультимедіа-технології.
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.
23. Органи прокуратури як спеціальні суб'єкти високотехнологічного інформаційного права.
24. 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.

© Синьокий О.В., 2010

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Абрамчук, Н. С. Нанотехнологии. Азбука для всех : [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 : [учебник] / Е. Т. Аксенов ; Санкт-Петербургский гос. политехнический ун-т. – Санкт-Петербург : 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 : [монография] / Ю. Альтман ; (пер. с англ.). – М. : Техносфера, 2006. – 421 с.
4. Ананян, М. Опыт преодоления / М. Ананян // Вестник инноваций. – № 1 (2). – январь 2005 г. <http://www.tpprf.ru/img/uploaded/2005022114594983.doc>
5. Андрианов, С. Н. Волоконно-оптические системы / С. Н. Андрианов, С. О. Мирумянц, Л. А. Трофанчук // Оптический журнал. – 1997. – Том 64. – С. 102.
6. Андрианов, С. Н. Волоконно-оптические системы технического зрения для применения в науке, промышленности и делопроизводстве / [С. Н. Андрианов, В. А. Зуйков, А. А. Калачев, В. С. Максимюк, С. О. Мирумянц, В. В. Самариев, Л. А. Трофанчук, А. М. Шегеда] // Известия Российской академии наук. – 2002. – Том 66. – №3. – С. 369-372.
7. Арістова, І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади : автореф. дис. ... докт. юрид. наук ; 12.00.07 – адміністративне право і процес, фінансове право, інформаційне право. / І. В. Арістова ; Національний університет внутрішніх справ. – Харків : НУВС, 2002. – 39 с.
8. Аркуша, Л. І. Проблеми взаємодії та інформаційного забезпечення правоохоронних органів у боротьбі з економічною організованою злочинною діяльністю / Л. І. Аркуша // Інформаційне забезпечення протидії організованим злочинностям / [Збір. наук. статей] ; 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 постнеклассической науки : автореф. дис. докт. 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 : [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 / Н. Ахтирська, В. Антошук // Вісник прокуратури. – 2008. – №3. – С. 84-94.
12. Ашурбеков, Т. Правовой мониторинг угроз национальным интересам / Т. Ашурбеков // Законность. – 2007. – №5. – С. 47-50.
13. Бабаев, Д. Ю. Акмеологический мониторинг как средство обеспечения качества подготовки кадров управления : 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 / А. Д. Бавижев, В. В. Кореньков // Сообщения объединенного института ядерных исследований. – Дубна, 1988. – С. 1.
15. Баган В. А. Наноструктурные волоконные температуры для активных и нелинейных применений / В. А. Баган, Ю. К. Чаморовский, С. А. Никитов, О. Г. Охотников // [newrusnano.explosion.ru/sadm_files/disk/Docs/3/2/2%20\(4\).pdf](http://newrusnano.explosion.ru/sadm_files/disk/Docs/3/2/2%20(4).pdf)

16. Балабанов, В. Нанотехнологии. Наука будущего : [фантастические возможности ближайшего будущего] / В. Балабанов. – М. : Эксмо, 2009. – 246, [1] с.
17. Бандурин, С. Г. АРМ руководителя следственного подразделения. АРМ следователя : [методическое 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 : [навчальний посібник] / О. А. Баранов. – К. : Видавничий дім «СофтПрес», 2005. – 316 с.
19. Бачило, И. Л. Информационное право : [учебник для вузов] : (специальный курс) / И. Л. Бачило ; Ин-т государства и права Российской академ. 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 : [монографія] / М. С. Вертузаєв, В. О. Голубєв, О. І. Котляревський, О. М. Юрченко / Під ред. О. П. Снігерьова. – Запоріжжя : ПВКФ «Павло», 1998. – 316 с.
21. Березиков, С. Перспективы технологии «волокно в дом» для строительства сетей КТВ / С. Березиков, Б. Рябов, В. Чулком, С. Песков // ТелеМультиМедиа. – 2002. – №3. – С. 4-10.
22. Беляков, К. І. Питання визначення правопорушень, що вчинюються з використанням інформаційних технологій: аксіоматичний підхід / К. І. Беляков // http://mndc.naiu.kiev.ua/Gurnal/9text/g9_20.htm.
23. Богущ, В. М. Інформаційна безпека держави : [навчальний посібник] / В. М. Богущ, О. К. Юдін. – М. : «МК-Прес», 2005. – 432 с.
24. Богуцький, О. Щодо проблем правового визначення суб'єктів телекомунікаційних послуг / О. Богуцький // Право України. – 2006. – №6. – С. 72-76.
25. Бутузов, В. М. Злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : [науково-практичний коментар] / В. М. Бутузов, С. Л. Остапєць, 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 / 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: 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 / В. Б. Вейнберг // Оптико-механическая промышленность. – 1967. – №11. – С. 48-51.
29. Вертузаєв, М. С. Внимание, вас слушают ... : обзор рынка приборов, выявляющих прослушивание телефонных переговоров / М. С. Вертузаєв, А. М. Вертузаєв // Бизнес и безопасность. – 2002. – №4. – С. 50-51.
30. Вертузаєв, М. С. Реальности виртуального терроризма: Нью-Йорк, Киев, Одесса ... далее везде? / М. С. Вертузаєв // Бизнес и безопасность. – 2002. – №2. – С. 19-22.
31. Власов, А. А. Актуальные проблемы прокурорского реагирования на нарушения прав личности в сети Интернет / А. А. Власов, Т. П. Кесарева // Российский следователь. – 2000. – №5. – С. 2-4.
32. Военные нанотехнологии : возможности применения и превентивного контроля вооружений : [учебное пособие] / Ю. Альтман ; [пер. с англ. А. В. Хачояна]. – М. : Техносфера, 2006. – 421 с.

