Міністерство освіти і науки, молоді та спорту України
Національний університет
«Юридична академія України імені Ярослава Мудрого»

# ІНТЕГРАЦІЯ ПРАВА ТА ІНФОРМАТИКИ: ПРИКЛАДНИЙ І ЗМІСТОВНИЙ АСПЕКТИ

**Монографія**

За загальною редакцією
*В. Г. Іванова, В. Ю. Шепітька, В. В. Карасюка*

Харків
«Право»
2012

УДК 340(477)
ББК 67.9(4УКР)
І-73

*Рекомендовано до видання вченою радою Національного університету «Юридична академія України імені Ярослава Мудрого» (протокол № 10 від 15 червня 2012 р.)*

Рецензенти:

*О. С. Куценко*, доктор технічних наук, професор, завідувач кафедри системного аналізу і управління Національного технічного університету «Харківський політехнічний інститут»;

*В. О. Коновалова*, доктор юридичних наук, професор, професор кафедри криміналістики Національного університету «Юридична академія України імені Ярослава Мудрого»

Авторський колектив:

*В. Г. Іванов*, доктор технічних наук, професор — вступ, розділи 1, 3 (у співавт.); *В. Ю. Шепітько*, доктор юридичних наук, професор — розділи 2, 3 (у співавт.); *М. Г. Любарський*, доктор фізико-математичних наук, професор — розділ 4; *В. В. Карасюк*, кандидат технічних наук, доцент — розділи 3, 8 (у співавт.); *С. М. Іванов*, кандидат технічних наук, доцент — розділ 8 (у співавт.); *Ю. В. Ломоносов*, кандидат технічних наук, доцент — розділи 2, 3 (у співавт.); *Н. А. Кошева*, кандидат технічних наук, доцент — розділ 5; *М. В. Гвозденко,* старший викладач — розділ 6; *Н. І. Мазниченко,* старший викладач — розділ 7

І-73 **Інтеграція** права та інформатики: прикладний і змістовний аспекти : монографія / В. Г. Іванов, В. Ю. Шепітько, М. Г. Любарський та ін. ; за заг. ред. В. Г. Іванова, В. Ю. Шепітька, В. В. Карасюка. — Х. : Право, 2012. — 248 с.

ISBN 978-966-458-409-5

Наведено погляди і науково-практичні результати, отримані на стику вирішення завдань права й інформатики. Здійснено аналіз сучасних тенденцій процесу інтеграції цих наук, можливостей верифікації та ідентифікації мовних повідомлень з використанням вейвлет-перетворень, наведено практичні результати побудови інформаційно-аналітичних систем зберігання й обробки зображень у криміналістичній діяльності, розглянуто технологічні і правові аспекти захисту авторських прав мультимедійних даних, а також питання лінгвістичної безпеки електронних документів й ідентифікації користувачів інформаційно-комп'ютерних систем.

Рекомендовано для широкого кола юридичної громадськості, студентів, аспірантів і викладачів юридичних ВНЗ, а також фахівців у галузі обробки сигналів і зображень різної фізичної природи.

**УДК 340(477)**
**ББК 67.9(4УКР)**



ISBN 978-966-458-409-5

# Зміст

**РОЗДІЛ 4**
**ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ НА МУЛЬТИМЕДІЙНІ ТВОРИ**



**РОЗДІЛ 5**
**ЗАХИСТ АВТОРСЬКИХ ПРАВ АУДІОДАНИХ**

**РОЗДІЛ 6**
**ЛІНГВІСТИЧНА БЕЗПЕКА ЕЛЕКТРОННИХ ДОКУМЕНТІВ**



**РОЗДІЛ 7**
**ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ**
**ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ**

# Вступ

У теперішній час формується особливе місце існування і життєдіяльності людей — складається інформаційне суспільство. Суспільство, в якому немає жодної сфери людської діяльності, не зв'язаної тим або іншим чином з процесами створення, зберігання, пошуку, отримання і обробки інформації. Суспільство, в якому знання є основним капіталом і головним ресурсом всього життя. А динамізм сучасного життя примушує професіоналів активно переміщатися як у просторі, так і соціальними сходами, і все частіше самостійно ухвалювати відповідальні рішення, творчо підходити до будь-якої справи, уміти постійно самоудосконалюватися і оновлювати свої знання з використанням комп'ютерних і Internet-технологій, систем дистанційного навчання, розподілених електронних бібліотек, сховищ і баз даних.

Роль інформатики у вирішенні цього завдання важко переоцінити. Зараз наступає новий період розвитку інформатики як міждисциплінарного наукового напряму, що виконуватиме інтеграційні функції для інших напрямів як природничонаукових, так і гуманітарних. Інформатика передає їм свою наукову методологію, головними досягненнями якої сьогодні слід вважати методологію інформаційного моделювання, а також інформаційний підхід до аналізу об'єктів, процесів і явищ у природі і суспільстві.

З розвитком інформаційного суспільства зростають потоки інформації, швидкість її обробки і поширення, і у зв'язку з цим виникає гостра необхідність у захисті інтересів суб'єктів, що використовують інформацію у своїй діяльності, природа якої не укладається у звичні форми предметів правових відносин.

Тому інтенсивне зближення інтересів права й інформатики, яке ми спостерігаємо сьогодні, є об'єктивним і закономірним процесом, що показує гостру необхідність у взаємному використанні результатів новітніх досягнень, отриманих цими науками, і має два взаємозв'язані аспекти: прикладний

і змістовний, тобто прикладне використання останніх досягнень у галузі інформаційних технологій, пристосованих або спеціально розроблених для розвитку і функціонування юридичної науки і практики, з одного боку, і юридичне закріплення питань, пов'язаних з впровадженням у будь-яку сферу суспільних відносин новітніх інформаційних технологій — з другого.

Дуже важливо знайти такі правові механізми, які забезпечать правове регулювання нового класу суспільних відносин — інформаційних, що дозволить економічно більш ефективно розвивати цю галузь людської діяльності з виробництва і використання інформації, а також протистояти різним порушенням і злочинам у цій сфері.

Так, відкрити сторінку в Internet або розтиражувати книгу на CD-R набагато простіше, швидше і дешевше, ніж налагодити випуск і збут друкарської продукції. Досить придбати один екземпляр твору і сканер для його оцифрування. Проте в результаті вказаних дій автор твору, безумовно, позбавляється винагороди, на яку він міг би розраховувати при нормальному обороті екземплярів на ринку. У зв'язку з цим, не зважаючи на очевидні переваги електронних засобів запису, передачі і обробки інформації, постає безліч правових питань, пов'язаних з дотриманням майнових інтересів власників авторських прав.

При захисті прав автора сайту виникає проблема ідентифікації мережевих інформаційних ресурсів як об'єкта права: чи є вони різновидом бази даних або програмою для ЕОМ, чи можна віднести сайт до засобів масової інформації тощо. Дуже важливими є питання безпеки і конфіденційності роботи в мережі Internet.

Тобто необхідне вирішення дуже важливого завдання — інформатизації правової сфери, з одного боку, і правозабезпечення інформатизації — з другого. Для вирішення цього завдання необхідна взаємодія фахівців різних професійних галузей, а від юриста вимагають знання і розуміння всіх технічних й технологічних особливостей інформаційних об'єктів та процесів.

По суті, йдеться про необхідність формування нового покоління юристів (медіа-юристів), що компетентно володіють обчислювальною технікою і добре орієнтуються в методах пошуку, обробки, представлення і аналізу правової інформації, що дасть їм можливість ефективно і змістовно створювати, розвивати і застосовувати законодавство про інформатику й інформацію.

У пропонованій книзі автори діляться з читачами своїми поглядами і науково-практичними результатами, отриманими на стику вирішення завдань права й інформатики. Проводять аналіз сучасних тенденцій процесу інтеграції цих наук, можливостей верифікації й ідентифікації мовних повідом-

лень з використанням вейвлет-перетворень, наводять практичні результати побудови інформаційно-аналітичних систем зберігання, пошуку й обробки зображень у криміналістичній діяльності, розглядають технологічні та правові аспекти захисту авторських прав мультимедійних даних, а також питання лінгвістичної безпеки електронних документів й ідентифікації користувачів інформаційно-комп'ютерних систем, розглядають наукові та технологічні аспекти побудови комп'ютерної мережі Національного університету «Юридична академія України імені Ярослава Мудрого».

При підготовці і подачі матеріалів автори прагнули висловлювати його доступною і звичною мовою, зберігаючи, де це необхідно, формальну і математичну чіткість викладу.

Автори сподіваються, що книга буде цікава і корисна широкому колу юридичної громадськості, студентам, аспірантам і викладачам юридичних вузів, а також фахівцям у галузі обробки сигналів і зображень різної фізичної природи.

# РОЗДІЛ 1

# ІНФОРМАТИЗАЦІЯ ПРАВА І ПРАВОЗАБЕЗПЕЧЕННЯ ІНФОРМАТИЗАЦІЇ

## 1.1. Інформаційне суспільство й інформатика

Бурхливий розвиток комп'ютерної техніки й інформаційних технологій стимулював розвиток суспільства, яке побудоване на використанні інформації і знань і яке отримало назву інформаційного суспільства. *Інформаційне суспільство* — це суспільство, в якому обробкою інформації зайнято більше людей, ніж обробкою сировини і матеріалів [1]. Японські фахівці, котрі запропонували цей термін, доповнили його визначення, позначивши, що він характеризує суспільство, в якому удосталь циркулює висока за якістю інформація, а також є всі необхідні засоби для її зберігання, розподілу і використання. Інформація легко і швидко поширюється на вимогу зацікавлених людей і організацій і видається їм у звичній для них формі. Вартість користування інформаційними послугами настільки невисока, що вони доступні кожному.

Вчені вважають, що в інформаційному суспільстві процес комп'ютеризації надасть людям доступ до надійних джерел інформації, позбавить їх від рутинної роботи, забезпечить високий рівень автоматизації обробки інформації у виробничій і соціальній сферах [2; 3]. Рушійною силою розвитку суспільства має стати виробництво інформаційного, а не матеріального продукту. Матеріальний же продукт стане більш інформаційно ємним, що означає збільшення частки інновацій, дизайну і маркетингу в його вартості.

В інформаційному суспільстві зміняться не лише виробництво, але і весь устрій життя, система цінностей, зросте значущість куль-

турного дозвілля по відношенню до матеріальних цінностей. Порівняно з індустріальним суспільством, де все спрямовано на виробництво і споживання товарів, в інформаційному суспільстві виробляють і споживають інтелект, знання, що приводить до збільшення частки розумової праці. Від людини буде потрібна здібність до творчості, зросте попит на знання.

Відповідно до концепції З. Бжезінського, Д. Белла, О. Тоффлера, підтримуваної й іншими зарубіжними ученими [5; 4; 6], інформаційне суспільство — різновид постіндустріального суспільства. Розглядаючи суспільний розвиток як «зміну стадій», прихильники цієї концепції інформаційного суспільства пов'язують його становлення з домінуванням «четвертого», інформаційного сектора економіки, наступного за трьома відомими секторами — сільським господарством, промисловістю і економікою послуг. При цьому вони стверджують, що капітал і праця як основа індустріального суспільства поступаються місцем інформації і знанням в інформаційному суспільстві.

Існують різні критерії визначення факту переходу суспільства до інформаційної стадії. Так, наприклад, як критерій переходу суспільства до постіндустріальної і далі до інформаційної стадії розвитку може служити відсоток населення, зайнятого у сфері послуг: якщо в суспільстві більше 50 % населення зайнято у сфері послуг, наступила постіндустріальна фаза; якщо в суспільстві більше 50 % населення зайнято у сфері інформаційних послуг, то суспільство стало інформаційним. Згідно з цим критерієм, наприклад, США вступили в постіндустріальний період свого розвитку в 1956 році (штат Каліфорнія подолав цей рубіж ще в 1910 році), а інформаційним суспільством США стали в 1974 році.

Можна виділити такі ознаки інформаційного суспільства:

1. Усвідомлення суспільством пріоритетності інформації перед іншим продуктом діяльності людини.

2. Першоосновою всіх напрямів діяльності людини (економічним, виробничим, політичним, освітнім, науковим, творчим, культурним і тому подібне) є інформація.

3. Інформація ж є продуктом діяльності сучасної людини.

4. Інформація в чистому вигляді (сама по собі) є предметом купівлі-продажу.

5. Рівні можливості в доступі до інформації всіх верств населення.

6. Безпека інформаційного суспільства та інформації.

7. Захист інтелектуальної власності.

8. Взаємодія всіх структур держави і держав між собою на основі інформаційно-комунікаційних технологій (ІКТ).

9. Управління інформаційним суспільством з боку держави, громадських організацій.

Окрім позитивних моментів прогнозуються і небезпечні тенденції:

– зростає вплив на суспільство засобів масової інформації;

– інформаційні технології можуть зруйнувати приватне життя людей і організацій;

– існує проблема відбору якісної і достовірної інформації;

– багатьом людям важко адаптуватися до середовища інформаційного суспільства;

– існує небезпека розриву між «інформаційною елітою» (людьми, що займаються розробкою інформаційних технологій) і споживачами.

Як вважає професор У. Мартін [7], під інформаційним суспільством розуміють «розвинене постіндустріальне суспільство», що виникло перш за все на Заході. На його думку, не випадковим є той факт, що інформаційне суспільство затверджується передусім у тих країнах — в Японії, США і Західній Європі, в яких у 60–70-х роках XX століття сформувалося постіндустріальне суспільство.

У. Мартін зробив спробу виділити і сформулювати основні характеристики інформаційного суспільства за такими критеріями:

– технологічний (ключовий чинник) — широке застосування інформаційних технологій у виробництві, установах, системі освіти і в побуті;

– соціальний — інформація виступає як важливий стимулятор зміни якості життя, формується і затверджується «інформаційна свідомість» при широкому доступі до інформації;

– економічний — інформація є ключовим чинником в економіці як ресурс, послуги, товар, джерело доданої вартості і зайнятості;

– політичний — свобода інформації, що веде до політичного процесу, який характеризується зростаючою участю і консенсусом між різними класами і соціальними верствами населення;

– культурний — визнання культурної цінності інформації за допомогою сприяння затвердженню інформаційних цінностей на користь розвитку окремого індивіда і суспільства в цілому

*Матеріальною і технологічною базою інформаційного суспільства* стануть різного роду системи на базі комп'ютерної техніки і комп'ютерних мереж, інформаційні технології телекомунікаційного зв'язку, тобто засоби інформатики.

Інформатика порівняно нове слово. Воно виникло на початку 60-х років у французькій мові і позначало широку сферу людської діяльності по автоматизованій обробці інформації за допомогою електронних обчислювальних машин. Французький термін «informatique» утворений шляхом злиття слів «information» (інформація) і «automatique» (автоматика) і означає «інформаційна автоматика або автоматизована переробка інформації».

Якщо говорити коротко, то інформатика — це наука про інформацію.

Зараз інформатика є однією з фундаментальних галузей наукового знання, що формує системно-інформаційний підхід до аналізу навколишнього світу, вивчає інформаційні процеси і системи, а також технічні, організаційні та правові методи й засоби створення, зберігання, пошуку, захисту, перетворення, передачі, відображення і використання інформації в різних галузях людської діяльності.

Концептуальне і перманентне завдання сучасної інформатики — зняти просторові, часові, змістовні і технологічні обмеження в роботі з інформацією, але в межах, передбачених законом [8]. Це дозволить якісно змінити професійну, культурну і економічну діяльність сучасної людини.

Для вирішення цього завдання інформатика використовує свої і залучає, узагальнює і розвиває широкий спектр результатів теорії і практики таких наукових дисциплін:

– розробка персональних ЕОМ, обчислювальних систем і програмного забезпечення до них;

– теорія інформації і кодування, що вивчає процеси, пов'язані з передачею, прийомом, перетворенням, стисненням і зберіганням інформації;

– математичне моделювання, методи обчислювальної і прикладної математики;

– інтелектуальні інформаційні технології розпізнавання, зберігання і пошуку текстових даних, зображень, мови і звуку;

– системний аналіз, що вивчає методологію підготовки і обґрунтування рішень по складних проблемах різного характеру;

– соціальна інформатика й інформаційне право, які вивчають процеси інформатизації і використання інформації в суспільстві;

– телекомунікаційні системи і мережі, зокрема, глобальні комп'ютерні мережі та ін.

З наведеного переліку можна побачити, що основними об'єктами інформатики є: інформація, комп'ютери і інформаційні системи.

***Інформатика і кібернетика***

Сучасний погляд на предмет інформатики багато в чому відрізняється від уявлень про предмет цієї науки, що склалися до моменту її формування як галузі наукового знання і практичної діяльності людини. Інформатика виникла не на голому місці, а за наявності ряду дисциплін кібернетичного циклу, що вже склалися [9]. Вона не замінює і не знецінює напрями кібернетики, теорії інформації, системотехніки, що виникли раніше, а відгалужується від них і, звичайно, тісно взаємодіє з ними.

Кібернетика з'явилася як наука, що вивчає загальні властивості цілеспрямованих систем біологічної, технічної і соціальної природи [10]. Відповідно й інформація виступала в трьох видах — біологічна інформація (усередині живих організмів і між ними), машинна (усередині машин і між машинами), соціальна (усередині людських співтовариств і між ними). Інші форми інформаційних потоків і інші інформаційні системи не були відомі, поки не з'явилися автоматизовані інформаційні системи (АІС) — людино-машинні або, точніше, соціально-технічні системи. Можна сказати, що це інформаційні системи «четвертої природи», що реалізовують людино-машинні (ерготехнічні) інформаційні процеси. У них внутрішньомашинні

і міжмашинні потоки інформації органічно зливаються з потоками соціальної («людської») інформації (глобальна комп'ютерна мережа Internet). Це принципово новий і важливий історичний феномен, що знаменує перехід суспільства на новий рівень життєдіяльності.

Таким чином, предмет інформатики особливий. Він не збігається з предметом суспільних наук і з предметом системотехніки. Предмет інформатики складніший. Він охоплює системи суспільно-технічної природи, що виникають штучним шляхом, шляхом соціального інженерного проектування.

Інформатика поза сумнівом має проблеми, загальні з проблематикою наук кібернетичного циклу. Та все ж головна відмінність вбачається в розвитку вчення про інформацію, її роль, «рушійну силу» в соціальних системах [11]. Інформація, що зберігається і циркулює в інформаційному соціальному середовищі, є чимось істотно іншим у порівнянні з інформацією, що управляє службовим сигналом у кібернетичній системі, оскільки виступає як перетворена форма знання, що дозволяє транслювати це знання в суспільстві. Нове знання відкриває людині додаткові можливості роздумів і дій, збільшує її свободу. Інформація, що діє як управляючий сигнал, зменшує невизначеність допустимих станів керованої кібернетичної системи. Тому народження інформатики пов'язане з гострою потребою осмислити інформацію зі змістовного боку, зрозуміти її як «рушійну силу» в системах соціальної природи.

Інформатика виступає не як наука про ЕОМ (це кібернетика і системотехніка) і не як наука про передачу повідомлень каналами зв'язку (це канонічна теорія інформації), а як наука про інформаційне (соціальне) середовище, те середовище, куди упроваджуються ЕОМ і де вони працюють як підсилювачі людського інтелекту.

Наявна теорія інформації робить акцент на зв'язку одержувача з джерелом повідомлень. А для чого одержувачеві те або інше повідомлення? Як інформація «працює» в системі користувача? Яку соціальну користь вона приносить, як збільшити цю користь? Ці питання в теорії інформації, як і в системотехніці, навіть не виникають. У інформатиці вони посідають центральне місце. Інформатика на перше місце ставить динаміку різних соціальних середовищ під дією інформації.

Таким чином, можна говорити, що предметом інформатики виступають інформаційні процеси й інформаційні системи, що функціонують у соціальному (людському) середовищі і забезпечують динаміку (розвиток) цього середовища на базі комп'ютерно-інформаційних технологій і їх правового забезпечення.

## 1.2. Правові аспекти інформатизації

З розвитком інформаційного суспільства зростають потоки інформації, швидкості її обробки і поширення, і у зв'язку з цим виникає гостра необхідність у захисті інтересів суб'єктів, що використовують інформацію у своїй діяльності, природа якої не укладається у звичні форми предметів правових відносин.

Тому інтенсивне зближення інтересів права і інформатики, яке спостерігається сьогодні, є об'єктивним і закономірним процесом, що показує гостру необхідність у взаємному використанні результатів новітніх досягнень, отриманих цими науками, і що має два взаємозв'язані аспекти: прикладний і змістовний. Тобто прикладне використання останніх досягнень у галузі інформаційних технологій, пристосованих або спеціально розроблених для розвитку і функціонування юридичної науки і практики, з одного боку, і юридичне закріплення питань, пов'язаних з впровадженням в будь-яку сферу суспільних відносин новітніх інформаційних технологій, — з іншого.

Дуже важливо знайти такі правові механізми, які забезпечать правове регулювання нового класу суспільних відносин, — інформаційних, що дозволить економічно ефективно розвивати цю галузь людської діяльності з виробництва й використання інформації, а також протистояти різним порушенням і злочинам у цій сфері. По суті, це означає необхідність всесторонньої розробки нової комплексної юридичної галузі — інформаційного права. Ця теза знайшла своє віддзеркалення в Законі Україні від 4 лютого 1998 року № 74/98-ВР «Про національну програму інформатизації» (Відомості Верховної Ради. — 1998. — № 27–28. — Ст. 181) і у Законі України від 9 січня 2007 року № 537-V «Про основні засади розвитку інформаційного

суспільства в Україні на 2007–2015 роки» (Відомості Верховної Ради. — 2007. — № 12. — Ст. 102), в яких сказано, що інформатизація — це сукупність взаємозв'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, направлених на створення понять для задоволення інформаційних потреб громадян і суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів і інформаційних технологій, побудованих на основі застосування сучасної обчислювальної і комунікаційної техніки.

Інформаційне законодавство повинне регламентувати державне управління, планування і звітність у галузі інформатики, право власності, правову охорону об'єктів обчислювальної техніки, фінансування і ціноутворення в цій сфері, передбачати види відповідальності за правопорушення у сфері інформатики, а також вирішити нові проблеми, пов'язані з використанням глобальних інформаційних комп'ютерних систем і мереж в економіці, політиці й інших соціальних сферах.

Так, відкрити сторінку в Internet або розтиражувати книгу на CD-R набагато простіше, швидше і дешевше, ніж налагодити випуск і збут друкарської продукції. Досить придбати один екземпляр твору і сканер для його оцифрування. Проте в результаті вказаних дій автор твору, безумовно, позбавляється винагороди, на яку він міг би розраховувати при нормальному обороті екземплярів на ринку. У зв'язку з цим, не зважаючи на очевидні переваги електронних засобів запису, передачі і обробки інформації, постає безліч правових питань, пов'язаних з дотриманням майнових інтересів володарів авторських прав.

При захисті прав автора сайту виникає проблема ідентифікації мережевих інформаційних ресурсів як об'єкта права: чи є вони різновидом бази даних або програмою для ЕОМ, чи можна віднести сайт до засобів масової інформації тощо. Дуже важливими є питання безпеки і конфіденційності роботи в мережі Internet. Тобто захист комп'ютера від зараження вірусом і запобігання несанкціонованому доступу, недопущення перехоплення особистої електронної пошти та іншої секретної інформації.

Практично одноголосно Сенат США затвердив 24 жовтня 2001 року законопроект USA Uniting and Strengthening America Act (http://ru.wikipedia.org/wiki), який передбачає дуже суворі заходи покарання за терористичну діяльність. Особливий інтерес становить положення 814 «Перешкода і запобігання кібертероризму». Цей закон досить жорстко ставиться до мережевих зломщиків. Викриті в проникненні в корпоративні або державні мережі переслідуватимуться в кримінальному порядку, якщо сума збитку за останні 12 місяців перевищить 5 тис. дол.

Актом кібертероризму тепер вважатиметься будь-яке несанкціоноване проникнення в комп'ютер користувача. Цікаво зазначити, що в цьому контексті негативно «засвітилася» асоціація RIAA (Recording Industry Association of America), яка в мережі відома, в основному, боротьбою з музичним піратством. Вона запропонувала Конгресу внести поправку до визначення кібертероризму. Так, отримання неавторизованого доступу до файлів користувача не вважається незаконним, якщо проникнення було зроблене з метою захисту авторських прав.

Інший, один з найбільш суперечливих проектів законодавчих актів в історії комп'ютерної індустрії в США Uniform Computer Information Transactions Act (http://en.wikipedia.org/wiki/Uniform_Computer_Information_Transactions_Act) (далі — UCITA) поки що не отримав визнання на федеральному рівні, але, враховуючи існування самостійних судових систем штатів, докладаються зусилля щодо його просування на локальному рівні. Відповідно до цього проекту виробник програмного забезпечення (далі — ПЗ) звільняється від відшкодування збитку, який був завданий некоректною роботою програми.

Найбільш суперечливе положення UCITA — можливість віддалено відключати ПЗ на комп'ютері користувача. Чорні ходи, що прозвали «бомбами», дозволяють софтверній компанії отримувати докладну інформацію про роботу програми на комп'ютері користувача, і у разі виявлення порушень ліцензійної угоди вона має юридичне право «відключити» програму через Internet.

Слід так само сказати, що безперервне розширення глобальних комп'ютерних мереж у всьому світі, включаючи Україну, не тільки створює абсолютно нові можливості отримання, поширення, обміну інформацією, використання колосальних освітніх, комерційних, роз-

важальних, культурних ресурсів, але і викликає нові правові проблеми. Часто вони не можуть бути ефективно вирішені тільки в рамках національного законодавства [12; 13; 14; 15; 16].

Проблеми, пов'язані з використанням Internet, досить різнопланові. До них належать: порушення прав інтелектуальної власності; проникнення в системи управління; поширення інформації, що негативно впливає на соціальне здоров'я суспільства, зокрема, безконтрольне розповсюдження образливих і непристойних матеріалів і доступ до них дітей; розповсюдження недобросовісної реклами; проведення шахрайських комерційних операцій; несанкціонований доступ до конфіденційної інформації юридичних осіб і органів влади; порушення прав та законних інтересів особи в процесі інформаційного обміну; визначення правового статусу учасників інформаційного обміну.

Крім того, необхідно вирішувати проблему юрисдикції, яка обумовлена перш за все екстериторіальністю Internet, що не дозволяє повною мірою здійснювати контроль у межах конкретної держави за переміщенням інформації в комп'ютерних мережах і дією її на суб'єктів. З глобальним, міжнародним характером комп'ютерних мереж пов'язані питання не лише про норми права, що підлягають застосуванню, але і про можливість застосування будь-яких норм. Рух інформації в Internet через специфіку цієї мережі часто не може бути регламентований законодавством якої-небудь однієї країни, у зв'язку з чим виникає необхідність підготовки міжнародно-правових актів.

Вказані проблеми зрештою можна звести до трьох груп: захист прав на об'єкти інтелектуальної власності; захист прав та законних інтересів особи, суспільства і держави при використанні загальнодоступних комп'ютерних мереж; захист циркулюючої в них інформації. Вирішення цих проблем ускладнюється тим, що чинне законодавство орієнтоване на традиційні відносини, і при використанні глобальних комп'ютерних мереж не всі його норми виявляються застосовними. Виникає ряд прогалин у праві, які долаються у міру накопичення досвіду регулювання, знаходження оптимальних рішень. Наочний приклад — законодавство про засоби масової інформації.

Вже зараз в українському сегменті Internet досить широко представлені засоби масової інформації. Значна частина з них — електрон-

на (цифрова) версія традиційних друкованих засобів масової інформації (журналів, газет, радіостанцій). Проте є і суто цифрові видання. Крім того, існують проміжні варіанти, коли електронна версія частково дублює зміст друкованого видання. Можна стверджувати, що формується новий об'єкт правового регулювання, до якого неможливо повною мірою застосувати норми Закону України від 16 листопада 1992 року № 2782-XII «Про друковані засоби масової інформації (пресу) у Україні» (Відомості Верховної Ради. — 1993. — № 1 — Ст. 1).

Дуже важливо визначити критерії, за якими те або інше видання можна віднести до засобів масової інформації. Потребують уточнення такі основні критерії, як періодичність у мережі, постійність назви видання, форми подання інформації, передбачувана територія його поширення та інші параметри. Так, зміну назви для традиційних друкованих засобів масової інформації припускає проходження складної процедури, чого не вимагають для зміни назви «видання» на інтернетовському сайті. При реєстрації друкованого засобу масової інформації встановлюється передбачувана територія його поширення. Особливо це важливо для радіо- і телемовлення, які здійснюються в рамках ліцензії, що обмежує діяльність виділеними частотами теле- і радіомовлення і територією (ст. 14 Закону України від 23 грудня 1993 року № 3759-XII «Про телебачення і радіомовлення» (Відомості Верховної Ради. — 2006. — № 18. — Ст. 115)). При розповсюдженні друкованого засобу масової інформації через Internet обмеження за територією практично знімається.

Прогалини в праві, що виникли у зв'язку з використанням глобальних комп'ютерних мереж, не обмежуються наведеними прикладами. Вже зараз їх виразно можна побачити в процесуальному законодавстві, в першу чергу щодо проблеми доказів, в авторському праві, в законодавстві, що регулює використання електронного цифрового підпису, в забезпеченні в Україні правового порядку дистанційного оформлення і виконання операцій із застосуванням електронних засобів і технологій і в багатьох інших випадках.

У зв'язку з цим особливо гостро постає питання про підготовку юристів, що мають необхідну кваліфікацію з питань інформації та інформатизації, інформаційної безпеки.

По суті, йдеться про необхідність формування нового покоління юристів (медіа-юристів), що компетентно володіють обчислювальною технікою і добре орієнтуються в методах пошуку, обробки, представлення і аналізу правової інформації, що надасть їм можливість ефективно і змістовно створювати, розвивати і застосовувати законодавство про інформатику та інформацію.

## 1.3. Інформатика в системі юридичної освіти

Основне завдання сучасної професійної освіти, в тому числі й юридичної, полягає сьогодні не лише в тому, щоб дати майбутнім фахівцям знання, але і в тому, щоб озброїти їх умінням знаходити і засвоювати ці знання самостійно з використанням комп'ютерних та Internet-технологій, систем дистанційного навчання, розподілених електронних бібліотек, сховищ і баз даних. Роль вивчення інформатики у вирішенні цього завдання важко переоцінити.

Аналіз останніх досліджень і публікацій, присвячених інформатиці і її освітнім аспектам [17; 18; 19; 20; 21; 22] дозволяє зробити висновок, що наступає новий період розвитку інформатики як міждисциплінарного наукового напряму, який виконуватиме інтеграційні функції для інших напрямів як природничо-наукових, так і гуманітарних. Інформатика передає їм свою наукову методологію, головними досягненнями якої сьогодні слід вважати методологію інформаційного моделювання, а також інформаційний підхід до аналізу об'єктів, процесів і явищ у природі і суспільстві [23].

Саме тому вивчення інформатики як фундаментальної науки в системі освіти має виключно велике значення для формування сучасного наукового світогляду і ставить її в один ряд з такими науками, як узагальнений системний аналіз, кібернетика, фізика, юриспруденція та ін.

Відзначимо той факт, що розвиток предмета інформатики є далеким від завершення, і це підтверджується різноманіттям підходів до визначення змісту предмета і основних завдань інформатики як науки і як

освітньої дисципліни [8; 24; 25; 26; 27]. Це, у свою чергу, стримує вирішення дуже важливого завдання — інформатизації правової сфери, з одного боку, і правозабезпечення інформатизації — з другого. Для вирішення цього завдання необхідна взаємодія фахівців різних професійних галузей, а від юриста вимагаються знання і розуміння всіх технічних та технологічних особливостей інформаційних об'єктів і процесів.

Будь-яка правова система з погляду процесів, що відбуваються в них, пошуку, збору, передачі, систематизації, сприйняття й обробки інформації, є інформаційною системою. Отже, закони функціонування цих систем і інформаційні процеси, що відбуваються в них, підкоряються законам інформатики і можуть бути досліджені за допомогою методів, розроблених цією наукою.

Інформатика, або правова інформатика, одночасно і у взаємозв'язку вивчає природно-наукову суть цих процесів з урахуванням юридичних властивостей інформації та інформаційних об'єктів. Метою вивчення є, з другого боку, необхідність ефективної організації інформаційних процесів у всіх видах юридичної діяльності, а з іншого боку, виявлення їхніх особливостей, облік яких необхідний для грамотного правового регулювання тих суспільних відносин, до виникнення яких ці інформаційні процеси спричиняють.

Інформаційні технології тривалий час розглядалися правовою інформатикою тільки з погляду ефективної організації юридичної діяльності. Проте останнім часом необхідність взаємодії фахівців різних професійних галузей, завдання, що стоять перед галузевими юридичними науками (особливо перед інформаційним правом), вимагають від юриста знання і урахування всіх технічних та інформаційних особливостей цих об'єктів. У цьому розумінні правова інформатика одночасно є інструментальним засобом і джерелом знань, які необхідні для вирішення безлічі проблем правового регулювання нових суспільних відносин.

Як вже наголошувалося, сьогодні ми стоїмо на порозі якісно нового суспільства — інформаційного. І природно, що життя і практична діяльність у ньому нерозривно пов'язані з освоєнням і використанням сучасних інформаційних технологій. У зв'язку з цим правова інформатика як частина загальної інформатики дає знання і уміння вико-

ристовувати ті інформаційні засоби і методи, які необхідні будь-якому повноцінному членові інформаційного суспільства.

Юристові знання правової інформатики дозволяють підвищити свій професійний рівень. Сьогодні лавинні потоки соціально-правової інформації, що обрушуються на юриста, настійно вимагають від нього володіння сучасними інформаційними технологіями — довідковими правовими системами, юридичними експертними системами, сучасними програмними й технічними засобами захисту інформації, засобами забезпечення електронного цифрового підпису, інформаційними технологіями, які є основою функціонування сучасних комп'ютерних мереж і глобальної мережі Internet, тощо.

Але для юриста знання інформаційних технологій — це не лише інструмент у його практичній діяльності. Інформація, інформаційні процеси, інформаційні системи сьогодні є об'єктами правовідносин і предметом вивчення галузевих правових наук.

В інформаційному законодавстві, яке активно формується, юристам необхідно провести правове регулювання нових суспільних відносин, що утворюються з приводу таких об'єктів, як «інформаційні ресурси», «інформаційні системи», «інформаційні технології», «комп'ютерні мережі». Для грамотного, повного правового регулювання необхідне чітке розуміння сутності цих інформаційних об'єктів, їх особливостей і принципів функціонування, всього того, що вже побудоване і обґрунтоване в теорії інформатики і правовій інформатиці. З цієї точки зору правова інформатика для юриста — це джерело знань, необхідних йому для вирішення професійних завдань. Нарешті, інформатика дає в руки юристові системно-інформаційний метод дослідження. Тому дуже важливим завданням є створення методології змістовного наповнення і використання сучасної інформатики в юридичній освіті на основі концептуальних принципів взаємодії і об'єднання інтересів права й інформатики, що дозволить економічно й ефективно розвивати інформаційну галузь, а також протистояти різним порушенням і злочинам у цій сфері.

Нам видається, що учбові курси з основ інформатики для студентів юридичних вузів повинні бути досить гнучкими і максимально орієнтуватися на практику. Тут доцільно виокремити два рівні підготовки — базовий і спеціальний.

Базовий курс «Основи інформатики і обчислювальної техніки» дає студентам можливість отримати комплекс необхідних теоретичних знань про персональні ЕОМ, а також практичні уміння і навички їх використання для створення, зберігання, пошуку, обміну і подання інформації різної фізичної природи.

У рамках цього курсу студенти знайомляться з історією виникнення і розвитку інформатики й обчислювальної техніки, предметом, структурою і завданнями сучасної інформатики, її основними поняттями — інформацією, знаннями, даними і методами їх кодування.

Вивчають архітектуру сучасних персональних ЕОМ і програмні принципи автоматичної обробки даних, способи організації зберігання і доступу до комп'ютерної інформації, методи роботи в операційній системі MS Windows, стандартні програми цієї операційної системи, а також нові прийоми роботи з документами в процесорі MS Word та табличному процесорі MS Excel. Засвоюють методи автоматизованого перекладу електронних документів і принципи роботи в автоматизованих бібліотечних комплексах, з антивірусними засобами захисту даних, а також програмні і системні засоби їх архівації, технологічні основи функціонування Internet і використання електронної пошти, методи пошуку і отримання інформації з Internet, створення і публікації власних Web-документів.

Спеціальна підготовка має на меті знання обчислювальних і інформаційних систем у площині можливостей їх застосування в судочинстві, в прокурорській і слідчій діяльності, судовій експертизі, в господарській діяльності і в державному управлінні. Це досягається в рамках подальшого вивчення дисципліни «Правова інформатика і комп'ютерні технології в юридичній діяльності» [28].

У рамках цієї дисципліни студент має ознайомитися з поняттями «правова інформатика» та «правова інформація», математичними моделями, які використовуються в юридичній діяльності, основними цілями національної програми правової освіти населення, а також розглянути принципи побудови інформаційних систем державно-правового характеру, поглибити і розширити свої знання і уміння роботи у пакеті MS Office, оволодіти організаційними, правовими та програмними засобами захисту інформації у комп'ютерних системах, у тому числі програмою

для створення електронного підпису; вивчити технологічні особливості комп'ютерних злочинів, нормативні документи, що регулюють електронний документообіг і електронний цифровий підпис; засади інформаційно-аналітичного забезпечення законотворчої, правозастосовної та правоосвітньої діяльності, організацію та прийоми пошуку інформації в загальноправових базах даних; основи використання комп'ютерних технологій у нотаріальній діяльності, цивільному, кримінальному та адміністративному судочинстві, опанувати методи пошуку інформації у бібліотечних системах і принципи доступу до цієї інформації через локальні і глобальні комп'ютерні мережі; ознайомитися з перспективними напрямами розвитку інформаційних технологій у правознавстві, відеоконференцзв'язком та голосовими порталами у судочинстві.

Причому вивчення інформатики необхідно тісно пов'язати із засвоєнням загальних і спеціальних юридичних дисциплін. Такий взаємозв'язок може бути досягнуто шляхом включення в зміст останніх окремих питань і тем, що стосуються застосування ЕОМ. Поява таких міждисциплінарних зв'язків предметів, що вивчаються, і математизація загальнонаукових і спеціальних дисциплін дозволить студентам гуманітарних вузів оволодіти сучасними методами і засобами наукової діяльності. При цьому комп'ютер вже виступатиме переважно як засіб, інструмент навчання юридичним дисциплінам, але разом з тим поглиблюватимуться знання про нього, закріплюватимуться практичні навички роботи з ЕОМ і тим самим реалізовуватиметься принцип безперервності вивчення інформатики, що надасть можливість студентам юридичних вузів отримати необхідний сучасний рівень інформаційної компетентності.

## 1.4. Інформатизація державно-правової сфери

Перманентним і основним завданням будь-якої держави є організація і реалізація комплексу системних заходів з попередження і розкриття злочинів. Роль сучасної криміналістики у вирішенні цього завдання важко переоцінити [29; 30; 31; 32; 33].

### 1.4.1. Інформатизація криміналістичної діяльності

Сучасний розвиток криміналістики характеризується формуванням її загальної теорії, розробкою і впровадженням сучасних науково-технічних засобів та інформаційних технологій у практику боротьби зі злочинністю, вдосконаленням прийомів криміналістичної тактики, пропозицією окремих методик розслідування нових видів злочинів [34].

Інтенсивність криміналістичних знань пов'язана з науково-технічним прогресом сучасного суспільства. Інформатизація соціального середовища призвела до «технологізації» криміналістики, розробки і впровадження інформаційних, цифрових, телекомунікаційних технологій. Інформаційні технології — нова категорія криміналістики, що претендує посісти належне місце в її структурі [34; 35; 36]. Використання технологічного підходу здійснюється не лише в криміналістичній техніці, але і криміналістичній тактиці і методиці (технології виробництва окремих слідчих дій, слідчі або криміналістичні технології) [34; 37; 38; 39].

У нових умовах криміналістика від вивчення традиційних матеріально-фіксованих слідів вимушена перейти до дослідження звукових (акустичних), електронних або геномів слідів [34]. Змінюються також способи, прийоми і методи роботи з такими слідами, порядок їх збирання і фіксації. У сучасних умовах революційні науково-технічні зміни приводять до того, що традиційні криміналістичні методи вже не задовольняють у повному обсязі. Спектр проблем і можливостей сучасної криміналістики досить широкий — від обговорення необхідності загальної дактилоскопічної реєстрації і необхідності ухвалення спеціального закону «Про дактилоскопію» до пропозиції нових біометричних методів ідентифікації особи: генотипоскопічної реєстрації, ідентифікації за райдужною оболонкою або сітківкою ока, методу сканування венозної карти, відеокомп'ютерного розпізнавання людини за зображенням його обличчя та ін. Об'єктивні причини розвитку науки і техніки приводять до формування нових галузей криміналістичної техніки: криміналістичної вибухотехніки, судової акустики або криміналістичної фоноскопії, поліграфології, криміналістичної енграмології [34].

З урахуванням вищевикладеного можна стверджувати, що технологічною методологією сучасної криміналістики є багатофункціональні системи аналізу й обробки зображень і сигналів різної фізичної природи.

Авторами цієї монографії (В. Ю. Шепітько, В. Г. Іванов, Ю. В. Ломоносов, В. В. Карасюк) була запропонована і реалізована ідеологія побудови багатофункціональних інформаційно-аналітичних колекторів (баз даних), об'єднуючих у собі одночасно текстову і мультимедійну інформацію [40; 41].

Комплексна технологія побудови автоматизованих криміналістичних інформаційно-довідкових електронних баз даних (інформаційно-аналітичних колекторів) поєднує в собі окрім традиційних повнотекстових документів ще і відеоінформацію: малюнки протекторів шин автомобільних коліс, конфігурації і малюнки моделей фарного скла, малюнки підошов взуття, зображення відтисків печаток і штампів та ін. Таким чином, під багатофункціональним інформаційно-аналітичним колектором ми розуміємо апаратно-програмний комплекс управління й обробки компресованим інформаційним сховищем, що містить текстові і графічні файли.

Розроблений програмний комплекс складається з двох структурно-програмних модулів: Інформаційно-пошуковий модуль — автоматизована інформаційно-пошукова система (АІПС) «КЛІШЕ» і модуль «Автоматизоване робоче місце експерта-криміналіста» (АРМ Е-К).

Інформаційно-пошуковий модуль АІПС «КЛІШЕ» призначений для зберігання, відображення, перегляду, редагування і пошуку зображень відтисків печаток усіх районних відділень ДАІ УМВС України. Структура бази даних має конфігурацію, яка дозволяє за наявними атрибутами вносити до неї графічні зображення печаток і штампів будь-яких організацій і підприємств, які знаходяться як на території України, так і за кордоном.

Програмний модуль АРМ Е-К призначений для автоматизації проведення експертних криміналістичних досліджень і складання тексту експертного висновку.

Однією з основних функцій цього модуля є метод автоматичного накладення сітки на досліджуване зображення.

Авторами також були проведені теоретичні й практичні роботи, пов'язані з дослідженням математичного апарату вейвлет-перетворення мовних сигналів з метою подальшої ідентифікації того, хто говорить.

Розроблений і випробуваний алгоритм, що реалізовує отримання вейвлет-коефіцієнтів векторних даних (мова) і на площині (зображень). Реалізовані методи розкладання мовного сигналу в площині вейвлет-коефіцієнтів за схемами «гілка» і «дерево».

Представлена математична модель алгоритму швидкого вейвлет-перетворення з використанням квадратурних дзеркальних фільтрів (алгоритм Малла).

Для проведення експертиз фонограм голосу людини з використанням вейвлет-аналізу розроблена методика, що включає вирішення таких завдань:

1) вибір оптимальної пари квадратурних дзеркальних фільтрів, що враховує найбільш якісне виділення «тонкої» структури мови, в якій зосереджені характерні риси того, хто говорить. При вирішенні цього завдання необхідно оптимізувати пару квадратурних дзеркальних фільтрів розкладання і відновлення мовного сигналу. Необхідно знайти компроміс між тривалістю розкладаючого фільтру і якістю вейвлет-коефіцієнтів, що виділяються, який відображає «тонку» структуру мовного сигналу;

2) побудова «дерева» розкладання мовного сигналу за вейвлет-пакетами на задану глибину занурення (розкладання). Ця операція дозволяє точно диференціювати вейвлет-коефіцієнти за діапазонами і надалі обробка кожного вейвлет-пакета проводиться автономно. Визначення глибини занурення «розкладання» мовного сигналу за вейвлет-пакетами необхідно проводити із співвідношення кількість пакетів/якість обробки;

3) обчислення автокореляційної залежності коефіцієнтів кожного вейвлет-пакета з подальшим зберіганням автокореляційних функцій (АКФ) в окремих файлах, що істотно зменшить час обробки;

4) набір мінімальної мовної статистики для визначення середньостатистичного порогу. Для цього, згідно з теорією вірогідності і статистичного аналізу, потрібно як мінімум 50 ітерацій мовного сигналу, вимовленого одним автором у різних умовах. Ця процедура

виконується один раз і надалі використовуються тільки значення середньостатистичних порогів для кожного вейвлет-пакета.

Запропонована методика показала обнадійливі результати і може використовуватися як додаткова в діючих системах проведення фоноскопічних експертиз.

## 1.4.2. Електронне судочинство

У зв'язку із введенням у судочинство України фіксування судового засідання за допомогою звукозаписувальних технічних засобів може бути висунена проблема щодо перспектив «електронізації» судових процесів завдяки ширшому використанню в майбутньому комп'ютерних та телекомунікаційних технологій, які мають забезпечити інформаційну підтримку електронного (віртуального) судочинства [28]. Ця проблема стала майже головним питанням модернізації цивілістичних процесів у багатьох країнах (США, Канада, Нова Зеландія, Австрія, Італія, Англія, Німеччина тощо). Йдеться перш за все про електронну форму подання документів до суду, викликів і повідомлень сторін, вірогідність та доказову силу електронних документів тощо, що забезпечує електронне документування судового діловодства відповідно до вимог процесуального законодавства. У більш широкому аспекті впровадження інформаційно-комп'ютерних технологій, по суті, означає і більш широке поняття електронного (віртуального) судочинства як системи не лише фіксації судових процесів, але й способів комунікації учасників судочинства, проведення дистанційного розгляду судових справ, функціонування банку даних справ та судових рішень, автоматичного формування статистичної звітності про діяльність судів, розподіл навантаження на суддів тощо.