33. Волков, С. В. Нанохімія. Наносистеми. Наноматеріали. : [монографія] / [С. В. Волков, С. П. Ковальчук, В. М. Огенко, О. В. Решетняк] ; 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 практики організації оперативно-розшукової діяльності / 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 : 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» / К. С. Герасименко // Форум права. – 2009. – № 3. – С. 162-166 [Електронний ресурс]. – Режим доступа: <http://www.nbuv.gov.ua/e-journals/FP/2009-3/09covcrk.pdf>.
37. Годунов, И. В. Транснациональная организованная преступность в России : Пути и формы противодействия : дисс. ... докт. 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 : [учебник] / Ю. И. Головин. – М. : Машиностроение, 2007. – 493 с.
39. Городов, О. А. Информационное право : [учебник] / О. А. Городов. – М. : Проспект, 2009. – 242 с.
40. Горшенков, Г. Н. К понятию «информационная преступность» / Г. Н. Горшенков // Российский криминологический взгляд. – 2005. – №4. – С. 93 – 96.
41. Гриценко, В. Суспільство в інформаційну епоху: реалії і перспективи розвитку / В. Гриценко // Вісник Національної академії наук України. – 2005. – №6. – С. 28-32.
42. Гуляев, Ю. В. Стандарты информационных и нанотехнологий: проблемы и решения / Ю. В. Гуляев // Проблемы теории и практики управления. – 2008. – №10. – С. 8-16.
43. Гуцалюк, М. Протидія правопорушенням у мережі Інтернет / М. Гуцалюк // Вісник прокуратури. – 2002. – № 6. – С. 98 – 101.
44. Данилина, Е. А. Правовые и технологические проблемы создания и функционирования электронных библиотек / Е. А. Данилина, А. Б. Антопольский, Т. С. Маркарова. – М. : ИНИЦ «Патент», 2008. – 207 с.
45. Денісова, О. О. Інформаційні системи і технології в юридичній діяльності : [навч.-метод. посібник] / О. О. Денісова ; Київський національний економічний ун-т — К. : КНЕУ, 2005. – 256 с.
46. Державна програма інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю / Затвержена Постановою Кабінетом 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>].
47. Державна політика у сфері запобігання тероризму : міжнародний досвід і його актуальність для України : [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 / <http://www.mon.gov.ua/development/programs.doc>.
49. Джавадов, Ф. М. Экспертная деятельность и развитие науки судебной экспертизы / Ф. М. Джавадов. – Баку : Элм, 1998. – 187 с.

50. Дианов, Е. М. Волоконно-оптическая связь и ее роль в современном обществе / Е. М. Дианов, А. М. Прохоров // Вестник Российской академии наук. – 2002. – Том 72. – №6. – С. 483-486.
51. Дианов, Е. М. От тера-эры к пета-эре / Е. М. Дианов // Вестник Российской академии наук. – 2000. – №1. – С. 1010.
52. Дробатухин, В. С. Кибернетическое моделирование при расследовании преступлений : 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 : 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. – Санкт-Петербург, 2008. – 18 с.
54. Економіка та організація інноваційної діяльності : [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 : [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 / Е. А. Жигалов // Известия Алтайского государственного университета. – 2000. – № 2 (16). – С. 35-38.
57. Жигулин, Г. П. Информационная безопасность : [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. Жилиев, А. И. Криминологические аспекты информационной преступности / А. И. Жилиев, С. Н. Данилин // [http://www.cir.nnov.ru/pages/issues/vestnik/99990195_West_pravo_2003_2\(7\)/B_3-7.pdf](http://www.cir.nnov.ru/pages/issues/vestnik/99990195_West_pravo_2003_2(7)/B_3-7.pdf)
59. Загородній, А. Грід – нова інформаційно-обчислювана технологія для науки / А. Загородній, Г. Зінов'єв, Є. Мартинов, С. Свистунов, В. Шадура // Вісник Національної академії наук України. – 2005. – №6. – С. 17-25.
60. Загородній, В. Застосування сучасних інформаційних технологій у діяльності прокуратури Одеської області / В. Загородній, А. Іщенко // Вісник прокуратури. – 2006. – №6. – С. 116-120.
61. Загоруйко, Н. Г. Информационные технологии в генетике / Н. Г. Загоруйко, А. Г. Пичуева, О. А. Кутненко [и др.] // Информационные системы и технологии ИСТ-2003 : Труды Междунар. научн-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 : [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 точной механики и оптики. – Л. : МИПК при ЛИТМО, 1990. – 32 с.
63. Зайчук, О. В. Теорія держави і права. Академічний курс : [підручник] / О. В. Зайчук (ред.), А. П. Заєць, В. С. Журавський, О. Л. Копиленко, Н. М. Оніщенко (ред.). – 2-ге вид., переробл. і доп. – К. : Юрінком Інтер, 2008. – 688 с.
64. Закон України «Про спеціальний режим інноваційної діяльності технологічних парків» від 16 липня 1999 р. // Відомості Верховної Ради України. – 1999. – № 40. – Ст. 362.
65. Закон України «Про прокуратуру» від 5.11.1991 р. // Відомості Верховної Ради України. – 1991. – № 53. – Ст. 793.

66. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 25.03.1994 р. // Відомості Верховної Ради України. – 1994. – №31. – Ст. 286.
67. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – №48. – Ст. 650.
68. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. // Відомості Верховної Ради. – 2003. – № 36. – Ст. 275.
69. Закон України «Про телекомунікації» від 18 листопада 2003 року // Відомості Верховної Ради. – 2004. – № 12. – Ст. 155.
70. Закон України «Про Національну програму інформатизації» від 04.02.1998 р. // Відомості Верховної Ради. – 1998. – № 27-28. – Ст. 181.
71. Закон України «Про науково-технічну інформацію» від 25 червня 1993 р. // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.
72. Закон України «Про електронний цифровий підпис» від 22 травня 2003 р. // Відомості Верховної Ради. – 2003. – № 36. – ст. 276.
73. Закон України «Про наукову і науково-технічну експертизу» // Відомості Верховної Ради. – 1995. – № 9. – Ст. 56.
74. Закон України «Про судову експертизу» // Відомості Верховної Ради. – 1994. – № 28. – Ст. 232.
75. Захаров, В. П. Вдосконалення організації захисту інформації від несанкціонованого доступу / 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 : [методические рекомендации 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) : [монография] / Е. В. Иванова. – М. : ВЗФЭИ, 2009. – 170 с.
78. Інструкція про порядок функціонування дактилоскопічного обліку експертної служби МВС України / Затверджена наказом МВС України від 19.09.2001 р. № 785 // [<http://licasoft.com.ua/component/lica/?base=1&id=819586>].
79. Информатика : [учебник] / Под ред. проф. Н. В. Макаровой. – М. : Финансы и статистика, 2001. – 768 с.
80. Информационно-аналитическое обеспечение раскрытия и расследования преступлений правоохранительными органами : [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 / [отв. ред.: С. Ю. Малков, А. В. Коротяев]. – М. : КомКнига, 2005. – 184 с.
82. Калитич, Г. І. Творчість – стратегічна парадигма інноваційного розвитку / Г. І. Калитич, В. Я. Рубан // Науково-технічна інформація. – 2003. – №2. – С. 29-34.
83. Капани, Н. С. Волоконная оптика : принципы и применения : [монография] / Н. С. Капани ; [перевод с англ. под ред. В. Б. Вейнберга и Д. К. Саттарова]. – М. : Мир, 1969. – 464, [2] с.
84. Караулова, Ю. А. Правовое регулирование авторских прав в глобальном информационном пространстве (сравнительный анализ правоприменительной практики) : автореф. дис. ... канд. юрид. наук : 12.00.14 – административное право; финансовое право; информационное право) / Ю.А. Караулова ; Международный институт управления Московского

государственного института международных отношений (Университет) МИД РФ. – М. : МГИМО, 2009. – 24 с.

85. Каркач, П. М. Органи прокуратури України : [навчально-методичний посібник] / П. М. Каркач, С. М. Іванов. – Харків : СПД ФО Вапнярчук Н. М., 2007. – 360 с.

86. Карпенков, С. Х. Современные средства информационных технологий : [учебное пособие] / С. Х. Карпенков. – М. : КноРус, 2009. – 399, [1] с.

87. Карпусь, А. Інформатизація органів прокуратури: стан і перспективи / А. Карпусь // Право України. – 2007. – №6. – С. 89-90.

88. Карчевський, М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : автореф. дис. канд. юрид. наук: 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. / М. В. Карчевський ; Луганська академія внутрішніх справ МВС імені 10-річчя незалежності України. – Луганськ, 2002. – 22 с.

89. Кастельс, М. Информационная эпоха : Экономика, общество и культура / 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 : 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] : навч. посібник / Н. І. Клименко. – К. : Вид. Дім «Ін Юре», 2007. – 528 с.

92. Колдин, В. Я. Информационные процессы и структуры в криминалистике / В. Я. Колдин, Н. С. Полевой. – М. : Изд-во МГУ, 1985. – 133 с.

93. Колпаков, С. А. Организационно-правовые вопросы обеспечения информационной безопасности : [учебное 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 // Вісник Національної академії наук України. – 2009. – №6. – С. 27-31.

96. Копелев, І. Ю. Інформаційні загрози: суть і проблеми / І. Ю. Копелев // 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: автореф. дис... докт. юрид. наук: 12.00.07 – адміністративне право і процес, фінансове право, інформаційне право. / Б. А. Кормич ; Національний університет внутрішніх справ МВС України. – Харків, 2004. – 41 с.

98. Котлер Ф. Маркетинг. Загальний курс. – 5-те вид. : [навчальний посібник]. / Філіп Котлер, Гарі Армстронг ; пер. з англ. – М. : Видавничий дім «Вільямс», 2007. – 608 с.