Причинами пошуку альтернатив традиційним формам судочинства стали неефективність процедур судочинства, невдалість його реформ та сподівання, що завдяки використанню комп'ютерних технологій підвищиться якість правосуддя. Щодо цього висловлюється впевненість, що електронне судочинство має переваги, які виявляться значно пізніше. Воно переважно гарантуватиме доступ до правосуддя, швидкість розгляду справ судами, сприятиме підвищенню якості судових рішень, контролю сторін за розглядом справи та еко-

номії судових витрат, посилить змагальність та публічність судових процесів. Інформаційні технології в майбутньому стануть фундаментом судової системи, що викличе радикальні зміни у процесуальному праві. На думку прихильників такого підходу, традиційний судовий розгляд стає застарілим, оскільки існує обладнання, необхідне для проведення віртуальних судових процесів, а програмне забезпечення вдосконалюється досить швидко. Так, за прогнозами в межах десяти років систему віртуального цивільного процесу можна вдосконалити без великих фінансових вкладень з боку судів, адвокатів та сторін процесу. Враховуючи те, що цифрова інформація майже безкоштовна, має великий ступінь збережуваності, може передаватися на велику відстань, у перспективі слід очікувати, що в судових процесах будуть не лише використовуватися електронні комп'ютерні технології як такі, але й те, що основні процесуальні дії, в тому числі особисті пояснення і сам судовий розгляд, будуть здійснюватися через мультимедійну презентацію. Так, наприклад, електронний протокол судового процесу буде реєструвати докази, які мають надати сторони, показання свідків будуть записані до початку судового розгляду та розглянуті адвокатам сторін, як і інші документальні дані. Оскільки всі докази будуть зібрані, обмін ними та іншими змагальними паперами здійснений, то кожне питання підготовки справи до судового розгляду, в принципі, може бути вирішене до судового розгляду, а можливість тих чи інших несподіванок у ході судового розгляду буде повністю ліквідовано. На розгляд суду при цьому може бути покладено лише огляд мультимедійної презентації, допит свідків під присягою у звичний спосіб або в спосіб відеоконференції незалежно від місця знаходження свідка, проведення крос-допитів сторін та їх адвокатів для захисту мультимедійних презентацій судового розгляду.

Цифровий формат проведення судового процесу, як стверджується, має удосконалити також існуючу систему неефективних процедур офіційних повідомлень та запитів, обміну змагальними паперами, керування справою з боку судді тощо. Віртуальне середовище проведення судових процесів у принципі має суттєво вплинути і на територіальну юрисдикцію, яка може визначатися місцем здійснення тих чи інших правочинів.

Як приклад застосування нових електронних технологій можна навести новели Цивільного процесуального кодексу Німеччини (http://albookerk.ru/g/vitrum/grazhdanskij_processual'nyj_kodeks_frg_4.htm Zivilprozessordnung der BRD (Bonn, November 1996)). Цей Кодекс передбачає можливість участі у судовому засіданні учасників процесу завдяки використанню відео- та аудіозасобів (параграф 128а), використанню електронних документів (параграф 130а), врученню та доставці документів (параграф 174 ч. III), ознайомленню з матеріалами справи в електронній формі, огляду електронних документів (параграф 371 ч. 1 п. II), трансляції зображення та звуку судового розгляду у залі судового засідання представників та помічників сторін, які під час судового розгляду знаходяться в іншому місті (параграф 128а). У такому випадку зображення та звук судового розгляду транслюється в зал судового засідання та місце знаходження сторін, представників та адвокатів. Якщо стосовно підготовчих процесуальних документів, доданих до них клопотань, заяв сторін, а також пояснень, висловлювань, висновків і заяв третіх осіб передбачена письмова форма, то достатнім і належним за процесуальним законодавством Німеччини визнається викладення документа в електронній формі, якщо такий документ може бути оброблений судом (параграф 130а).

Зараз спостерігаються окремі випадки використання відеоконференцзв'язку в юридичній практиці. Так, третейський суд, що постійно діє при Асоціації «Український третейський союз», розглянув позов київської фірми «Інтерон» до київського підприємства «Укрпривінвест», який був поданий по електронній пошті і підписаний електронним цифровим підписом відповідно до чинного законодавства. Судове засідання проходило в режимі відеоконференції: кожен з учасників знаходився у своєму офісі (фізично — в різних містах України) і брав участь у розгляді справи з використанням зв'язку через Internet. Під час відеоконференції всі учасники процесу мали можливість бачити один одного, розглядати документи, ставити питання, заявляти клопотання і виступати в судових дебатах. При цьому здійснювався відеозапис третейського розгляду. Після дослідження обставин справи і з'ясування позицій сторін представники сторін були відключені від відеоконференції, і судді працювали над

рішенням у справі в закритому режимі. Після ухвалення суддями рішення представники сторін знову отримали доступ до відеоконференції і судом було оголошено рішення у справі. Рішення Третейського суду видане сторонам також і в паперовому вигляді з підписами суддів і печаткою.

Уперше на пострадянському просторі відеоконференція в судочинстві була організована в травні 1999 року в Челябінському обласному суді для дистанційної участі обвинувачуваних у касаційних судових засіданнях. Прийнята схема організації каналу відеоконференцзв'язку відповідала міжнародним стандартам і забезпечувала дистанційну участь обвинувачуваних у судовому засіданні.

***Голосові портали в судовій діяльності***

Поява так званих інтелектуальних голосових комерційних систем масового обслуговування телефонних абонентів дозволяє говорити про портали у сфері телефонних технологій як про реальність, яка може мати перспективу. Роль терміналу, з якого здійснюється доступ до мережних ресурсів, тут виконує будь-який стаціонарний або мобільний телефонний апарат. Такі системи називаються системами комп'ютерної телефонії, які забезпечують обробку телефонних дзвінків за допомогою комп'ютерів.

До недавнього часу телефонний інтерфейс з користувачем організовувався тільки за допомогою клавіатури апарату завдяки тому, що програма видає в трубку голосову підказку, а абонент реагує на неї, натискаючи одну з кнопок. Такий спосіб роботи має ряд недоліків: апарат повинен підтримувати тональний набір, клавіатура ускладнює навігацію за функціональним меню послуг, крім того, незручно користуватися телефоном, конструктивно виконаним у вигляді однієї трубки (більшість радіо- і стільникових моделей), доводиться то підносити його до вуха, то дивитися на клавіатуру, відсутній режим «вільні руки» (hands free), що важливо, наприклад, для водіїв авто, операторів та інших. Все це перешкоджало створенню достатньо привабливих рішень, які б сподобалися масовому споживачеві.

Абсолютно нові можливості відкрилися з появою у 1998–1999 роках реально працюючих технологій синтезу і, що найважливіше,

розпізнавання мови. Природний для людини мовний інтерфейс дозволяє звертатися по телефону до різних інформаційних джерел без попереднього навчання і тренування.

Одним з основних завдань судової влади є підвищення відкритості і прозорості судової діяльності. Вирішення цього завдання можливе тільки з використанням сучасних комп'ютерних та інформаційних технологій. Тому досить цікавим у зв'язку з цим є впровадження і використання окремими судами інноваційного рішення «Голосовий портал суду».

Незважаючи на те, що інформація про діяльність судів доступна зацікавленим особам через Web-портал, надання її по телефону, як і раніше, є актуальним, оскільки саме так часто запитується стандартна інформація, в першу чергу, номери телефонів фахівців, відомості про процесуальний стан справи, сплату держмита, як дістатися до суду тощо. Наявність «Голосового порталу» дозволяє автоматизувати надання такої інформації і значно зменшити навантаження на довідково-інформаційну службу суду.

Функціонально система складається з підсистем IVR (інтерактивне голосове меню) і маршрутизації запитів; розпізнавання мови; синтезу мови; інтеграції із зовнішніми системами (перш за все, з системою автоматизованого судового діловодства); підсистеми адміністрування і звітності. Наскільки відомо, цей комплекс упроваджено деякими арбітражними судами.

Програмне забезпечення дозволяє звертатися до потрібного пункту меню натисненням кнопки або голосом. Система розпізнає вимовлене людиною прізвище необхідного фахівця або номер справи, шукає потрібну інформацію в системі електронного судочинства і озвучує її абонентові за допомогою синтезованої мови.

«Голосовий портал» може обробляти п'ять запитів, що поступають одночасно. Проте можливості системи «Avaya» допускають значне масштабування числа запитів.

Автоматичний журнал обліку дзвінків фіксує час, дату і телефонний номер абонента, який дзвонив, а також вид даних, які він запитував.

### 1.4.3. Електронне управління

Інтенсивний процес формування інформаційного суспільства диктує і свої вимоги до зміни змісту процесу державно-правового регулювання суспільних відносин. Уряд теж стає електронним, тобто таким, в якому вся сукупність як внутрішніх, так і зовнішніх зв'язків і процесів підтримується і забезпечується відповідними інформаційними і комп'ютерними технологіями. Електронний уряд — це не механічне поєднання інформаційних технологій і функцій уряду. Це нова філософія державного управління, в основу якої покладений принцип свободи і комфортності існування особи.

Як правило, нове явище, що має широкий суспільний резонанс, супроводжується найжвавішими дискусіями. Не є винятком і ідея електронного уряду [42; 43; 44; 45; 46; 47]. Одне з основних проблемних питань серед великого кола обговорюваних — це майбутнє урядів взагалі. Існують дві полярні точки зору.

Перша з них полягає в тому, що в умовах щонайширшого поширення інформаційних комп'ютерних технологій роль держави, уряду, місцевих органів влади й інших централізованих владних інститутів нівелюватиметься. Це пояснюють тим, що «електронна демократія» (комп'ютерні технології) зможе забезпечити реальну можливість участі в ухваленні управлінських рішень найширшим верствам населення, всім без винятку громадянам. Дійсно, сучасні техніка і технології в принципі дозволяють це зробити. Але уявіть собі, щодня ви після роботи повинні сідати до монітора комп'ютера і висловлювати свою думку за всіма важливими і менш важливими питаннями держави, області, міста, району і так далі. При цьому вам необхідно вивчити історію питання, оцінити соціально-економічні, екологічні, політичні й інші наслідки ухвалення рішення. Напевно, для багатьох з нас це покажеться достатньо обтяжливим. Та і ухвалені рішення хтось повинен реалізовувати, контролювати їх виконання. Очевидно, якісь органи, наділені владними повноваженнями.

Тому найбільш реалістичною видається інша точка зору. Вона полягає в тому, що впровадження інформаційних технологій не призводить до зниження ролі державних інституцій, органів самоврядування, навпаки — підвищення ефективності діяльності цих органів,

що відбувається при цьому, визначає ще більшу їх значущість і відповідальність.

Але в чому мають рацію ініціатори цих дискусій, так це в тому, що в умовах широкого використання комп'ютерних технологій необхідно переглядати парадигму державного, адміністративного управління. Обов'язковою необхідною умовою переходу до електронного уряду є широка інформатизація всіх процесів, що мають місце в звичайній діяльності міністерств, відомств, місцевих органів виконавчої влади, причому як внутрішніх, так і зовнішніх. У цьому випадку з'являється реальна можливість забезпечити інформаційну, функціональну взаємодію уряду з кожним громадянином, кожним суб'єктом управління. Враховуючи деяку обмеженість технократичного підходу, все ж таки можна стверджувати: саме використання комп'ютерних технологій дозволить реалізувати декларативне твердження про те, що державний апарат знаходиться на службі у народу.

Електронний уряд не тільки корінним чином змінить сам характер діяльності державного апарату, але і підвищить ефективність його функціонування.

Модель електронного уряду повинна базуватися на ідеї, що держава — це інститут, який працює на благо суспільства. Відповідно, держава повинна служити інтересам звичайних громадян і надавати їм послуги в найбільш зручній для них формі [45; 46; 47; 48].

Головна мета електронного уряду — створити систематизований каталог державної інформації і послуг. І тоді для пошуку інформації нам не треба буде проглядати десятки державних сайтів — вся інформація буде зібрана в одному місці і впорядкована за проблемним підходом. У ідеалі держава в недалекому майбутньому надаватиме всі свої послуги через Internet [49; 50].

Електронний уряд повинен працювати не тільки на громадян, але і на бізнес, допомагаючи підприємцям з оформленням документів і оперативністю доведення до них державних рішень [51].

Таким чином, створення «електронного уряду» приведе не тільки до ефективнішого і менш витратного адміністрування, але і до кардинальної зміни взаємин між суспільством і урядом. «Електронний уряд» забезпечує, перш за все, прозорість роботи державного апара-

ту, знижує, якщо не ліквідовує, залежність громадянина або організації від свавілля чиновника і таким чином попереджає корупцію. А зрештою, уведення «електронного уряду» веде до вдосконалення демократії і підвищення відповідальності влади перед народом.

Як показує досвід зарубіжних країн [50; 52; 53], електронний спосіб керівництва в першу чергу повинна застосовувати виконавча влада. Проте слід пам'ятати, що чиновники намагатимуться всіляко перешкоджати тому, щоб Internet все ширше використовувався в політичній системі влади, оскільки впровадження комп'ютерних технологій вимагатиме зменшення кількості бюрократичних структур. «Електронний уряд» є новою, вищою стадією розвитку уряду в умовах інформаційного суспільства. За результатами щорічного огляду «електронних урядів», проведеного компанією Accenture, в ході якого були вивчені державні онлайнові служби 23 країн, перше місце присуджене державному порталу Канади. Критеріями були інформативність, інтерактивність і можливість здійснення трансакцій. На другому місці опинився Сінгапур, «електронний уряд» якого надає громадянам такі послуги, як реєстрація народження дитини, браку, пошук житла, відправлення повідомлень у поліцію. До речі, саме в цій країні вперше у світі була реалізована ідея урядового порталу. Третє місце отримав «електронний уряд» США. Із значним відривом від лідерів йдуть Австралія, Данія, Велика Британія, Фінляндія, Гонконг, Німеччина, Ірландія, Нідерланди, Франція і Норвегія. Суттю електронної форми уряду в цих країнах є об'єднання за допомогою Internet-технологій всіх міністерств і відомств в єдиний комплекс з вищим ступенем інтеграції внутрішніх процесів (документообіг) і єдиним інтерфейсом (вікном взаємодії) з громадянином (користувачем). Таким чином, громадянин дістане можливість спілкуватися не з п'ятьма — сімома відомствами по черзі, а з єдиним електронним посередником, що їх всіх представляє одночасно. Окрім цього, звернення або запит громадянина автоматично посилається у відповідні інстанції і в більшості випадків відповідь (юридична консультація, квитанція про оплату послуг, бюлетень для голосування, довідка, податкова декларація) приходить негайно.

Важливою перевагою «електронного уряду» є можливість участі населення в обговоренні законопроектів і урядових рішень. Під час

обговорення якогось важливого законопроекту або ухвали уряду кожен зможе висловити свою думку. Планується, що спеціальна аналітична система оброблятиме отриману інформацію і видаватиме результат, наприклад, у вигляді графіка. Якщо графік засвідчить збільшення кількості громадян, незадоволених нововведенням, то питання зніматиметься з обговорення.

В Україні також робляться певні кроки по створенню і розвитку принципів електронного управління [44; 50; 51]. Так, Кабінет Міністрів України постановою від 13 грудня 2010 року № 2250-р (Офіційний вісник України. — 2010. — № 97. — Ст. 3443) прийняв Концепцію розвитку електронного урядування в Україні, метою якої є визначення основ і створення умов для досягнення європейських стандартів якості послуг, відвертості і прозорості діяльності органів державної влади і органів місцевого самоврядування.

Впровадження електронного управління передбачає створення якісно нових форм організації діяльності органів державної влади і органів місцевого самоврядування, їх взаємодію з громадянами і суб'єктами господарювання шляхом надання доступу до державних інформаційних ресурсів, можливості отримання електронних адміністративних послуг, звернення до посадових осіб, використовуючи Internet.

Реалізація Концепції передбачена на період до 2015 року і складається з трьох основних етапів.

На першому етапі (2011–2012 роки) передбачається розробка необхідної нормативно-правової і нормативно-технічної бази, зокрема щодо надання адміністративних послуг в електронній формі, а також єдиних стандартів, протоколів і регламентів взаємодії суб'єктів електронного управління, їх гармонізація з міжнародними стандартами, створення єдиної загальнодержавної системи електронного документообігу і Національного реєстру електронних інформаційних ресурсів та сайтів органів державної влади і органів місцевого самоврядування на всіх рівнях; забезпечення надання органами державної влади й органами місцевого самоврядування послуг в електронній формі громадянам і суб'єктам господарювання, використовуючи Internet.

На другому етапі (2013–2014 роки) планується: забезпечити організацію надання послуг в електронній формі у всіх сферах суспільного життя, створення сприятливих умов для залучення громадських організацій до управління державними справами; освоєння технологій інтерактивної взаємодії органів державної влади й органів місцевого самоврядування з громадянами і суб'єктами господарювання; впровадження в діяльність органів державної влади і органів місцевого самоврядування типових організаційно-технологічних рішень у сфері електронного управління, забезпечення передачі електронних документів у державні архіви, музеї, бібліотеки, їх довгострокове зберігання, підтримку в актуалізованому стані і надання доступу до них.

На третьому етапі (2014–2015 роки) передбачається створити: об'єднані Web-портали органів виконавчої влади, призначені для проведення відповідних транзакцій; єдину інформаційно-телекомунікаційну інфраструктуру органів державної влади і органів місцевого самоврядування; спеціальні центри (пункти) надання послуг, центри обслуговування населення (колл-центри), Web-портали надання послуг; єдиний Web-сервер — портал електронного уряду як єдине місце доступу до всіх видів електронних послуг для громадян і суб'єктів господарювання з урахуванням потреб громадян і функціональних аспектів; національний депозитарій електронних інформаційних ресурсів.

## 1.5. Висновки

Проведений аналіз основних складових складного і багатоструктурного процесу інформатизації права і правозабезпечення інформатизації, який диктується парадигмою сучасного інформаційного суспільства. Показано, що матеріальною і технологічною базою інформаційного суспільства стануть різного роду системи на базі комп'ютерної техніки і комп'ютерних мереж, інформаційних технологій, телекомунікаційного зв'язку, тобто засоби інформатики. Визначені концептуальні й перманентні складові сучасної інформатики. Подано нове визначення предмета інформатики, який звучить таким чином: предметом

інформатики виступають інформаційні процеси й інформаційні системи, що функціонують у соціальному (людському) середовищі і забезпечують динаміку (розвиток) цього середовища на базі комп'ютерно-інформаційних технологій і їх правового забезпечення.

Розглянуті правові аспекти процесу інформатизації в Україні показали, що не зважаючи на очевидні переваги електронних засобів запису, передачі і обробки інформації, виникає маса правових питань, пов'язаних з дотриманням майнових інтересів володарів авторських прав.

Internet в Україні не лише створює абсолютно нові можливості отримання, розповсюдження, обміну інформацією, використання колосальних освітніх, комерційних, розважальних, культурних ресурсів, але і викликає нові правові проблеми. Часто вони не можуть бути ефективно вирішені тільки в рамках національного законодавства.

У зв'язку з цим дуже важливим є завдання оцінки і змісту інформатики в системі юридичної освіти, яка покликана дати майбутнім фахівцям не лише певні знання, а також навчити їх умінню знаходити і засвоювати ці знання самостійно з використанням комп'ютерних і Internet-технологій, систем дистанційного навчання, розподілених електронних бібліотек, сховищ і баз даних. Роль вивчення інформатики у вирішенні цього завдання важко переоцінити.

Для юриста знання інформаційних технологій — це не лише інструмент в його практичній діяльності. Інформація, інформаційні процеси, інформаційні системи сьогодні є об'єктами правовідносин і предметом вивчення галузевих правових наук.

У монографії також наголошується, що інформатизація соціального середовища призвела до «технологізації» криміналістики, розробки і впровадження інформаційних, цифрових, телекомунікаційних технологій. Інформаційні технології — нова категорія криміналістики, що претендує посісти належне місце в її структурі.

У розділі проаналізовано питання становлення електронного судочинства в Україні, яке може стати ефективною альтернативою існуючому. Цифровий формат проведення судового процесу, відеоконференцзв'язок, голосові портали — основні знакові складові судочинства вже сьогодні.

Торкаючись питання електронного управління та «електронного уряду», автори роблять висновок, що інтенсивний процес формування інформаційного суспільства диктує і свої вимоги до зміни змісту процесу державно-правового регулювання суспільних відносин. Уряд теж стає електронним. Наголошується, що «електронний уряд» — це не механічне поєднання інформаційних технологій і функцій уряду. Це нова філософія державного управління, в основу якої покладений принцип свободи і комфортності існування особи. Розглянуто досвід створення електронного уряду в закордонних країнах, докладно представлені етапи реалізації Концепції розвитку електронного управління в Україні, яка прийнята Кабінетом Міністрів України 13 грудня 2010 року.

# РОЗДІЛ 2

# ІДЕНТИФІКАЦІЯ МОВНИХ ПОВІДОМЛЕНЬ НА ОСНОВІ ВЕЙВЛЕТ-АНАЛІЗУ ДАНИХ

## 2.1. Методики вейвлет-аналізу мовного сигналу

За останні 15 років була виконана величезна кількість наукових та дослідних робіт, які пов'язані з дослідженням і розробкою математичного апарату вейвлет-перетворень [1; 2; 3; 4]. На практиці результати цих досліджень стали базою для їх широкого впровадження в системи аналізу та обробки різноманітних типів даних.

Найбільш потужний розвиток отримали методи кодування мультимедійних даних на основі узагальнення форматів JPEG та вейвлет-технологій при обробці сигналів різного фізичного походження [4; 5; 6; 7]. Але необхідно визнати, що найбільш складним було і залишається завдання знаходження способів аналізу та синтезу сигналів (знаходження ортогональних базисів).

Розглянуто широкий спектр можливостей використання вейвлет-перетворень, що стосуються аналізу, стиснення, зберігання і передачі мовних і графічних даних у цифровій формі. На окрему увагу заслуговують методи, що реалізують отримання вейвлет-коефіцієнтів як векторних даних (аудіосигнали, людська мова тощо), так і даних на площині (зображення різних класів).

При проведенні досліджень у роботі окремо були розглянуті методи розкладання мовного сигналу в площині вейвлет-коефіцієнтів за схемами «гілка» і «дерево». За результатами проведених досліджень були обрані оптимальні перетворення як векторних даних, так і даних, представлених у вигляді растрових зображень.

Основною математичною моделлю алгоритму швидкого вейвлет-перетворення була вибрана модель, побудована на квадратурних дзеркальних фільтрах (алгоритм Малла) [2].

Для проведення досліджень фонограм голосу людини з використанням вейвлет-аналізу розроблена досить проста методика, що включає вирішення таких завдань:

1) вибір оптимальної пари квадратурних дзеркальних фільтрів, що враховує найбільш якісне виділення «тонкої» структури мови, в якій зосереджені відмінні риси того, хто говорить. При вирішенні цього завдання необхідно оптимізувати пару квадратурних дзеркальних фільтрів розкладання і відновлення мовного сигналу. Дуже важливо знайти компроміс між тривалістю розкладаючого фільтру і якістю вейвлет-коефіцієнтів, що виділяються і відображають «тонку» структуру мовного сигналу;

2) побудова «дерева» розкладання мовного сигналу за вейвлет-пакетами на задану глибину занурення (розкладання). Ця операція дозволяє точно диференціювати вейвлет-коефіцієнти за діапазонами. Надалі обробка кожного вейвлет-пакета проводиться автономно. Визначення глибини занурення «розкладання» мовного сигналу за вейвлет-пакетами необхідно проводити зі співвідношення (кількість пакетів/якість обробки);

3) обчислення автокореляційної залежності коефіцієнтів кожного вейвлет-пакета з подальшим зберіганням автокореляційних функцій (АКФ) в окремих файлах, що істотно зменшить час обробки мовного сигналу при подальшому порівняльному аналізі;

4) набір мінімальної мовної статистики для визначення середньостатистичного порогу. Для цього, згідно з теорією вірогідності і статистичним аналізом, потрібно мати як мінімум 50 зразків мовного сигналу, вимовленого одним диктором у різних умовах. Ця процедура виконується один раз, і надалі використовується тільки значення середньостатистичних порогів для кожного вейвлет-пакета;

5) при обчисленні значень середньостатистичних порогів необхідно проводити розрахунок взаємно-кореляційної функції (ВКФ) однойменних пар вейвлет-пакетів з подальшим визначенням усеред-

неної різниці двох функцій АКФ і ВКФ ($\Delta = \frac{1}{N}\sum_{i=0}^{N}(AKF_i - VKF_i)$), за умови поєднання (вирівнювання) їх максимальних значень.

Отримані таким чином значення порогів дозволять проводити порівняльний аналіз двох мовних сигналів по значеннях статистичних характеристик у кожному діапазоні вейвлет-коефіцієнтів в автоматичному режимі. Цей алгоритм не потребує визначення і обґрунтування основних (головних) і окремих індивідуальних ознак мовного сигналу кожного диктора.

Результат перевищення статистичного порогу розпізнавання для кожного вейвлет-пакета визначатиме основу ухвалення рішення щодо ідентифікації диктора за мовним повідомленням.

Вирішення вищевикладених завдань вимагає певного часу на набір і обробку статистичного матеріалу (створення бази даних мовних сигналів дикторів, банка АКФ для кожного вейвлет-пакета), а також на створення оптимального алгоритму і комп'ютерної програми [8; 9].

Як перспективне впровадження цього методу можна розглядати наявність певних результатів при використанні запропонованої методики аналізу мовних сигналів на основі обчислення вейвлет-коефіцієнтів для систем доступу з автоматичною ідентифікацією диктора за мовним повідомленням.

Цей факт заснований на тому, що кожний вейвлет-пакет є прообразом початкового мовного сигналу, зменшеного в 2*N рази. Головним фактором є те, що зменшення довжини вейвлет-пакета є пропорційним, але зменшення динамічного діапазону в кожному пакеті відбувається по-різному щодо оригінального мовного зразка. Основною різницею між вейвлет-пакетами є домінуюча присутність у структурі кожного із них або «грубої» або «тонкої» складової оригінального мовного сигнала.

Багатомасштабний біортогональний аналіз досліджуваного мовного сигналу з використанням кореляційно-різницевого методу оцінювання статистичних характеристик сигналу не вимагає пошуку і обґрунтування інформативних ознак розпізнавання, визначення вирішального правила при ідентифікації мови тощо. Більш того, вейвлет-аналіз мовного сигналу не виключає, а може доповнити інформацію

для ухвалення правильного рішення при використанні тих методів і способів обробки, які мають позитивний досвід вирішення цієї проблеми на сучасному етапі.

## 2.2. Теоретичні основи використання вейвлет-аналізу

Застосування вейвлет-аналізу на площині дає можливість отримання вищого ступеня стиснення зображень при однакових середньоквадратичних помилках алгоритму, порівняно з технологією JPEG [6; 7]. Це, у свою чергу, дозволяє зберігати, передавати і обробляти великі масиви графічної інформації різного характеру.

Окремим пунктом потрібно відзначити можливість створення «вейвлет-мікроскопа». Використовуючи збільшення амплітудних значень вейвлет-коефіцієнтів, що відображають «тонку» структуру досліджуваного зображення, можна отримувати чіткішу картину «розмитих» деталей початкового зображення. Досить просто вирішується завдання регулювання яскравості, а головне — контрастності досліджуваних зображень. Ця корисна властивість може дозволити поліпшити якість досліджуваного зображення (або його фрагмента) на користь вирішення завдань як звичайних досліджень, так і криміналістичної експертизи графічних даних.

Одним із найбільш популярних сьогодні напрямів у світі персональних комп'ютерів є мультимедіа. За допомогою застосування технологій мультимедіа текстова, графічна, аудіо- і відеоінформація об'єднуються, і користувач може управляти перебігом подання цієї інформації. При цьому обсяг інформації, що підлягає обробці або передачі, є досить великим. Це говорить про те, що ефективне використання мультимедійних даних на персональних ЕОМ можливе тільки після їх обробки спеціальними програмами кодування.

За багато років роботи над проблемою обробки аудіоінформації накопичилася безліч продуктів, методів, алгоритмів, які перетинаються між собою, часто мають кілька різних назв і функцій [10–22]. На жаль, використання вейвлет-перетворювань при обробці звукових

сигналів зараз досліджене недостатньо глибоко. Тому інтерес становить можливість використання вейвлет-перетворень при обробці мовних і аудіосигналів.

### 2.2.1. Вейвлет-базис

Розглянемо мовний сигнал *x(t)*, визначений на числовій осі $t \in R$ з кінцевою енергією $\int_{-\infty}^{+\infty} x^2(t)dt$. Простір всіх таких сигналів позначають символом $L^2(R)$. Це Гільбертовий простір зі скалярним множенням:

$$\langle f, g \rangle = \int_{-\infty}^{+\infty} f(t)g(t)dt, \qquad f, g \in L(R^2). \tag{2.1}$$

Ідея *вейвлет-аналізу,* або інакше *багатомасштабного аналізу,* полягає в розкладанні сигналу *x(t)* за дуже спеціальним ортонормованим базисом у $L^2(R)$ [1; 2]. Цей базис породжується всього однією функцією $\psi(t)$ і складається з її масштабних перетворень за часом, кратних числу 2, і цілочисельних зрушень:

$$\left\{2^{-j/2}\psi(2^j t - i), i, j \in Z\right\} \tag{2.2}$$

(множник $2^{-j/2}$ потрібний для нормування).

Функція називається *вейвлетом, що породжує*, а побудований за нею базис — *вейвлет-базисом*. Основною особливістю вейвлета є те, що він добре локалізований за часом, тобто швидко убуває на нескінченності або має обмежений носій. Ця властивість і пояснює назву: вейвлет — «маленька хвиля». Для практичних цілей використовуються вейвлети з обмеженим носієм.

Якщо розкласти сигнал *x(t)* за вейвлет-базисом:

$$x(t) = \sum_{i,j} c_{ij} 2^{-j/2} \psi\left(2^j t - i\right),$$

то індекс *j* указує на часовий масштаб кожного доданку, а індекс *i* — на його положення на часовій осі. Доданки цієї суми зручно згрупувати за масштабом:

$$x(t) = \sum_j y_j(t), \tag{2.3}$$

$$y_j(t) = \sum_i c_{ij} 2^{-j/2} \psi\left(2^j t - i\right). \tag{2.4}$$

Тоді сигнал *x(t)* буде представлений у вигляді суми сигналів, кожен з яких має свій «характерний» часовий масштаб.

Бажано, щоб вейвлет мав якомого більшу кількість нульових моментів:

$$M_n = \int_{-\infty}^{+\infty} t^n \psi(t)\, dt = 0, \quad n = 0,1,\ldots . \tag{2.5}$$

і був гладкою функцією. У цьому випадку він краще апроксимує гладкі сигнали, і значущих доданків у сумі (2.3) стає менше.

Застосування багатомасштабного аналізу в цілях стиснення сигналу повністю аналогічно використанню в тих же цілях рядів Фур'є для періодичних функцій. Потрібно замінити тільки поняття частоти поняттями масштабу і часової локалізації. Можна чекати, що деякі масштаби початкового сигналу *x(t)* на певних проміжках часу будуть відсутні або будуть малі. Тоді їх можна або повністю відкинути, або записати коротшими словами. Крім того, можна чекати, що масштабні складові $y_j(t)$ виявляться однорідніші за часом, ніж початковий сигнал. У цьому випадку до них з більшим успіхом, ніж до початкового сигналу, можна застосовувати стандартні алгоритми стиснення.

Відзначимо відразу, що додаток описаної схеми до практики в обчислювальному сенсі не зручний через те, що початковий сигнал, як правило, заданий дискретним чином. Тому вейвлети, хоча і відіграють важливу теоретичну роль, в обчислювальних алгоритмах в явному вигляді не використовуються.

Нижче нам знадобляться такі поняття.

Хай $\{x_i\}$ — дискретний сигнал, і $\{h_s\}$ — деяка послідовність. Операцію *згортки*, що перетворює сигнал $\{x_i\}$ на сигнал за формулою

$$y_i = \sum_s h_s x_{i-s}, \tag{2.6}$$

називають застосуванням *фільтру* $\{h_s\}$ до сигналу $\{x_i\}$.

Дискретним *перетворенням Фур'є* сигналу називають функцію

$$x(\omega) = \sum_s x_s e^{-i\omega k}. \tag{2.7}$$

У термінах перетворень Фур'є застосування фільтру записується так:

$$y(\omega) = h(\omega)x(\omega), \tag{2.8}$$

що власне і пояснює назву «частотний фільтр».

*Зв'язаним* до фільтру $h$ називається фільтр, такий що $h_s^* = h_{-s}$.

## 2.2.2. Багатомасштабний аналіз і алгоритм Малла

Задається часовий масштаб за допомогою системи підпросторів $\{V_j, j \in Z\}$ простору $L^2(R)$ таких, що виконані такі умови:

1) $V_j \subset V_{j+1}$, (2.9)

2) $v(t) \in V_j \Leftrightarrow v(2t) \in V_{j+1}$, (2.10)

3) $\bigcup V_j = L^2(R), \bigcap V_j = \varnothing$, (2.11)

4) існує функція, така, що система її цілочисельних зрушень утворює ортонормований базис у підпросторі $V_0$.

Властивість 2 означає, що підпростори $V_j$ відрізняються один від одного тільки часовим масштабом вхідних у них функцій і вкладені один в одного так, що мінімальний часовий масштаб функцій з $V_j$ удвічі більше, ніж з $V_{j+1}$. Мінімальний масштаб функцій з підпростору $V_0$ за властивістю 4 задається функцією $\varphi(t)$. Тому така система підпросторів називається *багатомасштабним аналізом (МА), а функція $\varphi(t)$ — масштабною (або скейлінг-) функцією. Сукупність її цілочисельних зрушень називають скейлінг-базисом.*

Уніфікована структура підпросторів МА дозволяє розглянути тільки два з них, наприклад, $V_0$ і $V_{-1}$. Будь-яка інша пара підпросторів, що йде підряд, відрізняється тільки масштабом.

Зазначимо, що завдяки властивостям 2 і 4 система функцій $\{2^{-1/2}\varphi(t/2 - i), i \in Z\}$ є скейлінг-базисом підпростору $V_{-1}$, а функція $2^{-1/2}\varphi(t/2)$, що породжує цей базис, може бути виражена через скейлінг-базис простору $V_0$:

$$\varphi(t/2) = \sqrt{2}\sum_i h_i \varphi(t - i). \tag{2.12}$$

Послідовність коефіцієнтів розкладання, яку надалі трактуватимемо як фільтр, відіграє основну роль.

Позначимо через $W_{-1}$ ортогональне доповнення до підпростору $V_{-1}$ в $V_0$. Чудовим фактом є те, що в підпросторі $W_{-1}$ існує ортонормований базис, що породжується функцією

$$\psi(t/2) = \sqrt{2}\sum_i g_i \varphi(t-i), \tag{2.13}$$

де фільтр $g = \{g_i\}$ пов'язаний з фільтром $h$ співвідношенням:

$$g_i = (-1)^i h_{1-i}. \tag{2.14}$$

Це і є вейвлет, пов'язаний зі скейлінг-функцією $\varphi(t)$.

Хай $x_0(t)$ — заданий сигнал. З першої властивості МА слідує, що сигнал при деякій заданій точності можна вважати таким, що належить одному з підпросторів МА. Позначимо цей підпростір через $V_0$, тобто приймемо за одиницю мінімальний масштаб, що міститься в цьому сигналі.

Ортогональна проекція $x_{-1}(t)$ сигнала на підпростір $V_{-1}$ являє собою ту його частину, яка має мінімальний масштаб 2. Частина, що залишилась, є ортогональною проекцією на підпростір $W_{-1}$ і має масштаб 1. Вона збігається з функцією $y_{-1}(t)$ з сукупності (2.4). Обидві ці проекції легко знайти. Допустимо $\{a_i\}$ — це відомі коефіцієнти розкладання сигнала $x_0(t)$ за скейлінг-базисом простору $V_0$, а $\{b_i\}$ і $\{c_i\}$ — коефіцієнти розкладання проекцій $x_{-1}(t)$ і $y_{-1}(t)$ відповідно в скейлінг-базисі простору $V_{-1}$ і в базисі підпростору $W_{-1}$, який був створений вейвлетом $2^{-1/2}\psi(t/2)$. Тоді використовуючи зв'язки (2.12) і (2.13) між базисами, легко знайти:

$$b_i = \sum_s h_s^* a_{2i-s} \quad \text{і} \quad c_i = \sum_s g_s^* a_{2i-s}. \tag{2.15}$$

Іншими словами, коефіцієнти розкладання проекцій виходять застосуванням зв'язаних фільтрів $h^*$ і $g^*$ з подальшим «проріджуванням» — відкиданням членів з непарними індексами.

Аналогічно, якщо відомі проекції $x_{-1}(t)$ О $V_{-1}$ і $y_{-1}(t)$ О $W_{-1}$ початкового сигналу, то його можна відновити застосуванням фільтрів $h$ і $g$:

$$a_i = \sum_s h_s b^1_{i-s} + \sum_s g_s c^1_{i-s}, \tag{2.16}$$

до послідовностей $\{b^1_s\}$ і $\{c^1_s\}$, отриманим з коефіцієнтів розкладання вставкою нулів на непарні місця. Наприклад, $b^1_{2i} = b_i$ і $b^1_{2i+1} = 0$.

До проекції $x_{-1}(t)$ можна знову застосувати ту ж процедуру, що і до початкового сигналу, тобто розкласти на дві складові з підпросторів $V_{-2}$ і таким чином виділити з сигналу компоненту $y_{-2}(t)$ масштабу 2. Після нескінченного повторення цієї процедури через другу властивість МА, що гарантує, що $x_{-j}(t)$ зникає при $j \to \infty$, виходить розкладання (2.3).

Вказаний алгоритм називають *швидким вейвлет-перетворенням* або *алгоритмом Малла*, а фільтри $h$ і $g$, зв'язані співвідношенням 2.14, — *квадратурними дзеркальними фільтрами*.

Звичайно, що для реального сигнала $x_0(t)$, який заданий з певною точністю та обмежений за часом, цей процес є кінцевим. Але і в цьому випадку його не обов'язково доводити до кінця. Можна обмежитися «глибиною занурення» $N$, що означає обчислення $y_{-1}(t)$, $y_{-2}(t)$, …, $y_{-N}(t)$ і $x_{-N}(t)$. Після цього необхідно провести певні дії по стисненню отриманих компонент, запам'ятати їх або передати. Для відновлення вихідного сигналу потрібно рекурентним чином, починаючи з $j = N$, по функціях $x_{-j}(t)$ і $y_{-j}(t)$ відновити $x_{-j+1}(t)$ за допомогою формули (2.16). І так продовжувати до момента, коли буде знайдений початковий сигнал $x_0(t)$.

Відзначимо, що завдяки проріджуванню, вбудованому у формулу, коефіцієнтів $\{b_i\}$ і $\{c_i\}$ в сумі стільки ж, скільки і коефіцієнтів $\{a_i\}$. Тому представлення сигналу $x_0(t)$ у вигляді його масштабних компонент, скільки б їх не було, містить у сумі стільки ж числових значень, скільки і початковий сигнал.

Істотно, що в робочих формулах явно не беруть участь ні скейлінг-функція, ні вейвлет $\psi(t)$. Тільки на початковому етапі потрібно розкласти сигнал $x_0(t)$ за скейлінг-базисом. Проте якщо сигнал заданий у дискретному вигляді, то можна обійтися і без скейлінг-функції. Просто вважати, що заданий дискретний сигнал і є розкладання певного сигналу $x_0(t)$ в скейлінг-базисі.

Проте не треба вважати, що формули (2.15) і (2.16) справедливі при будь-якому виборі фільтру $h$. Цей фільтр має важливу характеристичну властивість, яку можна отримати, застосувавши першу з формул (2.15) до сигналу, заданого рівнянням (2.13):

$$\sum_s h_s^* h_{2i-s} = \delta_i \,, \qquad (2.17)$$

де $\delta_0 = 1$ — єдиний відмінний від нуля член послідовності $\{\delta_i\}$.

Виявляється, що якщо фільтр $h$ задовольняє цій властивості і деяким іншим менш істотним вимогам, то за ним можна відновити всю схему МА. Наприклад, скейлінг-функція $\varphi(t)$ отримується як рішення функціонального рівняння (2.12). Тому при побудові МА виходять саме з цієї умови, яка в зручнішому вигляді записується в термінах перетворень Фур'є:

$$\left|h(\omega)\right|^2 + \left|h(\omega+\pi)\right|^2 = 2. \qquad (2.18)$$

Родина рішень цього рівняння була знайдена Інгрід Добеши. При довжині фільтру $2_n$ вони дають вейвлет з $n$ нульовими моментами (2.5). Клас таких рішень досить вузький, і вони незручні з практичної точки зору. Наприклад, вони недостатньо гладкі і за винятком вейвлета Хаару ($n$ = 1) не можуть бути симетричними.

## 2.2.3. Біортогональний багатомасштабний аналіз і вейвлет-пакети

Можна вказати просту модернізацію конструкції МА, для якої клас допустимих фільтрів помітно ширше, вони можуть бути симетричними, достатньо гладкими і простіше обчислюються. Це — біортогональний МА (БМА). Для нього зберігається алгоритм Малла, але у формулах (2.15) для розкладання сигналу на складові і відновлення сигналу використовуються різні пари фільтрів. Пара $\{\tilde{h}, \tilde{g}\}$ при розкладанні і пара $\{h, g\}$ при відновленні. (Інакше кажучи, у формулах (2.15) над $h$ і $g$ потрібно поставити тильду, а формулу (2.16) залишити без зміни. Фільтри в кожній парі зв'язані співвідношенням вигляду (2.14). Кожній парі відповідають свої скейлінг-функція і вейвлет. Але породжені ними базиси не є ортогональними і не ортогональні один одному. Кожен із них біортогональний відповідному базису іншої пари фільтрів.

Характеристична властивість (2.18), що дозволяє знайти фільтри $h$ і $\tilde{h}$ в БМА, має вигляд:

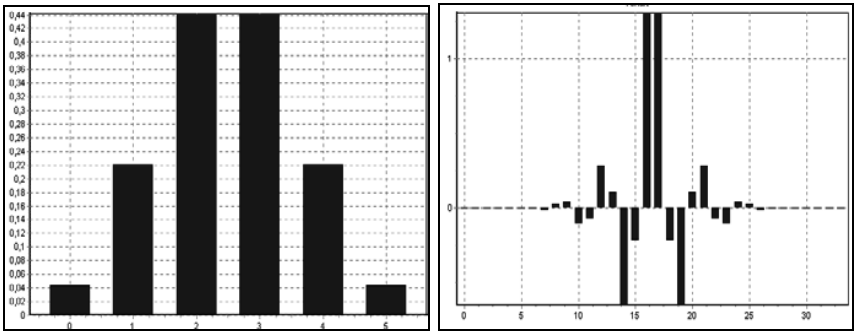
$$\overline{h(\omega)}\tilde{h}(\omega) + \overline{h(\omega+\pi)}\tilde{h}(\omega\pi) = 2. \qquad (2.19)$$

Для цього рівняння є родина рішень, залежна від двох параметрів:

$$h_n(\omega) = \sqrt{2}\left(\frac{1+e^{i\omega}}{2}\right)^n, \quad \tilde{h}_{n,m}(\omega) = \sqrt{2}\left(\frac{1+e^{i\omega}}{2}\right)^n P_m\left(\sin^2\frac{\omega}{2}\right)e^{-im\omega}, \quad (2.20)$$

де $P_m(x) = \sum_{s=0}^{m-1} C_{m-1+s}^{s} x^s$ — *багаточлен Добеши*.

Відповідне цим рішенням сімейство фільтрів є симетричним. Розкладаючий вейвлет має достатньо нульових моментів, що ростуть з номером, а гладкість поновлюючого вейвлета збільшується із зростанням параметра *m*. При цьому довжина фільтрів відповідно збільшується. Приклад фільтрів (n=5, m=10), використаних для конкретних обчислень, показаний на рис. 2.1 ($h, \tilde{h}$).



$h$ $\tilde{h}$

*Рис. 2.1.* Фільтри $h$ і $\tilde{h}$

Ефективність стиснення сигналу збільшується, якщо перейти до так званої схеми вейвлет-пакетів. Вона відрізняється від алгоритма Малла таким.

При першому кроці алгоритм Малла (в МА або БМА однаково) сигнал $x_0(t)$ розкладається на дві складові $x_{-1}(t)$ і $y_{-1}(t)$. За алгоритмом Малла друга складова $y_{-1}(t)$ запам'ятовується, а до першої складової $x_{-1}(t)$ застосовується процедура розкладання на дві складові.

За алгоритмом вейвлет-пакетів процедура розкладання застосовується і до другої складової $y_{-1}(t)$ і таким чином будується бінарне дерево.

Загальна схема обробки звукових сигналів представлена на рис. 2.2.

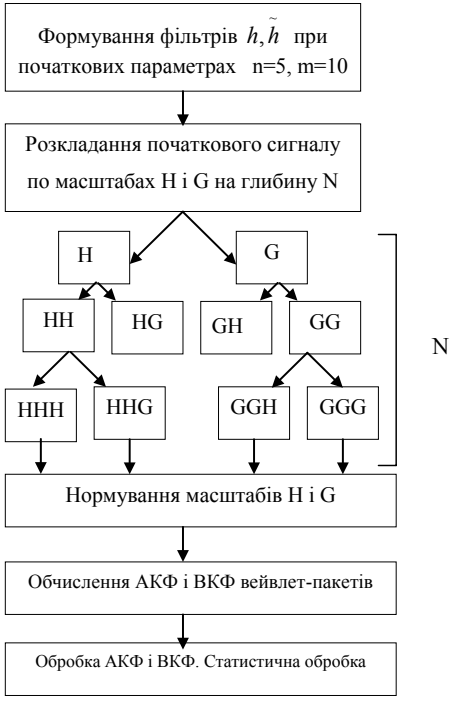



*Рис. 2.2.* Схема обробки звукових сигналів

## 2.3. Практичні результати

За запропонованою схемою обробки звукових сигналів (рис. 2.2) формується деревовидна структура розкладання, яка дозволяє представити початковий звуковий сигнал по відповідних масштабах $H_i$ і $G_j$. Необхідно відзначити, що за рахунок вибору оптимального дерева для цього класу сигналу можна підвищити ступінь і якість обробки. Вибір квазіоптимального «дерева» заснований на оцінці «інформативності» набору коефіцієнтів кожного масштабу, який визначає рівень «занурен-

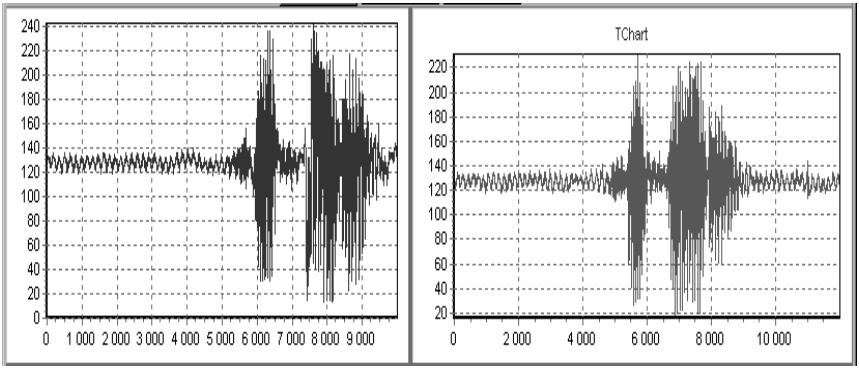
ня». Як початкові звукові сигнали використовувалися файли формату *.wav, що містять мовні повідомлення певного диктора.