99. Котляр В. В. Нанопотоника – манипулирование светом с помощью наноструктур / 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 / О. Кохановська // Підприємництво, господарство і право. – 2004. – №12. – С. 144-147.
101. Кохановська, О. В. Форми захисту інформаційних прав у доктрині і законодавстві України / 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 : 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 / 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.) // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.
105. Криминология : [учебник для студентов высших учебных заведений, обучающихся по специальности «Юриспруденция»] / [С. В. Ванюшкин, Ю. В. Ващенко, А. Я. Гришко, Ю. Н. Демидов 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: 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 / 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 : [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 / М. Куршев // Уголовное право. – 2003. – № 4. – С. 124 – 126.
110. Лаврик, О. Л. Академическая библиотека в современной информационной среде / О. Л. Лаврик. – Новосибирск : ГПНТБ СО РАН, 2003. – 250 с.
111. Лебедев, О. Волоконно-оптические компьютерные сети доступа / 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» / В. І. Лебеденко // Науковий вісник Національної академії внутрішніх справ України : [Науково-теоретичний журнал. Частина 2.] – К: НАВСУ, 2000. – № 1. – С. 46–56.
113. Леонтьева, Л. С. Синергетический контекст масс-медийного становления / 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) / 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 / Г. Л. Лисенко, С. Є. Тужанський, Осам Ф Ф Абудайя // Вісник Вінницького політехнічного інституту. – 2005. – №2. – С. 69-76.
116. Логінов, О. В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : автореф. дис. ... канд. юрид. наук: 12.00.07 – адміністративне право і процес,

фінансове право, інформаційне право. / О. В. Логінов ; Національна академія внутрішніх справ України. – Київ, 2005. – 22 с.

117. Лукашевич, В. Г. Криміналістика як інтегрована наукова дисципліна / 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. I. – С. 139-141.

118. Мазур, И. И. Управление проектами : [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 / А. В. Макиенко, А. В. Борбат // Российский следователь. – 2004. – № 12. – С. 29–35.

120. Мартинес-Дуарт, Дж. М. Нанотехнологии для микро- и оптоэлектроники / 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 : [навчальний посібник] / А. І. Марущак. – К. : Видавничий дім «Скіф», КНТ, 2008. – 344 с.

122. Марущак, А. І. Правові основи захисту інформації з обмеженим доступом : [курс лекцій] / А. І. Марущак. – К. : КНТ, 2007. – 208 с.

123. Межуев, В. М. Ценности современности в контексте модернизации и глобализации / В. М. Межуев // Знание. Понимание. Умения : [электронный журнал]. – 2009. – №1. [<http://www.zpu-journal.ru/e-zpu/2009/1/Mezhuev>].

124. Мірошніченко, М. Системно-інформаційний підхід у контексті методологічного забезпечення наукового аналізу проблем теорії правової системи України / М. Мірошніченко // Право України. – 2007. – №6. – С. 22-25.

125. Михальчук, Т. В. Напрямки використання телекомунікаційних технологій у правоохоронній сфері / 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 / 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 : автореф. дис. ... канд. юрид. наук: 12.00.09 – кримінальний процес та криміналістика; судова експертиза. / О. І. Мотлях ; Академія адвокатури України. – Київ, 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» // 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 № 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 : [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) : [научно-методическое 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 : [навч. посібник] / І. Ш. Невлюдов, Б. О. Малик, М. А. Омаров, О. М. Цимбал ; 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 / В. Ніндипова // Вісник прокуратури. – 2007. – № 2. – С. 52–60.
135. Новая криминальная ситуация : оценка и реагирование / 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 // Постановление Правительства РФ от 22.04.2009 г. №30. <http://www.russianpeople.ru/en/old/135629>.
137. Овчинский, А. С. Информация и оперативно-розыскная деятельность : [монография] / А. С. Овчинский ; Моск. ин-т МВД России. – М. : Инфра-М, 2002. – 95, [2] с.
138. Овчинский, А. С. Правоохранительные инфотехнологии : [научный доклад] / А. С. Овчинский. – М. : Норма, 2009 (Казань : ПИК Идел-Пресс). – 142 с.
139. Оглоблин С. И. Инструментальная «детекция лжи»: [академический курс] / С. И. Оглоблин, А. Ю. Молчанов. – Ярославль : Ньюанс, 2004. – 464 с.
140. Одрін, В. Технологія наукової і технічної творчості : нова наука та високоінтелектуальна інформаційна метатехнологія / В. Одрін // Вісник Національної академії наук України. – 2005. – №6. – С. 43-64.
141. Оліфіренко, М. М. Новітні інформаційні технології як інструмент міжнародного тероризму : [аналіт. нотатки] / М. М. Оліфіренко. – К. : МаНІ, 2004. – 75 с.
142. Оптическая связь : [Перевод с японского И. А. Фомичева / под ред. И. И. Теумина]. – М. : Радио и связь, 1984. – 384 с.
143. Організаційно-правові основи захисту інформації з обмеженим доступом : [навчальний посібник] / 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 : [науково-практичний посібник] / 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 : автореф. дис. ... канд. юрид. наук ; 12.00.08 – кримінальне право та криминологія; кримінально-виконавче право. / С. О. Орлов ; Національний університет внутрішніх справ. – Харків : НУВС, 2004. – 20 с.
146. Оружие России : Федеральный электронный справочник вооружения и военной 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 року № 537 // Відомості Верховної Ради України – 2007. – №12. – Ст. 102.
148. Основи інформаційного права України : [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 : 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. – Санкт-Петербург, 2008. – 20 с.

150. Пастухов, О. М. Авторське право у сфері функціонування всесвітньої інформаційної мережі Інтернет: 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 / Б. Патон, В. Москаленко, І. Чекман, Б. Мовчан // Вісник Національної академії наук України. – 2009. – №6. – С. 18-26.