При формуванні звукових файлів вибиралися такі параметри запису:

– розмірність звукових файлів (.wav) формату — 0,5–3,5 МБ;
– частота дискретизації сигналу — 8, 11, 22, 44 кГц;
– динамічний діапазон амплітуд звукового сигналу 0–255 або 8 біт;
– кількість каналів — моно.

Кількість масштабів визначається числом рівнів занурення N (рис. 2.2).

Після отримання вейвлет-пакетів на кожному рівні розкладання і їх нормування (застосування нормуючих операцій дозволить виключити з аналізу вплив абсолютного значення динамічного діапазону досліджуваних мовних сигналів) обчислюються автокореляційні функції кожного вейвлет-пакета. Чим більше рівень занурення (розкладання), тим більше вейвлет-пакетів необхідно обробити і обчислити їх АКФ. На рис. 2.3 представлені мовні повідомлення, вимовлені одним диктором (як зразок диктор вимовляв слово «чотири»).




*а)* *б)*

*Рис. 2.3.* Мовні сигнали одного диктора (слово «чотири»):
*а)* зображення еталонного мовного сигналу;
*б)* зображення досліджуваного мовного сигналу

Розкладання проводилося на глибину занурення, яка дорівнює 3, таким чином, число вейвлет-пакетів дорівнює $2^3 = 8$.

На рис. 2.4 представлені фільтри розкладання і відновлення при параметрах L=4, N=3, вирази (2.18, 2.19), глибина занурення (D) відповідно вибиралася рівною 3, а на рис. 2.5 приведені зображення вейвлет-пакетів кожної фрази (еталонної і досліджуваної).

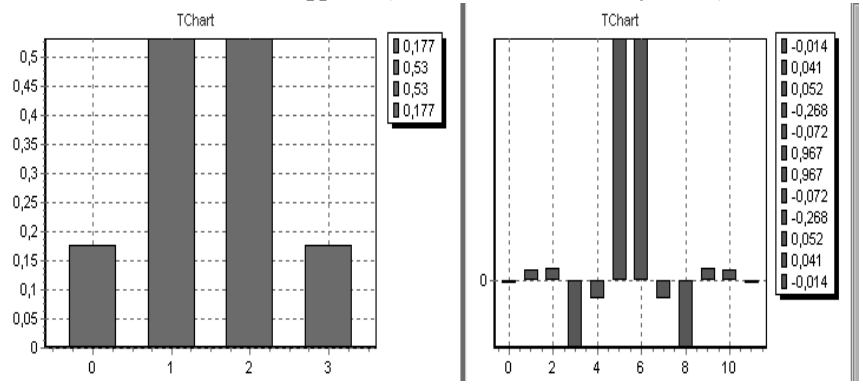
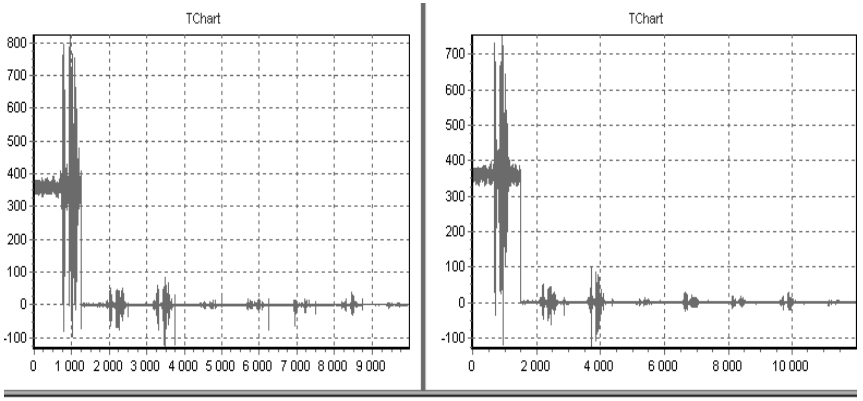


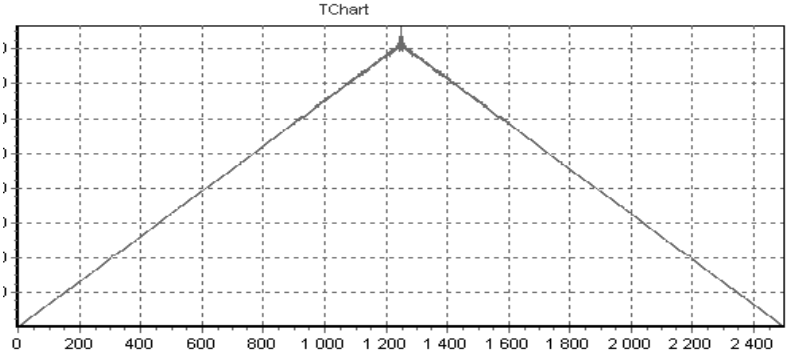

*Рис. 2.4.* Фільтри розкладання і відновлення при L=4, N=3, D=3



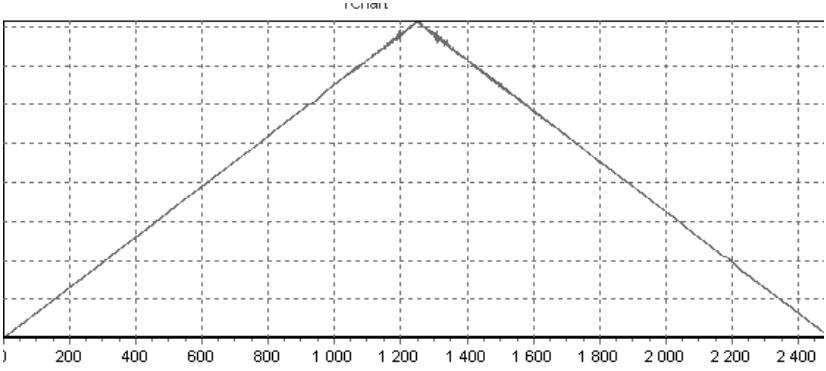

*а)* *б)*

*Рис. 2.5.* Зображення вейвлет-пакетів кожної фрази:
*а)* зображення вейвлет-пакетів еталонного мовного сигналу;
*б)* зображення вейвлет-пакетів досліджуваного мовного сигналу

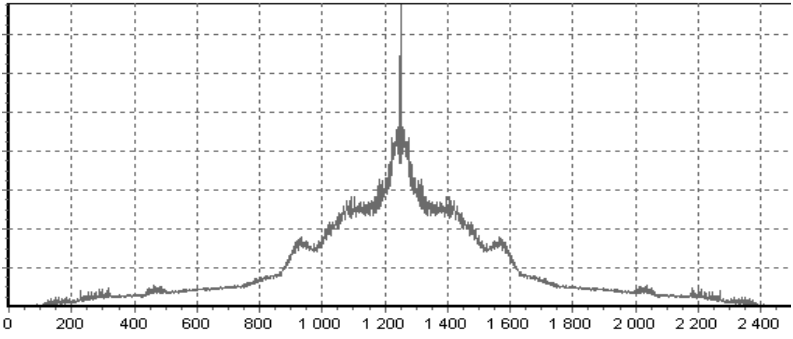
На рис. 2.6 представлені пари автокореляційних і взаємокореляційних функцій однойменних вейвлет-пакетів еталонного і досліджуваного мовного сигналу (всього 8 функцій).



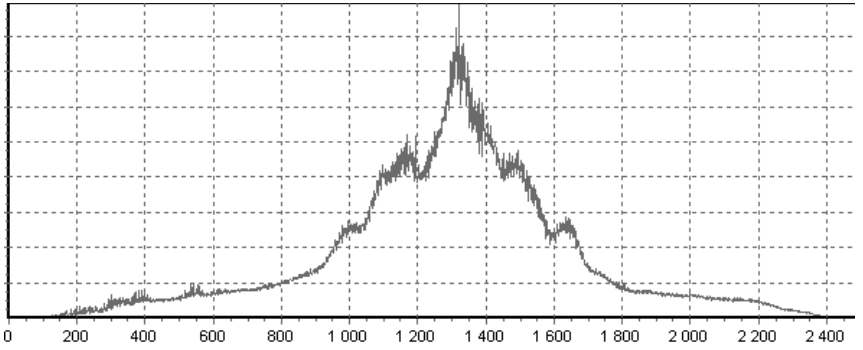

АКФ 1-го вейвлет-пакета



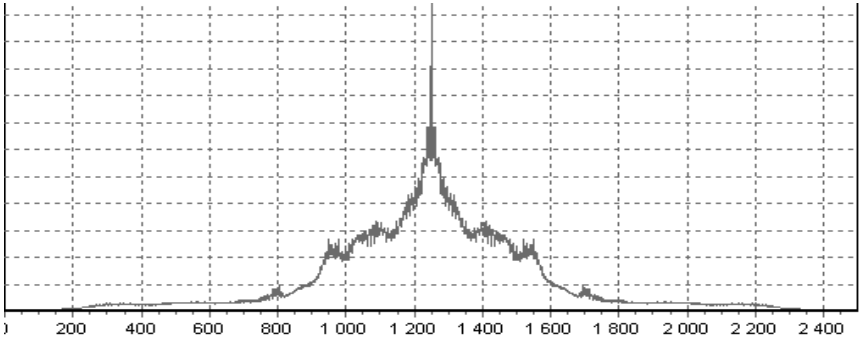

ВКФ 1-го вейвлет-пакета



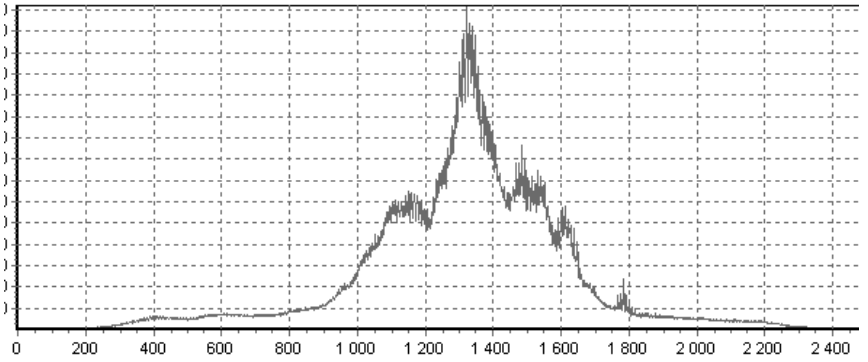

АКФ 2-го вейвлет-пакета



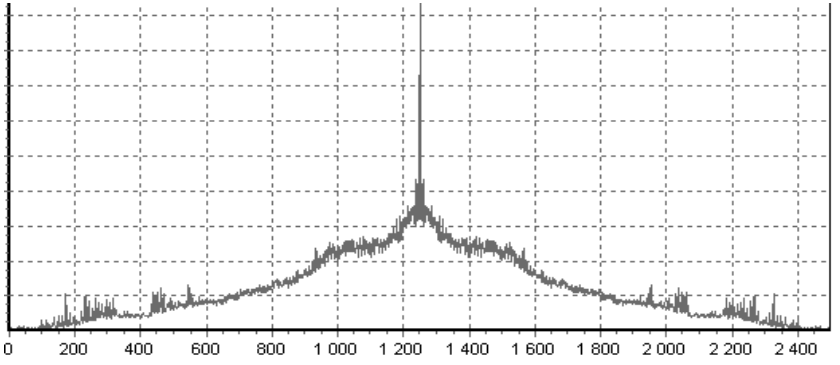

ВКФ 2-х вейвлет-пакетів



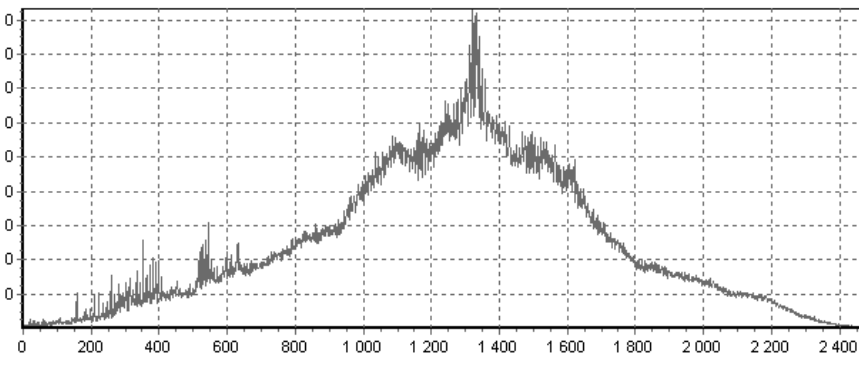

АКФ 3-го вейвлет-пакета



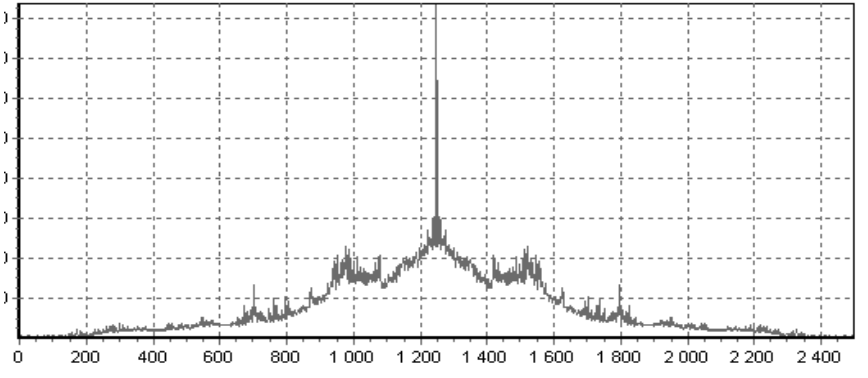

ВКФ 3-х вейвлет-пакетів



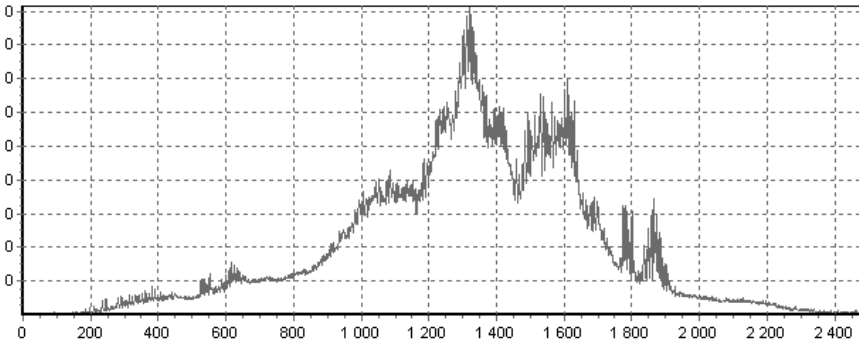

АКФ 4-го вейвлет-пакета



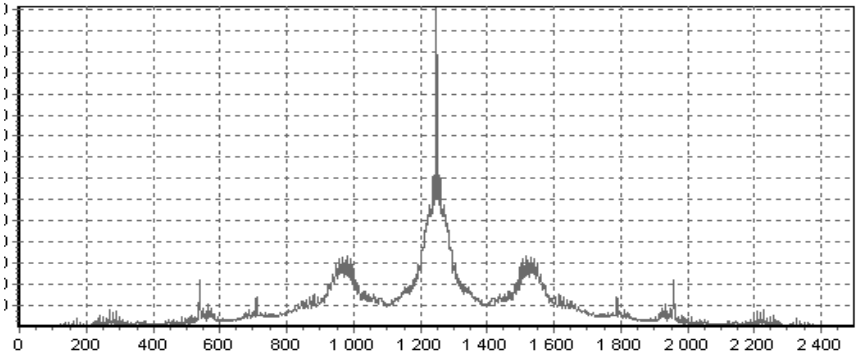

ВКФ 4-х вейвлет-пакетів



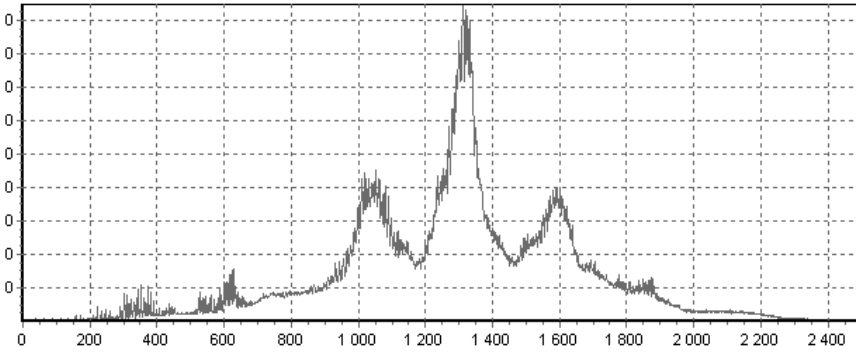

АКФ 5-го вейвлет-пакета



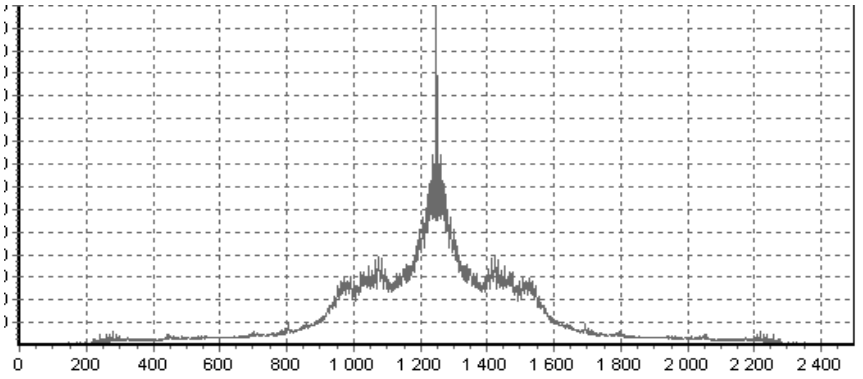

ВКФ 5-х вейвлет-пакетів



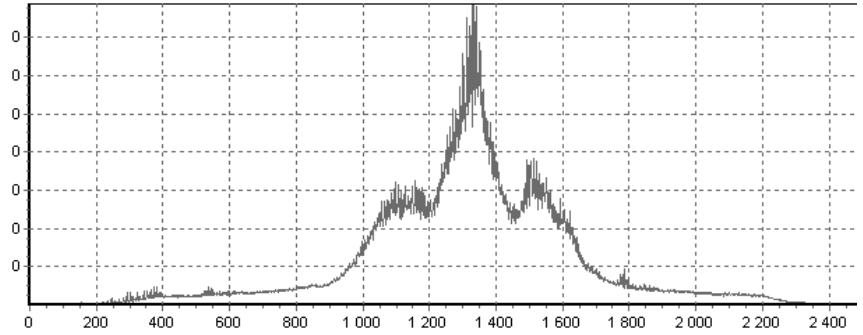

АКФ 6-го вейвлет-пакета



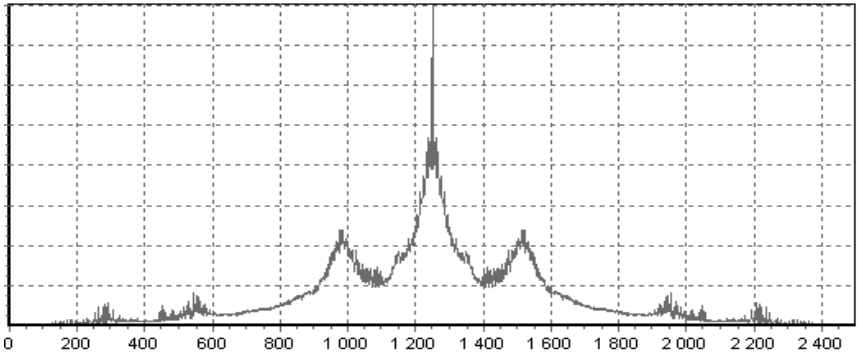

ВКФ 6-х вейвлет-пакетів



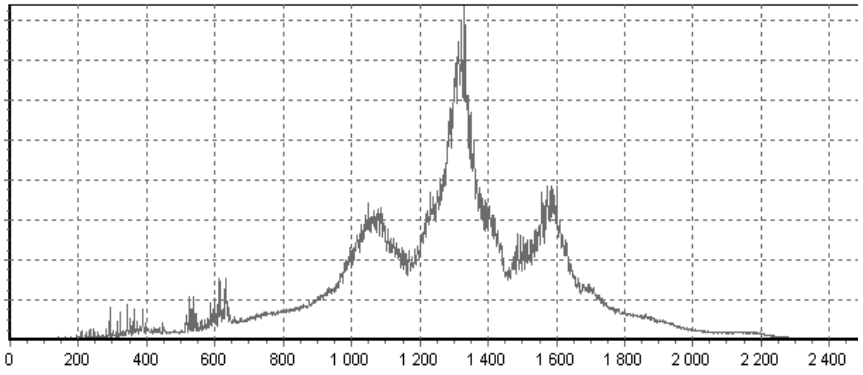

АКФ 7-го вейвлет-пакета




ВКФ 7-х вейвлет-пакетів




АКФ 8-го вейвлет-пакета




ВКФ 8-х вейвлет-пакетів

*Рис. 2.6.* Пари АКФ і ВКФ однойменних вейвлет-пакетів еталонного і досліджуваного мовного сигналу

Згідно з методикою оцінки ідентичності двох мовних повідомлень (еталонного і досліджуваного) після обчислення АКФ і ВКФ відповідних пакетів необхідно обчислювати середнє значення модуля різниці між однойменними відліками АКФ і ВКФ за умови поєднання максимальних значень нормованих кореляційних функцій. Незбіг максимумів АКФ і ВКФ однойменних вейвлет-пакетів пояснюється різним розташуванням еталонного і досліджуваного мовного сигналу у вікні часового аналізу. Це наочно можна побачити на рис. 2.3, де виразно спостерігається часове зрушення мовного сигналу один відносно одного. Тому максимальне значення ВКФ не збігатиметься з максимальним значенням АКФ. Факт неспівпадання максимальних значень кореляційних функцій не є інформативним з погляду ідентифікації диктора, що говорить.

З погляду ідентифікації мовного повідомлення цікава форма лінії, що огинає порівнювані кореляційні функції при поєднаних максимальних значеннях.

Далі необхідно порівняти значення усередненого модуля різниці АКФ і ВКФ кожного вейвлет-пакета при заданій глибині занурення з середньостатистичним порогом. Рішення про належність мовного сигналу одному дикторові ухвалюється після порівняння значення

усередненого модуля різниці АКФ і ВКФ кожного вейвлет-пакета з відповідним статистичним порогом. Перевищення статистичного порогу буде означати, що мовні сигнали належать різним дикторам.

## 2.4. Висновки

Очевидно, що наявні значні труднощі, які пов'язані з обчисленням статистичного порогу для кожного вейвлет-пакета при різних рівнях занурення. Для вирішення цього завдання буде потрібно як мінімум 50 реалізацій однієї фрази одного і того ж диктора. Додатково буде необхідно обчислити статистичний поріг на кожному рівні розкладання мовного сигналу за вейвлет-пакетами.

Подібний набір статистичного матеріалу вимагає певного часу для його створення, але надалі сформований банк даних значно прискорить час аналізу досліджуваних мовних сигналів.

Ще одну значну перевагу подібний підхід має за рахунок того, що при проведенні дослідження практично не вимагається вибору і обґрунтування інформативних ознак мовного сигналу, який підлягає дослідженню, оскільки сама форма кореляційної функції містить повну статистичну інформацію про мовний сигнал. І чим ближче статистичні характеристики авто- і взаємнокореляційних функцій порівнюваних мовних сигналів, тим більше підстав для ідентифікації диктора.

Розглянутий підхід з вирішення завдання ідентифікації особи за мовними сигналами цікавий тим, що він не вимагає конкретних ознак розпізнавання (і їх обґрунтування). Це відбувається за рахунок того, що обробка досліджуваних мовних сигналів здійснюється на основі отриманої статистичної інформації при дослідженні прообразів порівнюваних зразків з домінуючим змістом «тонкої» або «грубої» структури мовного сигналу, яка міститься в кожному вейвлет-пакеті. Сфера можливого застосування подібних систем — це автоматичні системи доступу за мовним повідомленням.

Подібні системи автоматичної ідентифікації дозволяють вирішувати поставлені завдання на рівні до 90 % правильного опізнавання диктора за мовним повідомленням. Цей процент значно нижчий ана-

логічних показників для систем ідентифікації за відбитками пальців людини або систем аналізу райдужної оболонки очного яблука, але системи ідентифікації людини за мовним повідомленням можуть бути використані як додаткові системи ідентифікації людини. Наведений метод також неможливо застосовувати, коли йдеться про великий потік людей, яких необхідно дуже швидко ідентифікувати за будь-якими біометричними даними, наприклад це збір біометричних даних у посольствах іноземних держав, при реєстрації пасажирів в аеропортах тощо.

Найбільш імовірне застосування подібних систем можливе в тих умовах, коли необхідно проводити багаторазову ідентифікацію однієї людини. У цьому випадку є сенс у часових витратах на формування банку даних мовних повідомлень одного диктора, розрахунок статистичних параметрів, отримання рівнів порогу допуску для подальшого їх використання при ідентифікації людини за мовним повідомленням.

# РОЗДІЛ 3

# СИСТЕМА ЕФЕКТИВНОГО КОДУВАННЯ ТА ПОШУКУ ЗОБРАЖЕНЬ ПЕЧАТОК І ШТАМПІВ «КЛІШЕ»

## 3.1. Загальна характеристика роботи

### 3.1.1. Автоматизовані інформаційні системи в криміналістичній діяльності

У загальному вигляді під автоматизованою інформаційною системою (АІС) розуміють таку інформаційну систему, у якій приведення в дію її основних компонентів здійснюється автоматичним пристроєм, дії якого піддаються математичному опису [1; 2; 3; 4].

У практичній реалізації будь-яка автоматизована інформаційно-пошукова система (ІПС) — це людино-машинна система, функціонування якої припускає наявність інформаційного фонду, реалізованого на машинних носіях; мови запитів і відповідей; технічних засобів введення, зберігання й обробки інформації, а також виведення запитуваних даних.

Інформаційний фонд АІС, які використовуються у сфері криміналістичної діяльності, може створюватися з інформації, що розрізняється за своєю генетичною природою і юридичним значенням. Перш за все це криміналістична інформація, тобто інформація, використання якої пов'язане з подією злочину, особою злочинця і його діями, а також діями суб'єктів, діяльність яких направлена на розкриття і розслідування злочинів або управління такою діяльністю.

Такого роду АІС правомірно називати власне криміналістичними або розглядати як основну ланку в структурі інформаційного забезпечення діяльності по боротьбі зі злочинністю [5; 6; 7].

Разом з ними останніми роками все більшого значення в плані інформаційного забезпечення криміналістичної діяльності (особливо судово-експертної) набувають АІС, інформаційний фонд яких комплектується з інформації, яка не має прямого зв'язку з конкретним злочином (злочинцем), але за певних обставин може бути використана як допоміжно-довідкова при вирішенні ряду криміналістичних завдань. Системи з таким інформаційним фондом часто називають банками допоміжних даних і розглядають їх як дуже важливий елемент у структурі інформаційного забезпечення органів кримінальної юстиції [8].

Не зважаючи на відмічену специфіку, названі системи мають і багато спільного. Так, крім їх цільового призначення — служити засобом оптимізації інформаційного забезпечення діяльності органів кримінальної юстиції — їх ріднить ряд загальних принципів організації і використання.

1. Як і будь-яка інша автоматизована інформаційна система, криміналістичні системи і банки допоміжних даних повинні створюватися лише в тих випадках, коли вирішувані ними завдання зустрічаються достатньо часто, не є тривіальними, а їх вирішення обмежене певними строками.

2. Розробку таких систем необхідно здійснювати фахівцями різних наукових галузей, серед яких повинні бути: фахівці з автоматизованих систем (системотехніки); фахівці того виду діяльності, для інформаційного забезпечення якої створюється система (оперативні працівники органів МВС, експерти, працівники картотек кримінальної реєстрації тощо); фахівці з організації і машинної обробки інформації в системі (математики-програмісти, фахівці з обчислювальної техніки і систем обробки даних різної фізичної природи).

3. Функціонуюча система повинна забезпечувати можливість її використання відповідними співробітниками органів кримінальної юстиції, зокрема, що не мають спеціальних пізнань у галузі обчислювальної техніки, але знайомі з принципами і умовами функціонування системи, а також особливостями підготовки відповідної інформації для її введення в ЕОМ і оцінки даних, що їх видає система.

Як показує практика, виконання цього принципу найповніше забезпечується включенням у структуру технічних засобів системи

дисплейних та інших периферійних пристроїв індивідуального і колективного користувача для уведення і виведення інформації, що зберігається в системі.

4. Оскільки криміналістичні інформаційні системи оперують з інформацією спеціального призначення, вони повинні бути організовані так, щоб виключався доступ до системи непередбаченого користувача або видачі інформації іншого роду.

5. Ефективність систем, зокрема інформаційно-пошукових, може бути забезпечена лише за умови, що введена в банк даних системи інформація використовується багато разів, а вводиться в систему один раз. Крім того, опис об'єкта пошуку, включеного в систему, й інформаційний запит на його пошук повинні відповідати один одному щодо засобів їх реалізації, зокрема, за прийнятою для цієї системи штучною інформаційно-пошуковою мовою.

6. Формалізована мова представлення об'єкта в системі повинна забезпечувати точність опису аж до його індивідуалізації, бути максимально ємною і нескладною у використанні.

7. Технічні засоби системи повинні забезпечувати можливість матеріальної фіксації даних, що їх видає система, і передачу користувачеві системи.

Вказаним вимогам (з урахуванням конкретного виду системи) краще всього відповідають системи з автоматизованим банком даних (АБД), який можна визначити «як систему інформаційних, математичних, програмних, мовних, організаційних і технічних засобів (включаючи дані, що зберігаються, а також персонал, зайнятий в технологічному процесі), призначену для централізованого накопичення і колективного багатоаспектного використання даних з метою отримання необхідної інформації».

### 3.1.2 Автоматизовані системи в судово-експертних дослідженнях

Вдосконалення провадження судових експертиз, як жоден інший вид криміналістичної діяльності, неможливий без сучасного інформаційного забезпечення і комп'ютерних технологій.

Це випливає з того, що, по-перше, в сучасних умовах об'єктами експертного дослідження можуть бути тисячі різновидів матеріалів, речовин і виробів, кожне з яких характеризується безліччю характерних для нього властивостей і ознак, а отже, інформацією про них. По-друге, отримання інформації про об'єкт дослідження і її аналіз можливі з використанням різних засобів і методів, на базі яких нині розроблена безліч методик вирішення експертних завдань, зокрема одного характеру. По-третє, арсенал об'єктів дослідження і вживаних для цього засобів і методів, що все розширюється, неминуче приводять до розширення кола завдань, які можуть бути вирішені у формі експертного дослідження.

Із цього випливає, що експерт повинен мати можливість оперувати величезним обсягом не лише криміналістичної, але і допоміжно-довідкової інформації стосовно об'єктів, методів і окремих методик експертного дослідження, а також вирішуваними за їх допомогою завданнями.

У цих цілях в експертних установах і створюються автоматизовані системи, банки даних яких акумулюють відповідну інформацію. Це перш за все інформаційно-пошукові системи. Проте роль інформаційного пошуку в таких системах має певну специфіку, яка виявляється вже в тому, що його можна розглядати як один із методів експертизи, оскільки без нього багато експертних завдань у принципі не вирішуються. До таких завдань можна віднести, наприклад, визначення вигляду й різновиду холодної зброї, фарного скла, типу і виду транспортного засобу, аналіз зображень відтисків печаток і штампів і так далі.

При цьому як теоретичні основи експертного інформаційного пошуку можуть бути використані загальні положення теорії криміналістичної ідентифікації, зокрема того її розділу, який присвячений класифікаційним методам встановлення групової приналежності. Проте специфіка тут полягає в тому, що ідентифікують пошукові ознаки, якими характеризуються об'єкти, введені до інформаційного фонду системи. Разом з тим слід зазначити, що процес інформаційного пошуку в цих системах відрізняється від процесу ідентифікації.

Перша з таких відмінностей полягає в тому, що, здійснюючи процес експертного дослідження певного об'єкта, експерт має можливість аналізувати і використовувати всю гаму ознак, що належать йому,

і властивостей, виокремлених у ідентифікаційному полі. Будь-яка ж ІПС оперує не зі всіма ознаками, а лише з тими, які введені в дану систему. При цьому може статися, що вони не повністю відповідають один одному за об'ємом і характером.

Результатом цього можуть бути дві негативні ситуації: або система видасть дуже велику кількість об'єктів (у числі яких буде і той, що його шукають), або відбудеться так званий «пропуск мети», тобто коли шуканий об'єкт хоча і буде знаходитися в інформаційному фонді, але система не видасть дані про нього, «не знайде» його.

От чому і позитивний результат інформаційного пошуку, строго кажучи, не може розглядатися як рівнозначний експертному дослідженню зі встановлення індивідуальної тотожності. Для вирішення цього питання необхідне судово-експертне дослідження. Власне ж інформаційний пошук можна розглядати як один з цих етапів, одну зі стадій такого дослідження.

Проте це ніяк не зменшує значення інформаційного пошуку і ролі самих ІПС цього типу, а навпаки говорить про їх важливість у загальній системі інформаційного забезпечення діяльності з розкриття і розслідування злочинів.

## 3.2. Математичні і технологічні основи побудови АІПС «КЛІШЕ» / АРМ Е-К

### 3.2.1. Інформаційно-пошуковий модуль АІПС «КЛІШЕ»

Традиційні інформаційні технології створення, розвитку і використання політематичних електронних бібліотек значною мірою орієнтовані на атрибутний пошук, коли він здійснюється, наприклад, за назвою документа, автором, датою, джерелом публікації, місцем публікації і так далі.

Становить інтерес комплексна технологія побудови автоматизованих криміналістичних інформаційно-довідкових електронних баз даних (інформаційно-аналітичних колекторів), об'єднуючих у собі,

окрім традиційних повнотекстових документів, ще і відеоінформацію: малюнки протекторів шин автомобільних коліс, конфігурації і малюнки моделей фарного скла, малюнки підошов взуття, зображення відтиснень печаток і штампів та ін. Таким чином, під багатофункціональним інформаційно-аналітичним колектором ми розуміємо апаратно-програмний комплекс управління і обробки скомпресованим інформаційним сховищем, що містить текстові і графічні файли.

Розроблений програмний комплекс складається з двох структурно-програмних модулів: Інформаційно-пошуковий модуль — автоматизована інформаційно-пошукова система «КЛІШЕ» і модуль «Автоматизоване робоче місце експерта-криміналіста».

Інформаційно-пошуковий модуль АІПС «КЛІШЕ» призначений для зберігання, відображення, перегляду, редагування і пошуку зображень відтисків печаток усіх районних відділень ДАІ УМВС України. Структура бази даних має конфігурацію, яка дозволяє за наявними атрибутами вносити до неї графічні зображення печаток і штампів будь-яких організацій і підприємств, які знаходяться як на території України, так і за кордоном.

Розробка програмного комплексу припускає виконання процедур формального представлення безлічі різних зображень, які належать одному з управлінь МВС України, а також формального відображення будь-якого зображення за допомогою безлічі його параметрів.

Для виконання формального представлення конкретного зображення печаток необхідно виокремити ряд параметрів, які дозволяють не лише його ідентифікувати, але і локалізувати, прив'язати до додаткових атрибутів. Це переслідує мету надання зацікавленим особам додаткової систематизованої інформації для оперативної роботи. Фактично реалізація цієї процедури зводиться до вирішення завдання параметризації зображення.

Класифікаційні ознаки (держава, область, район, організація, адреса, номер печатки) дозволяють кодувати зображення печаток у межах множини, але не дають повного уявлення про зображення. Для ідентифікації різноманітних зображень позначимо $n_{mas}^{cdr}$ зображення печатки у множині $\mu_0$, де $\mu_0$ — множина значень індексу n, в наочній області — обсяг реєстру печаток. Індекси c, d, r, m, a, s використову-

ються відповідно для позначення приналежності державі — c, області — d, району — r, організації — m, адресі — a, внутрішньому порядковому номеру — s. Використовуючи вказану систему класифікації, будь-яке зображення $n_{mas}^{cdr}$ формально можна представити таким чином:

$$n_{mas}^{cdr} = \left\{ c, d, r, m, a, s \middle| \begin{matrix} c = \overline{1,4}; d = \overline{1,26}; r = \overline{1,\approx 40}; \\ m = \overline{1,\approx 5}; a = \overline{1,\approx 5}; s = \overline{1,10} \end{matrix} \right\}, \quad (3.1)$$

а множина

$$\mu_0 = \sum_{c=1}^{4} \sum_{d=1}^{26} \sum_{r=1}^{40} \sum_{m=1}^{5} \sum_{a=1}^{5} \sum_{s=1}^{10} n_{mas}^{cdr}. \quad (3.2)$$

Розглянуту сукупність параметрів вважатимемо складовими множини $p^n$ параметрів, властивих кожному $n_{mas}^{cdr} \in \mu_0$. Ці вирази показують неоднорідність зображень і дозволяють забезпечити їх розділення на робочі групи для подальшої реєстрації, обліку і експлуатації в межах своєї групи. Формально, наприклад, групу печаток, що має однакове значення атрибуту держава, можна представити:

$$\Delta c = \sum_{d=1}^{26} \sum_{r=1}^{40} \sum_{m=1}^{5} \sum_{a=1}^{5} \sum_{s=1}^{10} n_{mas}^{cdr}. \quad (3.3)$$

Аналогічно виокремлюють групи за іншими ідентифікаційними ознаками. Наведені вирази є рішенням задачі формального подання множини зареєстрованих зображень печаток. Зображення разом із сукупністю ознак реєструються в структуровану базу даних (БД) під управлінням розробленого АРМ. Як модель даних у базі використовують класичну реляційну модель. За множиною $p^n$ сформовані таблиці БД. Таблиці знаходяться в нормалізованих відносинах відповідно до правил Кодда. ERD (Entity Relation Diagram) семантичної моделі даних представляє зоряно-ієрархічну форму, що поєднується.

Практична реалізація розглянутої моделі виконана за допомогою СУБД InterBase з використанням мови SQL для визначення і маніпулювання даними в таблицях.

Основні режими роботи АІПС «КЛІШЕ»: режим «Просмотр», режим «Поиск», режим «Расширенный поиск», режим «Редактирование», режим «Бланки». Вибір режимів виконується незалежно.

Режим «Просмотр» дозволяє здійснювати перегляд загального виду зображень відтисків печаток, проводити вибір фрагмента зо-

браження з необхідним коефіцієнтом збільшення, встановлювати прямокутну сітку із заданим значенням осередка на досліджуваному зображенні, проглядати інформацію про атрибути відтисків і реквізити власника печаток. Вибір зображення відтисків печаток проводиться в діалоговому режимі за допомогою списків-меню за будь-яким з атрибутів.

Пошукові функції системи реалізовані в режимі «Поиск» і дають можливість здійснювати пошук зображень відтисків печаток у базі даних за всіма заданими атрибутами (повним або частковим), реквізитами власника цієї печатки, а також за часовими параметрами експлуатації печаток. Пошук зображень відтисків печаток здійснюється в короткому часовому інтервалі, незалежно від кількості шуканих зображень, заданих у запиті пошуку. Одна з основних особливостей цієї системи полягає в тому, що обсяг одного запису основного довідника складає в середньому 2,5 Мб. Ця обставина накладає певні обмеження на швидкодію системи в цілому. У зв'язку з цим при операціях пошуку був узятий за основу механізм динамічного створення уявлень, відповідних вказаним критеріям пошуку. Цей метод рідко використовується в теорії баз даних, оскільки база даних повинна бути статичною і об'єкти бази не повинні змінювати свою структуру. Використовуючи такий метод, час пошуку не залежить від обсягу таблиці і при правильному визначенні індексів час вибору даних, що задовольняють заданим атрибутам пошуку, змінюється небагато і лежить в межах 1с (залежно від вибраного сервера БД і апаратної потужності комп'ютера). Слід відмітити, що цей метод не накладає обмежень на використання цієї системи при мережевому варіанті доступу до даних.

При мережевому варіанті доступу до даних слід враховувати, що передача по мережі таких великих обсягів інформації не є доцільною. У зв'язку з цим всі зображення (як найбільш об'ємний масив даних) перед записом у базу необхідно стиснути, а перед відображенням проводити декомпресію. Подібні операції можуть привести до деяких часових затримок (які, втім, можуть бути в кілька разів менше, ніж при реалізації системи без методів компресії і недостатньо великій пропускній спроможності каналів передачі даних), а також «потовщення» клієнтської частини програми, тобто частина навантаження по обробці масивів даних повинна бути перенесена на клієнтське місце.

Вибір методів і алгоритмів компресії (стиснення) даних базувався на узагальненні і розвитку результатів робіт [9; 10; 11], а також інтеграцію їх з методами вейвлет-перетворень на основі універсальних конструкцій функцій ортогонального базису Хаара [12; 13] і статистичного кодування [14]. Переваги обробки повідомлень з використанням ортогональних перетворень випливають з особливостей розподілу енергії серед коефіцієнтів перетворення. Унаслідок кореляційних зв'язків між елементами початкового повідомлення енергія його узагальненого спектру виявляє тенденцію концентруватися у відносно невеликому числі відліків, тобто елементи $y_i$ ($y_{ij}$) вектора (матриці) $Y$ в перетвореному просторі, на відміну від компонент початкового вектора (матриці) $X$, мають різну інформативність. Хай ця інформативність може бути оцінена дисперсією елементу $y_i$ ($y_{ij}$). Це приводить до простої ідеї подальшої обробки перетвореного повідомлення: кожен елемент $y_i$($y_{ij}$) квантується числом $M_i$($M_{ij}$), залежним від дисперсії цього елементу, кодується і потрапляє на зберігання або передачу. При цьому, очевидно, доцільно в більш інформативні елементи вносити менші помилки (квантування з великим числом рівнів), ніж у малоінформативних (грубе квантування). Така процедура обробки в літературі називається кодуванням шляхом лінійних перетворень і блокового квантування та дозволила істотно скоротити обсяг графічних цифрових даних у системі.

Подальше підвищення ефективності стиснення можливе шляхом об'єднання статистичних методів кодування, методів на основі узагальнених ортогональних перетворень, вейвлет-перетворень і структурних методів розпізнавання образів, що дозволить розглядати ці методи з єдиних позицій і вирішити завдання гранично стислого опису об'єктів дослідження.

Доступ до системи в цілому не має будь-яких обмежень і визначається лише правами користувача в операційній системі.

У зв'язку зі специфікою інформації, що зберігається і знаходиться в базі даних, права користувача обмежені тим рівнем, який йому наданий адміністратором БД. У базі даних представлено три рівні доступу: адміністратор БД, досвідчений (відповідальний) користувач і звичайний користувач. Адміністратор БД має всі права на перегляд,

пошук і редагування даних, а також права на установку/зняття аудиту даних, конфігурацію і оптимізацію роботи сервера БД. Досвідчений (відповідальний) користувач має права на перегляд, пошук і редагування даних, але не має прав на роботу з аудитом, конфігурацією і оптимізацією роботи сервера БД. Звичайний користувач має права тільки на перегляд і пошук даних. Ідентифікація користувача відбувається на етапі запуску програми, шляхом введення імені і пароля користувача. Захист даних забезпечується засобами сервера БД.

Цей підхід є достатнім на сучасному рівні захисту серверів БД і в той же час дозволяє максимально спростити логіку програми, оскільки механізм забезпечення безпеки доступу до даних повністю покладений на сервер БД.

У цілому система орієнтована на користувача-непрофесіонала у сфері інформаційних технологій, містить інтуїтивно зрозумілий інтерфейс і контекстну допомогу, а діалог ведеться в інтерактивному режимі з контролем правильності дій користувача і блокуванням тупикових ситуацій.

Усі графічні зображення печаток і штампів, які знаходяться в базі, мають роздільну здатність 1200 dpi, глибину кольору — 8 біт. Вибір таких параметрів зображень заснований на вимогах, які ставляться до проведення експертних досліджень. Але ці параметри не є обов'язковими, в обох програмних модулях передбачена можливість використання графічних файлів з нижчою роздільною здатністю 150, 300, 600 dpi і довільною глибиною кольору.

### 3.2.2. Структурно-програмний модуль «Автоматизоване робоче місце експерта-криміналіста»

Структурно-програмний модуль «Автоматизоване робоче місце експерта-криміналіста» (АРМ Е-К) є самостійним програмним продуктом, але може використовуватися разом з інформаційними архівами, які зберігають зображення в графічних форматах представлення даних.

Програмний модуль «Автоматизоване робоче місце експерта-криміналіста» призначений для автоматизації проведення експертних криміналістичних досліджень і складання тексту експертного висновку.

Однією з основних функцій цього модуля є метод автоматичного накладення сітки на досліджуване зображення.

У програмному модулі «АРМ Е-К» використовується об'єктна модель стандартного шаблону сітки накладення. При побудові стандартного шаблону сітки накладення радіальної структури використовується векторна графіка, яка має ряд переваг перед растровим зображенням. Менший обсяг даних сприяє вищій швидкості і точності обробки інформації. Це особливо актуально при виконанні таких операцій, як: редагування шаблону, модифікація, переміщення в декартовій і азимутній системах координат.

Виходячи з того, що шаблони сіток накладення за своєю природою є «властивостями» растрових зображень, якими представлені всі відтиски печаток, наявні в базі даних, опис шаблонів зручно подати у вигляді множини точок таких, що задовольняють певним виразам. Загальний вигляд стандартного шаблону сітки накладення представлений на рис. 3.1. Як бачимо з рис. 3.1, стандартний шаблон сітки накладення має радіально-азимутну структуру, тому доцільно спочатку представити вираз, що описує радіальну складову (кола різного радіусу зі спільним центром), і окремо виділити азимутну складову.


*Рис. 3.1.* Зображення з відмітками

Вираз, що характеризує радіальну структуру стандартного шаблону сітки накладення, можна представити як поєднання деяких підмножин. Кожне коло стандартного шаблону сітки накладення може бути представлене множиною ($A_i$) такого вигляду:

$$A_i = \left\{ (X,Y) \in R^2 \;\middle|\; (X - X_0)^2 + (Y - Y_0)^2 = r_i^2 \right\}, \qquad (3.4)$$

де $A_i$ — геометричне місце точок на площині, що задовольняють рівнянню $(X - X_0)^2 + (Y - Y_0)^2 = r_i^2$;

$R^2$ — площина можливих значень, яка визначається растровим зображенням відтиску печаток;

($X$, $Y$) — координати точки, що лежить на колі з радіусом $r_i$ і з центром кола в точці з координатами $X_0$, $Y_0$.

Для побудови радіальної структури необхідно використовувати сукупність множини точок, представлених виразом (3.4). Кінцевий вираз має вигляд:

$$B = \bigcup_{i=1}^{N} A_i , \qquad (3.5)$$

де $A_i$ представлено виразом (3.4), а $B$ — множиною точок, які створюють радіальну структуру стандартного шаблону сітки накладення з кількістю кіл, рівних $N$, і загальним центром у точці з координатами $X_0$, $Y_0$. Азимутна складова формується як окрема підмножина точок і об'єднується з виразом (3.5).

Модуль «АРМ Е-К» дозволяє також в автоматизованому режимі сформувати звіт, який буде поміщений у файл формату Word-документ. При формуванні звіту вибирається зображення або фрагмент зображення.

Поле відміток (додаткове поле) формується автоматично і розташовано праворуч від зображення і завжди містить інформацію про збільшення зображення щодо реального друкарського відбитку у форматі «М 1:Х». Установка відміток здійснюється в напівавтоматичному режимі із «жорсткою» наскрізною нумерацією. При редагуванні відміток наскрізна нумерація підтримується автоматично. Коментарі до відміток записуються у звіт, який можна завантажити з реєстру вимірювань або з файлу. Звіт зберігається у форматі .rtf, який сумісний з форматом текстового процесора Word.

Вибраний фрагмент зображення разом з відмітками можна зберегти у файл формату .bmp (рис. 3.1) і надалі використовувати спільно з текстовою інформацією звіту.

# 3.3. Аналіз можливостей стиснення даних архіву зображень печаток і штампів АС «КЛІШЕ»

## 3.3.1. Кодування кольорових зображень на основі узагальнених перетворень Фур'є в термінах JPEG-технологій

Кодування кольорових зображень на основі узагальнених перетворень Фур'є в термінах JPEG-технологій можна представити у вигляді блок-схеми, зображеної на рис. 3.2.

У цій схемі кольорове зображення представлене сигналами координат кольору джерела *R(j,k), G(j,k), B(j,k)*, що визначають червону, зелену і сині складові для кожного елементу зображення з координатами (*j,k)*.

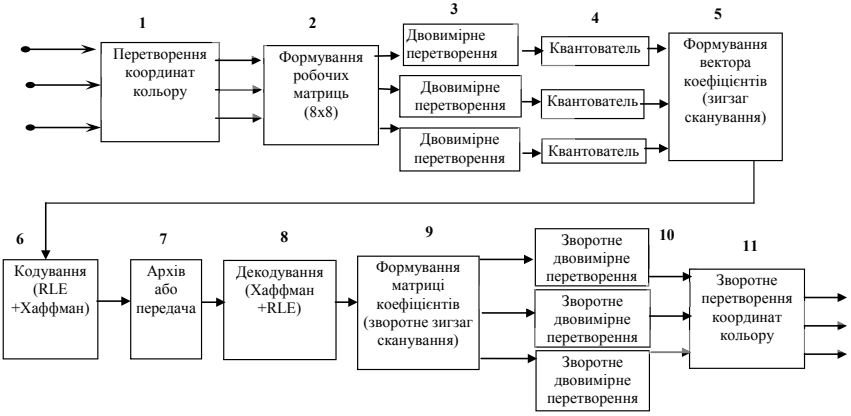



*Рис. 3.2.* Схема кодування кольорових зображень у термінах JPEG-технологій

На першому кроці система координат кольору джерела перетвориться на іншу тривимірну систему координат *Y(j,k), Cr(j,k), Cb(j,k)*. У ній *Y(j,k)* — складова яскравості, а *Cr* і *Cb* — компоненти, що відповідають за колір (хроматичний червоний і хроматичний синій). Перетворення координат визначається таким чином:

$$\begin{vmatrix} Y(j,k) \\ Cb(j,k) \\ Cr(j,k) \end{vmatrix} = \begin{vmatrix} 0{,}299 & 0{,}587 & 0{,}114 \\ 0{,}5 & -0{,}4187 & -0{,}0813 \\ 0{,}1687 & -0{,}3313 & 0{,}5 \end{vmatrix} \times \begin{vmatrix} R(j,k) \\ G(j,k) \\ B(j,k) \end{vmatrix} + \begin{vmatrix} 0 \\ 128 \\ 128 \end{vmatrix}. \quad (3.6)$$

Сигнали *Y*, *Cr* і *Cb* зручніше кодувати, ніж координати кольору R, G, B з тієї причини, що ці сигнали значною мірою декорельовані і основна частина їх енергії припадає на компоненту *Y*. У результаті з'являється можливість застосувати ефективніший квантователь за рахунок того, що людське око менш чутливе до кольору, ніж до яскравості, з'являється можливість зберігати масиви для *Cr* і *Cb* компонент з великими втратами і відповідно великими коефіцієнтами стиснення.

На другому кроці алгоритму здійснюється формування робочих матриць. З цією метою початкове зображення розбивається на матриці 8×8 і з кожної формується три робочі матриці по вісім біт окремо для кожної компоненти. При збільшенні ступеня стиснення зображення ділиться після компоненту *Y* як і в першому випадку, а для компонент *Cr* і *Cb* матриці набираються через рядок і через стовпець. Тобто з початкової матриці розміром 16×16 виходить тільки одна робоча матриця для ортогонального Фур'є-перетворення. При цьому не складно побачити, що ми втрачаємо в отриманій інформації колірні складові зображення і відразу отримуємо стиснення в два рази. На результуючому зображенні RGB, як показала практика, це позначається не сильно.

На вибір розмірності робочих матриць кодування роблять впливи дві взаємно суперечливих вимоги. З одного боку, вигідно збільшувати розміри одночасно кодованих груп елементів зображення для кращого використання зв'язків між ними, з другого боку, при цьому швидко зростають обчислювальні труднощі. Експерименти показали, що при збільшенні розмірів більш ніж 16×16 для всіх типів перетворень при фіксованому коефіцієнті скорочення цифрового потоку зменшення середнього квадрата помилки стає незначним, а труднощі реалізації різко збільшуються. Тому практично зручним компромісом є вибір матриць розмірності 8×8.

Ефективність схеми стиснення з використанням JPEG-технологій у цілому залежить від того, наскільки добре виконує свою роль кож-

не з перетворень, вироблюване в процесі всього ланцюжка кодування. Тривимірне перетворення координат кольору перерозподіляє енергію між трьома компонентами колориметричного опису зображення з метою її концентрації. Двовимірне перетворення перерозподіляє потім енергію кожної компоненти окремо, концентруючи її у вузькій області спектру.

У результаті прямого унітарного перетворення матриці зображення $F(n_1, n_2)$ розміру $N_1 \times N_2$ утворюється матриця перетвореного зображення того ж розміру, елементи якої дорівнюють:

$$F(m_1, m_2) = \sum_{n_1=1}^{N_1} \sum_{n_2=1}^{N_2} F(n_1, n_2) A(n_1, n_2; m_1, m_2), \tag{3.7}$$

де $A(n_1,n_2;m_1,m_2)$ — ядро прямого перетворення.

Перетворення називають роздільним, якщо його ядро можна представити в такі формі:

$$A(n_1,n_2;m_1,m_2) = AC(n_1,m_i)\, AR(n_2,m_2), \tag{3.8}$$

де через $AC$ і $AR$ позначені відповідно одновимірні оператори перетворення рядків і стовпців. Тому результат дії двовимірного унітарного перетворення можна знаходити у два етапи. Спочатку виконується одновимірне перетворення за всіма стовпцями матриці зображення, причому утворюється матриця з елементами:

$$P(m_1, n_2) = \sum_{n_1=1}^{N_1} F(n_1, n_2) A_C(n_1, m_1). \tag{3.9}$$

Потім виконується друге одновимірне перетворення за всіма рядками отриманої матриці, в результаті якого утворюється масив чисел вигляду:

$$F(m_1, m_2) = \sum_{n_2=1}^{N_2} P(m_1, n_2) A_R(n_2, m_2). \tag{3.10}$$

Ядро одновимірного косинусного перетворення для третього кроку має такий вигляд:

$$L_x(0) = \frac{1}{\sqrt{N}} \sum X(m); \qquad L_X(R) = \sqrt{\frac{2}{N}} \sum_{m=0}^{N-1} X(m) \cos \frac{(2m+1)k\pi}{2N}. \tag{3.11}$$

У цій формулі $X(m)$ значення звітів у рядках відповідних робочих матриць, отриманих на другому кроці JPG-технологій, $Lx(k)$ — коефіцієнти дискретного косинусного перетворення, а значення $m$ змі-

нюються відповідно від *0* до *N-1* і від 1 до *N-1* з кроком один. Слід відмітити, що множина базисних векторів

$$\left\{\frac{1}{\sqrt{N}}, \sqrt{\frac{2}{N}}\cos\frac{(2m+1)k\pi}{2N}\right\} \tag{3.12}$$

фактично утворює клас дискретних багаточленів Чебишева [15]. Якщо задатися визначенням багаточленів Чебишева у вигляді:

$$T_0(p) = \frac{1}{\sqrt{N}} \quad \text{і} \qquad T_k(Z_m) = \sqrt{\frac{2}{N}}\cos\left[k\arccos(Z_m)\right], \tag{3.13}$$

де *m* змінюється від *1* до *N-1*, а $T_k(Z_m)$ є *к-й* багаточлен Чебишева, то нулі N-го багаточлена $T_N(Z_m)$ можуть бути визначені з формули:

$$Z_m = \cos\frac{(2m+1)k\pi}{2N}, \tag{3.14}$$

де *m=0, 1 . . . N-1*.

Підставляючи вираз (3.14) в (3.13), визначимо значення $\{T_l(Z_m)\}$, *l=0, 1 . . N-1* в нулях $T_N(Z_m)$. Ця процедура приводить до множини дискретних багаточленів Чебишева:

$$T_0(m) = \frac{1}{\sqrt{N}}, \quad T_k(m) = \sqrt{\frac{2}{N}}\cos\frac{(2m+1)k\pi}{2N}, \qquad m=0, 1 \ldots N-1, \tag{3.15}$$

які еквівалентні множині базисних векторів дискретного косинусного перетворення.

У разі використання перетворень Хаара для отримання коефіцієнтів необхідно обчислити попередньо узагальнені проміжні суми Хаара:

$$X_i^n = \sum_{k=2i-1}^{2i} X_k^{n-1}, \text{ при } n=1,2...(logN-1),\ i = 1,2,...\frac{N}{2^n}, \tag{3.16}$$

а потім отримати і самі коефіцієнти:

$$C_{mj} = \frac{1}{N}2^{\frac{m-1}{2}}\left[X_k^{(\log N-1)-m} - X_{k+1}^{(\log N-1)-m}\right], \tag{3.17}$$

де *m=1, 2 . . . logN*; $j=2^{m-1}$, а для виразу, що стоїть в квадратних дужках, *m=m–1; k=2j–1*.

Вільний член визначається виразом:

$$C_{01} = \frac{1}{N}\left[X_k^{(\log N-1)} + X_{k+1}^{(\log N-1)}\right], \tag{3.18}$$

причому значення $X^0_к$ в (3.16) є початковими даними матриць яскравості і кольоровості.

При цьому як і в разі дискретного косинусного перетворення, так і в разі перетворення Хаара, ми отримуємо матриці, в яких коефіцієнти в лівому верхньому кутку відповідають низькочастотній складовій зображення, а в правому нижньому — високочастотною.

Процес квантування в схемі на рис. 3.2 є простим діленням отриманих матриць після перетворення на матрицю квантування поелементно. Для кожної компоненти (*Y*, *Cr*, *Cb*) в загальному випадку задається своя матриця квантування (МК) q(u,v):

$$Yq(u,v) = Ц\left[\frac{Y(u,v)}{q(u,v)}\right], \qquad (3.19)$$

де *Ц*[] означає цілу частину числа.

На цьому кроці здійснюється управління ступенем стиснення і відбуваються найбільші втрати. Задаючи МК з великими коефіцієнтами, ми отримаємо більше нулів і, отже, великий ступінь стиснення, що рівносильно методу зонального відбору значущих коефіцієнтів.

У стандарт JPEG включені рекомендовані МК, які побудовані дослідним шляхом. Так, для складової яскравості використовується вектор значень, отриманий з матриці МК, рівний 16, 11, 12, 14, 12, 10 . . . 60, 57, 51, 56, 103, 104, 103, 62, 77, 113, 121, 112, 100, 120, 99, 101, 109, 99, а для складових кольору — 17, 18, 18, 24, 21, 24, 47, 26, 26, 47, 99, 66, 56, 66, 99, 99, 99. Матриці для більшого або меншого коефіцієнтів стиснення отримують шляхом множення МК на певне число. Втрати в низьких частотах можуть бути настільки великі, що зображення розпадається на квадрати 8×8. Втрати у високих частотах можуть виявитися в так званому «ефекті Гіббса», коли навколо контурів з різким переходом кольору утворюється своєрідний ореол.

Подальші кроки алгоритму вимагають перекладу матриці коефіцієнтів перетворення на 8×8 в 64-елементний вектор за допомогою «зигзаг»-сканування, тобто беруться елементи з індексами (0,0), (0,1), (1,0), (2,0) і так далі (рис. 3.3). Це дозволяє отримати достатньо однорідну і регулярну двійкову структуру.

Кодування масиву двійкових значень здійснюється з використанням відомих алгоритмів стиснення без втрат — алгоритму групового кодування RLE і алгоритму Хаффмана.

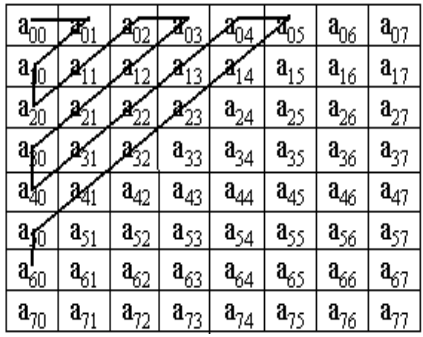



*Рис. 3.3.* «Зигзаг»-сканування (вибір) коефіцієнтів

Процес відновлення зображень у схемі JPEG-стиснення повністю симетричний.

### 3.3.2. Аналіз практичних результатів стиснення зображень печаток АІПС «КЛІШЕ»

Використання дискретного косинусного перетворення (ДКП) при обробці статичних зображень у структурі технології JPEG, а також сама ідеологія представлення зображень при обробці (розбиття всього зображення на сегменти 8×8 з попереднім переходом від компонент кольоровості RGB до яскравості і хроматичним складовим кольоровості) приводять до того, що тонка структура початкового зображення, особливо чіткі і контрастні переходи є достатньо важким матеріалом для методів стиснення з втратами даних. Ця обставина підтверджується експериментально при обробці архіву зображень печаток і штампів АС «КЛІШЕ» з різним значенням рівнів квантування коефіцієнтів. Стиснення зображення майже удвічі є оптимальним з погляду представлення зображення з метою його подальшої багатофункціональної обробки в програмному модулі АРМ Е-К (рис. 3.4 (б)).

Треба відзначити, що практично отримане стиснення забезпечують ентропійні методи кодування, які застосовуються в цій технології. Подальше збільшення рівня квантування коефіцієнтів, отриманих після ДКП, приводять до істотного погіршення початкового зображення, хоча при цьому зростає коефіцієнт стиснення (рис. 3.4 (в, г)).


Оригінал: 256×256, 8-битий RGB, 96 dpi, V=65 kb *(а)*


K=2.0; J=150 *(б)*


K=4.0; J=320 *(в)*


K=6.0; J=430 *(г)*

*Рис. 3.4.* ДКП JPEG:
*а* — оригінал зображення; *б* — коефіцієнт стиснення 2 рази;
*в* — коефіцієнт стиснення 4 рази; *г* — коефіцієнт стиснення 6 разів

Аналогічна ситуація, але з ще нижчою якістю при відновленні, простежується і при використанні перетворення Хаара в структурі JPEG-технології. Максимально допустимий рівень стиснення так само не більше 2 разів з урахуванням стиснення без втрат (рис. 3.5 (а, б, в, г)).

Висновок: для подальшої обробки придатні зображення при коефіцієнті стиснення не більш 2 разів, як для ДКП, так і для перетворення Хаара в структурі JPEG-технології.


K=2.0; J=19 *(а)*


K=4.0; J=40 *(б)*


K=6.0; J=52 *(в)*


K=8.0; J=70 *(г)*

*Рис. 3.5.* Перетворення Хаара JPEG:
*а* — коефіцієнт стиснення 2 рази; *б* — коефіцієнт стиснення 4 рази;
*в* — коефіцієнт стиснення 6 разів; *г* — коефіцієнт стиснення 8 разів

Перетворення Хаара в структурі вейвлет-технологій має більш стаціонарний характер залежності зміни коефіцієнта стиснення від середньоквадратичної помилки (СКП), що вноситься (рис. 3.6). Збільшення помилки обумовлене вищим рівнем квантування вейвлет-коефіцієнтів, які піддаються пороговій обробці і забезпечують більш рівномірний розподіл вейвлет-коефіцієнтів (W-коефіцієнтів) перед ентропійним кодуванням.

**Використання перетворення Хаара**
**і «довгих» фільтрів у вейвлет-технології**

| E | 0,04 | 0,06 | 0,08 | 0,1 | 0,12 | 0,13 | 0,15 | 0,16 | 0,17 |
|---|---|---|---|---|---|---|---|---|---|
| K Haar | 1,5 | 2,4 | 3,5 | 4,8 | 6 | 8 | 9 | 11 | 12 |
| K long | 1,5 | 1,6 | 1,8 | 4 | 6 | 7 | 8 | 11 | 12 |

Вейвлет-перетворення з використанням квадратурних дзеркальних фільтрів з параметрами формування: (D=4) — глибина занурення, (N=3, L=9) — параметри фільтрів, назвемо вейвлет-«long». На рис. 3.7 (а, б, в, г) наведені практичні результати компресії зображень при використанні вейвлет-«long».

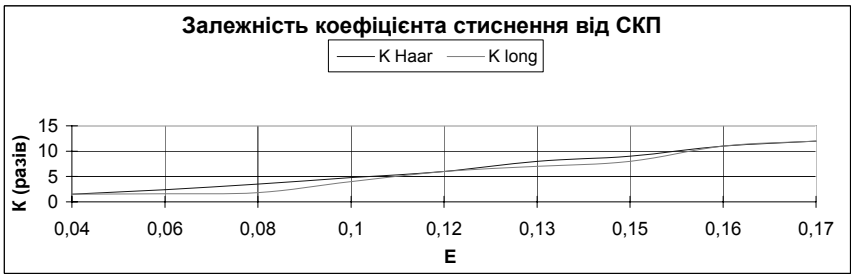



*Рис. 3.6.* Залежність до стиснення
від середньоквадратичної помилки (СКП)

За таких параметрів формування довжина розкладаючого фільтра становить близько 30 відліків, що порівняно з аналогічним фільтром, який забезпечує отримання вейвлетів Хаара (2 відліки), значно більше. Ця обставина істотно впливає на швидкість обчислення вейвлет-коефіцієнтів при виконанні операції згортки. Швидкість обчислень з використанням вейвлетів Хаара є однією з основних переваг цього перетворення.


E=0,07; K=1,8; Cor=0 *а)*


E=0,1; K=4; Cor=1 *б)*


E=0,12; K=6; Cor=2 *в)*


E=0,15; K=8; Cor=3 *г)*

*Рис. 3.7.* Результати обробки вейвлет-«long»:
*а* — коефіцієнт стиснення 1,8; *б* — коефіцієнт стиснення 4,0;
*в* — коефіцієнт стиснення 6,0; *г* — коефіцієнт стиснення 8,0

На рис. 3.8 (а, б, в, г) наведені практичні результати компресії зображень при використанні вейвлетів Хаара. Добрі результати при обробці вейвлетами Хаара можна чекати, коли початкове зображення має велику кількість різких перепадів у вертикальному і горизонтальному напрямах. Виявлення таких перепадів у вертикальних і горизонтальних напрямах обумовлене самою технологією обчислення вейвлет-коефіцієнтів, а форма функцій базису Хаара значною мірою буде узгоджена зі структурою таких зображень. Ця якість має особливе значення при обробці зображень з різкими і чіткими перепадами.


E=0,04 K=1,5 Cor=0 *а)*


E=0,06 K=2,4 Cor=1 *б)*


E=0,08 K=3,5 Cor=2 *в)*


E=0,1 K=4,8 Cor=3 *г)*

*Рис. 3.8.* Результати обробки вейвлетами Хаара:
*а* — коефіцієнт стиснення 1,5; *б* — коефіцієнт стиснення 2,4;
*в* — коефіцієнт стиснення 3,5; *г* — коефіцієнт стиснення 4,8

## 3.4. Дослідження можливостей методів проектної геометрії для ідентифікації графічних зображень у системі «КЛІШЕ»

### 3.4.1. Графічні методи аналізу зображень у інформаційно-аналітичних системах

Графічні методи аналізу і подання криміналістичної інформації належать до тих небагатьох засобів, які ще на початку становлення криміналістики були визнані як необхідні і дуже важливі в діяльності з розкриття і розслідування злочинів.

Багатообразні види графічної форми виразу і аналізу криміналістичної інформації й у сфері судової експертизи. Застосування графічного способу виразу криміналістичній інформації на сучасному рівні розвитку криміналістики пояснюється двома основними причинами. По-перше, на практиці це або одна з форм її аналізу з використанням математичного апарату (наприклад, проектної геометрії), або один із засобів її підготовки для такого аналізу, зокрема з використанням ЕОМ.

По-друге, з появою ефективних дисплейних пристроїв відображення інформації в сучасних ЕОМ графічна форма інформації виявилася найбільш зручною для оперативного і разом з цим найбільш образного виразу результатів дослідження криміналістичної інформації.

Тому в практиці криміналістичного аналізу зображень знайшли широке застосування методи графічних ідентифікаційних алгоритмів, що задають певний порядок графічних побудов, при яких початковими даними є системи точок, що виділяються на безпосередніх об'єктах дослідження (наприклад, на досліджуваних фотознімках). Цілі таких побудов можуть бути різними. Однією з них є вирішення питання про перспективну відповідність або невідповідність двох систем точок, властивих порівнюваним об'єктам дослідження (наприклад, зображенням двох відтисків печаток). При цьому якщо буде встановлено, що дві такі системи точок знаходяться в перспективній відповідності, то з геометричної точки зору це означатиме, що об'єкти, яким вони належать, конгруентні. У теорії проектної геометрії дві геометричні

фігури називаються конгруентними, якщо вони якимсь рухом (або сумою рухів) можуть бути суміщені всіма своїми точками. Інакше кажучи, можна сказати, що ці системи точок належать двом відображенням одного і того ж об'єкта.

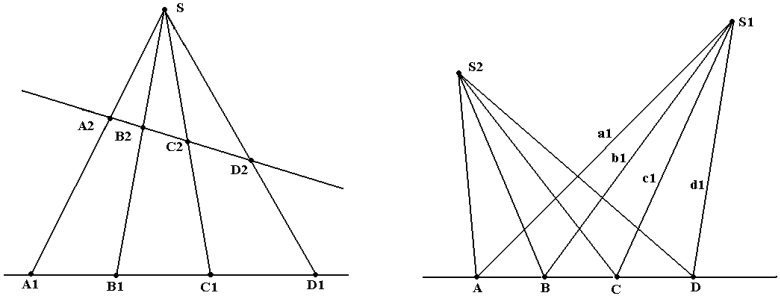
Неважко помітити, що за своєю суттю це ідентифікаційне завдання. Тому графічні алгоритми, що використовуються для вирішення завдань такого класу, називаються ідентифікаційними.

Спочатку такого роду алгоритми були розроблені і застосовані для вирішення завдань, пов'язаних з ідентифікацією осіб за їхніми фотозображеннями [16; 17].

Подальше вивчення можливостей графічних ідентифікаційних алгоритмів показало, що вони з успіхом можуть бути використані і для ідентифікації інших об'єктів за їхніми зображеннями, у тому числі і при дослідженні документів.

Науковими основами графічних ідентифікаційних алгоритмів, з одного боку, є положення проектної геометрії — науки, що вивчає проектні властивості фігур, з другого — положення теорії криміналістичної ідентифікації [18; 19; 20; 21].

Розглянемо деякі аспекти цих теорій, які допоможуть з'ясувати суть графічних ідентифікаційних алгоритмів і їх особливості як методу криміналістичного дослідження.




*а)* *б)*

*Рис. 3.9: а)* перспективний ряд точок;
*б)* перспективні пучки прямих

Для цього відтворимо спочатку деякі відправні положення проектної геометрії. Такими, зокрема, є: дві точки визначають пряму; дві прямі визначають точку. Якщо кілька точок розташовані на одній прямій, їх називають прямолінійним рядом точок (на рис. 3.9 а, це точки A1, B1, C1, D1 і точки A2, B2, C2, D2); якщо кілька прямих проходять через одну точку, їх називають пучком прямих [18].

Між точками двох прямолінійних рядів точок або між прямими двох пучків можуть існувати певні геометричні зв'язки, що іменуються відповідністю. Найбільший інтерес (з урахуванням цього питання) становлять перспективні відповідності. Відповідність між точками прямолінійних рядів називають перспективною, якщо прямі, що поєднують пари відповідних точок цих рядів, сходяться в одній точці (на рис. 3.9 це точка S).

У перспективній відповідності можуть знаходитися не лише точки двох прямолінійних рядів, але і системи точок, що знаходяться на площині або в просторі. Покажемо це на двох системах точок A, B, C, D, E і A1, B1, C1, D1, E1 (рис. 3.10.).

Для цього оберемо центр проектування для кожної з систем точок. У цьому випадку ним є точка B і відповідно B1. Проведемо з цих точок прямі через точки $A_0$, $C_0$, $D_0$, $E_0$ і відповідно через $A_1$, $C_1$, $D_1$, $E_1$. Потім отримані пучки прямих перетнемо довільними прямими $e_0$ і $e_1$. У результаті ми отримаємо два прямолінійні ряди чотирьох точок: $A_0$, $E_0$, $D_0$, $C_0$ і $A_1$, $E_1$, $D_1$, $C_1$ (рис. 3.10.).

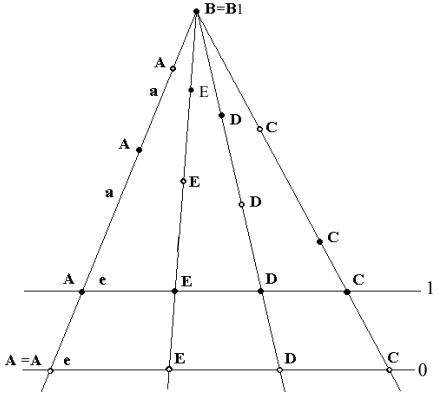



*Рис. 3.10.* Приклад перспективної відповідності двох систем точок

Встановити, чи є два отримані ряди точок проектними, можна двома шляхами: визначенням їх складного відношення і графічно.

У першому випадку відношення точок можна виразити так:

$$\frac{A_0E_0}{E_0C_0}:\frac{A_0D_0}{D_0C_0}=\frac{A_1E_1}{E_1C_1}:\frac{A_1D_1}{D_1C_1}\ . \qquad (3.20)$$

Якщо ці відношення однакові, це означає прямолінійні ряди, а отже, і системи точок, що розглядаються нами, є проектними. Графічним шляхом це відношення може бути виражене кількома варіантами, зокрема поєднанням точок або поєднанням прямих [22].

При методі поєднання точок прямі e і $e_1$ розташовують довільно, але так, щоб дві які-небудь відповідні точки, наприклад $A_0$ і $A_1$, лежачі на цих прямих, поєдналися. Якщо при цьому з'ясується, що прямі, які поєднують інші точки, перетинаються в одній точці (на рис. 3.10 це точка B ≡ B1), це означає, що системи точок, які розглядаються нами, є проектними.

При методі поєднання прямих пучки променів з центрами B і B1 розміщуються так, щоб один з променів, наприклад, (a) пучка B співпав з променем ($a_1$) пучка B1. Якщо при цьому з'ясується, що не лише промені (a) і ($a_1$), але й інші, зокрема (e) і ($e_1$); (d) і ($d_1$); (c) і ($c_1$) перетинаються на одній лінії (на рис. 3.10 в точках $A_0$, $E_0$, $D_0$ і $C_0$), це означає, що ці системи точок проективні.

Але згідно з положенням проектної геометрії системи точок можуть бути приведені в проектну відповідність тоді, коли вони належать відображенням, отриманим з одного і того ж об'єкта.

Отже, якщо ми тим або іншим шляхом встановили, що дві системи точок проективні, у нас з'являється підстава вважати, що вони належать двом різним відображенням одного і того ж об'єкта. На мові теорії криміналістичної ідентифікації це означає встановлення тотожності того об'єкта, відображення якого були предметом порівняльного дослідження. Саме це і визначає принципову можливість використання методів встановлення проектної подібності геометричних фігур (а точніше — систем точок, що виражають їх) для вирішення ідентифікаційних завдань.

## 3.4.2. Практична реалізація методу проектної геометрії в АІПС «КЛІШЕ»

Практична реалізація методу проектної геометрії з використанням комп'ютерних технологій включає такі основні етапи.

Відповідність між двома вибраними системами точок може бути приведена в проектну відповідність тоді, коли обидві системи точок належать зображенням одного і того ж об'єкта. Визначити, чи є вибрані системи проектними, можна двома шляхами: визначенням їх складного відношення або графічно.

При обчисленні коефіцієнтів відповідності обираються системи точок на кожному досліджуваному зображенні. Початкове зображення представлене в .bmp форматі з роздільною здатністю 1200 dpi і глибиною кольору 8 біт. Початкове зображення досліджуваного відтиску печаток представлене на рис. 3.11.


*Рис. 3.11.* Зображення досліджуваного зображення

Вибір точок на досліджуваному зображенні проводиться користувачем у рамках інтерфейсу програми за допомогою маніпулятора «миша». Кожна обрана точка відображається на досліджуваному зображенні за допомогою мітки «хрестик» і відповідної букви латинського алфавіту. Обрана система точок дозволяє побудувати аналітичні вирази, що враховують відношення довжин відрізків, які обмежені точками обраної системи. Аналогічна процедура проводиться на другому досліджуваному зображенні, яке має аналогічні характеристики роздільної здатності і глибини кольору та відображається в другому вікні інтерфейсу програми (рис. 3.12).

Після вибору систем точок програма здійснює розрахунок заданих відносин. У даному прикладі ці відносини виглядають таким чином:

$$\frac{AB}{CD} : \frac{AC}{BD} = \frac{A_1B_1}{C_1D_1} : \frac{A_1C_1}{B_1D_1}. \qquad (3.21)$$

Якщо обидві частини рівняння однакові, то згідно з теорією криміналістичної ідентифікації це означає встановлення тотожності порівнюваних об'єктів, відображення яких були предметом порівняльного дослідження. Інакше тотожність відсутня.


*Рис. 3.12.* Вибір системи точок

У цьому прикладі коефіцієнт К1 відображає числове значення лівої частини рівняння, яка дорівнює 3,137. Аналогічний йому коефіцієнт К2, що відображає числове значення правої частини рівняння, дорівнює 3,097 (рис. 3.13).


*Рис. 3.13.* Порівняльний аналіз двох зображень


k=0,4059


k=0,4060

*Рис. 3.13.* Порівняльний аналіз двох зображень (продовження 1)


k=0,4059


k=0,4162

*Рис. 3.13.* Порівняльний аналіз двох зображень (продовження 2)

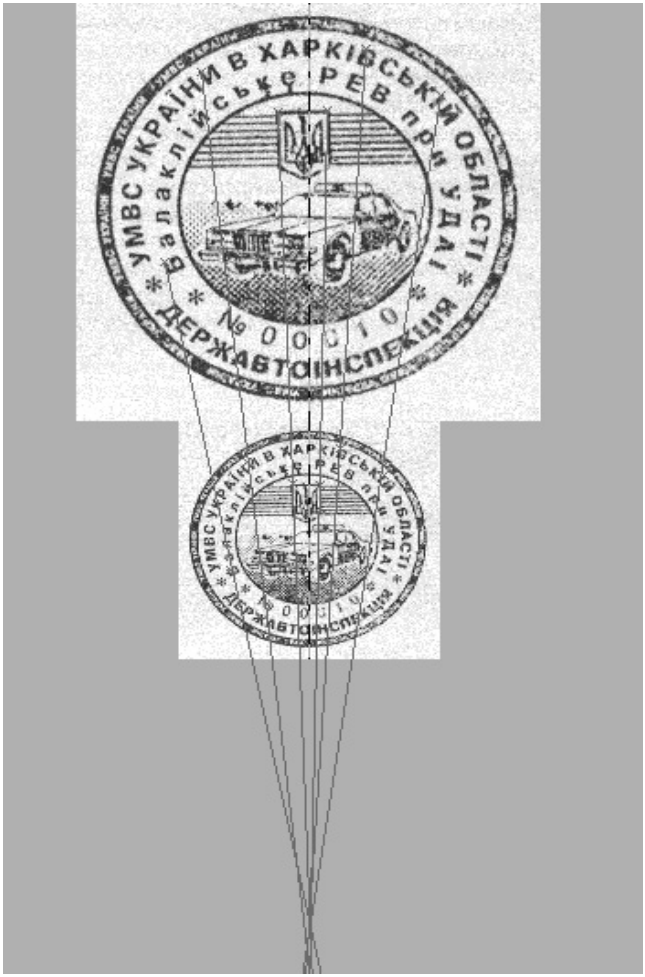



*Рис. 3.13.* Порівняльний аналіз двох зображень (продовження 3)
Однаковий штамп

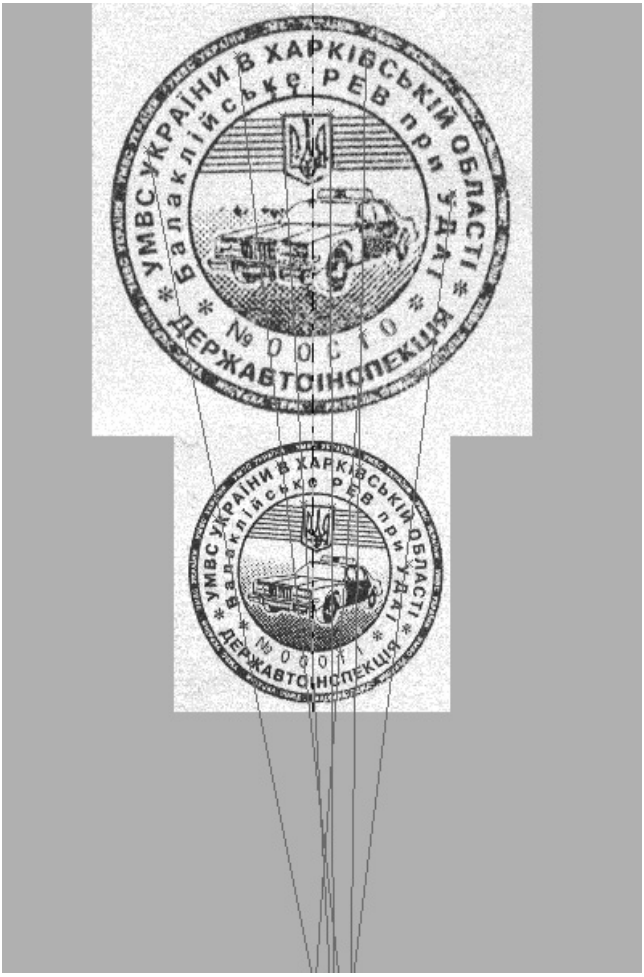



*Рис. 3.13.* Порівняльний аналіз двох зображень (продовження 4)
Різний штамп

Розроблена програма надає можливість розрахувати коефіцієнт співвідношення між обраними точками на досліджуваному зображенні. Розрахунок коефіцієнта співвідношення дає оцінку відповідності порівнюваних параметрів, а саме — відстаней між точками обраної системи. Отримання цього коефіцієнта дає оцінку пропорційності між точками обраної системи. Порівняння двох коефіцієнтів, отриманих на різних зображеннях, дозволяє оцінити ступінь відповідності (ідентичності) систем точок на порівнюваних зображеннях. Цей метод порівняння використовується як один з варіантів методу проектної геометрії.

Якщо два коефіцієнти мають близьке значення, можна стверджувати, що відстані між обраними точками кожної системи пропорційні, а отже, дві системи точок є проектними.

Мовою теорії криміналістичної ідентифікації це означає встановлення тотожності порівнюваних об'єктів, відображення яких були предметом порівняльного дослідження. Саме це і визначає принципову можливість використання методів встановлення проектної відповідності геометричних фігур (а точніше систем точок, що виражають їх) для вирішення ідентифікаційних завдань.

Розкид числових значень між параметрами К1 і К2, які дозволяють говорити про тотожність або невідповідність об'єктів дослідження, є результатом подальшого дослідження на статистично представницькій вибірці досліджуваних об'єктів. Хоча вже за отриманими аналітичними і графічними результатами можна говорити про перспективність комп'ютерної методики ідентифікації зображень відтисків печаток і штампів.

Ця програма розроблена у візуальному середовищі програмування Borland C++ Builder 6.0. Програма включає два основні модулі (файли), в яких знаходиться основний текст програми.

## 3.5. Інтерфейс користувача АІПС «КЛІШЕ»/АРМ Е-К

Загальний вид головної форми АІПС «КЛІШЕ» представлений на рис. 3.14. Доступ до ресурсів бази даних можливий при введенні ключового слова в полі «Password», яке знаходиться у вікні, що висвічується при

завантаженні програми prKLISHE.EXE. Головна форма містить чотири функціональні клавіші — «Печати», «Бланки», «Автоматизированное рабочее место эксперта-криминалиста (АРМ Э-К), «Выход». За допомогою цих клавіш користувач може вибрати режим подальшої роботи. При виборі «Печати» буде відкритий режим «Просмотр», який відображає зображення відтисків печаток. При виборі «Бланки» відкривається режим «Бланки». Клавіша «АРМ Э-К» дозволяє користувачеві відкрити головну форму програмного модуля — Автоматизоване робоче місце експерта-криміналіста. Клавіша «Выход» завершує роботу програми КЛІШЕ.


*Рис. 3.14.* Загальний вид головної форми АІПС «КЛІШЕ»

*Режими роботи АІПС «КЛІШЕ».* Основними режимами роботи бази даних «КЛІШЕ» є:

- режим «Просмотр»;
- режим «Поиск»;
- режим «Расширенный поиск»;
- режим «Редактирование»;
- режим «Бланки».

*Режим «Просмотр».* Режим «Просмотр» АІПС «КЛІШЕ» призначений для перегляду загального виду зображень відтисків печаток, що знаходяться в базі даних, виведення інформації про атрибу-

ти відтиску і реквізити власника печаток. Вибір зображення відтисків печаток проводиться в діалоговому режимі за допомогою списків-меню, що розкриваються, по кожному з атрибутів відтиску печаток.

Режим «Просмотр» є основним режимом роботи в АІПС «КЛІШЕ», який надає якнайповнішу інформацію про зображення відтисків, містить вбудовані режими, а також дозволяє здійснити вибір або перехід в будь-який інший режим роботи, включаючи вихід в головну форму «КЛІШЕ».

*Склад форми режиму «Просмотр».* Виклик форми режиму «Просмотр» здійснюється з головної форми АІПС «КЛІШЕ» шляхом натиснення клавіші «Печати». Загальний вигляд форми режиму «Просмотр» представлений на рис. 3.15. У верхній частині форми «Просмотр» знаходиться рядок назви, який містить найменування програми і режиму роботи АІПС «КЛІШЕ» (в даному випадку — «Печати (просмотр)».


Під рядком назви розташований рядок меню, який містить пункти: «Файл», «Вид», «Редактирование», «Поиск», «Бланки», «Помощь».

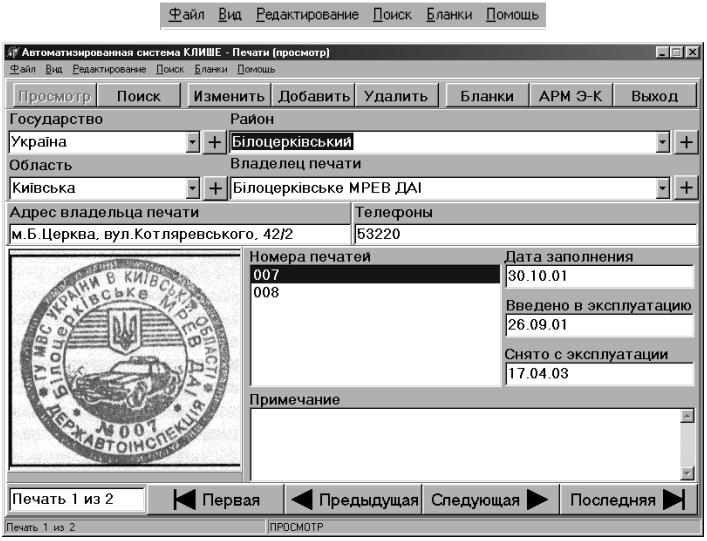



*Рис. 3.15.* Загальний вигляд форми режиму «Просмотр»

За допомогою пунктів рядка меню можна здійснити вибір операції, яку необхідно виконати користувачеві, або провести перехід в інший режим роботи АІПС «КЛІШЕ».

Під рядком меню форми режиму «Просмотр» розташована панель інструментів, кнопки якої дублюють основні функції, представлені в рядку меню, що дозволяє прискорити вибір будь-якого з режимів роботи АІПС «КЛІШЕ» і зробити інтуїтивно зрозумілим інтерфейс форми. Активна форма (обрана в даний момент) або недоступні режими роботи для поточного моменту роботи мають більш бліде забарвлення в назві клавіш, розташованих на панелі інструментів.

Панель інструментів містить кнопки: «Просмотр», «Поиск», «Изменить», «Добавить», «Удалить», «Бланки», «АРМ Э-К», «Выход».

*Режими роботи АРМ Е-К.* Основними режимами роботи інтегрованого програмного модуля «Автоматизоване робоче місце експерта-криміналіста» є:

– режим «Изображение»;
– режим «Сетки»;
– режим «Измерение»;
– режим «Отчет».

*Режим «Изображение».* Режим «Изображение» є стартовим режимом АРМ Е-К, який призначений для вибору зображень відтисків печаток, що знаходяться як у базі даних АІПС «КЛІШЕ», так і в окремих файлах формату .bmp на магнітних дисках. Цей режим дозволяє викликати будь-яку кількість зображень, формувати розміри і положення вікон, що відображають викликані зображення, збільшувати або зменшувати досліджуване зображення, переходити в інші режими АРМ Е-К («Сетки», «Измерение», «Отчет»). Режим «Изображение» дозволяє також проводити поворот зображення на встановлений кут або розрахунковий кут, який визначається програмою після використання методу накладення сіток при порівняльному аналізі. У вікні кожного зображення є горизонтальні і вертикальні масштабні лінійки, які відображають лінійні розміри представленого зображення.

*Склад форми режиму «Изображение».* Виклик режиму «Изображение» здійснюється в АРМ Е-К шляхом вибору закладинки «Изображение» на панелі «Режимы АРМ Э-К». Панель «Режимы АРМ Э-К» може

бути встановлена в будь-яке місце екрана на розсуд користувача. Загальний вигляд режиму «Изображение» представлений на рис. 3.16.

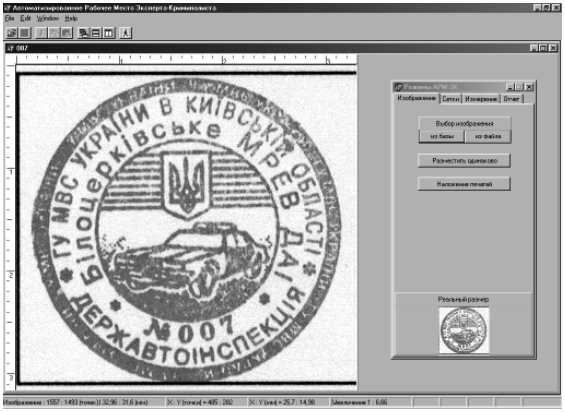


*Рис. 3.16.* Загальний вид форми режиму «Изображение»

У цьому випадку на рис. 3.16 відображене зображення з бази даних АІПС «КЛІШЕ». Структура форм і стиль оформлення АРМ Е-К виконані за аналогією з інтерфейсом АІПС «КЛІШЕ», тому детально описувати склад і призначення таких елементів, як рядок назви (відображає назву програми і містить кнопки управління самим вікном), рядок меню (відображає основні команди по відкриттю, закриттю зображення, розташуванню вікон із зображеннями і їх конфігурації), панель інструментів (містить ряд кнопок, які несуть те ж функціональне призначення, що і команди рядка меню) недоцільно. У нижній частині форми режиму «Изображение» є рядок стану, який відображає таку інформацію про зображення в активному вікні:

- розмір зображення в точках — 1557 : 1493;
- розмір зображення в мм — 32,96 : 31,6;
- поточне положення курсора на зображенні (у точках) — 485 : 282;
- поточне положення курсора на зображенні (у мм) — 27,5 : 14,98;
- коефіцієнт збільшення зображення (раз) — 1 : 6,66.