152. Петров, Є. В. Інформація як об'єкт правовідносин / Є. В. Петров // Вісник Національного університету внутрішніх справ; Спецвипуск. – Х., 2001. – С. 249-252.

153. Пиявский, С. Информатизация сферы культуры и молодежной политики / 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 / М. А. Погорецький // Вісник Верховного Суду України. – 2003. – № 2. – С. 36–39.

155. Погосов, В. В. Введение в физику зарядовых и размерных эффектов. Поверхность, кластеры, низкоразмерные системы : [учебное пособие]. – М. : Физматлит, 2006. – 328 с.

156. Покутний, С. И. Оптика наносистем : [монография] / С. И. Покутний, В. А. Сминтина, А. П. Шпак, В. М. Уваров. – Одесса : Астропринт, 2007. – 304 с.

157. Политология : [учебник] / под ред. В. И. Буренко, В. В. Журавлева. – М. : Экзамен, 2004. – 320 с.

158. Положение о методах и способах защиты информации в информационных системах персональных данных : Приложение к Приказу Федеральной Службы по техническому и экспортному контролю РФ (2010) //www.ispdn.ru/news/detail_industry.php?ELEMENT_ID=5397.

159. Полотнянко, Л. И. Современные высокие технологии и автоматизированные системы в лабораторной службе : [учебное пособие] / Л. И. Полотнянко. – М. : ВУНМЦ Росздрава, 2008. – 361 с.

160. Полякова, М. В. Шляхи вирішення проблеми пошуку графічної інформації на персональному комп'ютері / 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 : [учебное 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 / 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 року «Про дотримання законодавства щодо розвитку науково-технічного потенціалу та інноваційної діяльності в Україні» // 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» // 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» // 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» // *Офіційний вісник України*. – 2005. – № 31. – Том 2. – Ст. 1869.

167. Постанова Кабінету Міністрів України від 9 серпня 2005 р. №720 «Про затвердження Правил надання та отримання телекомунікаційних послуг» // *Офіційний вісник України*. – 2005. – № 32. – Ст. 1935.

168. Постиндустриальная цивилизация и культура управления : [монография] / [В. Е. Амелин и др.; под общ. ред. Г. Я. Узилиевского]. – Орел : Изд-во ОРАГС, 2005. – 247 с.

169. Проект Закону України «Про інформацію» (2007) // narodna.prawda.com.ua/politics/46b39475d80f0/.

170. Про кібернетичну злочинність : Конвенція Ради Європи ; [офіційний переклад українською мовою] // 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) : [учебное пособие] / А. Н. Прокопенко, А. А. Кривоухов. – Белгород : Изд-во БелГУ, 2007. – 220, [1] с.

172. Прокуратура України : Академічний курс : [підручник] / В. В. Сухонос, В. П. Лакизюк, Л. Р. Грицаєнко, В. М. Руденко; За заг. ред. В. В. Сухоноса. – Суми : ВТД «Університетська книга», 2005. – 566 с.

173. Прослушивание телефонов в международном праве и законодательстве одиннадцати европейских стран / 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 / Розпорядження Кабінету Міністрів України від 19 вересня 2007 року № 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. / Розпорядження Кабінету Міністрів України від 3 квітня 2009 року № 331-р // *Офіційний вісник України*. – №26. – 2009 (17.04.2009).

176. Пул, Ч. Нанотехнологии. / Ч. Пул, Ф. Оуэне. – М. : Техносфера, 2006. – 260 с.

177. Ратнер, М. Нанотехнология : простое объяснение очередной гениальной идеи = Nanotechnology : A Gentle Introduction To The Next Big Idea : Пер. с англ. / Марк Ратнер, Даниэль Ратнер ; [перевод и редакция А. В. Назаренко]. – М. : Издательский дом «Вильямс», 2004 ; Москва – Санкт-Петербург – Киев, 2007. – 240 с.

178. Розенфельд, Н. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів) / Н. Розенфельд // *Вісник прокуратури*. – 2002. – №4. – С. 23-27.

179. Рудейчук, В. Суть прокурорського нагляду / 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 / 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 : 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 / М. Я. Сегай // *Вісник Академії правових наук України*. – 2001. – №4. – С. 191.

183. Симоненко, Т. В. Інформаційне забезпечення пріоритетних напрямів інноваційної діяльності в Україні / Т. В. Симоненко // *Бібліотечний вісник*. – 2003. – № 5. – С. 20-22.