*Режим «Сетки».* Режим «Сетки» призначений для конфігурації, накладення і модифікації шаблонів сіток стандартного вигляду щодо досліджуваних зображень відтисків печаток. Цей режим дозволяє виконувати такі операції:

– на досліджуване зображення накладати стандартний шаблон;

– використовуючи список шаблонів сіток накладення, здійснювати вибір вже існуючих шаблонів, які були використані на досліджуваному зображенні;

– зберігати створений шаблон сітки в список шаблонів;

– приховувати шаблон сітки накладення з використовуваного зображення без збереження;

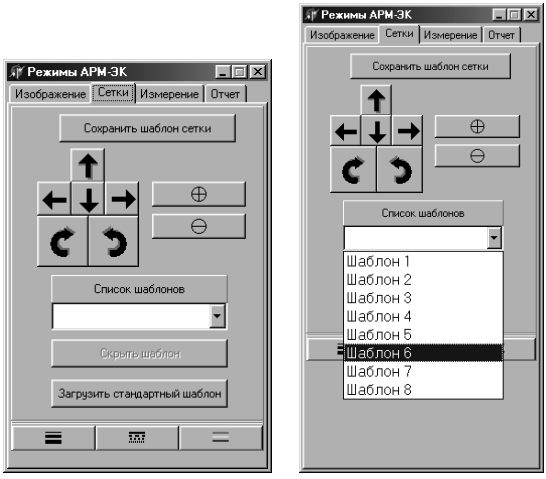
– здійснювати переміщення вибраного шаблону сітки накладення на всіх напрямках щодо досліджуваного зображення відтиску печаток;

– збільшувати або зменшувати розміри шаблону сітки накладення щодо досліджуваного зображення;

– здійснювати вибір товщини, типу і кольору лінії шаблону сітки накладення.

Для активізації режиму «Сетки» користувач повинен відкрити закладку «Сетки» на панелі «Режимы АРМ Э-К» (рис. 3.17). Перед роботою в режимі «Сетки» необхідно вже мати досліджуване зображення відтисків печаток у вікні відображення АРМ Е-К.

*Склад форми режиму «Сетки».* Загальний вигляд панелі «Режимы АРМ Э-К» у режимі «Сетки» представлений на рис. 3.17 (а).




*а)* *б)*

*Рис. 3.17.* Переміщувана панель «Режимы АРМ Э-К» в режимі «Сетки»: *а* — загальний вигляд; *б* — з розгорненим списком шаблонів

На переміщуваній панелі в режимі «Сетки» є кнопки, функціональне призначення яких написане на самих кнопках («Сохранить шаблон сетки», «Загрузить стандартный шаблон», «Скрыть шаблон»). Поле, що відображає список збережених шаблонів, призначено для відображення найменування того шаблону, який викликаний із списку шаблонів. Для відображення всього списку наявних шаблонів необхідно використовувати кнопку списку, що розкривається в полі «Список шаблонов» (рис. 3.17 (б)).

Кнопки переміщення викликаного шаблону (стандартний — кнопка «Загрузить стандартный шаблон» або викликаного із списку (рис. 3.17 (б)) розташовані разом і на кнопках вказаний напрям переміщення шаблону щодо досліджуваного зображення.

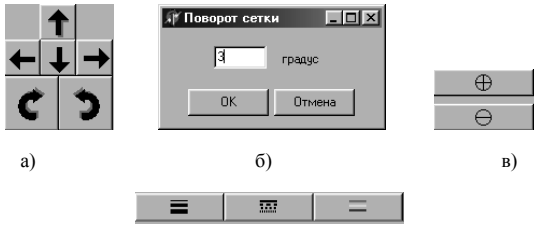



*Рис. 3.18.* Елементи управління шаблоном сітки накладення

Якщо необхідно провести ротацію шаблону щодо зображення, користувач повинен обрати напрям обертання шаблону (рис. 3.18 а) і після цього вказати величину кута повороту в допоміжному вікні (рис. 3.18 б), яке автоматично з'являється після вибору напряму повороту. Для виконання дії натиснути кнопку «ОК» в діалоговому вікні «Поворот сетки», для виходу з режиму повороту необхідно натиснути кнопку «Отмена» або закрити вікно кнопкою в рядку назви (рис. 3.18 б). При повороті шаблону сітки накладення вікно відображення зображення повинне бути активним.

За необхідності збільшення або зменшення шаблону щодо досліджуваного зображення необхідно використовувати кнопки, представлені на рис. 3.18 в відповідно. Кнопки, представлені на рис. 3.18 г, дозволяють встановити товщину, тип і колір лінії, якою представлений шаблон у вікні відображення режиму «Сетки».

Загальний вигляд зображення печаток, викликаних з бази даних «КЛІШЕ», і стандартним шаблоном сітки накладення представлений на рис. 3.19.

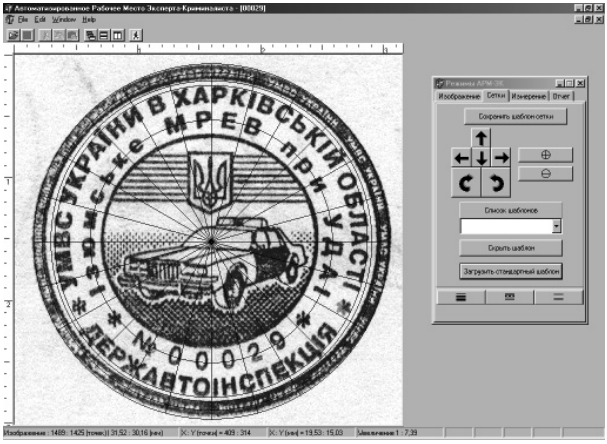



*Рис. 3.19.* Загальний вигляд зображення печаток зі стандартним шаблоном сітки накладення

Сітка накладення за допомогою кнопок переміщення шаблону і кнопок збільшення/зменшення розміру сітки щодо зображення розміщена таким чином, що зовнішній контур зображення печаток суміщений із зовнішнім колом сітки накладення.

Слід нагадати, що прямокутна сітка зі встановлюваною величиною «клітинки» викликається в будь-якому з режимів роботи АРМ Е-К через контекстне меню (одне клацання правою клавішею миші в полі вікна відображення). Прямокутна сітка знімається із зображення так само через контекстне меню вікна відображення.

Для того щоб зняти шаблон сітки накладення із зображення досліджуваного відтиску, користувач обов'язково повинен активізувати режим «Сетки» і використовувати кнопку «Скрыть шаблон» на переміщуваній панелі «Режимы АРМ Э-К».

*Робота АРМ Е-К в режимі «Сетки».* При роботі в режимі «Сетки» користувач повинен дотримуватися такої методики:

– визначити, який шаблон буде використовуватися (стандартний або зі списку шаблонів);

– обрати відповідний розмір шаблону сітки за допомогою кнопок збільшення/зменшення, якщо це необхідно;

– встановити сітку накладення на зображення печаток за допомогою кнопок переміщення і повороту шаблону;

– встановлена сітка накладення на зображення зберігається у всіх режимах роботи АРМ Е-К;

– якщо цей шаблон необхідно зберегти в список шаблонів, необхідно використовувати кнопку «Сохранить шаблон сетки», при цьому цей шаблон буде поміщений у список зі своїм номером в кінець списку;

– вибір товщини і кольору ліній шаблону можна використовувати в міру необхідності в ситуаціях, коли колір ліній шаблону сітки накладення збігається з кольором зображення відтиску печатки (товщина лінії шаблону за умовчанням завжди дорівнює 1-й точці в зображенні печаток);

– при використанні повороту шаблону сітки накладення на встановлений кут щодо зображення печаток необхідно обрати крок кута повороту, при переміщенні шаблону можна використовувати комбінації клавіш: (Ctrl + стрілка) — крок 0,1 мм, (Ctrl + Alt + стрілка) — крок 1 мм, кнопка навігатора — 0,5 мм. При збільшенні/зменшенні шаблону: (Shift + стрілка) — крок 0,1 мм, (Shift + Alt + стрілка) — крок 1 мм, кнопка на панелі навігатора — 0,5 мм;

– зняти накладення шаблону сітки із зображення відтиску печатки можливо тільки в режимі «Сетки» за допомогою клавіші «Скрыть шаблон».

## 3.6. Висновки

У цьому розділі представлені основні результати по створенню багатофункціональних інформаційно-аналітичних баз даних, які на практиці реалізуються у вигляді автоматизованих інформаційно-пошукових систем зберігання, пошуку і обробки криміналістичної інформації [23; 24].

Були наведені основні математичні і технологічні принципи створення автоматизованої інформаційно-пошукової системи «КЛІШЕ»

з інтегрованим програмним модулем робочого місця експерта-криміналіста (АІПС «КЛІШЕ»). Система призначена для зберігання, відображення, перегляду, редагування і пошуку зображень відтисків печаток всіх районних відділень ДАІ УМВС України. Окрім зображень печаток, система містить повні реквізити власників печаток, дату заповнення даних, часові параметри введення і зняття з експлуатації печаток, а також зображення типових бланків документів.

На основі інформаційно-пошукового модуля АІПС «КЛІШЕ» розроблений структурно-програмний модуль — «Автоматизоване робоче місце експерта-криміналіста», який призначений для автоматизації проведення експертних досліджень документів, що містять форми з відтисками печаток.

Наголошується також, що в практиці криміналістичного аналізу зображень широко застосовуються методи графічних ідентифікаційних алгоритмів, науковими основами яких, з одного боку, є положення проектної геометрії, з другого — положення теорії криміналістичної ідентифікації.

Проведено практичний комп'ютерний аналіз зображень відтисків печаток методами проектної геометрії, розглянуті і розвинені основні поняття і положення комп'ютерної графіки, які використовувалися при створенні автоматизованого робочого місця експерта-криміналіста (АРМ Е-К) системи «КЛІШЕ».

Порівняння числових значень коефіцієнтів відношень, а також результатів графічних побудов дозволяє оцінити ступінь відповідності (ідентичності) систем точок на порівнюваних зображеннях.

Програмна реалізація системи здійснена у віртуальному середовищі програмування Borland C++ Builder 6.0.

Також був проведений аналіз можливостей сучасних математичних методів дискретного косинусного перетворення, перетворень Хаара і вейвлет-перетворень для стиснення архіву зображень відтисків печаток і штампів АС «КЛІШЕ».

Показано, що ступінь стиснення цих зображень коливається від 2 до 4 в алгоритмах на базі ДКП і від 1,5 до 8 з використанням вейвлетів Хаара за умови збереження прийнятної якості для подальших експертних досліджень.

# РОЗДІЛ 4

# ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ НА МУЛЬТИМЕДІЙНІ ТВОРИ

## 4.1. Юридичні та технічні проблеми захисту творів в електронно-цифровому вигляді

Авторське право на інтелектуальну власність захищено в Україні Законом України «Про інтелектуальну власність та суміжні права» (остання редакція 09.05.2011 року) і, крім того, рядом міжнародних угод. Авторськими правами є інтелектуальні права на наукові, літературні та мистецькі твори.

Зокрема, серед об'єктів Закону є аудіовізуальні твори (кінофільми, телефільми, відеофільми), статичні зображення (фотографії, зображення тексту, логотипи), комп'ютерні ігри, інші комп'ютерні програми та комп'ютерні бази даних. Важливо, що твори цих видів, як правило, мають електронно-цифровий вигляд, тобто представлені як послідовність двійкових чисел, записаних на магнітній плівці, магнітному диску, компакт-диску тощо. Крім того, традиційні твори такі, як літературні, науково-технічні, педагогічні та медичні праці, зараз теж переважно представлені в електронно-цифровому вигляді.

Електронно-цифрова форма твору, з одного боку, набагато спрощує його тиражування (копіювання) та розповсюдження (наприклад, через Интернет), але, з другого боку, збільшує вірогідність порушення авторських та суміжних прав на нього. Справа в тому, що, на відміну від традиційних видів зберігання та розповсюдження творів (рукописи, книги, часописи, плівки), для їх електронного представ-

лення існує проблема, як доказати, що цей твір був створений цим автором або права на нього має та чи інша фізична або юридична особа. Закон «Про авторське право та суміжні права» від 23.12.1993 року № 3792-XII в редакції від 11.07. 2001 року № 2627-III (Відомості Верховної Ради. — 2001. — № 43. — Ст. 214) передбачає для захисту авторських прав використання технічних засобів захисту і (або) технологічних розробок, призначених для створення технологічної перешкоди порушенню авторського права і суміжних прав при сприйнятті і (або) копіюванні електронно-цифрових творів.

Нижче розглядаються технічні аспекти захисту авторських і суміжних прав на мультимедійні твори, тобто на відео- й аудіопродукцію та зображення, графічні чи символьні. При цьому в основному можна зосередитися лише на методах захисту зображень, тому що методи захисту інших мультимедійних творів є або аналогічними, або похідними від них.

Якнайкраще для захисту авторських та суміжних прав на мультимедійну продукцію підходять методи *стеганографії* — давньої науки про засоби таємного передавання повідомлень. Термін «стеганографія» походить від грецьких слів steganos (секрет, таємниця) і graphy (запис) і, таким чином, означає буквально «тайнопис». На відміну від криптографії, яка блокує доступ до інформації шляхом шифрування, стеганографія має на меті приховати сам факт існування секретного повідомлення. Цим секретним повідомленням, впровадженим у мультимедійний твір, може бути, наприклад, ім'я його автора з іншими реквізитами або зображення логотипу юридичної особи, яка має права на цей твір. Таке секретне повідомлення в жодному разі не повинно погіршувати технічну якість твору, але за допомогою спеціальної програми його можна виявити, що стане вагомим доказом, наприклад у суді.

У наш час під стеганографією, точніше *комп'ютерною стеганографією,* розуміють приховування інформації в текстових, графічних, аудіо- або відеофайлах шляхом використання спеціального програмного забезпечення. Далі на базі аналізу відкритих інформаційних джерел розглядаються можливості стеганографії стосовно проблеми захисту інформації шляхом приховання її у файлах символьних і графічних зображень.

## 4.2. Основні визначення й принципи стеганографії

У 1996 році на конференції Information Hiding: First Information Workshop була прийнята єдина термінологія.

1. *Стеганографічна система* (*стегосистема*) — поєднання методів і засобів, що використуються для створення прихованого каналу при передачі інформації. Побудова цієї системи передбачає таке:

а) супротивник знає алгоритм роботи використовуваної стеганографічної системи. Невідомим для нього є ключ, за допомогою якого можна довідатися про факт існування прихованого повідомлення та його зміст;

б) при виявленні супротивником наявності прихованого повідомлення він не може витягти повідомлення до тих пір, поки не буде мати ключ;

в) супротивник не має технічних та інших переваг.

2. *Повідомлення* — це термін, який використовується для загальної назви переданої прихованої інформації.

3. *Контейнер* — будь-яка інформація для приховування таємного повідомлення. *Порожній* контейнер — контейнер, що не містить секретного повідомлення. *Заповнений* контейнер (*стегоконтейнер*) — контейнер, що містить секретне повідомлення. У наш час як контейнер використовують файли, що містять або зображення, або звук, або відео.

4. *Стеганографічний канал* (*стегоканал*) — канал передачі стегоконтейнера.

5. *Ключ* (*стегоключ*) — секретний ключ, потрібний для приховування повідомлення у стегоконтейнері. Як і при шифруванні, ключі в стегосистемах бувають двох типів: *секретні* й *відкриті*. Секретний ключ повинен бути створений або до початку обміну повідомленнями, або переданий захищеним каналом. Відкритий ключ, за яким неможливо відтворити секретний ключ, можна передавати незахищеним каналом.

*Комп'ютерна стеганографія* — напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи. Як стегоконтейнер використовують файли, що передаються відкрито та називаються *файлами-контейнерами*. Прихована інформація, закладена у файл-контейнер, також являє собою файл, що називається *файлом-повідомленням*.

Стегосистема вбудовує й видаляє файл-повідомлення з файла-контейнера. Вона складається з таких основних елементів, що подані на рис. 4.1.

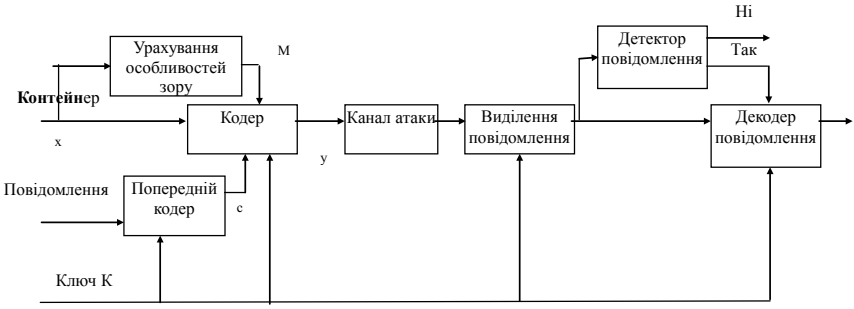



*Рис. 4.1.* Структурна схема стегосистеми

Терміни, використані на рис. 4.1, означають таке:

– *попередній кодер* — пристрій, призначений для перетворення приховуваного повідомлення до вигляду, зручного для вбудовування в стегоконтейнер;

– *кодер* — пристрій, призначений для вбудовування повідомлення в контейнер з урахуванням його структури;

– *канал атаки* — вплив супротивника на заповнений контейнер;

– *виділення повідомлення* — пристрій виділення вбудованого повідомлення з контейнера;

– *детектор повідомлення* — пристрій, призначений для визначення наявності прихованого повідомлення;

– *декодер повідомлення* — пристрій, що відновлює приховане повідомлення (цей вузол може бути відсутнім).

Основними положеннями сучасної комп'ютерної стеганографії є такі:

1. Методи приховання повинні забезпечувати *автентичність* і *цілісність* файла-повідомлення. Тобто інформація, витягнута зі стегоконтейнера, повинна збігатися з інформацією, що була в нього закладена.

2. Передбачається, що супротивникові повністю відомі всі можливі стеганографічні методи.

3. *Безпека методів* ґрунтується на збереженні у стеганографічному перетворенні основних властивостей відкрито переданого файла-контейнера при внесенні в нього секретного повідомлення.

4. Навіть якщо факт приховання повідомлення став відомий супротивникові через спільника або яким-небудь іншим чином, видобути секретне повідомлення є складним обчислювальним завданням.

## 4.3. Огляд стеганографічних методів

У наш час методи комп'ютерної стеганографії розвиваються у двох основних напрямах:

1. Методи, засновані на використанні спеціальних властивостей комп'ютерних форматів.

2. Методи, засновані на надмірності аудіо- та візуальної інформації.

Зупинимося на порівняльних характеристиках існуючих стеганографічних методів. Почнемо з *методів використання спеціальних властивостей комп'ютерних форматів даних*.

*Методи використання зарезервованих для розширення полів комп'ютерних форматів даних*. Ці методи засновані на тому, що поля розширення є в багатьох мультимедійних форматах, і вони заповнюються нульовою інформацією. Спеціальні програми можуть використовувати ці поля для запису прихованого повідомлення. Перевага зазначених методів складається із простоти програмного забезпечення, а недоліками є, по-перше, низький ступінь прихованості й, по-друге, малий обсяг приховуваної інформації.

*Методи спеціального форматування текстових файлів*. До цих методів належать:

— *методи використання певного зсуву слів, позицій та абзаців*. Ця група методів заснована на зміні положення рядків і розміщення слів, що забезпечується вставкою додаткових пропусків між словами;

— *методи вибору певних позицій букв (нульовий шифр)*. Прикладом цього методу є акровірш, у якому секретне повідомлення складається з перших літер кожного рядка;

— *методи, що використовують спеціальні властивості полів форматів, які не відображуються на екрані*. Такі поля зазвичай призначені для форматування або організації виносок і посилань. Найпростішим методом такого типу є призначення шрифту того ж кольору, що й фон. Наприклад, білий шрифт не можна побачити на білому фоні. Приховане повідомлення з'явиться, коли адресат поверне шрифту чорний колір.

Перевага методів спеціального форматування текстових файлів полягає у простоті реалізації, а загальні для цих методів недоліки — слабка продуктивність й низький ступінь прихованості;

— *методи приховування інформації в місцях гнучких дисків*, що не використовуються, наприклад, на нульовій доріжці. Як і всі наведені вище методи відзначається простотою, але ще й малою продуктивністю та низьким ступенем прихованості;

— *методи, які використовують імітуючі функції* (mimic-function) є узагальненням акровірша. Для таємного повідомлення генерується осмислений текст, що приховує саме повідомлення. Ці методи мають ту важливу перевагу, що наявність прихованого повідомлення не виявляється системами моніторингу мережі. Але продуктивність цих методів не велика;

— *методи видалення заголовка файла,* ґрунтується на тому, що приховане повідомлення шифрується, і з отриманого файла видаляється ідентифікуючий заголовок — залишаються тільки шифровані дані. Адресат заздалегідь знає про передачу такого повідомлення й має пустий заголовок. Існує багато програмних засобів (White Noise Storm, S-Tools), що реалізують цей метод з алгоритмом шифрування PGP, але серйозним недоліком є необхідність заздалегідь передати частину інформації одержувачеві.

Останнім часом інтенсивно розвиваються *методи використання надмірності мультимедійної інформації*. Ці методи відрізняються дуже високою продуктивністю й високим ступенем прихованості. Вони дають можливість прихованої передачі великого обсягу інформації, дозволяють захистити авторські права, внести приховане зображення товарної марки, реєстраційного номера тощо. Ці методи засновані на тому, що молодші розряди цифрових відліків містять дуже мало корисної інформації. Їхнє заповнення додатковою інформацією практично

не впливає на якість сприйняття, що й дає можливість приховання конфіденційної інформації. Однак і в цих методах є недолік — через введення додаткової інформації спотворюються статистичні характеристики цифрових потоків. Для зниження компрометуючих ознак потрібна корекція статистичних характеристик сигналу.

Цифрові фотографії, цифрова музика, цифрове відео є послідовностями чисел, які кодують інтенсивність яскравості або гучності в дискретні моменти часу або в дискретних точках простору. Усі ці числа певною мірою приблизні, тому що є неточними пристрої оцифровування аналогових сигналів. Ця погрішність називається *шумами квантування*. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку й візуального образу. Їхня зміна відчутно не впливає на якість сприйняття, що й дає можливість для приховування додаткової інформації.

Графічні кольорові файли зі схемою змішування RGB кодують кожну точку малюнка трьома байтами. Кожна така точка складається з яскравостей трьох складових кольорів: червоного, зеленого, синього. Зміна кожного із трьох найменш значимих бітів приводить до зміни менш ніж 1 % яскравості цієї точки. Це дозволяє приховувати в стандартному графічному зображенні обсягом 800 Кбайт близько 100 Кбайт інформації, що абсолютно не помітно при перегляді зображення.

Більшість сучасних досліджень присвячено використанню як стегоконтейнери файлів зображень. Це обумовлено такими причинами:

– високою затребуваністю захисту фотографій, картин, відео від незаконного тиражування й поширення;

– відносно великим обсягом цифрового подання зображень, що дозволяє впроваджувати приховані повідомлення великого обсягу;

– заздалегідь відомим розміром контейнера, відсутністю обмежень, що накладаються вимогами реального часу;

– наявністю в більшості реальних зображень текстурних ділянок, що мають шумову структуру й добре підходять для вбудовування інформації;

– слабкою чутливістю людського ока до незначних змін кольорів зображення, його яскравості, контрастності, наявності в ньому шуму, перекручуванням поблизу контурів;

– добре розробленими останнім часом методами цифрової обробки зображень.

Однак є й істотні труднощі, основна з яких полягає в тому, що практично всі формати зберігання й передачі зображень, які використовують зараз, є стиснутими. Причому всі методи здійснюють стиснення із втратами. Це означає, що при стисненні зображення видаляється надлишкова інформація, що незначно позначається з погляду людини на якості зображення. Але саме цю надлишкову інформацію найпростіший стеганографічний алгоритм, що описаний вище, підмінює прихованим повідомленням. Тому стеганографічні алгоритми насправді набагато складніші. Стеганографія тісно пов'язана з теорією й практикою стиснення зображень, а також із фізіологією зору людини.

За способом вбудовування інформації стеганографічні алгоритми можна поділити на *лінійні* (*адитивні*), *нелінійні* й інші. Алгоритми адитивного впровадження інформації полягають у лінійній модифікації вихідного зображення, а її виділення у декодері робиться кореляційними методами. Ці алгоритми будуть розглянуті в підрозділі 4.4. У нелінійних методах вбудовування інформації використовується скалярне або векторне квантування. Огляд відповідних алгоритмів проводиться в підрозділі 4.5. Серед інших методів певний інтерес становлять методи, що використовують ідеї фрактального кодування зображень. Їхній огляд наведений у підрозділі 4.6.

## 4.4. Адитивні алгоритми

Почнемо з випадку, коли відомі й вихідне зображення (без прихованого повідомлення), і вбудоване повідомлення, що може бути, а може й не бути вбудованим у нього. У цьому випадку завдання полягає тільки в перевірці наявності повідомлення. На практиці таке завдання виникає для перевірки, чи є на зображенні водяний знак, що вказує, скажімо, на особу, яка має авторські права. Крім того, у такій постановці завдання можна вибрати водяний знак, який найбільше підходить для приховування.

В адитивних методах повідомлення являє собою послідовність чисел $w_i$ довжини $N$, що впроваджується в обрану підмножину відліків вихідного зображення $f$. Основна й найбільш часто використовувана формула для вбудовування інформації в цьому випадку є:

$$f'(m,n) = f(m,n)(1+\alpha w_i), \tag{4.1}$$

де α — ваговий коефіцієнт, а $f'$ — модифікований піксель зображення.

Інший спосіб вбудовування водяного знака був запропонований І. Коксом [1]:

$$f'(m,n) = f(m,n) + \alpha w_i , \tag{4.2}$$

або при використанні логарифмів коефіцієнтів:

$$f'(m,n) = f(m,n)e^{\alpha w_i} . \tag{4.3}$$

При вбудовуванні повідомлення за формулою (4.1) воно відновлюється в декодері в такий спосіб:

$$w_i^* = \frac{f^*(m,n) - f(m,n)}{\alpha f(m,n)} . \tag{4.4}$$

Тут під $f^*$ розуміють відліки отриманого зображення, що містять або не містять повідомлення $w$. Після знаходження послідовності $w_i^*$ вона порівнюється зі справжнім повідомленням $w$. Причому як міра ідентичності водяних знаків використовується значення коефіцієнта кореляції послідовностей $w$ і $w^*$:

$$\delta = \frac{w^* w}{\|w\|^* \|w\|} . \tag{4.5}$$

Ця кількість варіюється в інтервалі [–1; 1]. Значення, близькі до одиниці, свідчать про те, що витягнута послідовність зі значною ймовірністю є вбудованим водяним знаком. У цьому випадку робиться висновок, що аналізоване зображення містить водяний знак.

У декодері може бути встановлений деякий поріг $\tau = \frac{\alpha}{SN}\sum|f'|$ (тут $S$ — стандартне середньоквадратичне відхилення), що визначає ймовірність помилок першого й другого роду при виявленні водяного знака. При цьому коефіцієнт α може не бути постійним, а адаптив-

но змінюватися відповідно до локальних властивостей вихідного зображення. Це дозволяє зробити водяний знак більше *робастним* (стійким до видалення).

Для збільшення робастності повідомлення в багатьох алгоритмах застосовують широкосмужні сигнали. При цьому інформаційні біти можуть бути багаторазово повторені, закодовані із застосуванням коригувального коду або до них може бути застосоване яке-небудь інше перетворення, після чого вони модулюються за допомогою псевдовипадкової гаусівської послідовності. Така послідовність є доброю моделлю шуму, що присутній у реальних зображенях. У той же час синтетичні зображення (створені на комп'ютері) не містять шумів і в них складніше непомітно вмонтувати таку послідовність.

Звичайно, легше спочатку згенерувати рівномірно розподілену послідовність, а потім перетворити її на гаусівську послідовність, наприклад, за допомогою алгоритму Бокса–Мюллера.

Для видобування впровадженої інформації в адитивній схемі вбудовування водяного знака, звичайно, необхідно мати вихідне зображення, що досить сильно обмежує сферу застосування подібних методів.

Авторами [2; 3; 4] були запропоновані «сліпі» методи видобування водяного знака, що обчислюють кореляцію послідовності $w$ з усіма $N$ коефіцієнтами отриманого зображення $f^*$:

$$\delta = \frac{\sum_N f(m,n)^* w_i}{N} . \tag{4.6}$$

Потім отримане значення коефіцієнта кореляції $\delta$ порівнюється з деяким порогом виявлення $\tau$:

$$\tau = \frac{\alpha}{3N} \sum_N \left| f(m,n)^* \right| . \tag{4.7}$$

Основним недоліком цього методу є те, що саме зображення в цьому випадку розглядається як шумовий сигнал. Існує гібридний підхід («напівсліпі» схеми), коли в ході видобування доступна лише частина інформації про вихідне зображення.

Кореляційний метод дозволяє тільки виявити наявність або відсутність водяного знака. Для одержання ж усіх інформаційних бітів

потрібно протестувати всі можливі послідовності, що є вкрай складним завданням через необхідність перевіряти величезне число можливих варіантів.

Найбільш яскравим представником алгоритмів впровадження водяного знака на основі використання широкосмужних сигналів є *алгоритм Кокса* [5; 6]. Передбачається, що водяний знак являє собою послідовність псевдовипадкових чисел, розподілених за гаусівським законом з довжиною в 1000 чисел. Для модифікації відбираються 1000 найбільших коефіцієнтів дискретного косинус-перетворення. Вбудовування інформації виконується відповідно за формулою (4.2), а видобування водяного знака здійснюється відповідно до виразу (4.4).

Перевагою алгоритму є те, що завдяки вибору найбільш значимих коефіцієнтів водяний знак є більш робастним при стисненні й інших видах обробки сигналу. Разом із тим алгоритм уразливий для атак Гравера. Крім того, обчислення двовимірного дискретного косинус-перетворення дуже трудомістке.

Існує ще багато цікавих алгоритмів, заснованих на лінійному вбудовуванні даних, що знайшли своє практичне застосування. Звернемо увагу на такі наукові праці [8; 9; 10; 11].

Якщо замість послідовності псевдовипадкових чисел у зображення вбудовується інше зображення, наприклад, логотип фірми, то відповідні алгоритми впровадження називаються *алгоритмами злиття*. Розмір впроваджуваного повідомлення набагато менший розміру вихідного зображення. Перед вбудовуванням воно може бути зашифрованим або перетвореним яким-небудь іншим чином. У таких алгоритмів є дві переваги.

По-перше, можна допустити деяке перекручування прихованого повідомлення, тому що людина однаково зможе розпізнати його.

По-друге, наявність впровадженого логотипа є більше переконливим доказом авторських прав, ніж наявність певного псевдовипадкового числа.

Розглянемо як приклад впровадження зображень у зображення за допомогою *алгоритму Че* [12].

Алгоритм впроваджує чорно-біле зображення (логотип), розміром до 25 % від розміру вихідного зображення. Перед вбудовуванням виконується однорівнева декомпозиція як вихідного зображення, так

і емблеми із застосуванням фільтрів Хаара. Вейвлет-коефіцієнти вихідного зображення позначаються *f (m, n)*, а вейвлет-коефіцієнти логотипа — *w (m, n)*.

Модифікації піддаються всі коефіцієнти перетворення, як це показано на рис. 4.2.

Спочатку коефіцієнти кожного субдіапазону як вихідного зображення, так і логотипа, представляються 24 бітами (з яких один біт припадає на знак). Через те що розмір логотипа в 4 рази менший вихідного зображення, то необхідно збільшити кількість його коефіцієнтів. Для цього виконуються такі дії.

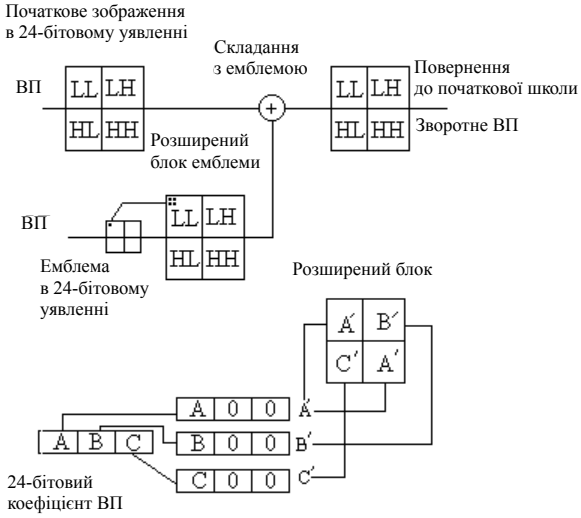



*Рис. 4.2.* Схема вбудовування логотипа з використанням вейвлет-перетворювань (ВП)

Позначимо через *A*, *B* і *C* відповідно старший, середній і молодший байти 24-бітного подання логотипа. На рис. 4.2 показане формування трьох 24-бітних чисел $A'$, $B'$ і $C'$. Старший байт кожного із цих чисел являє собою відповідно *A*, *B* або *C*, два інших байти заповнюються нулями. Потім формується розширений в чотири рази блок коефіцієнтів логотипа. Після чого він поелементно складається з 24-бітною версією вихідного зображення:

$$f'(m,n) = \alpha f(m,n) + w(m,n) \cdot \tag{4.8}$$

Отримане значення відображається до вихідної шкали на основі значень мінімального й максимального коефіцієнта субдіапазону. Після чого здійснюється зворотне дискретне вейвлет-перетворення.

Для видобування водяного знака використовується інверсна формула, аналогічна формулі (4.4).

Цей алгоритм дозволяє приховати досить значний обсяг даних у вихідному зображенні: до чверті від розмірів вихідного зображення.

Цікава модифікація щойно розглянутого алгоритму належить Кандьо [13].

## 4.5. Стеганографічні методи на основі квантування

Під *квантуванням* розуміють процес приведення великої (можливо й нескінченної) множини значень до деякої, як правило, значно меншої скінченної множини чисел. Зрозуміло, що при цьому відбувається зменшення обсягу інформації за рахунок її перекручування. Квантування знаходить застосування в алгоритмах стиснення із втратами. Розрізняють *скалярне* й *векторне квантування*. При векторному квантуванні, на відміну від скалярного, відбувається відображення не окремо взятого відліку, а їх сукупності (вектора). З теорії інформації відомо, що векторне квантування ефективніше скалярного за ступенем стиснення, але має більшу складність. У стеганографії знаходять застосування обидва види квантування.

У кодері квантівника вся область значень вихідної множини ділиться на інтервали і в кожному інтервалі обирається число, що його представляє. Це число є *кодовим словом* квантівника й зазвичай буває центром інтервалу квантування. Множина кодових слів називається *книгою квантівника*. Усі значення, що потрапили в цей інтервал, замінюються в кодері на відповідне кодове слово. У декодері прийнятому числу зіставляється деяке значення. Інтервал квантування зазвичай називають кроком квантівника.

Вбудовування інформації із застосуванням квантування належить до нелінійних методів. У роботі Д. Егерса, Дж. Су і В. Гіроза [15] було показано, як може бути побудована подібна «сліпа» стегосистема, пропускна здатність якої еквівалентна пропускній здатності стегосистеми, що має на прийомі вихідний сигнал. При цьому робиться припущення про гаусівський характер вихідного сигналу.

Модель стегосистеми, яка не потребує наявності вихідного сигналу в декодері, подана на рис. 4.3. Передане повідомлення *m* для непомітності має обмежену енергію. Перешкодами є вихідний сигнал і ще одна гаусівська перешкода — шум обробки (квантування). Кодеру відомий вихідний сигнал, декодер повинен витягти повідомлення *m* без знання обох складових перешкоди. Така схема придатна для приховання й передачі секретного повідомлення.

У роботі [16] М. Костою запропонований метод боротьби з перешкодами, що, однак, є непрактичним через необхідність виконання повного перебору кодових слів у книзі великого розміру. Тому були запропоновані численні поліпшення методу Коста, що полягають у застосуванні різних структурованих квантівників (наприклад, ґратчастих або деревоподібних).

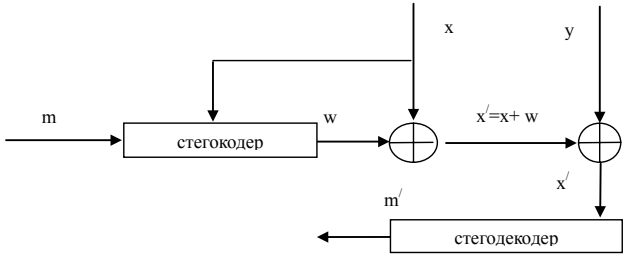



*Рис. 4.3.* Модель «сліпої» стегосистеми

Найбажаніше впровадження інформації у спектральну сферу зображення. Якщо при цьому використовуються лінійні методи, то вбудовування повідомлення роблять у середні смуги частот. Це пояснюється тим, що енергія зображення зосереджена в основному в низькочастотній області. Отже, у детекторі в низькочастотному діапазоні спостерігається сильний шум самого сигналу. У високочастотних областях більшу величину має шум обробки, наприклад, стиснення. На відміну від лінійних, нелінійні

схеми вбудовування інформації можуть використовувати низькочастотні сфери, тому що потужність упроваджуваного повідомлення не залежить від амплітуди коефіцієнтів. Це пояснюється тим, що в нелінійних алгоритмах приховання даних не використовують кореляційний детектор — коефіцієнти малої й великої амплітуди обробляються однаково.

Як показано на рис. 4.3, впроваджуване повідомлення $m$ певним чином модулюється й складається з вихідним сигналом $x$, у результаті чого виходить заповнений контейнер $s\ (x, m)$. Цей контейнер може розглядатися і як ансамбль функцій від $x$, індексованих по $m$, тобто $s_m\ (x)$. Ці функції мають такі властивості:

1) кожна з них повинна бути близька, яку візуально не можна відрізнити від $x$;

2) точки однієї функції повинні перебувати на достатній відстані від точок іншої функції, щоб забезпечити можливість робастного детектування повідомлення.

У ролі таких функцій може виступати сімейство квантівників. Число будь-яких $m$ визначає необхідне число квантівників; індекс $m$ визначає квантівник, який використовується для подання повідомлення $m$. Для випадку $m = 2$ одержуємо бінарний квантівник. На рис. 4.4 пояснюється принцип вбудовування інформації із застосуванням модуляції індексу квантування. Для вкладення біта $m$ О {1, 2}, точка зображення переводиться в одне із прилеглих кодових слів. Мінімальна відстань між кодовими словами різних квантівників визначає робастність стегосистеми.

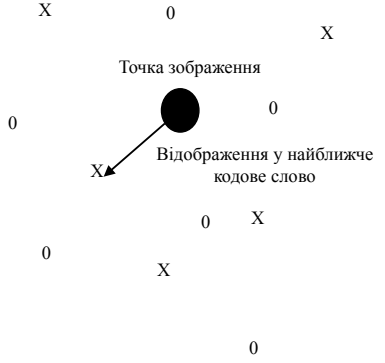



*Рис. 4.4.* Відображення точки зображення в кодове слово з найближчого оточення

У роботах [17; 18] розглядається застосування у схемі модуляції індексу квантування так званого *дизеризованого квантівника*. *Дизеризація* полягає в тому, що перед квантуванням до сигналу додається певне число $d_i$, яке віднімається після квантування:

$$s_i = Q\left(x_i + d_i\right) - d_i, \qquad 0 \le i \le L\,. \tag{4.9}$$

Таким чином, сімейство дизеризованих квантівників утворюється на основі одного квантівника $Q$ й вектора дизеризації $d$ довжиною $L$. Розглянемо для прикладу бінарний скалярний рівномірний квантівник $Q$ із розміром кроку $\Delta$. Сімейство дизеризованих квантівників може бути отримано, наприклад, шляхом генерації вектора $d(1)$ як випадкової рівномірно розподіленої послідовності довжиною $L$, члени якої приймають значення в діапазону $[-\Delta / 2; \Delta / 2]$. Так само, як і вектор $d(2)$, обираємо вектор

$$d_i\left(2\right) = \begin{cases} d_i\left(1\right) + \Delta/2, & d_i\left(1\right) < 0 \\ d_i\left(1\right) - \Delta/2, & d_i\left(1\right) \ge 0 \end{cases} \qquad 0 \le i < L\,. \tag{4.10}$$

Цікавою особливістю розглянутого дизеризованого квантівника є те, що помилка квантування не залежить від вхідного сигналу [18].

Дизеризований квантівник може застосовуватися й у техніці розширення спектра сигналу в стеганографії. Заміна звичайного методу вбудовування з розширенням спектра полягає в простій заміні додавання на операцію квантування. Вкладення інформації за допомогою сигналів із розширенням спектра може бути представлене як

$$s\left(x, m\right) = x + a\left(m\right) \cdot u\,, \tag{4.11}$$

де $u$ — нормалізований псевдовипадковий вектор. Цей вираз може бути переписаний у вигляді:

$$s\left(x, m\right) = \left(\tilde{x} + a\left(m\right)\right) \cdot u + \left(x - \tilde{x} \cdot u\right), \tag{4.12}$$

де $\tilde{x}$ — проекція сигналу $x$ на вектор $u$: $\tilde{x} = x \cdot u$. Тепер замінимо операцію додавання $\tilde{s} = \tilde{x} + a\left(m\right)$ на операцію квантування. Тоді формула для вбудовування повідомлення буде мати вигляд:

$$s\left(x, m\right) = \left(Q\left(\tilde{x} + a\left(m\right)\right) - a\left(m\right)\right) \cdot u + \left(x - \tilde{x} \cdot u\right). \tag{4.13}$$

Звернемо увагу на алгоритми вбудовування інформації з використанням квантування, що належать Чу [19] та Хсу [20].

Вище розглядався випадок, коли на вхід квантівника подавалися скалярні значення, і кожне кодове слово квантівника являло собою одиничний відлік виходу джерела. Методика квантування, що передбачає роботу з послідовностями або блоками відліків, називається векторним квантуванням. Проблема в цьому випадку полягає в генерації множини послідовностей, що має назву кодова книга. Цей процес проілюстрований на рис. 4.5.

Алгоритм квантування повинен відшукувати найближчий вектор у досить великій кодовій книзі для заданого вектора джерела з обмеженою обчислювальною складністю.

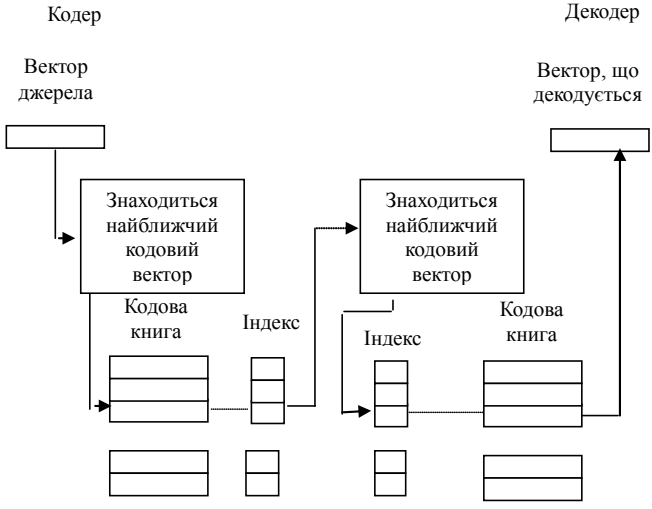



*Рис. 4.5.* Векторне квантування

Розглянемо як приклад *алгоритм Чо* [21].

Водяний знак у цьому алгоритмі є послідовністю символів, отриманою з логотипа, розмір якого в чотири рази менший за розміри контейнера. *n* коефіцієнтів вейвлет-перетворення групуються для формування *n-мірного* вектора. Зокрема, при $n = 4$ створюється ґратчаста структура $D_4$. Для впровадження одного коефіцієнта логотипа здійснюється маніпуляція вектора квантованих коефіцієнтів зображення-контейнера.

Вектор коефіцієнтів дискретного вейвлет-перетворення $v_i$ модифікується відповідно до масштабованого кодового слова, що становить $w_i$:

$$v_i = v_i + \alpha C(w_i). \tag{4.14}$$

Таким чином, при $n = 4$ для вбудовування одного коефіцієнта логотипа необхідно змінити чотири коефіцієнти контейнера.

Для видобування інформації потрібне вихідне зображення. Вектор помилки обчислюється за формулою $e = \frac{v^* - v}{\alpha}$ і потім для відновлення вкладення за кодовою книгою шукається найближче кодове слово:

$$w_i = \min_{w_i} \|C(w_i) - e\|. \tag{4.15}$$

Якщо кодова книга індексована, то пошук може бути виконаний швидко. У цілому автори зазначають, що метод упровадження за допомогою векторного квантування є більш гнучким порівняно зі скалярним аналогом і дозволяє краще контролювати робастність, рівень перекручувань і якість впроваджуваного зображення за допомогою параметра α.

## 4.6. Стегоалгоритми, що використовують фрактальні перетворення

В алгоритмах цього підрозділу використовуються ідеї, запозичені з галузі кодування зображень. Тема фрактального стиснення зображення, напевно, найоригінальнішого алгоритму стиснення, стала популярною в середині 90-х років XX століття. Цьому методу не давалися величезні аванси, повідомлялося про фантастичні досягнуті коефіцієнти стиснення (біля декількох тисяч). Як з'ясувалося пізніше, значна частина цих публікацій мала суто рекламний характер, а експерименти були поставлені некоректно. Наскільки відомо, то кращі фрактальні кодери не значно перевершують за ефективністю стиснення алгоритм JPEG і значно поступаються алгоритму JPEG 2000. Важливою перевагою фрактального методу стиснення для багатьох

додатків є його різка асиметричність. Декодер реалізується винятково просто. Так, стиснутий цим методом відеофільм може бути відтворений навіть на 386DX-40.

Основна ідея методу стиснення полягає в пошуку послідовності афінних перетворень (поворот, зрушення, масштабування), що дозволяють апроксимувати блоки зображення малого розміру (рангові) блоками більшого розміру (доменами). Тобто вважається, що зображення *самоподібне*. Ця послідовність перетворень і передається декодеру. Будучи застосованими до будь-якого зображення, ці перетворення дають у результаті шукане зображення. Фрактальне кодування може розглядатися як різновид векторного квантування, причому як кодова книга виступають різні перетворення.

Розглянемо *алгоритм Баса* [22], що використовує фрактальне перетворення.