184. Симоненко, Т. В. Проект «відкритого доступу» – портал «Наукова періодика України» / Т. В. Симоненко // *Бібліотечний вісник*. – 2009. – № 1. – С. 3-6.
185. Синеокий, О. В. Адвокатура как институт правовой помощи и защиты : [учебное пособие] / О.В. Синеокий : [передм. проф. д.ю.н. Т. О. Коломоец]. – Харьков : Право, 2008. – 496 с.
186. Синеокий, О. В. Інформаційні технології криміноперверсологічного моніторингу : інноваційний підхід розвитку / О. В. Синеокий // *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.
187. Синеокий, О. В. Інформаційне право України : інформаційно-телекомунікаційні технології в прокурорській діяльності : [навчальний посібник] / О. В. Синеокий. – Запоріжжя : ЗНУ, 2009. – 191, [3] с.
188. Синеокий, О. В. Інформаційне право України : [навч. посібник] / О. В. Синеокий. – Запоріжжя : ЗНУ, 2008. – 100 с.
189. Синеокий, О. В. Міждержавні спеціалізовані слідчо-оперативні групи : окремі психолого-організаційні проблеми / О. В. Синеокий // *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 / О. В. Синеокий // *Уголовное право*. – Москва : [Академия Генеральной прокуратуры РФ]. – 2009. – №2. – С. 115–121.
191. Синеокий, О. В. Мониторинг транснациональной педофилии / О. В. Синеокий // *Психопедагогика в правоохранительных органах*. – Омск : [Омская академия МВД России]. – 2009. – №3. – С. 34-39.
192. Синеокий, О. В. Нанонаука – розвитку судово-експертних технологій / О. В. Синеокий // *Вісник Запорізького національного університету* : [збір. наук. стат.] / юридичні науки. – Запоріжжя, 2009. – №2. – С. 137-142.
193. Синеокий, О.В. Нанотехнологічні методики виявлення латентних слідів та дослідження мікрооб'єктів – криміналістичні інновації майбутнього / О.В. Синеокий // «Держава і право : De Lege Praeterita, Instante, Futura» [матеріали Міжнародна науково-практична конференція «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 / О. В. Синеокий // *Региональный вестник Востока*. – Усть-Каменогорск : [Восточно-Казахстанский государственный университет]. – 2008. – № 3. – С. 31-37.
195. Синеокий, О.В. Організаційно-правові й медико-психологічні особливості одержання оперативної інформації спеціалізованою слідчо-оперативною групою з розслідування серійних сексуальних убивств за допомогою поліграфу та під гіпнозом / О.В. Синеокий // *Вісник Донецького національного університету* : [серія В. Економіка і право]. – Донецьк, 2008. – №2. – С. 330-338.
196. Синеокий, О. В. «Охотники за маньяками» : организационно-психологическая модель специализированной следственно-оперативной группы как инновационной антикриминальной институции / О. В. Синеокий // *Вісник Донецького національного університету* : [серія В. Економіка і право]. – Донецьк, 2009. – №1. – С. 452-458.
197. Синеокий, О. В. Перспективи впровадження волоконно-оптичних технологій в інфокриміналістику прокурорської діяльності / О.В. Синеокий // *Проблеми удосконалення*

законодавства і практики протидії злочинності у сфері господарської діяльності : [Збірник наукових 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.

198. Синеокий, О. В. Проблеми моніторингу сексуальної агресії та криміноперверсологічний контроль соціально небезпечних статевих аномалій / О. В. Синеокий // Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах : [матеріали Всеукраїнської науково-практичної конференції] / Запорізький юридичний інститут ДДУВС (м. Запоріжжя, 31 жовтня 2008 р.) : [у 2 ч.] – Запоріжжя : ЗЮІ ДДУВС, 2008. – Ч. II. – С. 140–143.

199. Синеокий, О. В. Прокуратура України як контрольно-наглядова інституція у сфері боротьби зі злочинністю. Психологія прокурора-криміналіста : [навчальний посібник з психологічним словником прокурора-криміналіста] / О. В. Синеокий. – Запоріжжя : ЗНУ, 2009. – 263, [2] с.

200. Синеокий, О. В. Прокурорський моніторинг. Проблеми теоретичного визначення в юридичній психології / О. В. Синеокий // Реформування сучасної правової системи : [Збірник тез Міжнародної науково-практичної конференції студентів, аспірантів і молодих учених] ; (м. Донецьк, 10-11 квітня 2009 р.) – Донецьк : ДонНУ, 2009. – С. 102-104.

201. Синеокий, О. В. Психологічні аспекти прокурорського нагляду за забезпеченням законності слідчо-оперативної діяльності. Досвід прокурора-криміналіста (за матеріалами умисних убивств) : [монографія] / О. В. Синеокий ; [передмова – прокурор Запорізької області, державний радник юстиції 3 класу, канд. юрид. наук В. В. Кулаков]. – Запоріжжя : ЗНУ, 2009. – 445, [2] с.

202. Синеокий, О. В. Психолого-правові проблеми кримінальної сексопатології. Вступ до криміноперверсології : [монографія] / О. В. Синеокий ; [передм. докт. юрид. наук О. О. Дудорова]. – Харків : Право, 2009. – 752 с.

203. Синеокий, О. В. Психологічні особливості управління міжвідомчими слідчо-оперативними групами / О. В. Синеокий // Вісник прокуратури. – К., 2008. – №3. – С. 72–80.

204. Синеокий, О. В. Психологічні проблеми прийняття рішень слідчо-оперативною групою / О. В. Синеокий // Науковий вісник Дніпропетровського державного університету внутрішніх справ : [збір. наук. статей]. – Дніпропетровськ, 2008. – №3. – С. 272-278.

205. Синеокий, О. В. Психологічні технології щодо вирішення групових завдань в професійній діяльності міжвідомчих слідчо-оперативних груп / О. В. Синеокий // Психологические технологии в экстремальных видах деятельности : [материалы IV Международной научно-практической конференции] / Донецкий юридический институт ЛГУВД им. Э.А. Дидоренко ; (г. Донецк, 22-23 мая 2008 г.). – Донецк : ДонЮИ ЛГУВД им. Э.А. Дидоренко. – С. 126–127.

206. Синеокий, О. В. Системні медико-психологічні підходи до мінімізації патосексуальних проявів в інтернет-просторі / О. В. Синеокий // Психологія і суспільство. – Тернопіль, 2009. – №2. – С. 122–127.