Цікаво, що «зовнішній» водяний знак у цьому алгоритмі взагалі відсутній. Інформація вбудовується за рахунок такої зміни зображення, щоб воно стало містити самоподібні. У такий спосіб може бути впроваджено 15 різних водяних знаків.

Алгоритм працює в такий спосіб. Спочатку вибираються «особливі» точки з використанням відомого із фрактального кодування методу Стефана–Харріса. Кожна особлива точка визначає блок розміром 4x4 навколо неї й 16 блоків розміром 4x4, що утворять доменний пул. Для кожної особливої точки виконують зміну доменного блоку в тій же позиції так, щоб він був більше схожий на ранговий блок, ніж будь-який інший доменний блок. (Тому всього можна вибрати 15 блоків, це дає можливість впровадити всього 15 водяних знаків.) Доменний блок, що вийшов, визначається виразом:

$$W_j = \alpha \frac{D_j - \bar{D}_j}{\max\left(D_j - \bar{D}_j\right)} \ , \tag{4.16}$$

де $D_j$ середнє значення пікселів у $D_j$. Він додається до $R_j$ відповідно до виразу:

$$R_j^{'} = W_j + \mathrm{int}\left(\frac{R_j}{s}\right)s + \frac{s}{2} \ , \tag{4.17}$$

де $s$ — коефіцієнт, що враховує квантування.

При видобуванні водяного знаку спочатку відновлюються значення особливих точок $D_j$ і $W_j$. Для кожного блоку $R_j$ обчислюється

$$\hat{W}_j' = R_j - \mathrm{int}\left(\frac{R_j}{s}\right)s - \frac{s}{2} \ . \qquad (4.18)$$

Далі знаходять найбільш схожий блок, що повинен бути тим же, що й у процесі вбудовування. Число блоків, що збіглися, є мірою ймовірності того, що водяний знак присутній у зображенні.

## 4.7. Атаки на системи цифрових водяних знаків і їх класифікація

Виникає питання, чи є цифрові водяні знаки досить надійним засобом для захисту авторських прав на мультимедійні твори? Наприклад, чи може потенційний порушник цих прав:

а) виявити, що на зображенні присутній водяний знак;

б) зробити цей знак неможливим для читання;

в) поставити власний водяний знак.

Відповіді на всі ці запитання, на жаль, позитивні. Це викликано тим, що цифрові водяні знаки на зображенні повинні задовольняти суперечливим вимогам візуальної непомітності й стійкості до основних операцій обробки сигналів.

Звернемося, наприклад, до розглянутої вище системи вбудовування повідомлень шляхом модифікації молодшого значущого біта пікселів. Практично будь-який спосіб обробки зображень може привести до руйнування значної частини убудованого повідомлення. Наприклад, розглянемо операцію обчислення ковзного середнього за двома сусідніми пікселями $(a + b) / 2$, що є найпростішим прикладом низькочастотної фільтрації. Після цієї операції значення молодшого значущого біта зміниться після усереднення приблизно у половини випадків.

Ще один спосіб — зміна шкали квантування, скажімо, з 8 до 7 біт. Аналогічний вплив робить і будь-яке стиснення зображень із втратами.

Існують також і набагато згубніші для цифрового водяного знаку операції обробки зображень, наприклад, масштабування, повороти,

усікання, *перестановка* пікселів. Ситуація погіршується ще й тим, що перетворення зображення можуть здійснюватися не лише порушником, але й законним користувачем, або бути наслідком помилок при передачі по мережі.

Невеликий зсув пікселів може привести до неможливості виявлення цифрового водяного знака в детекторі. Такий зсув непомітний для ока, але приводить до повного руйнування водяного знака.

Розглянемо атаки, специфічні для систем цифрового водяного знака. Можна виділити такі категорії атак [23].

1. Атаки проти вбудованого повідомлення, які спрямовані на видалення або псування водяного знака шляхом зміни всього зображення. Методи атак із цієї категорії не намагаються оцінити й виділити водяний знак. Прикладами таких атак можуть бути лінійна фільтрація, стиснення зображень, додавання шуму, вирівнювання гістограми, зміна контрастності й т. ін.

2. Атаки проти стегодетектора спрямовані на те, щоб ускладнити або унеможливити правильну його роботу. При цьому водяний знак у зображенні залишається, але втрачається можливість його перегляду. У цю категорію входять такі атаки, як афінні перетворення (тобто масштабування, зсув, повороти), усікання зображення, перестановка пікселів і т. д.

3. Атаки проти протоколу використання цифрового водяного знака, які в основному пов'язані зі створенням фальшивих цифрових водяних знаків.

4. Атаки проти самого цифрового водяного знака. Ці атаки спрямовані на оцінювання й видобування водяного знака із зображення, по можливості без перекручування останнього. У цю групу входять такі атаки, як статистичне усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації та ін.

Зазначимо, що розглянута класифікація атак не є єдино можливою й повною. Крім того, деякі атаки (наприклад, видалення шуму) можуть бути віднесені до кількох категорій. У роботі Ф. Петітколаса, Р. Андерсона і М. Кюна [24] була запропонована інша класифікація атак, що також має свої переваги й недоліки.

Відповідно до цієї класифікації всі атаки на системи вбудовування цифрового водяного знака можуть бути поділені на чотири групи:

1) атаки, спрямовані на видалення цифрового водяного знака;

2) геометричні атаки, спрямовані на перетворення контейнера;

3) криптографічні атаки, тобто атаки, які вчиняються методами, розвиненими в криптографії;

4) атаки проти використовуваного протоколу вбудовування й перевірки цифрового водяного знака.

Безліч методів виявлення або зміни цифрового водяного знака не повинна розчаровувати. Взагалі будь-який захист, створений однією людиною, інша людина, витративши певний час і кошти, може обійти. Тут ключові слова «певний час і кошти». Завдання стеганографії, як, скажімо, і криптографії, створити такий захист, щоб її подолання обходилося значно дорожче, ніж вигоди, які одержить порушник у випадку її злому. Пояснимо цю думку на прикладі.

Якщо при нанесенні цифрового водяного знака стоїть завдання зробити його непомітним і стійким до різного роду перетворень, то перед зломником стоїть ще більш складне завдання — нейтралізувати цифровий водяний знак, не погіршивши відповідними перетвореннями якість контенту (того, що захищено водяним знаком). Швидше за все, коли завдання зломником буде вирішено, контрафактну продукцію можна тільки продавати за безцінь на дешевих розпродажах, тому що попит на неї до цього моменту вже буде цілком задоволений.

## 4.8. Висновки

У сучасному світі все гостріше постає проблема захисту об'єктів авторського права, що зберігаються і (або) передаються в електронно-цифровому вигляді. Зокрема, це стосується і мультимедійних творів. Останні зміни в законодавстві ряду країн, у тому числі й України, показують, що питанням захисту таких об'єктів авторського права приділяється дуже велике значення. У більшості держав активно розвиваються призначені для цього технічні засоби, що призвело до швидкого розвитку стеганографії — науки про приховання інформації.

На сучасному етапі давня наука стеганографія знайшла новий подих, ставши наймолодшою наукою в галузі захисту інтелектуальної власності — цифровою стеганографією. За короткий час (із кінця минулого сторіччя) цифрова стеганографія збагатилася великою кількістю ефективно працюючих методів приховування інформації в мультимедійних творах. Вже існує велика кількість додатків, що успішно реалізують ці алгоритми й ефективно захищають авторські права на мультимедійні твори.

Якщо вас зацікавили питання, розглянуті у цьому розділі, то рекомендуємо звернутися за детальною інформацією до монографії В. Грибуніна, І. Окова та та І. Турінцева [10]. Крім того, у статті І. Швидченка [11] можна знайти опис майже всіх сучасних стеганографічних програм та результати їх детального тестування.

Зі спеціальними питаннями впровадження цифрових водяних знаків в аудіосигнали можна ознайомитися в огляді Н. Кошкіної [25].

# РОЗДІЛ 5

# ЗАХИСТ АВТОРСЬКИХ ПРАВ АУДІОДАНИХ

## 5.1. Розвиток проблеми захисту авторських прав

Інформатизація суспільства веде до створення єдиного світового інформаційного простору, у рамках якого здійснюється накопичення, обробка, зберігання та обмін інформацією між суб'єктами. Мультимедійний Web-документ, являє собою сукупність різних об'єктів, що захищаються законом про авторське право.

У той же час існує ряд технічних особливостей мережі, які істотно ускладнюють захист авторських і суміжних прав. Наприклад, легкість створення копій в необмеженій кількості, а також легкість запису на жорсткий диск персонального комп'ютера частин Internet-сайту (що є порушенням права на відтворення) робить кожного користувача мережі потенційним порушником законодавства. Цілком очевидно, що в цьому випадку порушується право копіювання.

Проблема незаконного копіювання виникла ще задовго до появи цифрових і навіть аналогових пристроїв відтворення і копіювання творів. Механічні піаніно (піаноли), популярні на початку XX століття, використовували перфострічку для управління клавішами. У США компанії-виробники переводили традиційний нотний запис у запис для піанол на перфострічці без сплати гонорарів видавцям і композиторам. Незважаючи на незадоволеність останніх, їх вимога повністю заборонити випуск нових відтворюючих пристроїв не була задоволена, проте виробники були зобов'язані виплачувати певну суму за кожен випущений запис [1].

Пізніше проблема знову виникла з появою аудіомагнітофонів, а потім відеомагнітофонів. У США це привело до так званої справи Betamax, у якій студія Universal намагалася заборонити корпорації

Sony виробляти відеомагнітофони з можливістю запису. Справа вирішилася на користь Sony, створивши прецедент, згідно з яким законне виробництво систем, які, крім нелегальних застосувань (створення нелегальних копій фільмів, що транслюються по телебаченню), мають істотне легальне застосування (запис телепередач для подальшого їх перегляду у кращий для користувача час — це застосування також було визнане добросовісним використанням у ході судового розгляду) [1].

Пізніше фільми також почали продаватися на відеокасетах, і незабаром з'явилася перша система для захисту від копіювання від Macrovision. Вона «обдурювала» автоматичне регулювання посилення, що використовувалось під час запису відеокасети, додаючи імпульси в порожній інтервал вертикальної розгортки, які не впливали при цьому на якість відтворення. Хоча Macrovision запатентувала не тільки саму систему DRM, але й способи її обходу, пристрій для усунення захисту було досить легко дістати [1].

Перехід на цифрові методи зберігання й передачі інформації тільки підсилив стурбованість правовласників. Тоді як аналогові записи неминуче втрачають свою якість не лише при копіюванні, але навіть і при нормальному використанні, цифрові записи можуть бути скопійовані або відтворені необмежену кількість разів без втрати якості. У сукупності зі значним поширенням Internet і файлообмінних мереж це привело до збільшення обсягів нелегального розповсюдження медіапродукції до значних розмірів.

Зазвичай, ґрунтуючись на особливостях мови HTML, інформацію про авторство на відповідних сторінках указують трьома основними способами: безпосередньо у тексті сторінки, зазвичай внизу; у вигляді коментарів у документі; за допомогою тега. Проте всі ці види вказівок на авторство Web-документа легко піддаються модифікації і згодом достатньо проблематично довести право на авторство того або іншого документа. Тому крім правових необхідно використовувати й інформаційні (технічні) способи захисту з урахуванням положень Закону України «Про авторське право і суміжні права» від 23.12.1993 року № 3792-XII у редакції від 11.07.2001 року № 2627-III (Відомості Верховної Ради. — 2001. — № 43. — Ст. 214).

### 5.1.1. Огляд сучасних методів захисту авторських прав

Одним з можливих рішень у боротьбі з «піратством» є розробка технології розпізнавання контрафактного контенту, про що згадувалося вище. Так, зокрема, в Російській Федерації представники музичної і кіноіндустрії готові спільно з Internet-провайдерами розробити подібні технології, для чого правовласники надаватимуть провайдерам «каталоги контенту» й інші матеріали про об'єкти творчості, що потребують охорони, на основі яких оператор може підготувати і використовувати технічні засоби захисту, які мають застережувати незаконне застосування контрафактних об'єктів.

Сьогодні можна виокремити два основні напрями захисту авторських прав аудіоданих [2]:

*технічні засоби захисту авторських прав* (*DRM* — Digital rights management — управління цифровими правами, неофіційно іноді Digital restrictions management) — частіше програмні, рідше програмно-апаратні засоби, які ускладнюють створення копій творів (поширюваних в електронній формі), що захищаються, або дозволяють відстежити створення таких копій;

використання прийомів *стеганографії* — наприклад, упровадження в музичний файл певної секретної мітки або даних за аналогією з реєстраційним ключем для програмного забезпечення. Якщо ключ користувача збігається із секретною міткою, то цей користувач зможе відтворити музику, записану у звуковому файлі. Крім того, за допомогою прийомів стеганографії у звукових файлах можна приховано передати додаткову інформацію, наприклад, прізвище композитора.

### 5.1.2. Технології DRM

Технічними засобами захисту авторських прав визнаються будь-які технології, технічні пристрої або їх компоненти, які контролюють доступ до твору, що запобігають або обмежують здійснення дій, які не дозволені автором або іншим правовласником щодо твору.

Метою технологій DRM є контроль над використанням цифрових носіїв і даних та унеможливлення неавторизованого доступу, копіювання або конвертації в інший формат користувачем. Ще до появи

цифрових або навіть електронних носіїв власники прав на продукт або інші фінансово зацікавлені сторони впроваджували бізнесові та юридичні обмеження щодо технологій копіювання, оскільки воно призводить до втрати прибутків та зміни ситуації на ринку.

Поява цифрових медіа та технологій аналогово-цифрового конвертування, особливо таких, що можуть легко використовуватися на значно поширених ПК, викликала хвилю занепокоєння приватних осіб та організацій — власників авторських прав, особливо в галузях музичної та кіноіндустрії, оскільки ці організації або індивідууми є частково або повністю фінансово залежними від доходів, генерованих унаслідок надання прав користування об'єктами авторського права третім особам.

На відміну від аналогових носіїв або пристроїв, що використовують аналогові методи копіювання цифрового вмісту, наприклад, магнітофонів, якість сигналу при використанні яких неминуче погіршується внаслідок копіювання, а в деяких випадках просто за рахунок тривалого використання, цифрові носії або файли можуть копіюватися в необмеженій кількості без будь-яких втрат якості в кожній копії.

Перетворення персонального комп'ютера на звичайний побутовий пристрій вкрай спростило для кінцевого споживача запис інформації (як вільної, так і захищеної авторським правом) з будь-якої початкової форми (радіосигнал, телетрансляція тощо) та створення цифрових копій (здирання). Все це в поєднанні з Internet та засобами роздачі файлів значно полегшило розповсюдження неавторизованих копій цифрових носіїв, захищених авторським правом (піратство).

Технології DRM дозволили видавцям запровадити політики доступу до носіїв, які не лише запобігають порушенню авторських прав, але також перешкоджають законному використанню творів, захищених авторським правом або навіть обмежують використання вільних (незахищених авторським правом) творів, розповсюджуваних видавцями, наприклад, розміщення DRM на деяких public-domain або open-licensed електронних книжках або застосування DRM у засобах побутової електроніки для перешкоджання запису будь-якої інформації, в тому числі і не захищеної авторським правом.

Найширше технології DRM використовують в індустрії розваг (кіноіндустрія та звукозапис). Багато з-поміж онлайнових музичних магазинів, таких, як Apple Inc.'s iTunes Store, а також видавців e-book запровадили технології DRM до своїх продуктів. Останніми роками деякі з телевізійних продюсерів запровадили DRM у пристроях побутової електроніки для забезпечення контролю доступу до їх передач, що транслюються відкритими телеканалами і можуть бути записані користувачами.

*Огляд систем DRM. Система шифрування змісту.* Одним з перших випадків застосування DRM була Content Scrambling System (CSS), запроваджена DVD Forum на кіно-DVD у 1996 році. CSS використовувала простий алгоритм шифрування та зобов'язувала виробників побутової електроніки підписувати ліцензійні угоди, які обмежували технологічні можливості пристроїв, наприклад, використання деяких цифрових виходів, які могли б бути використані для отримання високоякісних цифрових копій. Таким чином, DVD Forum взяв у свої руки (хоча й непрямо) повний контроль над єдиним видом побутової електроніки, спроможним декодувати DVD, обмежуючи використання цих пристроїв. Така ситуація існувала до 1999 року, коли Д. Йохансен випустив DeCSS, що дозволяв програвати DVD, зашифрований за допомогою CSS, на ПК, використовуючи операційну систему Linux, для якої не існувало ліцензії на використання ПЗ [3; 4].

*Програма захисту медіа Microsoft Windows Vista.* Програмне забезпечення від Microsoft Windows Vista включає систему DRM під назвою Protected Media Path, яка використовується для обмеження програвання DRM-захищеного контенту за допомогою неліцензованого ПЗ. Окрім того, PMP може шифрувати інформацію під час її передачі на монітор або графічну карту, таким чином обмежуючи можливості неавторизованого копіювання.

*Покращена система доступу.* Advanced Access Content System (AACS) — система DRM, призначена для використання в HD DVD та Blu-ray Disc, розроблена AACS Licensing Administrator, LLC (AACS LA) — консорціумом, у який входять Disney, Intel, Microsoft, Matsushita (Panasonic), Warner Brothers, IBM, Toshiba та Sony. У грудні 2006 року

ключ, що використовувався для шифрування, був опублікований в Internet хакерами, таким чином уможливлюючи повний доступ до AACS-захищеного змісту HD DVD. Після відкликання зламаного ключа були опубліковані нові зламані ключі [5].

*Аудіо CD.* Одним із засобів захисту є логотип, що відображується на звукових компакт-дисках, які відповідають стандарту. Диски, що використовують технології DRM, не відповідають стандарту запису Audio CD, а є носіями CD-ROM. Таким чином, на них не може використовуватися логотип «CD», на відміну від тих дисків, що відповідають стандарту, який відомий як Red Book. Внаслідок невідповідності стандарту такі диски можуть не відтворюватись на деяких моделях CD-програвачів. Багато споживачів також не в змозі програвати такі диски на ПК. На деяких ПК під управлінням Microsoft Windows можливі загальні проблеми з функціонуванням операційної системи під час спроби програти такий CD [5].

У 2005 році корпорація Sony BMG застосувала технологію DRM, яка встановлювала ПЗ на комп'ютер користувача без будь-якого попередження або запиту на підтвердження. Це ПЗ включало вірус rootkit, який відкривав серйозну вразливість у системі безпеки ПК. Після того, як ця інформація стала публічною, корпорація Sony намагалася зменшити серйозність вразливостей, але врешті-решт була змушена відкликати мільйони компакт-дисків та випустити «заплатки» для ПЗ аби, принаймні, видалити rootkit. Було ініційовано кілька судових процесів проти корпорації, які були закриті за згодою корпорації та прийшлося виплатити відступні постраждалим споживачам.

Фактично ПЗ, застосоване корпорацією Sony BMG, включало дуже обмежені можливості для запобігання копіюванню, оскільки воно могло використовуватися лише на ПК під управлінням ОС Windows. Окрім того, захист можна було легко обійти, наприклад, тримаючи клавішу під час вставляння компакт-диска. У той самий час вразливість у системі захисту ПК, створена цим ПЗ, потенційно представляла набагато серйознішу проблему для кінцевого користувача.

У січні 2007 року корпорація EMI припинила випуск аудіо CD з використанням DRM, стверджуючи, що «витрати на DRM не відповідають результатам». Слідом за EMI, Sony BMG була останнім ви-

давцем, який повністю відмовився від використання DRM, з того часу аудіо CD, що випускаються під чотирма торговельними марками корпорації, не включать технологій DRM [6].

*Захист музичних творів в Internet.* Багато онлайнових музичних магазинів, серед яких iTunes, Napster music store, Sony, Kazaa, використовують DRM для обмеження використання музики, придбаної та звантаженої он-лайн.

Стандарти, що використовують різні компанії, на цей час не є інтероперабельними, за винятком використання однієї і тієї ж технології (наприклад, у випадку Napster, Kazaa та Yahoo Music). Практично всі магазини потребують звантаження та встановлення певного виду клієнтського програмного забезпечення або плагінів.

Хоча DRM використовує переважна більшість музичних Internet-постачальників, деякі онлайнові магазини, наприклад Amazon, не використовують технології захисту, але закликають користувачів запобігати неавторизованому копіюванню та розповсюдженню.

Хоча DRM покликані перешкодити лише неправомірному копіюванню творів, як правило, вони не допускають або обмежують будь-яке копіювання, зокрема добросовісне, оскільки поки що неможливо технічними засобами автоматично відрізнити «законне» копіювання від «незаконного». Таке обмеження можливостей користувача викликає критику DRM з боку правозахисників.

На відміну від захисту від копіювання, під DRM мають на увазі більш загальний клас технологій, які можуть дозволяти обмежене копіювання, а також можуть накладати інші обмеження, такі як обмеження строку, протягом якого можливий перегляд або відтворення твору, що захищається. При цьому під DRM розуміють саме технічні засоби захисту, тоді як захист від копіювання може включати також організаційні, юридичні й інші заходи.

*Ефективність систем DRM.* Більшість сучасних систем DRM використовують криптостійкі алгоритми захисту, проте ці методи не можуть використовуватися повноцінно, оскільки засновані на припущенні, що для діставання доступу до зашифрованої інформації потрібен секретний ключ. Проте в разі застосування DRM типовою є ситуація, коли обмеження обходяться правомірним власником копії, який для можливості перегляду (відтворення) повинен мати і зашиф-

ровану інформацію, і ключ до неї, що зводить до нуля весь захист. Тому системи DRM намагаються приховати від користувача використовуваний ключ шифрування (зокрема, використовуючи апаратні засоби), проте це не можна здійснити достатньо надійно, оскільки пристрої відтворення, які зараз використовуються (персональні комп'ютери, відеомагнітофони, DVD-програвачі), є достатньо універсальними і знаходяться під контролем користувачів.

Слід також зазначити, що дозволити відтворення і в той же час заборонити копіювання є принципово нерозв'язним завданням (так званий «аналоговий пролом», англ. analog hole): відтворення — читання інформації, її обробка і запис на пристрій виводу, копіювання — читання і запис інформації на пристрій зберігання. Тобто, якщо можливе відтворення (що включає проміжний етап читання інформації), можливе і її подальше копіювання. Тому ефективний технічний захист від копіювання при дозволеному відтворенні може бути досягнутий тільки тоді, коли весь пристрій (комп'ютер, програвач) знаходиться цілком під контролем правовласника.

### 5.1.3. Правова підтримка технології DRM

Оскільки DRM малоефективні самі по собі, для них встановлений правовий захист. Законодавці багатьох країн, йдучи назустріч волі найбільших правовласників, встановили відповідальність за обхід DRM.

Сьогодні практично кожний скачує який-небудь музичний або аудіовізуальний твір, фільм або телепередачу, дивився он-лайн ТБ або слухає Internet-радіо. Чи завжди це робиться законно? Чи не порушуються при цьому авторські і суміжні права власників цього контенту? Законодавство у сфері авторського права і суміжних прав вдосконалюється разом з розвитком науки і технологій. Основним завданням правової регламентації відносин у цій сфері є забезпечення ефективного захисту прав інтелектуальної власності.

В Україні правовідносини, пов'язані з авторським правом і суміжними правами, регламентуються Конституцією України, кодексами, законами, підзаконними нормативно-правовими актами, а також міжнародними договорами України.

Конституція України, прийнята 28.06.1996 року № 254К/96-ВР (Відомості Верховної Ради. — 1996. — № 30. — Ст. 141) як Основний Закон України закріплює право кожного володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності (ст. 41), а також гарантує свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності і забороняє використовувати або поширювати результати інтелектуальної, творчої діяльності без згоди правовласника, за винятком випадків, встановлених законом (ст. 54) [7].

Правове регулювання й охорона інтелектуальної і творчої діяльності, її результатів здійснюється також згідно з Книгою четвертою Цивільного кодексу України (далі — ЦК України, прийнятий 16.01.2003 року № 435-IV (Відомості Верховної Ради. — 2003. — № 40–44. — Ст. 356), що регламентує загальні засади авторського права і суміжних прав. Зокрема, закріплюються переліки об'єктів і суб'єктів як авторського права, так і права інтелектуальної власності в цілому, підстави виникнення (набуття) права на об'єкти інтелектуальної власності, положення про особисті немайнові і майнові права, строк чинності прав інтелектуальної власності, загальні положення про використання об'єкта права інтелектуальної власності, передання майнових прав інтелектуальної власності і здійснення права інтелектуальної власності, яке належить кільком особам, загальні положення про права інтелектуальної власності на службові твори й об'єкти, створені за замовленням, наслідки порушення права інтелектуальної власності і захист права інтелектуальної власності.

Глави 36 і 37 ЦК України присвячені авторському праву і суміжним правам. Серед майнових прав інтелектуальної власності на твір ЦК України (ст. 440) визначає право на використання твору, виключне право дозволяти використання твору, право перешкоджати неправомірному використанню твору, в тому числі забороняти таке використання. Під використанням твору в ЦК України (ст. 441) мають на увазі такі дії, як: опублікування, відтворення будь-яким способом та у будь-якій формі, переклад, переробка, адаптація, аран-

жування та інші подібні зміни, включення складовою частиною до збірників, баз даних, антологій, енциклопедій тощо, публічне виконання, продаж, передання в найм (оренду) тощо, імпорт примірників твору, примірників його перекладів, переробок тощо. Усі ці дії так чи інакше пов'язані з поширенням творів. У свою чергу ЦК України (ст. 445) передбачає право автора на плату за використання його твору. Крім того, використанням виконання вважають, зокрема, такі дії, як продаж та інше відчуження оригіналу чи примірника запису виконання і забезпечення засобами зв'язку можливості доступу будь-якої особи до записаного виконання з місця та в час, обраних нею (ст. 453). Таким чином, ЦК України побічно регламентує поширення аудіо- й відеоконтенту за допомогою Internet і он-лайн ТБ, радіо [8].

Центральне місце серед нормативно-правових актів, що регламентують поширення відео- й аудіоконтенту, посідає Закон України «Про авторське право і суміжні права» (далі — Закон). Цінність цього Закону, який у цілому відповідає міжнародним стандартам, полягає в прямій дії його норм і ринковій спрямованості. Закон визначає розповсюдження об'єктів авторського права і (або) суміжних прав як будь-яку дію, за допомогою якої об'єкти авторського права і (або) суміжних прав безпосередньо чи опосередковано пропонуються публіці, у тому числі доведення цих об'єктів до відома публіки таким чином, що її представники можуть здійснити доступ до цих об'єктів з будь-якого місця і в будь-який час за власним вибором (ст. 1). Серед майнових прав автора Закон, зокрема, називає розповсюдження творів шляхом першого продажу, відчуження іншим способом або шляхом здавання в майновий найм чи в прокат та шляхом іншої передачі до першого продажу примірників твору, подання своїх творів до загального відома публіки таким чином, що її представники можуть здійснити доступ до творів з будь-якого місця і у будь-який час за їх власним вибором, здавання в майновий найм і (або) комерційний прокат після першого продажу, відчуження іншим способом оригіналу або примірників аудіовізуальних творів, а також творів, зафіксованих у фонограмі чи відеограмі або у формі, яку зчитує комп'ютер (ст. 15) [9].

Окрім правових засобів слід використовувати й технічні засоби захисту авторського права і суміжних прав з урахуванням положень Закону, який визначає поняття технічних засобів захисту як технічних пристроїв і (або) технологічних розробок, призначених для створення технологічної перешкоди порушенню авторського права і (або) суміжних прав при сприйнятті і (або) копіюванні захищених (закодованих) записів у фонограмах (відеограмах) і передачах організацій мовлення чи для контролю доступу до використання об'єктів авторського права і суміжних прав (ст. 1); порушенням авторського права і (або) суміжних прав, що дає підстави для судового захисту, є, зокрема, будь-які дії для свідомого обходу технічних засобів захисту авторського права і (або) суміжних прав, зокрема виготовлення, розповсюдження, ввезення з метою розповсюдження і застосування засобів для такого обходу (ст. 50).

На розвиток законодавства України про авторське право, спрямований Закон України «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» від 23.03.2000 року № 1587-III в редакції від 10.07.2003 року № 1098-IV (Відомості Верховної Ради. — 2004. — № 7. — Ст. 46), що захищає права й інтереси осіб, які займаються поширенням примірників аудіовізуальних творів і фонограм, і регламентує їх відносини зі споживачами. У цьому Законі наводиться визначення розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних як їх введення в обіг шляхом їх продажу чи іншої передачі права власності (ст. 2). Проте цей Закон не регулює поширення аудіо- й відеоконтенту через Internet, оскільки передбачає супроводження процесу розповсюдження творів маркуванням творів контрольними марками [10].

Окрім перерахованих нормативно-правових актів, питанням регулювання відносин інтелектуальної власності присвячений ряд інших законів і прийнятих на їх основі підзаконних нормативно-правових актів: окремі статті нормативно-правових актів, що встановлюють адміністративну і кримінальну відповідальність, зокрема ст. 176 Кримінального кодексу України, прийнятий 05.04.2001 року № 2341-III (Відомості Верховної Ради. — 2001. — № 25–26. — Ст. 131)

і ст. $51^2$ Кодексу України про адміністративні правопорушення, прийнятий 07.12.1984 року № 8073-X (Відомості Верховної Ради УРСР. — 1984. — № 51. — Ст. 1122); міжнародні договори України у сфері авторського права і суміжних прав, зокрема Всесвітня конвенція про авторське право, прийнята у Женеві 06.09.1952 року (ОВУ. — 2006. — № 46. — Ст. 3104), Договір Всесвітньої організації інтелектуальної власності (ВОІВ) про авторське право, прийнятий у Женеві 20.12.1996 року (Бюлетень законодавства і юридичної практики України. — 2003. — № 3. — Ст. 136) і Договір ВОІВ про виконання і фонограми, прийнятий 20.12.1996 року (Бюлетень законодавства і юридичної практики України. — 2003. — № 3. — Ст. 174). Також частиною національного законодавства стали Міжнародна конвенція про охорону інтересів виконавців, виробників фонограм і організацій мовлення, прийнята у Римі 26.10.1961 року (Бюлетень законодавства і юридичної практики України. — 2003. — № 3. — Ст. 161 або Юридичний вісник України. — 2008. — № 13. — С. 2), Конвенція про охорону інтересів виробників фонограм від незаконного відтворення їхніх фонограм, прийнята 29.10.1971 року (Бюлетень законодавства і юридичної практики України. — 2003. — № 3. — Ст. 171 або Юридичний вісник України. — 2008. — № 13. — Ст. 9) [4].

Право на об'єкти інтелектуальної власності регулюється також договорами, які укладаються між особою, що володіє виключними правами, і користувачем інтелектуального продукту (авторський, ліцензійний договір) [11].

Слід зазначити, що на території України практика боротьби з порушеннями прав інтелектуальної власності в Internet зараз дуже незначна і досить часто обмежується вимогами до правопорушників припинити незаконне використання контенту без звернення до судів і правоохоронних органів. Для вирішення проблеми необхідно встановити розумний баланс між нормативно-правовою базою та інструментами саморегуляції в мережі. Практика цивілізованих країн показує, що механізми самоконтролю є досить дієвими і викликають довіру до тих, хто їх створює (наприклад, британська система саморегулювання Internet «Internet-вотч»). Можна констатувати, що нормативно-правова база істотно відстає від суспільних відносин, що

призводить до неврегульованості цієї сфери нормами законів, застосуванню в основному корпоративних норм або навіть відсутності будь-якого регулювання. Тому на цьому етапі перед фахівцями і законодавцями стоїть завдання адаптувати нормативно-правову базу для забезпечення правового регулювання та захисту виняткових прав у мережі Internet. Крім того, необхідне оновлення механізмів реалізації виключних прав і підвищення підготовки суддів у сфері інформаційних технологій.

*Обмеження використання DRM.* Головними недоліками самої концепції DRM є неминуче обмеження можливостей використання і пов'язане з цим обмеження на розголошування інформації. Додаткові обмеження, що накладаються в першу чергу на чесних споживачів аудіовізуальної продукції або пристроїв, які здійснюють запис або відтворення інформації і підтримують технології захисту авторських прав, є, на думку експертів, серйозною вадою. Самі принципи DRM і багато їх реалізацій можуть суперечити законодавству деяких країн [12]. Істотною проблемою є ще і те, що більшість систем DRM не сумісні: наприклад, музику, куплену за допомогою Apple iTunes і захищену DRM, неможливо прослуховувати на яких-небудь інших плеєрах, окрім iPod. Також часто системи DRM для персональних комп'ютерів використовують методи захисту від злому, що роблять роботу системи користувача нестабільною і становлять загрозу її безпеці.

Деякі з найбільш ефективних DRM вимагають для використання захищеної копії постійне мережне з'єднання з контролюючою системою. Коли підтримка системи контролюючою особою припиняється, захищені копії стають непрацюючими. Деякі компанії перед відключенням пропонують клієнтам компенсацію або копії в незахищеному форматі. Наприклад, у квітні 2008 року Microsoft вирішила закрити до кінця серпня MSN Music Store, що більше не діяв, і відключити сервери, необхідні для отримання ключів до раніше куплених в цьому магазині музичних творів, після чого користувачі не змогли б відтворювати їх після заміни комп'ютера. Проте після численних скарг користувачів Microsoft продовжила термін роботи серверів до 2011 року.

Існують цілі суспільні рухи, які пропагують відмову від використання технологій DRM і ставлять своєю метою попередження неінформованих про такі недоліки споживачів від придбання подібної продукції. Найбільш відомими є кампанія Defective by Design, запущена Free Software Foundation проти DRM, а також організація Electronic Frontier Foundation, однією з цілей роботи якої також є протидія DRM. У GNU GPL версії 3 прямо вказано, що твір, у якому використовується ця ліцензія, не повинен бути частиною DRM, а також вимагає не забороняти обхід DRM при передачі твору.

## 5.2. Стеганографічні методи захисту авторських прав аудіоданих

Основним напрямом застосування комп'ютерної стеганографії для захисту від копіювання та несанкціонованого використання аудіоданих [13; 14; 15] є використання надмірності аудіо- й візуальної інформації. Цифровий звук — це матриця чисел, у якій закодована інтенсивність звукового сигналу в послідовні моменти часу. Всі ці числа не точні, оскільки не точні пристрої оцифрування аналогових сигналів, є шуми квантування. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку і візуального образу. Їх заповнення відчутно не впливає на якість сприйняття, що і дає можливість для переховування додаткової інформації.

Наприклад, тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 біт у стереорежимі дозволяє приховати за рахунок заміни найменш значущих молодших розрядів на приховане повідомлення розміром близько 10 Кбайт інформації. При цьому зміна значень відліків складає менше 1 %. Така зміна практично не виявляється при прослуховуванні файла більшістю людей [16].

Вбудовування повідомлення в цифровий контейнер (зображення або аудіофайл) може проводитися за допомогою ключа, одного або декількох. Ключ — псевдовипадкова послідовність (ПВП) біт, поро-

джувана генератором, що задовольняє певним вимогам (криптографічний безпечний генератор). Як основа для роботи генератора може використовуватися, наприклад, лінійний рекурентний регістр. Тоді адресатам для забезпечення зв'язку може повідомлятися початкове заповнення цього регістра. Числа, що породжуються генератором ПВП, можуть визначати позиції відліків, що модифікуються, у разі фіксованого контейнера або інтервали між ними в разі потокового контейнера.

Таким чином, для захисту авторських прав на аудіофайли використовується впровадження в них прихованих об'єктів — цифрових водяних знаків (ЦВЗ), що досягається шляхом непомітного для людського ока або вуха зміни файлу.

Популярність мультимедіа-технологій викликала безліч досліджень, пов'язаних з розробкою алгоритмів ЦВЗ для використання в стандартах MIDI MPEG, JPEG, захисту DVD-дисків від копіювання [16; 17; 18].

*Методи і програми стеганографії.* Всі алгоритми вбудовування прихованої інформації можна поділити на кілька підгруп [19; 20; 21]:

– ті, що працюють із самим цифровим сигналом. Наприклад, метод найменш значущих бітів (Least Significant Bit, LSB) [22];

– «впаювання» прихованої інформації. У цьому випадку відбувається накладення прихованого зображення (звуку, іноді тексту) поверх оригіналу. Часто використовується для вбудовування ЦВЗ [23];

– використання особливостей форматів файлів. Сюди можна віднести запис інформації в метадані або в різні інші зарезервовані поля файла, які не використовуються.

У програмних реалізаціях застосовуються алгоритми, що використовують надмірність аудіовізуальної інформації. Друга назва цього методу — метод молодших бітів. Основними контейнерами в цьому способі приховування є формати так званого прямого кодування, наприклад, .bmp для графіки, або .wav для звуку. Цей напрямок — найпопулярніший серед розробників. Сучасні програми навчилися поводитися з форматами, які підтримують стиснення; для найпопулярніших розробок з'явилися дешифрувальники.

Відомо, що цифрові зображення є матрицею пікселів. Піксель є одиничним елементом зображення і має фіксовану розрядність двійкового представлення. Пікселі напівтонового зображення кодуються 8 бітами, і значення яскравості змінюються від 0 до 255.

Зараз найбільш поширеним, але найменш стійким є метод заміни молодших значущих бітів (LSB). Молодший значущий біт зображення несе в собі найменше інформації, і людина зазвичай не здатна помітити зміну в цьому біті.

Тому його можна використовувати для вбудовування інформації, і, наприклад, для напівтонового зображення обсяг вбудованих даних може становити 1/8 обсягу контейнера. У зображення розміром 512×512 пікселів можна вбудувати 32 кілобайта інформації.

Незважаючи на переваги цього методу, які полягають в його простоті й порівняно великому обсязі вбудованих даних, він має серйозні недоліки. По-перше, зловмисникові точно відомо, де знаходиться місце розташування всього повідомлення, і отже, не забезпечена секретність вбудовування інформації. По-друге, приховане повідомлення легко пошкодити, оскільки система людського зору не помітить зміни в цих бітах.

Для подолання зазначених недоліків пропонується вбудовувати таємні повідомлення не в усі пікселі зображення, а лише до деяких з них, що визначаються за псевдовипадковим законом відповідно до ключа, відомим законному користувачеві. Однак при цьому зменшується пропускна здатність стегосистеми.

Інший популярний метод вбудовування повідомлень пов'язаний з урахуванням особливостей форматів даних, що використовують стиснення з втратою даних, наприклад JPEG, MPEG [24]. На відміну від методу LSB, цей метод більш стійкий до геометричних перетворень і виявлення каналу передачі, тому що є можливість в широкому діапазоні варіювати якість стиснутого зображення, що не дозволяє визначити походження стиснення. Однак стенографічні методи впровадження інформації у відео, стискуються за стандартом MPEG, працюють у реальному часі і тому повинні бути сліпими і мати малу обчислювальну складність.

Крім цього, операція з упровадження повідомлення не повинна збільшувати розмір стислих відеоданих, оскільки можуть виникнути проблеми при передачі потокового відео по каналу фіксованої швидкості.

## 5.3. Огляд програм, які використовують методи стеганографії S-Tools

Один із поширених стеганографічних програмних продуктів у цій області для платформи Windows — це S-Tools (статус freeware). Програма S-Tools приховує інформацію у графічних файлах форматів .bmp і .gif, а також у звукових файлах формату .wav. Зовні робота з програмою виглядає так. Після розпакування архіву запускаємо файл S-tools.exe, потім Windows Explorer (Провідник). Він знадобиться, тому що S-tools використовує технологію drag and drop, відповідно вікна не повинні повністю перекриватися.

Перетягуємо за допомогою миші файл у вікно програми S-Tools, він відображається у вікні або як є (для картинки), або у вигляді лінії, яка зображує рівні сигналу (для звуку). У правому нижньому кутку вікна S-Tools з'явиться інформація про розмір даних, які можна заховати в цьому файлі.

Потім перетягуємо у вікно з картинкою або рівнем сигналу будь-який файл, призначений для приховання, розміром не більше зазначеного файла. Після перевірки розміру даних програма запросить пароль, набравши який можна буде відновити інформацію. Потім почнеться приховування, його час залежить від розміру даних (спостерігати за процесом можна у вікні Action). Коли все буде зроблено, з'явиться вікно Hidden data. Зберегти результат можна, клацнувши у вікні правою кнопкою миші і вибравши пункт «Save as ...», ввівши ім'я файла і натиснувши ОК. Для відновлення послання необхідно перетягнути картинку або звук у вікно S-Tools, клацнути на зображенні правою кнопкою і вибрати пункт «Reveal ...». Після введення пароля, якщо приховані дані є, почнеться їх відновлення, за процесом якого можна спостерігати у вікні Action Steganos for Win, якщо даних немає, то нічого не відбудеться.

*Steganos for Win.* Інша поширена стеганографічна програма — Steganos for Win, яка є простою у використанні, але все ж потужною програмою для шифрування файлів і приховування їх усередині файлів .bmp, .dib, .voc, .wav, .assii і .html. Вона має практично ті ж можливості, що й S-Tools, але використовує інший криптографічний алгоритм (hwy1) і, крім того, здатна приховувати дані не лише у файлах формату .bmp, .wav, а й у звичайних текстових і .html-файлах, причому дуже оригінальним способом — у кінці кожного рядка додається певна кількість пропусків. З новими властивостями і додатковими можливостями Steganos for Win є серйозним конкурентом на ринку інформаційної безпеки.

*Masker 7.0.* Програма Masker 7.0 дозволяє приховувати повідомлення серед виконуваних, відео- й аудіофайлів, а також у зображеннях, причому підтримується величезне число форматів, серед яких є як формати прямого кодування, так і ті, що стискають (.jpeg, .mp3, .mpeg). Щоб почати працювати, потрібно або на панелі, або в меню вибрати пункт «Open Carrier File» і у вікні вказати файл-контейнер.

Після цього, залежно від ваших цілей, потрібно у наступному вікні перейти або на вкладку «Open Hideout», де можна отримати вже прихований файл, вказавши пароль, або на «Create New Hideout», де можна вказати пароль і алгоритм шифрування для нової порції приховуваних даних. Шифрування — один із основних елементів програми: підтримує сім алгоритмів, серед яких є BLOWFISH і TripleDES.

Після зазначення всіх параметрів в основній частині вікна будуть відображатися приховані файли. Щоб додати туди файли, потрібно натиснути правою кнопкою і вибрати «Hide / Add Files». З'явиться вікно, у якому потрібно буде вибрати ці файли, а потім і вказати параметри їх збереження. Наприклад, можна додати цілу папку, зберігши її структуру, або дати файлу-контейнера статус «read-only», щоб зберегти приховані файли більш надійно.

Витягнення файлів не викличе складнощів — при відкритті файла-контейнера потрібно зайти на потрібну вкладку, вказати пароль і з'явиться список прихованих файлів.

*Приклад використання програми Masker 7.0.* Послідовність роботи:

1. Запускаємо програму.

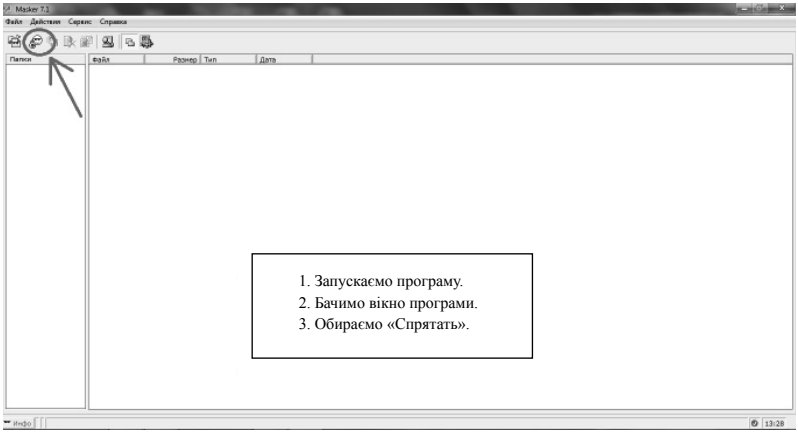



*Рис. 5.1.* Головне вікно програми

2. Обираємо команду «***Спрятать***».

3. У діалоговому вікні, що відкрилося, необхідно обрати файл, у якому буде зберігатися наша прихована інформація.

4. Вибираємо аудіофайл, до якого треба додати авторські права.

5. Вводимо пароль, за допомогою якого ми зможемо розшифрувати файл, а також алгоритм шифрування. Краще обрати стандартний.

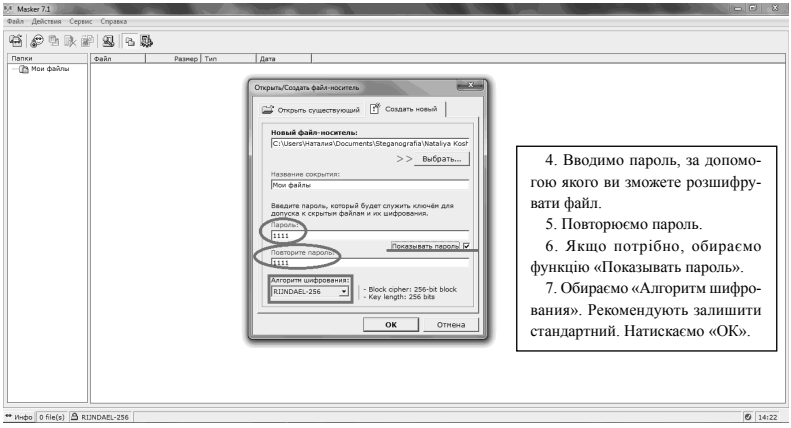



*Рис. 5.2.* Вибір пароля та алгоритму шифрування

6. Виділяємо текстовий файл, у якому зберігається інформація про авторські права. Обираємо потрібні налаштування.

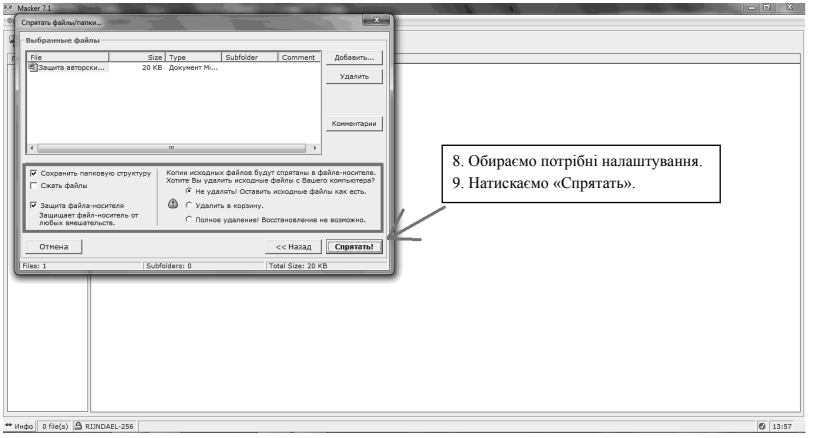



*Рис. 5.3.* Вибір налаштування текстового файла, у якому зберігаються записи про авторські права

7. Для перегляду інформації про авторське право необхідно запустити програму Masker 7.0, відкрити файл-носій, ввести пароль і відкрити прихований файл за допомогою поєднання клавішної комбінації CTRL+V.