207. Синеокий, О. В. Системні інформаційно-правові та медико-педагогічні заходи профілактики «фонових» явищ патосексуальної віктимізації молоді / О. В. Синеокий // Вісник Запорізького національного університету : [збір. наук. стат.] / педагогічні науки. – Запоріжжя, 2009. – №1. – С. 140-146.

208. Синеокий, О. В. Системні організаційно-інформаційні проблеми діяльності міждержавних змішаних спеціалізованих слідчо-оперативних груп в сучасних умовах / О. В. Синеокий // Міжнародна науково-практична конференція «Четверті Прибузькі юридичні читання» : «Сучасний вимір держави та права» [збірник наук. статей] ; (м. Миколаїв, 29 листопада 2008 р.) / за ред. В.І. Терентьева та О.В. Козаченка ; [Одеська національна юридична академія]. – Миколаїв : Ілліон, 2008. – С. 137-139.

209. Синеокий, О. В. Стратегії інноваційного проектування волоконно-оптичних технологій в криміналістиці / О. В. Синеокий // 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. I. – С. 162–165.

210. Синеокий, О. В. Теоретичні та практичні проблеми діяльності міждержавних змішаних слідчо-оперативних груп / О. В. Синеокий // Криміналістичний вісник / НДЕКЦ МВС України. – 2009. – № 1(11) – С. 44-51.

211. Системна інформатизація законотворчої та правоохоронної діяльності : [монографія] / [В. Буржинський, Б. Раціборинський, М. Целуйко, В. Хахановський та ін.; кер. авт. кол. Швець М. Я. ; За ред. В. В. Дурдинця]. – К. : Навч. книга, 2005. – 639 с.

212. Системна інформатизація правоохоронної діяльності : [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 / Г. В. Семенов. – М. : Юрлитинформ, 2008. – 333, [3] с.

214. Сергеев, Г. Б. Нанохимия : [учебное пособие] / Г. Б. Сергеев. – М. : Изд-во МГУ, 2003. – 288 с.

215. Серета, Г. Концептуальні засади наукового забезпечення інформатизації прокуратури / Г. Серета, І. Рогатюк, В. Цимбалюк // Вісник прокуратури. – 2006. – №5. – С. 14-19.

216. Скалозуб, Л. П. Інтелектуалізація злочинності. Варіант стримування / [Л. П. Скалозуб, В. М. Бутузов] // Боротьба з організованою злочинністю і корупцією. – 2004. – №9. – С. 193–198.

217. Словник термінів інформаційного права / 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» / В. Спирин // ТелеМультиМедиа. – 2002. – №3. – С. 11-14.

219. Стратегії економічного розвитку в умовах глобалізації : монографія / Б. В. Губський, Т. Т. Ковальчук, А. М. Поручник, Л. Л. Антонюк та ін.; За ред. д-ра екон. наук, проф. Д. Г. Лук'яненка. – К. : КНЕУ, 2001. – 538 с.

220. Стрельбицький, М. Нанотехнології в Україні як засіб боротьби з міжнародним тероризмом / 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 / В. С. Суходубов // Слідча практика України: із досвіду слідчої роботи органів прокуратури прокуратури [Східно-регіональний центр гуманітарно-освітніх ініціатив]. – 2003. – №3. – С. 44-47.

222. Сухонос, В. В. Прокуратура України у схемах, таблицях і діаграмах : [навчальний посібник] / В. В. Сухонос, О. Э. 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 / М. Требін // Віче. – 2002. – №4 (121). – С. 64-68.

224. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дисс. ... 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» // 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 // Офіційний вісник України. – 2006. – №5. – Ст. 212.

228. Фостер, Л. Нанотехнологии. Наука, инновации и возможности / Л. Фостер ; [пер. с англ. А. Хачояна]. – М. : Техносфера, 2008. – 349 с.

229. Фріс П. Л. Кримінально-правова політика України: автореф. дисс. ... д-ра юрид. наук : 12.00.08 – кримінальне права та кримінологія; кримінально-виконавче право. / П. Л. Фріс. – Київ, 2005. – 36 с.

230. Фролков, В. Н. Разработка специальных типов оптических волокон для систем управления : автореферат дис. ... канд. техн. наук : 05.11.07 – оптические и оптико-электронные приборы и комплексы. / В. Н. Фролков ; С.-Петербург. гос. ун-т информац. технологий, механики и оптики. – Санкт-Петербург, 2007. – 19 с.

231. Хараберюш, І. Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : [монографія] / І. Ф. Хараберюш, В. Я. Мацюк, В. А. Некрасов, О. І. Хараберюш. – К. : КНТ, 2007. – 196 с.

232. Хлынцов, М. Н. Криминалистическая информация и моделирование при расследовании преступлений : [учебное пособие] / М. Н. Хлынцов ; Под ред. В. Г. Власенко. – Саратов : Изд-во Саратов. ун-та, 1982. – 159 с.

233. Хрипко, С. Л. Інформаційне право : [навч.-метод. посібник] / С. Л. Хрипко. – Донецьк: ТОВ «Юго-Восток, Лтд», 2005. – 234 с.

234. Цимбалюк, В. Роль правової інформатики у модернізації прокуратури України / В. Цимбалюк // Право України. – 2006. – №11. – С. 73-77.

235. Цимбалюк, В. Щодо формування стратегії інформатизації прокуратури України в умовах розвитку інформаційного суспільства / В. Цимбалюк // Вісник прокуратури. – 2007. – №5. – С. 92-99.