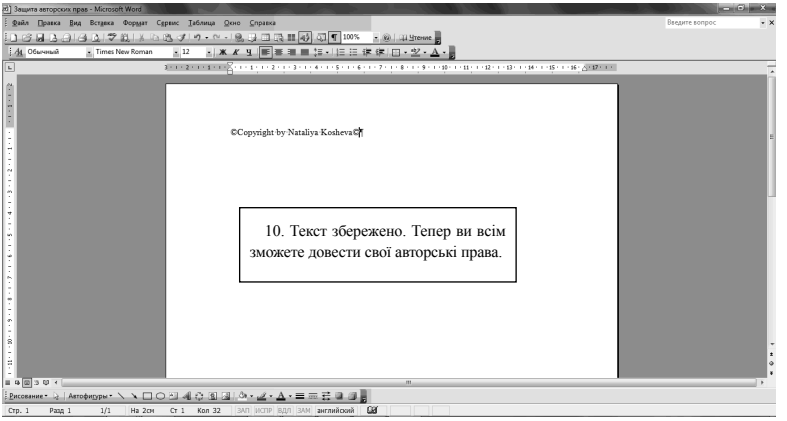



*Рис. 5.4.* Перегляд інформації про авторське право у прихованому файлі

*Steganos Security Suite 2007.* Найбільш відомим пакетом для захисту інформації, вже назва якого вказує на стеганографічний «вміст», є Steganos Security Suite 2007. Як уже було зазначено, це саме пакет — при запуску з'являється вікно для вибору конкретного додатка. Розглянемо розділ «File Manager», за допомогою якого можна приховувати файли. На головній панелі спочатку активні дві кнопки, перша з яких приховує файли, а друга витягує.

Після вибору пункту «New encrypted file» основна частина вікна — файловий менеджер — стане активною, туди потрібно буде додавати файли, які потрібно заховати. Коли всі файли додано, натискання на кнопку «Close» на тій же панелі запустить «Майстра збереження».

Спочатку потрібно буде вибрати, що ми хочемо зробити: просто зашифрувати або зашифрувати і сховати. Внаслідок того, що ми розглядаємо програму як засіб стеганографії, вибираємо другий пункт. З'явиться вікно, де потрібно буде вибрати, чи хочемо ми дати програмі можливість самостійного знаходження файла-контейнера (буде обраний перший-ліпший файл, відповідний за типом і розміром), або вкажемо його самі.

Програма підтримує три формати: .bmp, .jpeg і .wav. Після цього потрібно буде лише вказати пароль — файл надійно схований.

*MSU StegoVideo.* Наприкінці хотілося б розповісти про дуже цікавий і незвичайний продукт. Йдеться про програму MSU StegoVideo, написану студентами МДУ. Вона, як зрозуміло з назви, призначена для приховування повідомлень у відеофайлах, причому це може бути тільки текстова інформація. Але вона має один великий плюс: на відміну від конкурентів, тут інформація зберігається при стисненні популярними кодеками, наприклад, DivX. Коли інші програми упаковують файли і шифрують різними алгоритмами, єдиного зміненого біта може бути достатньо для втрати всього змісту. MSU StegoVideo, звичайно, не може зберегти весь переданий їй текст, але за певних умов втрати можуть не перевищувати 20 %, що цілком прийнятно для літературної мови — зміст повідомлення збережеться. Процес упаковки секретного повідомлення в цілому звичний: потрібно вказати вихідний відеофайл, текстовий файл з повідомленням, пароль і місце, куди зберігати заповнений контейнер.

Але, крім звичайних кроків, на одному з етапів потрібно вказати значення такого параметра, як «Data Redundancy» («Надмірність даних»). Чим більше значення ви вкажете, тим менше інформації ви зможете вмістити, але тим вищою буде її стійкість при стисненні.

Особливість цієї програми — збереження більшої частини інформації при стисненні відео — робить можливим її застосування в області цифрових водяних знаків. Так стеганографія використовується для збереження інформації про власника прав на інтелектуальну власність.

*ImageSpyer.* ImageSpyer Олександра М'ясникова — безкоштовна вітчизняна розробка, відома також як плагін StegoTC для програми «Total Commader». Реалізується варіант алгоритму LSB з можливістю установки довільного порядку біт у поєднанні із 40-симетричними криптографічними алгоритмами.

*DarkCryptTC.* DarkCryptTC безкоштовний плагін для Total Commander з графічною оболонкою DarkCrypt GUI є продовженням розробок ImageSpyer і StegoTC і реалізує алгоритм LSB (від 3 до 12 біт на піксель), використовуючи як контейнер для зашифрованих архівів зображення .png, .bmp, .tiff, .psd, .tga, .mga, аудіофайли .wav, текстові .xml і .html файли (алгоритм заміни символів).

## 5.4. Обмеження стеганографічних методів

Ітенсивні дослідження в галузі стеганографії ведуться в більшості провідних ВНЗ і науково-дослідних інститутів, а також у приватних і державних компаніях протягом останніх 20-ти років. За весь час дослідницької діяльності на основі обробки значної кількості звукових, графічних, текстових та інших файлів вдалося створити широку базу стеганографічних ознак і типів [25]. Зокрема, застосовуючи технологію контрольної суми даних, на перших етапах перевірки інформації вдається відсіяти велику кількість «порожніх» файлів.

Існують сайти, де міститься база даних файлів операційних систем і великої кількості відомого програмного забезпечення. Більшість програм стегоаналізу здатні самостійно довантажувати інформацію із сайтів, швидко відсіюючи непотрібні дані.

Існують тисячі способів включити повідомлення, звук або зображення в інший файл і пара десятків методів виявити таємну інформацію [26]. Співвідношення, на перший погляд, гнітюче. Однак, наприклад, прості некомерційні (freeware) програми для стеганографії використовують такий підхід приховування інформації (найчастіше у графічних файлах), який досить легко виявити. Навіть використання досить прогресивного методу LSB не дає успіху.

Прості методи дестеганографії полягають у такому: для початку потрібно знайти всі місця можливих закладок чужорідної інформації, які допускає формат файла-контейнера. Далі потрібно отримати дані з цих місць і проаналізувати їх властивості на відповідність стандартним значенням. Для вирішення першого завдання досить уважно вивчити специфікації використовуваних форматів файлів, а друге — зазвичай вирішується методами статистичного аналізу. Наприклад, якщо необхідно сховати якийсь текстовий фрагмент, то таке послання буде містити тільки символьну інформацію: 52 знака латиниці, 66 знаків кирилиці, знаки пунктуації та деякі службові символи. Статистичні характеристики такого повідомлення будуть різко відрізнятися від характеристик випадкової послідовності байтів, яку повинні нагадувати молодші біти RGB-картинки, зібрані разом (для методу LSB).

Крім того, важливим недоліком ЦВЗ є те, що його легко видалити із завіреного ним повідомлення, після чого приробити до нього новий підпис. Видалення підпису дозволить порушникові відмовитися від авторства, або ввести в оману законного одержувача щодо авторства повідомлення.

Проте завжди треба враховувати той факт, що людський розум безмежний, людина може сховати інформацію елементарним чином в дуже важкодоступне місце і дослідження в цьому напрямку тривають.

## 5.5. Висновки

Виходячи з аналізу літератури, можна зробити такі висновки. Стеганографія — поки ще відносно нове і незвичайне явище у сфері захисту інформації. Однак її технології сучасні і затребувані. Поряд з рядовим користувачем у ній зацікавлені і великі компанії, що працюють у сфері мультимедіа, які прагнуть захистити свій контент від незаконного використання. Якщо ще кілька років тому більшість програм користувалися однаковими алгоритмами, а їхній інтерфейс був надзвичайно складний, то сучасні програми забезпечують відповідний рівень зручності у використанні. Стеганографія зараз уже може успішно використовуватися для захисту цінної інформації.

Аналіз тенденцій розвитку комп'ютерної стеганографії показує, що в найближчі роки інтерес до розвитку її методів буде посилюватися все більше і більше [25]. Передумови до цього вже сформувалися. По-перше, загальновідомо, що актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З другого боку, бурхливий розвиток інформаційних технологій забезпечує можливість реалізації нових методів захисту. І, звичайно, сильним каталізатором цього процесу є лавиноподібний розвиток Internet, в тому числі такі невирішені суперечливі проблеми Internet, як захист авторського права, захист прав на особисту таємницю, організація електронної торгівлі, комп'ютерна злочинність і кібертероризм.

# РОЗДІЛ 6

# ЛІНГВІСТИЧНА БЕЗПЕКА ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Розповсюдження електронних видань у мережі Internet (зокрема, у вигляді гіпертексту) привели до різкого збільшення порушень прав правовласників і авторських прав, що пов'язане з появою безлічі приватних видавництв, засобів масової інформації і т. д. Літературні і наукові твори, авторські роботи без належного дозволу неправомірно копіюються, запозичуються, іноді злегка редагуються і перевидаються під іншим ім'ям. У цих умовах знання форм, засобів і способів виявлення плагіату або незаконного привласнення авторства, неправомірного запозичення всього твору або його частини (наприклад, оригінальної назви) за допомогою лінгвістики має особливу актуальність [1]. Із розвитком комп'ютерних технологій запозичувати тексти стало простіше і запозичувати їх почали частіше.

Найпростіший випадок — Copy-Paste, пряме копіювання. Звичайно вирішення питання про наявність такого копіювання не вимагає втручання експертів, оскільки відповідь на нього зрозуміла і без спеціальних знань.

*Авторознавча експертиза* — це дослідження тексту (найчастіше — друкарського) з метою встановлення авторства (атрибуція твору) або отримання яких-небудь відомостей про автора й умови створення текстового документа.

Авторознавча експертиза необхідна, якщо запозичений текст піддався глибокому редагуванню або був оброблений спеціальними комп'ютерними програмами для маскування запозичення (синонімайзерами, систематично замінюючими слова в тексті на синоніми) або запозичений з декількох джерел.

Не менш важливе дотримання техніки лінгвістичної безпеки при складанні текстів офіційних документів, тобто документів державних і недержавних органів і посадових осіб, які встановлюють наявність

або відсутність якого-небудь факту. Щодо економічних спорів господарчих суб'єктів, осіб, що займаються підприємницькою діяльністю, то неправильне складання тексту договору призводить до його неоднозначного прочитання, а також породжує документаційні спори і розгляди в третейських або арбітражних судах.

Тому здійснення лінгвістичної експертизи творів словесної творчості, які залучаються до документаційних та інформаційних суперечок, що є предметом судових розглядів не лише у цивільних й арбітражних, але і кримінальних справах, справах по адміністративних правопорушеннях, сьогодні стає життєво важливим для забезпечення лінгвістичної безпеки суспільства в цілому.

Цей розділ присвячений одному з найбільш актуальних видів лінгвістичних експертиз — авторознавчій експертизі й атрибуції тексту (співвідношення тексту відповідних йому атрибутів, до яких належать не тільки ім'я автора, але також жанр, час і місце створення тексту).

## 6.1. Види авторознавчої експертизи

Завдання авторознавчої експертизи поділяють на дві групи:

*1. Ідентифікаційні* (перевірка авторства):

– підтвердження авторства певної особи;

– виключення авторства певної особи;

– перевірка того, що автором усього тексту була одна й та ж людина;

– перевірка того, що виконавець тексту є одночасно його автором.

Ідентифікаційні завдання авторознавчої експертизи вирішуються в тих випадках, коли потрібно підтвердити або спростувати авторство певної особи (осіб) щодо того або іншого тексту, причому передбачуваний автор тексту відомий і безпосередньо доступний. У таких випадках експертиза полягає в порівнянні тексту, що перевіряється, з текстами, беззаперечним автором яких є персона, яка перевіряється [2].

*2. Діагностичні* — визначення особистих характеристик автора, таких як:

– освітній рівень;

– рідна мова, знання іноземних мов;

– походження, місце постійного мешкання;

– сфера діяльності, професія, хобі;

– стать, вік, соціальний стан, національність та інші соціальні характеристики;

– наявність навичок певного стилю писемної мови;

– визначення факту свідомого спотворення писемної мови.

Діагностичні завдання експертиза вирішує в тих випадках, коли необхідно встановити невідомого автора тексту, що є в наявності, наприклад, визначити автора анонімного листа або підробленого документа. У цих випадках порівняти досліджуваний текст з текстами автора, як правило, неможливо, і експертиза полягає у виявленні на підставі тексту особистих характеристик автора, знання яких дозволить обмежити коло осіб, які підлягають перевірці вже іншими методами. Після визначення підозрюваного автора можливе вирішення вже ідентифікаційного завдання — підтвердження або спростування авторства. Вирішуються і більш специфічні завдання, такі як визначення психічного стану автора в момент створення тексту, виявлення факту написання тексту в незвичайних умовах, розпізнання текстів, написаних під диктування іншої людини [2].

На практиці ідентифікаційна і діагностична установки нерідко об'єднуються в рамках єдиного комплексного дослідження.

## 6.2. Методи авторознавчої експертизи

Сьогодні експерти, лінгвісти-авторознавці використовують власні методики проведення авторознавчих експертиз, засновані на основних постулатах проведення судової експертизи. Офіційна методика проведення авторознавчої експертизи як така відсутня. У цілому авторознавча експертиза базується на уявленні, що кожній людині притаманний унікальний комплекс особливостей мовної поведінки, який може бути пізнаний і використаний для ідентифікації і діагностики. Вся сукупність методів експертизи спрямована на виділення цих особливостей, їх опис і порівняння.

Типові випадки авторознавчих експертиз описуються такими ситуаціями [1]:

1. Множинна невизначеність.

Існує безліч текстів або фрагментів. Необхідно встановити, скільки авторів їх писали і як розподілений авторський внесок по кожному конкретному тексту.

2. Порівняння за зразком.

Існує приклад тексту (текстів) певного автора X. Необхідно встановити, чи є він також автором деякого іншого тексту (текстів).

3. Конкуренція зразків.

Існують зразки текстів авторів X, Y, Z. Необхідно встановити, хто з них є автором текстів $X_1$, $X_2$, …$X_n$ [2; 3].

Методика діагностичної та ідентифікаційної судово-авторознавчої експертизи базується на комплексному використанні методів дослідження писемної мови, до яких належать:

1. Лінгвістичні методи (зокрема лінгвостатистичні методи, пов'язані зі з'ясуванням лінгвістичної природи встановлюваних у процесі дослідження мовних елементів, структур, явищ).

2. Психолінгвістичні, які припускають аналіз названих мовних факторів у плані їх обумовленості особливостями процесу породження мови.

3. Соціолінгвістичні, пов'язані з виявленням обумовленості мови тими або іншими соціальними параметрами досліджуваної ситуації писемного спілкування.

4. Соціолінгвістичні, пов'язані з аналізом обумовленості мови власне психологічними факторами досліджуваної ситуації діяльності і спілкування.

5. Логіко-психологічні, спрямовані на аналіз логічних елементів і структур тексту в плані встановлення властивостей дискурсивного мислення його авторів [4].

Названі методи — необхідні компоненти методики судово-авторознавчої ідентифікації і діагностики. Кожен автор володіє індивідуальними особливостями писемної мови, стилістичними, лексичними, граматичними навичками. Це може виражатися в наявності слів, що повторюються, неправильному вживанні фразеологізмів, присутності в тексті діалектизмів, професіоналізмів, наявності однотипних орфографічних і пунктуаційних помилок тощо. У писемній мові вирізняють загальні й окремі мовні навички.

До загальних мовних належать навички:

– стилістичні;
– синтаксичні;
– лексико-фразеологічні;
– орфографічні;
– пунктуаційні.

До окремих ознак писемної мови належать стійкі порушення мови, індивідуальні лексичні, граматичні навички, властиві конкретному виконавцеві.

Серед основних ознак, що вказують на автора тексту, зазвичай вирізняють такі.

*Семантичні ознаки* — тема документа, лейтмотив (основна думка), фактичні дані в документі (професійні знання, знання людей, місць, подій), архітектоніка (загальна побудова документа, наявність вступу, розділів, висновку, логічного зв'язку між окремими елементами документа).

*Стиль викладу* — офіційно-діловий, науковий, публіцистичний, літературно-художній, розмовний.

*Ознаки фразеологізмів* — використання вигуків, питальних і окличних речень, крилатих висловів тощо.

*Лексичні ознаки* — використання автором загальновживаних слів, і слів обмеженого вживання, властивих певній групі осіб. Лексичні ознаки — це використання:

– архаїзмів — застарілих або таких, що вийшли з ужитку слів;
– неологізмів — нових слів, що з'явилися в мові для позначення нових понять;
– професіоналізмів — професійних слів і виразів;
– діалектизмів — слів і оборотів, властивих для тих, що проживають у певній місцевості;
– варваризмів — слів, запозичених з інших мов, не властивих для мови, на якій написаний документ;
– жаргонізмів — слів і виразів, характерних для певної групи людей (злочинний жаргон, молодіжний жаргон);
– вульгаризмів — слів, зворотів мови, які не вживаються в літературній мові;
– слів-паразитів, звичних, скорочених слів, використання зменшувальних слів тощо.

*Граматичні ознаки* — дотримання правил використовуваної мови, узгодженість слів у відмінках, написання складних слів.

*Топографічні ознаки* розміщення тексту на сторінці:

– поля — розмір, конфігурація (звуження, розширення);
– абзаци — наявність, частота, спосіб виділення;
– рядки — проміжок між рядками;
– перенесення слів;
– розташування (наявність) підпису, дати.

Дослідження тексту на пунктуаційному й орфографічному рівні може характеризувати загальний рівень писемності автора, в деяких випадках — визначити, що текст написаний автором на нерідній мові, але так можуть досліджуватися лише тексти, які не піддавалися професійному редагуванню і були виконані безпосередньо автором. Відредаговані тексти своїми пунктуаційними й орфографічними особливостями характеризують вже не автора, а виконавця або редактора.

Синтаксичний, лексико-фразеологічний і стилістичний рівні, навпаки, не спотворюються при дрібному редагуванні. Вони утворюють у сукупності те, що зазвичай і називається «стилем автора». Саме їх аналіз становить найбільший інтерес і найбільшу складність [5]. Існує багато методів аналізу стилю. У цілому можна поділити їх на дві великі групи.

*Експертні методи* — припускають дослідження тексту професійним лінгвістом-експертом, який виокремить характерні особливості тексту, що перевіряється, текстів, написаних імовірним автором, якщо вони доступні, і на підставі їх вивчення зробить висновок.

*Формальні методи* — засновані на порівнянні обчислюваних характеристиках текстів.

## 6.3. Формальні методи авторознавчої експертизи

Теоретичною підставою для використання формальних характеристик з метою атрибуції є стохастична (імовірнісна) модель породження мовного вислову.

Із зростанням обсягу (довжини) тексту частота того або іншого мовного елементу стабілізується. І тоді ті частотні показники, які ха-

рактеризують організацію мовних елементів у цього індивіда, зрештою можуть бути виявлені. Зараз в експертизі авторства текстів використовуються в основному методи аналізу формальних характеристик писемної мови. Цими характеристиками є показники частоти повторювання тих або інших одиниць мови в досліджуваному тексті. Лінгвістична природа, кількість і рівень організації формальних характеристик можуть бути різними. До їх числа належать, наприклад: характеристики лексичного багатства текстів, що виражаються через показники співвідношення різних слів до всіх слів цього тексту; відносна поширеність різних частин мови в тексті; середня довжина речень та ін.

Що ж до кількості використовуваних при атрибуції формальних характеристик, то і тут діапазон достатньо широкий. Так, харківські дослідники виділяють до 63 формальних характеристик: від порівняно простих (відносне число опорних слів у тексті) до достатньо складних (частотність певних граматичних конструкцій у тексті) [6].

### 6.3.1. Критерії вибору аналізованого параметра

Основна проблема формальних методів аналізу авторства полягає у виборі параметрів. Існує цілий ряд формальних статистичних характеристик текстів, непридатних для встановлення авторства через один з двох недоліків:

– відсутність стійкості — розкидання значень параметра для текстів одного і того ж автора настільки великий, що діапазони можливих значень для різних авторів перекриваються. Очевидно, цей параметр не допоможе розрізняти авторів, а при використанні у складі групи параметрів лише відіграє роль додаткового шуму;

– відсутність розрізняючої здатності — параметр може набувати близьких значень для всіх або більшості авторів, оскільки його значення визначаються властивостями мови, якою написані тексти, а не індивідуальними особливостями творця тексту.

Тому параметри, що використовуються у формальних методиках визначення авторства, повинні заздалегідь досліджуватися на стійкість і розрізняючу здатність, бажано на текстах значної кількості різних авторів.

Сьогодні виокремлено такі три умови застосовності формального параметра:

1. Масовість — параметр повинен спиратися на ті характеристики тексту, які слабко контролюються автором на свідомому рівні. Це необхідно, щоб усунути можливість свідомого спотворення автором характерного для нього стилю або імітації стилю іншого автора.

2. Стійкість — параметр повинен зберігати постійне значення для одного автора. Природно, через випадкові причини деяке відхилення значень від середнього неминуче, але воно має бути досить незначне.

3. Розрізняюча здатність — в ідеалі параметр повинен набувати істотно різних значень (коливання, що перевищують можливі для одного автора) для різних авторів [7; 8].

З приводу останньої умови необхідно зазначити, що вибрати параметри, які гарантовано розділяють двох будь-яких авторів, украй складно. Якими б не були параметри, завжди існує вірогідність того, що два або більше авторів опиняться за даними параметрами близькі через випадковий збіг. Тому на практиці вважають достатнім, щоб параметр дозволяв впевнено розрізняти між собою різні групи авторів, тобто існувала достатньо велика кількість груп авторів, для яких середні значення параметра істотно розрізняються. Параметр, очевидно, не допоможе розрізнити тексти авторів з однієї групи, але дозволить упевнено розрізняти тексти авторів, що потрапили в одну групу. Розрізняти тексти авторів однієї групи можна за рахунок використання одночасно досить великого вектора різних за характером параметрів — у цьому випадку вірогідність випадкового збігу, відповідно, стане помітно меншою. Для упевненого висновку щодо текстів, для яких формально обчислена параметрична відстань мала, потрібне додаткове дослідження експертними методами.

## 6.4. Статистичні методи авторознавчої експертизи

Це формальні методи, які засновані на порівнянні обчислюваних характеристик текстів. Взагалі текст відображається у вектор обчислених для нього параметрів, кожен з яких об'єктивно характеризує деякий

набір особливостей тексту. Таким чином, текст графічно відображається в деяку точку n-вимірного простору. При такій формалізації автор також може бути представлений у вигляді аналогічного вектора параметрів — цим вектором буде вектор текстів, написаних цим автором.

Як критерій близькості двох текстів вводиться так чи інакше обчислювана «відстань» між відповідними векторами (у простому випадку можна представити набори параметрів як звичайні вектори в n-вимірному декартовому просторі, такі, що виходять з початку координат, і вважати за відстань між текстами звичайну декартову відстань між кінцями відповідних ним векторів, але це зовсім не обов'язково — є безліч інших варіантів). Саме «відстань» є у результаті інтегральною характеристикою відмінності текстів. Відстань певним чином нормується, і тексти, для яких відстань велика, вважають такими, що з високою вірогідністю належать до різних авторів. Таким чином, щоб порівняти авторство двох текстів, досить обчислити для них параметри і визначити відстань. Щоб порівняти текст з автором, порівнюють вектори параметрів автора і цього тексту, тобто, порівнюються два тексти — текст зі свідомо відомим автором і текст, авторство якого потрібно встановити, підтвердити або спростувати. Не існує принципових проблем щодо того, аби скласти вектори формальних параметрів, які розрізняють не конкретних авторів (або їх групи), а вирізняють певні характеристики авторів (наприклад, освітній рівень).

У більшості випадків як характеризуючі параметри тексту вибираються ті або інші його статистичні характеристики: статистика використання певних частин мови, деяких конкретних слів, розділових знаків, фразеологізмів, архаїзмів, рідкісних та іноземних слів, довжина речення (у словах, складах, знаках) і т. д. [9; 10; 11; 12].

### 6.4.1. Метод відносної ентропії

З математичної точки зору вирішуване завдання полягає в такому: існує текст Z невідомого походження; необхідно співвіднести його одному з текстів $A_1$ ..., $A_k$.

Підхід до вирішення завдання полягає в побудові певної оцінки відносної ентропії H(B|A) тексту B щодо тексту A. Потім послідов-

ність Z співвідноситься послідовності $A_i$, на якій відносна ентропія $H(Z|A_i)$ є мінімальною.

Відносна ентропія є узагальненням поняття ентропії, яке вводиться як до теорії вірогідності, так і до теорії інформації [13]. Існує два підходи до визначення ентропії, що приводять до різних обчислювальних алгоритмів для її оцінки.

Суто інформаційне визначення ентропії через складність ввів А. М. Колмогоров: складністю послідовності букв А є довжина (у двійковому алфавіті) мінімальної програми, яка виводить А, а ентропія А — це її складність, що ділиться на довжину А в бітах. Колмогорівська складність є величиною *необчислюваною*, тобто не можна написати програму, яка дозволяла б її обчислювати для будь-якої послідовності А [14]. Проте існують програми, які, по суті, намагаються обчислити колмогорівську складність тексту: програми стиснення тексту. Дійсно, текстом, стислим програмою Zip, є деяка програма, яка інтерпретується програмою UnZip таким чином, що на виході маємо початковий текст.

Тому за допомогою програми Zip можна визначити оцінку на відносну ентропію H(A|B) тексту В щодо тексту А. Для цього стиснемо текст А і виміряємо довжину архіву C(A), що вийшов, а потім стиснемо текст A+B, що вийшов приєднанням тексту А до тексту В, і виміряємо довжину C(A+B) архіву, що вийшов. Оцінка на відносну складність даватиметься формулою C(B | A) = C(A+B) — C(A).

Тепер, щоб визначити правильного автора тексту Z серед авторів текстів $A_1$ ..., $A_k$ треба обрати такий індекс і, що для всіх j, які не збігаються з і $C(Z | A_i) < C(Z | A_j)$.

Кращі результати серед архіваторів показує *RAR*.

Описаний метод працює в рамках завдання визначення авторства. Але він не дуже ефективний, тому що стиснення тексту — операція, що вимагає багато часу [14].

Ефективнішим є інший спосіб оцінки ентропії — імовірнісний.

Традиційне імовірнісне визначення ентропії засноване на розгляді ланцюга Маркова n-го порядку на послідовності А, яка випливає з ергодичного джерела. Для досить довгих А добра оцінка ентропії дається деякою функцією Hn(A), яка залежить тільки від частот вживань послідовної n+1 букви в тексті [15]. Аналогічно можна визначити

функцію відносної ентропії Hn(B|A). Був отриманий результат, коли в рамках завдання визначення авторства досить обмежитися функцією H1(B|A), тобто авторство тексту ефективно визначається лише інформацією про частоти пар букв, що послідовно йдуть у тексті.

Спочатку обчислюються ентропії $H(Z|A_1)$ ..., $H(Z|A_k)$ тексту Z щодо текстів $A_1$ ..., $A_k$ всіх авторів кількістю 353 з бази даних. Потім для кожної підвибірки (списку) вибирається трійка найбільш схожих. З отриманої трійки відсікаються за допомогою аналогічних ентропійних міркувань автори, що не мають відношення до тексту. Емпірична перевірка показує що помилка першого роду складає близько 10–15 %, тобто з вірогідністю 10–15 % текст буде класифіковано неправильно. Вірогідність помилки другого роду — менше 5 % [16; 17; 18].

На основі розглянутої методики створений програмний комплекс Лінгвоаналізатор (див. підрозд. 6.5.5) При аналізі запропонованого тексту програма видає літературний або науковий коментар. Наприклад:

*Літературний коментар:*

Я прочитал Ваш текст и я сомневаюсь, что его написал кто-либо из известных мне авторов. Впрочем, все равно отмечу, что если кто из них и написал этот текст, то это соавторы Аркадий Стругацкий и Борис Стругацкий (ранний период творчества), с малой вероятностью 21%. Текст, если он действительно был создан этими писателями, похож на следующие их совместные произведения: 21% в соавторстве Аркадий Стругацкий и Борис Стругацкий (ранний период творчества)

В наше интересное время
Песчаная горячка
Первые люди на первом плоту

Приведу ещё двух возможных претендентов:
писатель Марианна Алферова или писатель Андрей Столяров...

*Науковий коментар:*

В первом столбце находится энтропия данного текста относительно матрицы коэффициентов автора.

2.512804 | Аркадий Стругацкий, Борис Стругацкий
(ранний период творчества)
2.517823 | Марианна Алферова
2.518153 | Андрей Столяров

Аркадий Стругацкий, Борис Стругацкий (ранний период творчества)
В первом столбце — энтропия данного текста относительно матрицы коэффициентов произведения
2.462665 | В наше интересное время
2.471204 | Песчаная горячка
2.490497 | Первые люди на первом плоту

Для аналізу був переданий фрагмент твору А. і Б. Стругацьких «Повернення».

Обсяг цього фрагмента 12 Кб. Авторство фрагмента визначене правильно: текст має найменшу ентропію 2.512804 щодо творів ранніх Стругацьких.

Розглянемо твори, які відібрані серед творів ранніх Стругацьких. Очевидно, джерело фрагмента визначене неправильно (має бути «Повернення»). Це означає лише недолік аналізованої інформації — всього 12 Кб.

Зазначимо, що ентропія щодо перших двох творів («В наш цікавий час» і «Піщана гарячка») менше інших ентропій щодо творів інших письменників. Таким чином, можна зробити висновок, що твір «Перші люди на першому плоту» повинен серйозно відрізнятися від решти двох відібраних. Ознайомлення з текстом показує, що висновок правильний.

## 6.4.2. Метод стійкості частот

Для підвищення якості проведення авторознавчої експертизи можна запропонувати таку методику. Пошук числа повторень тієї або іншої службової частинки серед тисячі слів досліджуваного тексту ототожнюваний з відомим завданням математичної статистики про повторення випробувань, тобто кількість слів тексту вважатимемо числом випробувань, а кількість $m_i$ повторень частинки — числом появ події. Тоді можна ввести поняття частоти як відношення вказаних чисел [19]:

$$P_i = \frac{m_i}{n_i}. \qquad (6.1)$$

У математичній статистиці відомі випадки, коли при збільшенні числа випробувань числові значення частот коливаються близько

певної величини і відхилення частот від вказаної величини зменшуються із зростанням числа випробувань. Як правило, за таку величину береться середнє арифметичне частот $P_i$. Якщо у формулі (6.1) символом *i* позначатимемо номер серії випробувань, то $P_{ср}$ необхідно обчислювати так:

$$P_{\text{ср}} = \frac{\sum_i P_i}{N}, \qquad (6.2)$$

де $N$ — число серій [20].

У статистиці описаний факт повторюваності частот називається законом стійкості частот, а на основі відомої теореми Я. Бернуллі величина $P_{ср}$ приймається як вірогідність появи розшукуваної події.

Для виявлення закону стійкості частот стосовно головного прийменникового спектра (*у, на, з*) весь текст поділяється на фрагменти з тисячі слів. Далі починаємо розшукувати кількість повторень кожного прийменника цього спектра в першій тисячі слів. У цьому випадку число випробувань $n_1 = 1000$ назвемо першою серією випробувань, а отримане число $m_1$ повторень цієї службової частинки слід вважати числом появи розшукуваної події. Тепер за формулою (6.1) можна обчислити частоту $P_1$ першої серії випробувань. Для отримання частоти $P_2$ другої серії необхідно до першого фрагмента тексту додати другий і для $n_2 = 2000$ з урахуванням нового значення $m_2$ обчислити $P_2$ за формулою (6.1). Зазначений процес продовжити до тих пір, поки вказаним аналізом не буде охоплений весь досліджуваний текст. Отриманий таким чином набір чисел $P_i$ покаже, чи має місце закон стійкості частот. Якщо закон стійкості частот матиме місце, то середню частоту, що характеризує вірогідність появи цієї службової частини, обчислимо за формулою (6.2) [21].

### 6.4.3. Індекс Флеша (TheFleshIndex)

Одним з методів встановлення авторства є розрахунок індексу Флеша. Індекс Флеша створювався як методика визначення складності сприйняття тексту читачем.

*Індекс легкості для читання* — міра визначення складності сприйняття тексту читачем. Індекс легкості для читання може обчислюватися на основі кількох параметрів: довжини речень, слів, питомої кількості

найбільш частотних (або рідкісних) слів і т. д. Показник (індекс) легкості для читання Флеша використовувався військовими психологами для встановлення авторства захоплених ворожих документів. Індекс Флеша застосовувався при судових розглядах на Гамбургзькому і Нюрнберзькому процесах, коли встановлення авторства певних документів було важливе для притягнення до суду конкретних осіб.

Індекс Флеша розраховується за формулою:

$$FRE = 206{,}835 — (1{,}015 \times ASL) — (84{,}6 \times ASW), \qquad (6.3)$$

де ASL — середня довжина речення у словах *(AverageSentenceLength),* ASW — середня довжина слова у складах *(Average Numberof Syllablesper Word)* [22].

Для англійської мови значення 90–100 відповідає легкому тексту для молодших школярів, 60–70 — тексту, який можуть читати випускники школи, а тексти з індексом 0–30 призначені для людей з вищою освітою.

У зв'язку з тим, що в російській мові середня довжина речення менша (за рахунок меншого використання службових слів, таких як артиклі або допоміжні дієслова), а слова в середньому довші, було зроблено декілька спроб адаптувати цей індекс для російської мови. Зокрема, І. В. Оборнєва запропонувала індекс для російської мови, отриманий шляхом порівняння більше 100 оригінальних англійських текстів творів відомих англомовних авторів, класиків англійської й американської літератури та відповідних перекладів російською мовою:

$$FRE = 206{,}835 — (1{,}3 \times ASL) — (60{,}1 \times ASW). \qquad (6.4)$$

Слід зазначити, що текстовий процесор Word видає статистику легкості для читання після перевірки правопису. Ця статистика не завжди правильно відображає реальні дані про кількість речень і слів для тексту російською мовою. Наприклад, дужка, поставлена через пропуск, вважається словом. Крім того, якщо рядки тексту відокремлені знаком абзацу, то кожен рядок визначається як речення. У довідкових матеріалах MS Office Word наводиться формула для обчислення показників легкості читання текстів англійською мовою, яка дає негативні значення для російськомовних текстів.

### 6.4.4. FOG-індекс (The Gunning FOG Index)

FOG-індекс — індекс туманності (Fog Index) Роберта Ганнінга вимірює складність читання, виходячи із середньої довжини речення і відсотка слів, що складаються з трьох і більш складів. Індекс виводиться на основі підрахунку загальної кількості речень, що міститься як мінімум у двох текстах по 100 слів кожен.

Для розрахунку індексу слід:

1. 100 слів розділити на кількість речень для визначення середньої довжини речень.

2. У цьому уривку порахувати кількість слів, у яких три і більше складів (імена власні, жаргон, складені слова не враховуються).

3. Отримані результати в пунктах 2 і 3 складаються і помножуються на 0,4.

$$FI = (Nws + Nwt) \times 0,4, \quad (6.5)$$

де Nws — середнє число слів у реченні тексту;

Nwt — середнє число слів з довжиною три і більше складів (що припадають на одне речення тексту) [23].

### 6.4.5. Стилеметрія

Стилеметрія (статистична стилістика) — прикладна філологічна дисципліна, що займається вимірюванням стильових характеристик з метою систематизації і впорядкування (типології, атрибуції, датування, діагностики, реконструкції і т. д.) текстів і їх частин.

Об'єктом стилеметрії є текст, створений конкретним автором, в конкретний час, в конкретній ситуації. Предметом дослідження є елементи стилю, які розуміють як особливості периферії характеристики об'єкта. Стиль може бути описаний через факультативні, поверхневі ознаки тексту, котрі лише неявним чином зачіпають його сутнісні, глибинні характеристики [17].

Стилеметрія ґрунтується на:

– підрахунку частоти і природи лексичних, орфографічних, синтаксичних і граматичних помилок;

– дослідженні стилістичних факторів писемної мови (довжина слів, довжина речень; кількість складів, префіксів і суфіксів на 100 слів);

– підрахунку відсотка зустрічаємості в тексті частин мови: співвідношення дієслів до прикметників, дієслів — до іменників тощо, а також показник TTR (TypeTokenRatio) — представлення у формі десяткового дробу співвідношення кількості різних слів із загальною кількістю слів у тексті.

Прикладами стилеметричних методів можуть бути методи:

– опорних слів (далі — метод Фоменка) — підрахунок кількості появи сполучників, часток і прийменників;

– розділових знаків — підрахунок тільки кількості внутрішніх і зовнішніх розділових знаків;

– слів — підрахунок тільки слів певної довжини;

– речень — підрахунок тільки речень певної довжини;

– синтаксичний метод — підрахунок розділових знаків, слів і речень певної довжини знаків;

– комбінований — об'єднання методу Фоменка і синтаксичного методу [24].

Стилеметрія має справу з кількісною класифікацією, а ця галузь класифікаційних робіт тісно стикається з кількома науковими напрямами: теорією угрупувань, теорією оцінювання, розпізнаванням образів, теорією кореляції, кількісною таксономією, методами психологічного тестування і ін. Межі між цими напрямами стираються, і сьогодні можна говорити про комплекс підходів і методів, що займаються тими або іншими видами кількісної систематизації об'єктів довільної природи.

### 6.4.6. Підхід Колтарда

Одним з найбільш ефективних психолінгвістичних підходів до вирішення юридичних (судових) завдань, що вживаються останніми роками, є підхід Колтарда (Coulthard, 1994). Він не лише виявляє перспективні дані для досліджень, але і пропонує нові способи проведення власне текстуального аналізу. У рамках цієї методики психологи порівнюють деякі аспекти досліджуваного тексту із системою тієї мови, на якій написаний текст. Окрім основного словникового складу мовної системи, спеціальні відомості лексики, виведені з текстів різних видів (словникова система передсмертних записок само-

вбивць, листів із погрозами, записи телефонних переговорів злочинців, процесуальні тексти, протоколи допитів і т. д.). Методика виокремлює ряд лінгвістичних факторів, за якими може бути проаналізовано текст. Наприклад, найбільш частотні лексичні одиниці тексту можуть бути порівняні з «лідерами» цієї мовної системи, а розбіжності проаналізовані статистично або порівняні з відповідними одиницями іншого тексту, потім розбіжності піддані статистичному аналізу. При аналізі одиничного тексту, автор якого стверджує, що його частина була сфальсифікована іншою особою, спірна частина може бути порівняна з неоспорюваною.

Більшість текстів і мов в повсякденному житті складаються з ядра словникової системи (приблизно 2500 слів), таким чином, що поява слів, які не входять в це ядро, має особливе значення.

Ще однією характеристикою при аналізі є порядок сполучуваності слів, тобто взаємообумовленість появи в тексті двох або більше різних слів в одному поєднанні. Сполучуваність слів — явище дуже персоналізоване, і її облік при аналізі є дуже суттєвим.

Інші фактори аналізу: теперішний — минулий часи, пасивні — активні стани, стверджувальні — заперечні конструкції, опущення — заміна певного артикля і деякі інші характеристики, що дозволяють порівняти структуру тексту із системою мови, а за допомогою цього і з іншими текстами [25].

### 6.4.7. Лінгво-статистичний аналіз неповнозначної лексики

Лінгво-статистичний аналіз неповнозначної лексики проводиться в разі конкуренції зразків, коли є зразки текстів авторів X, Y, Z. Необхідно встановити, хто з них є автором текстів $X_1$, $X_2$, …$X_n$.

Цей метод припускає наявність двох корпусів текстів — еталонних текстів, що представляють авторський стиль передбачуваного автора (або авторів), і аналізованих (спірних) текстів. Далі аналіз проходить у вигляді експерименту, у ході якого на різних етапах здійснюються такі процедури:

– складання словників еталонного корпусу (корпусів — якщо передбачуваних авторів кілька) і корпусу (корпусів) спірних текстів

із вказівкою абсолютної відносної частоти вживань у відповідному корпусі;

– видалення повнозначних лексем з отриманих словників;

– порівняння словників, що включають тільки неповнозначну лексику для виявлення лексем з близькою частотою; поріг близькості частоти визначається в кожному конкретному випадку за спеціальною методикою;

– формування кластерів «авторських» лексем, що включають тільки ті неповнозначні слова, які є близькими за відносною частотою для цієї пари порівнюваних корпусів [26].

### 6.4.8. Розпізнавання автора тексту з використанням ланцюгів А. А. Маркова

Новий метод ґрунтується на формальній математичній моделі послідовності букв тексту як реалізації ланцюга А. А. Маркова. За тими творами автора, які достовірно ним створені, обчислюється матриця перехідних частот вживань пар букв. Вона служить оцінкою матриці вірогідності переходу з букви в букву. Матриця перехідних частот будується для кожного з авторів. Для кожного автора оцінюється вірогідність того, що саме він написав анонімний фрагмент тексту. Автором анонімного тексту вважається той, у якого обчислена оцінка вірогідності більша.

Такий метод виявляється дуже точним для природно-мовних текстів. Перевірка методу проводилася на творах 82 письменників, серед яких є російські письменники як XIX, так і XX століття.

Позначимо через $A$ деяку безліч букв. Через $A_k$ позначимо безліч слів довжини $k$ над алфавітом $A$. Нехай $A^* = \bigcup_{k>0} A_k$. Позначимо довжину слова $f \in A^*$ через $|f|$.

Завдання визначення автора тексту можна сформулювати таким чином. Нехай задані $n$ класів $C_i$, де $i=0...,n-1$. У кожному класі $C_i$ знаходяться послідовності $f_{i,j} \in A^*$, де $j=1..., m_i$, тобто $C_i=\{f_{i,j} | j=1..., m_i\}$. Наше завдання полягає в тому, щоб віднести $xA^*$ до одного з класів $C_i$.

Припустимо, що послідовності букв $f_{i,j}$ є реалізаціями ланцюга Маркова з перехідною матрицею $\Pi^i$. Побудуємо оцінку $P^i$. Позначимо через $h_{i,j,kl}$ число переходів букв $k \to l$ у фрагменті $f_{i,j}$, припустимо

$h_{i,kl} = \sum_j h_{i,j,k}$ , а $h_{i,kl} = \sum_l h_{i,kl}$ . Припустимо $P_{kl}^i = h_{i,kl} / h_{i,k}$ . Можливо, деякі $P_{kl}^i$ дорівнюють нулю. Позначимо через $Z_i$ множину таких впорядкованих пар (*к,l*), що $P_{kl}^i > 0$.

Припустимо, що *x* також є реалізацією ланцюга Маркова з матрицею перехідної вірогідності $P^q$, де *q* невідомий параметр, який приймає одне із значень 1..., *n*.

Позначимо через $v_{kl}$ число переходів $k \to l$ в *x*. Нехай також $v_k = \sum_l v_{kl}$ . Позначимо через

$$L_i(x) = -\sum_{k,l} v_{kl} \cdot l_n(v_{kl}(P_{kl}^i \cdot v_k)), \qquad (6.6)$$

де сума береться по парах $(k,l) \in Z_i$. Отже, $L_i(x)$ дорівнює мінус логарифму вірогідності *x* за умови, що *x* — реалізація ланцюга Маркова з матрицею перехідної вірогідності $P^i$. Назвемо *t(x) оцінкою максимальної правдоподібності* для невідомого параметра *q* [27]:

$$t(x) = \text{argmin}_{i=0,\ldots,n-1} L_i(x). \qquad (6.7)$$

*Схема експерименту.* Візьмемо $A = \{$маленькі букви кирилиці $\cup \{$символ пропуску$\}$. Припустимо, що у нас є досить довгі фрагменти творів *n* авторів російською мовою. Позначимо *j*-й фрагмент *i*-го автора через $g_{i,j}$. Можна вважати, що фрагмент $g_{i,j}$ є послідовністю символів певного розширеного алфавіту *B*, який включає, наприклад, знаки пунктуації, великі букви, латинські букви і т. д. (на персональному комп'ютері *B* зазвичай збігається з розширеною множиною символів *ASCII*).

Кожен фрагмент $g_{i,j} \in B^*$ можна відобразити в $A^*$ за допомогою певної функції F: $B^* \to A^*$. Нехай, наприклад, F перетворює всі великі букви на маленькі, зліплює слова з переносами, викидає всі знаки пунктуації і зайві знаки пропуску, залишаючи їх поодинці між словами, а також вставляє один пропуск на початку і один пропуск у кінці фрагмента у разі відсутності таких.

Крім того, ми розглядатимемо функцію G, яка створена так само, як і функція F, з тим доповненням, що всі слова, які у фрагменті $g_{i,j}$ починалися із великої букви, відкидаються. Наприклад, якщо

*y* =*«Крім* того, ми розглядатимемо функцію G»,

то F(*y*)=« крім того ми розглядатимемо функцію »,

а G(*y*)=« того ми розглядатимемо функцію ».

Тепер припустимо, що якийсь фрагмент тексту $y$ О $B^*$ належить одному з $n$ авторів, і нам невідомо, кому саме. Наше завдання: визначити автора фрагмента. Ми можемо знайти автора, застосовуючи оцінку (6.7) до послідовності $x = F(y)$ або до $x = G(y)$. Отже, ми отримуємо два способи визначення автора:

1) дійсний автор — $t(F(y))$;

2) дійсний автор — $t(G(y))$.

Важливо зазначити, що оцінки $t(F(y))$ і $t(G(y))$ обчислюються на основі інформації про частоти вживання пар букв. Оскільки між словами вставлені пропуски, оцінки $t(F(y))$ і $t(G(y))$ ніяк не залежать від порядку самих слів. Можливо, $t(F(y))$ і $t(G(y))$ характеризують послідовності морфем у словоформах російської мови, але, звичайно, зовсім не враховують синтаксичну інформацію (на основі останньої намагалися встановлювати авторство).