236. Шарупич Л. С. Оптоэлектроника : [учебник] / Л. С. Шарупич, Н. М. Тугов. – М. : Энергоатомиздат, 1984. – 256 с.

237. Швець, М. Правова інформатика : [підручник] / М. Швець, В. Брижко, В. Фурашев, Б. Раціборинський, М. Целуйко, 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 / Є. Шевченко, О. Червякова // Вісник прокуратури. – 2003. – №2. – С. 119-122.

239. Шевчук, Р. Сутність та зміст поняття «інформатизація» в інформаційно-правовій сфері / Р. Шевчук // Право України. – 2006. – №11. – С. 103-108.

240. Шеломенцев В. П. Фіксація фактичних даних про протиправні діяння у мережі Інтернет / 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'ютеризація органів прокуратури України: сьогодення та перспективи / 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 решением задач предупреждения и раскрытия

економічних преступлень / А. М. Юрченко // Матеріали міжнар. наук.-практ. семін. «Сучасні технології у судовій акустиці» (Україна, Київ, 17-18 жовтня 2002 року). – 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 / А. М. Юрченко // Бізнес і безпека. – 2004. – №5 (43). – С.4-6.

244. Юрченко, О. М. Злочини в сфері комп'ютерної інформації: способи скоєння та засоби захисту : [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 : [навч. посібник] / [Сущенко В. Д. (науковий керівник авторського колективу), 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 : дис. ... докт. 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.gsmrepeater.ru/articles/?id=141>.

256. <http://dic.academic.ru/dic.nsf/lower/17375>.

257. <http://www.allbest.ru/>.

258. <http://www.mirash.ru/doki/99.doc>.

259. <http://www.atlas.ua/ukr/ea.html>.

260. http://onat.edu.ua/?pg=cifrovoe_tv.

261. <http://stc.gov.ua/uk/publish/article/60966>.

262. http://www.high-info.ru/Ponyatie_inf_obiekta.htm.

263. <http://www.liga.net/smi/show.html?id=110912>.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

- АРМ – автоматизоване робоче місце
- ВАК – Вища Атестаційна Комісія
- 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 – дезоксирибонуклеїнова кислота, що забезпечує зберігання, передачу від покоління до покоління та реалізацію генетичної програми розвитку й функціонування живих організмів
- ДСТСЗІ – Департамент спеціальних телекомунікаційних систем та захисту інформації
- ЄІТС – єдина інформаційно-телекомунікаційна система
- ЕОМ – електронно-обчислювальні машини
- ЕС – експертна система
- ЕЦП – електронний цифровий підпис
- 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 – мікромметр, одна тисячна частина міліметра
- млрд. – мільярд
- МФТІ (ДУ) – Московський фізико-технічний інститут (Державний університет)
- НАН – Національна академія наук (України)
- НАСА (NASA – англ. *National Aeronautics and Space Administration*) – Національне агенство США з авіації 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

- ПДВ – податок на добавлену вартість
- ПК – персональний комп'ютер
- РАН – Російська академія наук
- р. (рр.) – рік, роки
- РФ – Російська Федерація
- сек. – секунда
- с. – сторінка
- 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 в центрі, інформація з якого зчитується за допомогою лазера
- DVD (англ. *Digital Versatile Disc* – цифровий багатоцільовий диск) – носій інформації, який виконаний у вигляді диску, зовні схожий з компакт-диском, однак має можливість зберігати більший обсяг інформації за рахунок 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 аббревіатура походить від англ. *Ukraine*, що означає ISO-код України.

© Синьокий О.В., 2010

Відомості про автора

Синеокий Олег Володимирович народився 30 червня 1966 р.



З 1983 р. навчався у Ленінградському інституту точної механіки та оптики (нині – Санкт-Петербурзький державний університет інформаційних технологій, механіки та оптики) за спеціальністю «Інтегральна та волоконна оптика».

Після закінчення Української державної юридичної академії (нині - Національна юридична академія України ім. Ярослава Мудрого) більше 10 років відпрацював в органах прокуратури Запорізької області: від слідчого до начальника відділу криміналістики облпрокуратури.

Член науково-методичної ради при прокуратурі Запорізької області (2002). Кандидат юридичних наук (2006). Доцент по кафедрі кримінального права і правосуддя (2008).

Автор близько 200 друкованих праць, серед яких 4 одноосібні монографії, 15 навчальних та навчально-методичних посібників, в тому числі 3 з грифом МОН України (у співавторстві), фахові статі у вітчизняних та зарубіжних наукових журналах з міжгалузевих проблем протидії злочинності тощо.

Останніми роками викладає навчальні курси «Інформаційне право України» на юридичному факультеті та «Правове регулювання інформаційної безпеки» на факультеті математики та економічної кібернетики Запорізького національного університету.

Систематизовані результати наукового дослідження та впровадження педагогічних інновацій у навчальний процес представлені цілісною авторською працею у вигляді електронного курсу лекцій **«ІНФОРМАЦІЙНЕ ПРАВО УКРАЇНИ ТА ЕЛЕКТРОННЕ ПРАВО ВИСОКИХ ТЕХНОЛОГІЙ»**.

Усі відгуки, можливі критичні зауваження, фахові повідомлення та побажання автор із вдячністю чекає на свою поштову скриньку за електронною адресою: olegwsineoky@rambler.ru