Статистичний експеримент показує, що автори визначаються дуже упевнено.

*Модельний експеримент.* Спочатку проведемо перевірку нашої методики на такому прикладі. Розглянемо такі твори К. Буличова, О. Волкова, М. Гоголя і В. Набокова.

Ми хочемо перевірити ефективність оцінки $t(F(y))$. Пропонується такий спосіб: вибрати кожного автора $i$ ($i = 1, 2, 3, 4$) по одному контрольному твору $y_i$, оцінити матриці $\Pi^i$ по інших творах $f_{i,j}$, а потім знайти $t(F(y_i))$. Якщо оцінка працює добре, то для кожного автора $i$ повинно бути $t(F(y_i)) = i$.

1. К. Буличов: Уміння кидати м'яч ($y_1$); Біле плаття попелюшки ($g_{1,1}$); Великий дух і утікачі ($g_{1,2}$); Вельмишановний мікроб ($g_{1,3}$); Закон для дракона ($g_{1,4}$); Улюбленець (Спонсори) ($g_{1,5}$); Марсіанське зілля ($g_{1,6}$); Мініатюри ($g_{1,7}$); Можна попросити Ніну? ($g_{1,8}$); Днями землетрус в Лігоне ($g_{1,9}$); Перевал ($g_{1,10}$); Свідчення Олі Н. ($g_{1,11}$); Помильник XX століття ($g_{1,12}$); Розкопи курганів в долині Репеделкінок ($g_{1,13}$); Тринадцять років шляху ($g_{1,14}$); Смерть поверхом нижче ($g_{1,15}$).

2. О. Волков: Сім підземних королів ($y_2$); Чарівник смарагдового міста ($g_{2,1}$); Урфін Джус і його дерев'яні солдати ($g_{2,2}$); Вогняний бог Марранів ($g_{2,3}$); Геніальний пень ($g_{2,4}$); На війні, як на війні ($g_{2,5}$);

Про що мовчали газети... ($g_{2,6}$); Злочин і покарання ($g_{2,7}$); Епілог ($g_{2,8}$); Жовтий Туман ($g_{2,9}$); Таємниця покинутого замку ($g_{2,10}$).

3. М. Гоголь: Оповідання і повісті ($y_3$, назви повістей: Повість про те, як посварився Іван Іванович з Іваном Никифоровичем, Старосвітські поміщики, Вій, Записки божевільного); Ревізор ($g_{3,1}$); Тарас Бульба ($g_{3,2}$); Вечори на хуторі біля Діканьки ($g_{3,3}$).

4. В. Набоков: Інші береги ($y_4$); Король, дама, валет ($g_{4,1}$); Лоліта ($g_{4,2}$); Машенька ($g_{4,3}$); Розповіді ($g_{4,4}$); Незавершений роман ($g_{4,5}$).

Наприклад, у О. Волкова контрольним твором є $y_2$, тобто «Сім підземних королів». Решта всіх творів використовується для обчислення $P^i$.

Результати обчислень подаються у табл. 6.1.

Таблиця 6.1

**Результати обчислень модельного експерименту**

| № | Автор | $c_1$ | $c_2$ | $c_3$ | $c_4$ |
|---|---|---|---|---|---|
| 1 | К. Буличов | 0 | 15 | 2 345 689 | 75 161 |
| 2 | О. Волков | 0 | 8 | 1 733 165 | 233 418 |
| 3 | М. Гоголь | 0 | 3 | 723 812 | 243 767 |
| 4 | В. Набоков | 0 | 5 | 1 658 626 | 367 179 |

Стовпчик $c_2$ містить загальне число файлів, у яких зберігаються твори автора. Зазначимо, що число файлів може не збігатися з числом творів через дві причини: по-перше, кілька творів одного автора можуть знаходитися в одному файлі (тут таке відбулося з О. Волковим — три повісті «Жовтий Туман», «Таємниця покинутого замку» і «Вогняний бог Марранів» були в одному файлі); по-друге, один великий твір може розбиватися на кілька частин (останнє необхідно враховувати при вивченні табл. 6.1).

У стовпці $c_3$ міститься сумарне число символів (букв і пропусків) у $F(g_{i,j}) : c_3 = \sum_j \left| F(g_{i,j}) \right|$. У стовпці $c_4$ міститься число символів у $F(y_i)$, тобто $c_4 = | F(y_i)|$. Наприклад, для К. Буличова загальний обсяг текстів $\sum_j F(g_{1,j})$ складає 2 345 689. Загальний обсяг $F(y_1)$, тобто число символів $A$ у повісті «Уміння кидати м'яч», обраною як контрольний текст, дорівнює 75 161.

У стовпці $c_1$ в рядку $j$ знаходиться ранг числа $\mathrm{L_j}(F(y_j))$, серед чисел $\{\mathrm{L_i}(F(y_j))| \, i = 1, 2, 3, 4\}$. Під *рангом* ми маємо на увазі номер

$L_j(F(y_j))$ серед чисел $\{L_i(F(y_j))|\ i = 1, 2, 3, 4\}$, розташованих у порядку незростання. Наприклад, якщо j=2 і $L_i$ розташувалися в порядку $L_1 \le L_4 \le L_3 \le L_2$, то рангом $L_2$ буде 4. А якщо j=1 і $L_i$ розташувалися в тому ж порядку $L_1 \le L_4 \le L_3 \le L_2$, то рангом $L_1$ буде 1. Ранг $L_j(F(y_j))$, серед чисел $\{L_i(F(y_j)|\ i=1, 2, 3, 4\}$ збігається з рангом $L_j(F(y_j))/|F(y_j)|$, серед чисел $L_i(F(y_j))/|F(y_j)|\ |\ i=1, 2, 3, 4$. Розташуємо в рядках $j=1,2,3,4$ такої матриці по чотири числа $L_i(F(y_i))/|F(y_i)|$, $i=1,2,3,4$:

$$L = \begin{matrix} 2{,}484569 & 2{,}508425 & 2{,}504301 & 2{,}493778 \\ 2{,}501061 & 2{,}473907 & 2{,}516797 & 2{,}492874 \\ 2{,}499033 & 2{,}504508 & 2{,}480202 & 2{,}483829 \\ 2{,}541367 & 2{,}538101 & 2{,}548842 & 2{,}520018 \end{matrix}$$

У кожному рядку знайдемо ранги чисел $L_i$:

$$R = \begin{matrix} 1 & 4 & 3 & 2 \\ 3 & 1 & 4 & 2 \\ 3 & 4 & 1 & 2 \\ 3 & 2 & 4 & 1 \end{matrix}$$

Шукані числа стовпця $c_1$ стоять на діагоналі. Згадуючи формулу (6.7), ми доводимо, що $t(F(y_j)) = j$ тоді і тільки тоді, коли ранг $L_j(F(y_j))/|F(y_j)|$ серед чисел $\{L_i(F(y_j))\ /|F(y_j)|\ |\ i = 1, 2, 3, 4\}$ просто дорівнює 1. Отже, якщо в якому-небудь рядку у стовпчику $c_1$ матриці L стоїть 1, то авторство контрольного тексту визначене правильно. З матриці L ми бачимо, що у всіх письменників авторство визначене правильно.

Перш ніж обговорити цей результат, пояснимо, чому стовпець $c_1$ заданий таким чином. Річ у тім, що якщо авторство визначене неправильно (тобто, з'ясувалось, що $t(F(y_j)) = j$), то нас може цікавити, наскільки ми були близькі до правильної відповіді. Якщо ранг $L_j(F(y_j))\ /|F(y_j)|$ серед чисел $\{L_i(F(y_j))\ /|F(y_j)|\ |\ i=1, 2, 3, 4\}$ дорівнює 2, то ми помилилися всього на одного письменника. Такий випадок істотно кращий за випадок рангу $L_j(F(y_j))/|F(y_j)|$, який дорівнює 4, оскільки тут правильний письменник опиняється у списку претендентів на його власний твір останнім, що свідчить про більшу помилку.

Крім того, матриця *R* сама по собі допускає цікаві інтерпретації. Наприклад, з першого рядка ми бачимо, що контрольний твір К. Буличова «Уміння кидати м'яч» після самого К. Буличова, більше є схожим на В. Набокова, потім на М. Гоголя і в останню чергу на твори О. Волкова. З подальших двох рядків можна зробити висновок, що контрольні твори О. Волкова і М. Гоголя також насамперед схожі на твори В. Набокова. Можливо, це викликано тим, що сам В. Набоков історично знаходиться між М. Гоголем і О. Волковим та К. Буличовим. Якщо ця гіпотеза правильна, то наш метод чутливий до історичної епохи, у яку створений твір. Деяке підтвердження тому ми знаходимо в останньому рядку матриці R: контрольний твір В. Набокова схожий насамперед на пару О. Волкова і К. Буличова, і лише потім — на М. Гоголя. Якби пара О. Волкова і К. Буличова розбивалася М. Гоголем, то ми мали б аргумент проти нашої гіпотези. Втім, можливі інші інтерпретації матриці *R*, і автор в жодному разі не наполягає на вищенаведеній гіпотезі.

Можна цікавитися залежністю матриці *R* від:

а) числа і обсягу текстів навчальних вибірок;

б) однорідності за жанром;

в) однорідності за тематикою;

г) довжини контрольного тексту;

г) одиниці аналізу (на рівні букв, слів і пропозицій) та ін.

Нижче ми наводимо інформацію щодо пункту а. Таким чином, методика працює задовільно (тобто, на діагоналі матриці *R* в основному стоять 1) при обсязі навчальної вибірки понад 100 тисяч символів *ASCII* і обсязі контрольного тексту понад 100 тисяч символів *ASCII* [28].

Повернемося до обговорення матриці L. Оскільки у стовпці $c_1$ усі числа дорівнюють 0, авторство всіх контрольних творів визначене правильно. Результат тим більше несподіваний, що ми використовували таку примітивну інформацію про текст як частоти вживання пар букв. Насправді простий комп'ютерний експеримент (результати якого тут не наведені) показав, що при невеликій кількості передбачуваних письменників (менше шести), навіть оцінка, заснована лише на підрахунку частот вжитку букв, дає дуже добрі результати.

## 6.5. Програми визначення авторства тексту

Формалізовані методи авторознавства дають можливість автоматизованого виявлення і підрахунку ідентифікаційних і діагностичних ознак письмової мови за допомогою спеціальних комп'ютерних програм.

### 6.5.1. Програма «Prostyle» (США)

Програма здійснює аналіз будь-якого тексту, що вводиться, і виводить за порядком номерів факторів, які дозволяють провести статистичний аналіз значення в будь-яких розбіжностях у двох досліджуваних текстах. Серед факторів, що враховуються програмою «Prostyle», знаходяться:

– граничний індекс чіткості (наскільки цей текст легкий або важкий для розуміння);

– індекси FOG і Флеша–Кінкейда;

– показник частотності конструкцій із пасивним станом, що дозволяє достатньо точно виявити індивідуальні особливості автора;

– кількість використовуваних лексичних одиниць, яка при обчисленні відсотка співвідношення із загальною кількістю слів у тексті дає показник словникового запасу автора;

– відсоток складних слів за префіксами, суфіксами, кількістю складів (у Prostyle — тільки за останнім фактором);

– середня довжина речення, що прямо корелює з рівнем освіти автора;

– «читацький вік», що представляє цей текст;

– кількість погрішностей письмового стилю в тексті (можливі помилки: неправильне використання абстрактних іменників; неправильне вживання дієслівних форм із прийменниками; опущення дієслова; недоречне вживання сленгу і жаргону; використання застарілих слів; порушення пасивних конструкцій; грубі і непристойні слова; слабке знання мови).

### 6.5.2. Програма «E'RIDAtextvisor»

Програма для аналізу тексту Web-сервером сторінок сайту «E'RIDAtextvisor « проводить загальний аналіз тексту сторінок сайту, аналіз тексту метатегів. Під час аналізу тексту сторінки програма:

– сканує текст сторінки;

– сканує текст у метатегах сторінки;

– сканує текст анкора (anchor) посилань на сторінці;

– сканує опис посилань (Alt).

Отримані результати представлені у вигляді:

– загальна кількість слів на сторінці, а так само окремо в «мета», «тексті» і «посиланнях»;

– загальна кількість символів на сторінці, а так само окремо в «мета», «тексті» і «посиланнях»;

– демонстрація кожного слова із вказівкою кількості однокорінних слів, а так само де і скільки кожне із слів розташовується («текст», «мета», «посилання»);

– процентне співвідношення кожного слова до загальної кількості слів, а так само окремо «% в мета» і «% в тексті» (зручно для контролю ключових слів).

Під час аналізу метатегів програма:

– сканує текст title;

– сканує текст description;

– сканує текст keywords.

Отримані результати представлені у вигляді:

– кількості слів у кожному з пунктів;

– кількості символів у кожному з пунктів;

– кількості кожного слова з урахуванням однокорінних слів;

– відсоткового співвідношення кожного слова в кожному з пунктів (окремо % у title, description і keywords);

– визначення, скільки кожного із слів знаходиться в кожному з пунктів.

Аналіз посилань:

– визначення тексту кожного посилання (anchor);

– визначення опису кожного посилання (alt).

Отримані результати представлені у вигляді:

– окремо опис і окремо текст посилання;

– розбір за словами опису і тексту посилання;

– визначення кількості слів і кількості символів як в описі, так і в тексті кожного посилання.

### 6.5.3 Програма «Антиплагіат»

eTXT Антиплагіат — програма перевірки унікальності тексту.

Програма дозволяє провести докладний аналіз унікальності тексту і визначити оригінальність статті у відсотковому співвідношенні. У програмі враховані особливості роботи копірайтера. Програма має дві версії: установка на комп'ютер користувача і режим он-лайн.

При роботі зі встановленою програмою користувач може:

– знаходити і виділяти неунікальні фрагменти тексту безпосередньо на відтвореній копії Web-сторінки, що значно полегшує визначення унікальності тексту;

– створювати докладні звіти перевірки унікальності контенту з можливістю налаштування різних параметрів пошуку — числа вибірок з тексту, кількості слів в шингле тощо;

– перевіряти на унікальність всі сторінки сайту, видаючи докладний звіт щодо сайту;

– вести пакетну перевірку всіх файлів з теки.

Он-лайн версія програми eTXT Антиплагіат дозволяє:

– перевірити текст на унікальність незалежно від зовнішніх факторів, таких як швидкість Internet-з'єднання або встановлена на ПК операційна система;

– не боятися блокування пошуковими системами;

– зберігати результати перевірки на сервері і мати можливість надати їх постійну адресу за необхідності;

– економити трафік.

### 6.5.4. Програма «Атрибутор»

Программа «Атрибутор» є лінгвістичним процесором для автоматичного порівняння і класифікації текстів за параметрами індивідуального авторського стилю. Мета програми — розпізнавання авто-

ра тексту або видачі списку найбільш близьких до нього за стилістикою авторів з числа вхідних у деякий заздалегідь заданий перелік «еталонних» авторів.

При роботі програми передбачено три ситуації:

– найбільш вірогідним автором є Х. Цей висновок означає, що в нашій вибірці є тексти надісланого на дослідження письменника;

– автора цього тексту в нашій базі немає. Цей висновок означає, що надісланий текст містить особливості індивідуального стилю, за якими він достатньо різко відрізняється від наявних у вибірці письменників. Цей текст, мабуть, не містить індивідуальних стилістичних рис;

– список найбільш близьких авторів (в порядку убування вірогідності). Цей висновок означає, що надісланий текст за стилістикою не збігається чітко з жодним з наявних у вибірці письменників і в той же час не має різких відмінностей від кількох з них.

Як ознаки для аналізу й оцінки індивідуального авторського стилю в цій версії атрибутора використовуються трьохлітерні поєднання — тріади. Обробку проходять всі слова тексту, причому початок і кінець слова доповнюються пропусками, які також враховуються в тріадах. Однакові тріади підсумовують, із зібраних за текстом тріад виходить профіль, який є пошуковим образом, що характеризує авторський стиль.

В обробку потрапляють всі слова тексту за винятком власних назв. У лінгвістичному сенсі трьохлітерні поєднання є інтегральною характеристикою, що об'єднує відразу кілька різнорідних стильових ознак. При такій методиці окремими тріадами в підрахунок потрапляють розподіли однолітерних і парами тріад — двохлітерних службових слів, а це значна частина найбільш частотних приводів, сполучників, часток і вигуків, які традиційно вважають значущими стилеметричними показниками. З цієї причини двох-, чотирьох- і більш літерні ланцюжки менш показові, що і було виявлено у процесі перевірки їх розрізнюючої сили.

Решта літеросполучень так чи інакше відображає і граматичні явища (частоту граматичних частин вжитих у тексті слів), і лексичні (літеросполучення з основи слова), причому нерозчленовано. Хоча розрізняльна сила окремих літеросполучень очевидно неоднакова, у цій версії атрибутора при оцінці і зважуванні це поки що не враховується.

### 6.5.5. Програма «Лінгвоаналізатор»

Програма виконує читання і обробку тексту невідомого походження з метою визначення близькості до одного з авторських еталонів, визначених заздалегідь.

«Лінгвоаналізатор» розбирає текст на елементарні складові, використовуючи математичну модель, у якій враховані такі характеристики тексту, як:

а) число службових слів (прийменників, сполучників і часток);

б) морфеми (префіксальні, кореневі, суфіксальні, флексійні) і їх послідовності;

в) складність граматичних конструкцій;

г) власне словник, що використовується автором.

Програма вимірює всі ці параметри і зводить у таблиці, що містять сотні змінних, які характеризують письменника. У кожного автора з бази даних є своя таблиця, яка є авторським еталоном. Початкові тексти «Лінгвоаналізатор» не зберігає.

При введенні аналізованого тексту відбувається побудова ще однієї таблиці за вхідним текстом. Після цього вхідна таблиця порівнюється з X таблицями за кожним автором і виводиться X інтегральних величин для оцінки близькості цього тексту до кожного з X письменників. Кожна з цих X інтегральних величин називається відносною ентропією. Програма повідомить імена трьох авторів, для яких відносна ентропія за цим текстом мінімальна. У більшості випадків програма правильно називає автора, навіть якщо пропонувати їй твори, що не містяться в базі даних. Це можливо лише тоді, коли алгоритм роботи програми не зводиться до повнотекстового пошуку по всій базі даних, а використовуються тільки інтегральні характеристики текстів.

## 6.6. Висновки

Розвиток електронних документів як у мережі Internet, так і на локальних ПК та локальних мережах призвів до різкого збільшення порушень і авторських прав, прав правовласників. Це явище вимагає

удосконалення існуючих та створення принципово нових методів авторознавчої експертизи.

У цьому розділі наведені завдання та види авторознавчої експертизи. З'ясовано, що найактуальнішим видом авторознавчої експертизи є ідентифікаційна еспертиза. Зазначені ситуації проведення авторознавчих експертиз — множинна невизначеність, конкуренція зразків, порівняння за зразком.

Доведено, що найточніші дані про автора документа надає аналіз стилю. Для дослідження аналізу стилю можуть використовуватися експертні та формальні методи. Оскільки саме формальні методи є найбільш ефективними, основна увага в підрозділі приділена саме їм. Доведено, що найбільш ефективними є статистичні методи авторознавчої експертизи, зокрема стилеметрія. Розглянуті критерії вибору аналізованого параметру — масовість, розрізняюча здатність, стійкість. Наведені види статистичного аналізу документа — індекс Флеша, FOG-індекс, стилеметрія, підхід Колтарда, лінгвостатистичний аналіз неповнозначної лексики, а також топографічний аналіз.

Таким чином, формалізовані методи авторознавчої експертизи дають можливість автоматизованого виявлення і підрахунку ідентифікаційних і діагностичних ознак писемної мови за допомогою спеціальних комп'ютерних програм.

# РОЗДІЛ 7

# ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ

## 7.1. Управління доступом до інформаційних ресурсів комп'ютерних систем

Під інформаційною безпекою мають на увазі техніку захисту інформації від навмисного або випадкового несанкціонованого доступу і завдання тим самим шкоди нормальному процесу документообігу і обміну даними в системі, а також розкрадання, модифікації і знищення інформації. Питання захисту інформації в інформаційних системах вирішується для того, щоб ізолювати нормально функціонуючу інформаційну систему від несанкціонованих управляючих дій і доступу сторонніх осіб або програм до даних з метою розкрадання. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [1].

Серед заходів і засобів захисту інформації можна виокремити ті, які забезпечують інформаційну безпеку за рахунок розмежування доступу до об'єктів захисту (програмним і технічним ресурсам комп'ютерних систем) окремих користувачів [2].

Управління доступом — ефективний метод захисту інформації, який регулює використання ресурсів інформаційної системи, для якої розроблена концепція інформаційної безпеки [3]. Методи і системи захисту інформації, що спираються на управління доступом, включають такі функції захисту інформації в інформаційних системах:

– ідентифікація користувачів, ресурсів і персоналу системи інформаційної безпеки;

– впізнання і встановлення достовірності користувача за обліковими даними, що вводяться (на цьому принципі працює більшість моделей інформаційної безпеки);

– допуск до певних умов роботи згідно з регламентом, наказаним кожному окремому користувачу, що визначається засобами захисту інформації і є основою інформаційної безпеки більшості типових моделей інформаційних систем;

– протоколювання звертань користувачів до ресурсів, інформаційна безпека яких захищає ресурси від несанкціонованого доступу і відстежує некоректну поведінку користувачів системи.

Під несанкціонованим доступом до інформації (НСД) розуміють доступ до інформації, що порушує встановлені правила розмежування доступу і здійснюється з використанням штатних засобів обчислювальної техніки або автоматизованих систем. НСД може мати випадковий або навмисний характер.

Система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від НСД будь-якої інформаційної системи [4].

Завданням систем ідентифікації і аутентифікації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи.

Ідентифікація дозволяє суб'єкту (користувачу, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). Ідентифікація — це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова «аутентифікація» іноді використовують словосполучення «перевірка достовірності». Аутентифікація — це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу.

Ці процедури (ідентифікація та аутентифікація) нерозривно зв'язані між собою, оскільки спосіб перевірки визначає, яким чином і що користувач повинен пред'явити системі, щоб отримати доступ.

Не зважаючи на уявну складність термінів «ідентифікація» і «аутентифікація», кожний користувач сучасних інформаційних систем

стикається з процедурами, що ховаються за цими термінами, неодноразово протягом робочого дня. Не заглиблюючись в технічні подробиці, можна сказати, що ці процедури виконують кожного разу, коли користувач вводить пароль для доступу до комп'ютера, в мережу, до бази даних або при запуску прикладної програми. У результаті їх виконання він отримує або доступ до ресурсу, або відмову в доступі.

## 7.2. Сучасні підходи до завдання ідентифікації користувачів інформаційних систем

Сьогодні існує кілька способів ідентифікації користувачів [5].

У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші — в інших. Однак у багатьох випадках немає чітко визначеного рішення [6]. А тому як розроблювачам програмного забезпечення, так і користувачам доводиться самостійно вирішувати, який спосіб ідентифікації реалізовувати у власних інформаційних комп'ютерних системах.

Існує три найпоширеніших види ідентифікації:

1) парольна ідентифікація. Ще не дуже давно парольна ідентифікація була ледве не єдиним способом визначення особи користувача. І в цьому немає абсолютно нічого дивного. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її зводиться до такого. Кожен зареєстрований користувач якої-небудь системи одержує набір персональних реквізитів (звичайно використовуються пари логін-пароль). Далі при кожній спробі входу він повинен вказати цю інформацію. Оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особу та ідентифікує її.

Головна перевага парольної ідентифікації — це простота реалізації й використання. Крім того, введення парольної ідентифікації не вимагає жодних витрат: цей процес реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною.

Тепер перейдемо до недоліків. На жаль, їх багато. І, мабуть, найголовніший — величезна залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. До них належать занадто короткі паролі, загальновідомі поєднання символів і т. д. Тому деякі фахівці в галузі інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів;

2) апаратна (або електронна) ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особи користувача за якимось предметом, ключом, що перебуває в його ексклюзивному користуванні. Природно, йдеться не про звичні для більшості людей ключі, а про спеціальні електронні [7]. Зараз найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т. д.) та так звані токени (token), які підключаються безпосередньо до одного з портів комп'ютера (USB, LPT).

Головною перевагою застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, у них реалізовано чимало різних захисних механізмів. Вбудований мікропроцесор дозволяє електронному ключу не лише брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Тепер поговоримо про недоліки апаратної ідентифікації. Мабуть, найбільш серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Другий мінус розглянутої технології — ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте для введення в експлуатацію системи такої ідентифікації однаково будуть потрібні деякі витрати. Адже кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися, крім того, вони можуть бути загублені й т. д. Тобто апаратна ідентифікація вимагає деяких експлуатаційних витрат;

3) біометрична ідентифікація. Біометрія — це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. Тобто можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особи людини. А тому рішення використати їх у галузі інформаційної безпеки виглядає цілком логічним. Причому цей напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак [8].

Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів. Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати.

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або може бути використана фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої значно стійкіші щодо подібної фальсифікації.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер. Звичайно, останнім часом ціни на біометричні пристрої постійно знижуються. Крім того, не дуже давно з'явилися миші й клавіатури з вбудованими дактилоскопічними сканерами. Причому їхня ціна ненабагато відрізняється від вартості «звичайної» периферії. Правда, слід відзначити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова в доступі зареєстрованому користувачеві). Тому користувачеві доводиться вибирати, який пристрій придбати — дорожчий і кращий або дешевший і гірший.

Поки що було розглянуто три види (або підходи) однофакторної ідентифікації користувачів інформаційних систем. Тобто в розглянутих системах для визначення особи користувача використовувався тільки один фактор. Однак подібні процеси сьогодні не можна назвати надійними. Але останнім часом набуває поширення комплексна

або багатофакторна ідентифікація, яку не можна виділити в окремий вид, але потрібно обов'язково про неї нагадати і розповісти.

Комплексна (або багатофакторна) ідентифікація. У системах комплексної ідентифікації для визначення особи користувача комп'ютерної інформаційної системи застосовується відразу кілька параметрів [9]. Причому комбінуватися ці параметри можуть у довільному порядку. Втім, сьогодні в переважній більшості випадків використовується тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбору його пароля зловмисником (без електронного ключа він працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Втім, у деяких системах застосовуються максимально надійні, можна навіть сказати, перебільшено надійні процедури ідентифікації. У них одночасно використовуються паролі, токени й біометричні характеристики людини.

## 7.3. Парольні системи захисту

Головна перевага парольної ідентифікації — простота і звичність [10]. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте за сукупністю характеристик їх слід визнати найслабкішим засобом перевірки достовірності. Саме слабкий парольний захист є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу. У 2008 році 84 % комп'ютерних зломів були здійснені внаслідок недосконалості парольного захисту. Голова правління Microsoft Білл Гейтс в одному зі своїх виступів ще в 2006 році передбачив загибель традиційних паролів, оскільки вони не в змозі з належною надійністю забезпечити інформаційну безпеку. Але поки символьний пароль — найпоширеніший спосіб ідентифікації і аутентифікації користувачів і ще довго ним залишатиметься.

Такі заходи дозволять значно підвищити надійність парольного захисту [11]:

– накладення технічних обмежень (пароль повинен бути не дуже коротким, він повинен містити букви, цифри, знаки пунктуації і т. п.);

– управління строком дії паролів, їх періодична зміна;

– обмеження доступу до файлу паролів;

– обмеження кількості невдалих спроб входу в систему (це ускладнює застосування «методу грубої сили»);

– використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може генерувати тільки благозвучні паролі, що запам'ятовуються).

### 7.3.1. Загальні підходи до побудови парольних систем

Для детальнішого розгляду принципів побудови парольних систем сформулюємо кілька основних визначень.

*Ідентифікатор користувача* — певна унікальна кількість інформації, що дозволяє розрізняти індивідуальних користувачів парольної системи (проводити їхню ідентифікацію). Часто ідентифікатор також називають ім'ям користувача або ім'ям облікового запису користувача.

*Пароль користувача* — певна секретна кількість інформації, відома тільки користувачу і парольній системі, яку може запам'ятати користувач і яка може бути пред'явлена для проходження процедури аутентифікації. Одноразовий пароль дає можливість користувачу однократно пройти аутентифікацію. Багаторазовий пароль може бути використаний для перевірки достовірності повторно.

*Обліковий запис користувача* — сукупність його ідентифікатора і його пароля.

*База даних користувачів* парольної системи містить облікові записи всіх користувачів цієї парольної системи.

Під *парольною системою* розуміємо програмно-апаратний комплекс, що реалізовує системи ідентифікації і аутентифікації користувачів автоматизованих систем (АС) на основі одноразових або багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати ряд додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів.

Основними компонентами парольної системи є:

– інтерфейс користувача;

– інтерфейс адміністратора;

– модуль зв'язку з іншими підсистемами безпеки;

– база даних облікових записів.

Парольна система є «переднім краєм оборони» всієї системи безпеки. Деякі її елементи (зокрема ті, що реалізують інтерфейс користувача) можуть бути розташовані в місцях, відкритих для доступу потенційному зловмиснику. Тому парольна система стає одним з перших об'єктів атаки при вторгненні зловмисника в захищену систему. Нижче перераховані *типи загроз безпеки парольних систем.*

1. Розголошування параметрів облікового запису через:

– підбір в інтерактивному режимі;

– підглядання;

– навмисну передачу пароля його власником іншій особі;

– захват бази даних парольної системи;

– перехоплення переданої мережею інформації про пароль;

– зберігання пароля в доступному місці.

2. Втручання у функціонування компонентів парольної системи через:

– впровадження програмних закладок;

– виявлення і використання помилок, допущених на стадії розробки;

– виведення з ладу парольної системи.

Деякі з перерахованих типів загроз пов'язані з наявністю так званого людського фактору, що виявляється в тому, що користувач може:

– вибрати пароль, який легко запам'ятати і також легко підібрати;

– записати пароль, який складно запам'ятати, і покласти запис в доступному місці;

– ввести пароль так, що його зможуть побачити сторонні;

– передати пароль іншій особі навмисно або помилково.

На додаток до вищесказаного необхідно наголосити на існуванні «парадоксу людського фактора». Полягає він у тому, що користувач нерідко прагне виступати скоріш супротивником парольної системи, як, втім, і будь-якої системи безпеки, функціонування якої впливає на

його робочі умови, ніж союзником системи захисту, тим самим послаблюючи її.

Захист від вказаних загроз ґрунтується на ряді перерахованих нижче організаційно-технічних заходів.

### 7.3.2. Вибір паролів

У більшості систем користувачі мають змогу самостійно обирати паролі або одержують їх від системних адміністраторів. При цьому для зменшення деструктивного впливу людського фактору необхідно реалізувати ряд вимог до вибору і використовування паролів, показаних у таблиці 7.1 [12].

Таблиця 7.1

**Вимоги до вибору і використання паролів**

| Вимоги до вибору пароля | Одержуваний ефект |
|---|---|
| Встановлення мінімальної довжини пароля | Ускладнює завдання зловмисника при спробі підглянути пароль або підібрати пароль методом «тотального випробування» |
| Використання в паролі різних груп символів | Ускладнює завдання зловмисника при спробі підібрати пароль методом «тотального випробування» |
| Перевірка та відбраківка пароля за словником | Ускладнює завдання зловмисника при спробі підібрати пароль за словником |
| Встановлення максимального строку дії пароля | Ускладнює завдання зловмисника по підбору паролів методом тотального випробування, зокрема без безпосереднього звернення до системи захисту (режим оф-лайн) |
| Встановлення мінімального строку дії пароля | Перешкоджає спробам користувача замінити пароль на старий після його зміни на попередню вимогу |
| Ведення журналу історії паролів | Забезпечує додатковий ступінь захисту на попередню вимогу |
| Вживання евристичного алгоритму, що бракує паролі на підставі даних журналу історії | Ускладнює завдання зловмисника при спробі підібрати пароль за словником або з використанням евристичного алгоритму |
| Обмеження кількості спроб введення пароля | Перешкоджає інтерактивному підбору паролів зловмисником |

Закінчення таблиці

| Вимоги до вибору пароля | Одержуваний ефект |
|---|---|
| Підтримка режиму примусової зміни пароля користувача | Забезпечує ефективність вимоги, що обмежує максимальний строк дії пароля |
| Використовування затримки при введенні неправильного пароля | Перешкоджає інтерактивному підбору паролів зловмисником |
| Заборона на вибір пароля самим користувачем і автоматична генерація паролів | Виключає можливість підібрати пароль за словником. Якщо алгоритм генерації паролів не відомий зловмиснику, він може підбирати паролі тільки методом «тотального випробування» |
| Примусова зміна пароля при першій реєстрації користувача в системі | Захищає від неправомірних дій системного адміністратора, що має доступ до пароля у момент створення облікового запису |

### 7.3.3. Зберігання паролів

Іншим важливим аспектом стійкості парольної системи є спосіб зберігання паролів у базі даних облікових записів. Можливі такі варіанти зберігання паролів:

– у відкритому вигляді;

– у вигляді згорток (хешування);

– зашифрованими за певним ключем.

Найбільший інтерес становлять другий і третій способи, які мають ряд особливостей.

Хешування (використання незворотної хеш-функції до будь-якої інформації перетворює її на унікальний код) не забезпечує захист від підбору паролів за словником у разі отримання бази даних зловмисником. При виборі алгоритму хешування, який буде використаний для розрахунку згорток паролів, необхідно гарантувати незбіг значень згорток, отриманих на основі різних паролів користувачів. Крім того, слід передбачити механізм, що забезпечує унікальність згорток у тому випадку, якщо два користувачі обирають однакові паролі. Для цього при розрахунку кожної згортки зазвичай використовують певну кількість «випадкової» інформації, яка, наприклад, видається генератором псевдовипадкових чисел.

При шифруванні паролів особливе значення має спосіб генерації і зберігання ключа шифрування бази даних облікових записів. Перерахуємо деякі можливі варіанти:

– ключ генерується програмно і зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження;

– ключ генерується програмно і зберігається на зовнішньому носієві, з якого прочитується при кожному запуску;

– ключ генерується на основі вибраного адміністратором пароля, який вводиться в систему при кожному запуску.

У другому випадку необхідно забезпечити неможливість автоматичного перезапуску системи, навіть якщо вона виявляє носій з ключем. Для цього можна зажадати від адміністратора підтверджувати продовження процедури завантаження, наприклад, натисненням клавіші на клавіатурі.

Найбільш безпечне зберігання паролів забезпечується при їх хешуванні і подальшому шифруванні отриманих згорток, тобто при комбінації другого і третього способів.

Враховуючи, що користувачі нерідко вибирають недостатньо стійкі паролі, можна зробити висновок, що отримання бази даних облікових записів або перехоплення переданого мережею значення згортки пароля становлять серйозну загрозу безпеці парольної системи.

### 7.3.4. Передача пароля мережею

У більшості випадків аутентифікація відбувається в розподілених системах і пов'язана з передачею мережею інформації про параметри облікових записів користувачів. Якщо передавана мережею в процесі аутентифікації інформація не захищена належним чином, виникає загроза її перехоплення зловмисником і використання для порушення захисту парольної системи [13]. Відомо, що багато комп'ютерних систем дозволяють перемикати мережевий адаптер у режим прослуховування адресованого іншим одержувачам мережевого трафіку в мережі, заснованій на передачі пакетів даних.

Нагадаємо основні види захисту мережевого трафіку:

– фізичний захист мережі;

– кінцеве шифрування;

– шифрування пакетів.

Поширені такі способи передачі мережею паролів:

– у відкритому вигляді;

– зашифрованими;

– у вигляді згорток;

– без безпосередньої передачі інформації про пароль («з нульовим розголошуванням»).

Перший спосіб застосовується і сьогодні в багатьох популярних додатках (наприклад, TELNET, FTP). У захищеній системі його можна застосовувати тільки у поєднанні із засобами захисту мережевого трафіку.

При передачі паролів у зашифрованому вигляді або у вигляді згорток мережею з відкритим фізичним доступом можлива реалізація таких загроз безпеці парольної системи:

– перехоплення і повторне використання інформації;

– перехоплення і відновлення паролів;

– модифікація інформації, що передається, з метою введення в оману перевіряючої сторони;

– імітація зловмисником дій перевіряючої сторони для введення в оману користувача.

Схеми аутентифікації «з нульовим знанням» або «з нульовим розголошуванням» вперше з'явилися в середині 80-х — на початку 90-х років XX століття. Їх основна ідея полягає в тому, щоб забезпечити можливість одному з пари суб'єктів довести істинність певного твердження другому, при цьому не повідомляючи йому жодної інформації про зміст самого твердження. Наприклад, перший суб'єкт (що «доводить») може переконати другого («перевіряючого»), що знає певний пароль, насправді не передаючи тому жодної інформації про сам пароль. Ця ідея і відбита в терміні «доказ з нульовим розголошуванням». Стосовно парольного захисту це означає, що якщо на місці перевіряючого суб'єкта виявляється зловмисник, він не отримує жодної інформації про доказуване твердження і, зокрема, про пароль.

Загальна схема процедури аутентифікації з нульовим розголошуванням складається з послідовності інформаційних обмінів (ітерацій) між двома учасниками процедури, по завершенню якої перевіряючий із заданою ймовірністю робить правильний висновок про істинність твердження, що перевіряється. Із збільшенням числа ітерацій зростає

ймовірність правильного розпізнавання істинності (або помилковості) твердження.

Ще одним способом підвищення стійкості парольних систем, пов'язаним з передачею паролів мережею, є застосування одноразових (one-time) паролів. Загальний підхід до застосування одноразових паролів заснований на послідовному використанні хеш-функції для розрахунку чергового одноразового пароля на основі попереднього. Спочатку користувач одержує впорядкований список одноразових паролів, який також зберігається в системі аутентифікації. При кожній реєстрації користувач вводить черговий пароль, а система розраховує його згортку і порівнює з еталоном, що зберігається в системі. У разі збігу користувач успішно проходить аутентифікацію, а введений ним пароль зберігається для використання як еталон при наступній реєстрації. Захист від мережевого перехоплення в такій схемі заснований на властивості необоротності хеш-функції. Найбільш відомі практичні реалізації схем з одноразовими паролями — це програмний пакет S/KEY і розроблена на його основі система OPIE.

## 7.4. Апаратна (або електронна) ідентифікація

Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння з собою. До електронних систем ідентифікації і аутентифікації належать:

1) переносні токени:

– асинхронні — користувач вводить рядок у пристрій, отримує відповідь і вводить її в комп'ютер;

– PIN/асинхронні — асинхронний метод доповнюється введенням PIN-коду в пристрій;

– синхронні — наприклад, токен синхронізований за часом з сервером і генерує для користувача в цю хвилину пароль, який вже і вводиться в систему;

– PIN/синхронні;

2) різноманітні карти — це пристрої, схожі на переносні аутентифікатори, але складніші за своїм складом.

Карти бувають: пасивні (карти з пам'яттю) і активні (інтелектуальні карти). Останні включають CPU, мініатюрну операційну систему, годинник, програми на ROM (read-only memory — пам'ять тільки для читання), буферну пам'ять (RAM) для криптографічних розрахунків, незалежну пам'ять або EEPROM (Electrically Erasable Programmable Read-Only Memory) для зберігання цифрових ключів. За допомогою смарт-карти проводиться розрахунок одноразових паролів і здійснюється взаємодія з пристроєм через картрідер. Після введення PIN-коду картрідер сам запитує смарт-карту, і подальший процес відбувається без участі людини, завдяки чому можна використовувати достатньо довгі ключі.

Карт досить багато, і працюють вони за різними принципами. Так, наприклад, досить зручні у використанні *безконтактні карти* (їх ще називають проксіміті-карти), які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважають смарт-карти — аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т. д.


Що таке USB-ключ, розглянемо на прикладі eToken від компанії Aladdin Software.

eToken — персональний засіб аутентифікації і зберігання даних, що апаратно підтримує роботу з цифровими сертифікатами і електронними цифровими підписами (ЕЦП). eToken може бути виконаний у вигляді USB-ключа або стандартної смарт-карти.

eToken підтримує роботу й інтегрується зі всіма основними системами і додатками, що використовують технології смарт-карт або PKI (Public Key Infrastructure).

Основне призначення:

– двохфакторна аутентифікація користувачів при доступі до захищених ресурсів (комп'ютерів, мереж, додатків);

– безпечне зберігання закритих ключів цифрових сертифікатів, криптографічних ключів, профілів користувачів, налаштувань додатків та ін. в незалежній пам'яті ключа;

– апаратне виконання криптографічних операцій в довіреному середовищі (генерація ключів шифрування, симетричне і асиметричне шифрування, розрахунок хеш-функції, формування ЕЦП).

eToken як засіб аутентифікації підтримується більшістю сучасних операційних систем, бізнес-додатків і продуктів з інформаційної безпеки.

Можливості застосування:

– сувора аутентифікація користувачів при доступі до серверів, баз даних, розділів Web-сайтів;

– безпечне зберігання секретної інформації: паролів, ключів шифрування, закритих ключів цифрових сертифікатів;

– захист електронної пошти (цифровий підпис і шифрування, доступ);

– системи електронної торгівлі, «клієнт-банк», «домашній банк»;

– захист комп'ютерів;

– захист мереж та каналів передачі даних за рахунок побудови VPN (virtual private network — віртуальних приватних мереж);

– клієнт-банк, домашній банк.

eToken забезпечує:

– аутентифікацію користувачів за рахунок використання криптографічних методів;

– безпечне зберігання ключів шифрування і ЕЦП, а також закритих ключів цифрових сертифікатів для доступу до захищених корпоративних мереж і інформаційних ресурсів;

– мобільність користувача і можливість безпечної роботи з конфіденційними даними в недовіреному середовищі (наприклад, на чужому комп'ютері) за рахунок того, що ключі шифрування і ЕЦП генеруються ключем eToken апаратно і не можуть бути перехоплені;

– безпечне використання — скористатися ключем eToken може тільки його власник, що знає PIN-код ключа;

– реалізацію як західних та російських, так і вітчизняних стандартів на шифрування і ЕЦП;

– зручність роботи — ключ виконаний у вигляді брелока зі світловою індикацією режимів роботи і безпосередньо підключається до USB-портів, якими зараз обладнано 100 % комп'ютерів, не вимагає спеціальних зчитувачів, блоків живлення, дротів тощо;

– використання одного ключа для вирішення безлічі різних завдань — входу в комп'ютер, входу в мережу, захисту каналу, шифрування інформації, ЕЦП, безпечного доступу до захищених розділів Web-сайтів, інформаційних порталів тощо.

Безконтактні смарт-карти поділяють на ідентифікатори Proximity і смарт-карти, що базуються на міжнародних стандартах ISO/IEC 15693 і ISO/IEC 14443. В основі більшості пристроїв на базі безконтактних смарт-карт лежить технологія радіочастотної ідентифікації.

Таблиця 7.2

**Радіочастотні ідентифікатори**

| **Характеристика** | **Proximity** | **Смарт-карти** | |
|---|---|---|---|
| | | **ISO/IEC 14443** | **ISO/IEC 15693** |
| Частота радіоканалу | 125 кГц | 13,56 Мгц | 13,56 Мгц |
| Дистанція читання | До 1 м | До 10 см | До 1 м |
| Вбудовані типи чипів | Мікросхема пам'яті, мікросхема з жорсткою логікою | Мікросхема пам'яті, мікросхема з жорсткою логікою, процесор | Мікросхема пам'яті, мікросхема з жорсткою логікою |
| Функції пам'яті | Тільки читання | Читання-запис | Читання-запис |
| Ємність пам'яті | 8–256 байт | 64 байт — 64 Кбайт | 256 байт — 2 Кбайт |
| Алгоритми шифрування і аутентифікації | Немає | Технологія MIRAGE, DES, 3DES, AES, RSA, ECC | DES, 3DES |

Основними компонентами безконтактних пристроїв є чип і антена. Ідентифікатори можуть бути як активними (з батареями), так і пасивними (без джерела живлення). Ідентифікатори мають унікальні 32/64 розрядні серійні номери.

Системи ідентифікації на базі Proximity криптографічно не захищені, за винятком спеціальних рекомендованих систем.

USB-ключі працюють з USB-портом комп'ютера. Виготовляються у вигляді брелоків. Кожний ключ має 32/64 розрядний серійний номер.

USB-ключі, представлені на ринку:

– eToken R2, eToken Pro — компанія Aladdin Knowledge Systems;

– iKey10xx, iKey20xx, iKey 3000 — компанія Rainbow Technologies;

– ePass 1000, ePass 2000 — фірма Feitian Technologies;

– ruToken — розробка компанії «Актив» і фірми «АНКАД»;

– uaToken — компанія ТОВ «Технотрейд».

USB-ключі — це спадкоємці смарт-карт, через це структури USB-ключів і смарт-карт ідентичні.

Таблиця 7.3

**Характеристики USB-ключів**

| Виріб | Ємність пам'яті, кБ | Розрядність серійного номера | Алгоритми шифрування |
|---|---|---|---|
| iKey 20xx | 8/32 | 64 | DES (ECB и CBC), DESX, 3DES, RC2, RC5, MD5, RSA-1024/2048 |
| eToken R2 | 16/32/64 | 32 | DESX (ключ 120 біт), MD5 |
| eToken Pro | 16/32 | 32 | RSA/1024, DES, 3DES, SHA-1 |
| ePass 1000 | 8/32 | 64 | MD5, MD5-HMAC |
| ePass 2000 | 16/32 | 64 | RSA, DES, 3DES, DSA, MD5, SHA-1 |
| ruToken | 8/16/32/64/128 | 32 | ГОСТ 28147-89, RSA, DES, 3DES, RC2, RC4, MD4, MD5, SHA-1 |
| uaToken | 8/16/32/64/128 | 32 | ГОСТ 28147-89 |

Розглянуті методи аутентифікації (парольна та електронна) мають один недолік — вони насправді аутентифікують не конкретного суб'єкта (особу користувача), а фіксують той факт, що аутентифікатор суб'єкта відповідає його ідентифікатору. Тобто всі перераховані методи не захищені від компрометації аутентифікатора.

## 7.5. Біометрична ідентифікація

Біометрична ідентифікація — це спосіб ідентифікації особи за окремими специфічними біометричними ознаками, властивими конкретній людині [14]. Сучасний рівень розвитку комп'ютерних технологій дозволив використовувати подібні ознаки як основу для ідентифікації людини і ухвалення рішення про можливість доступу до ресурсів комп'ютерних систем.

Серед біометричних механізмів ідентифікації можна виокремити такі:

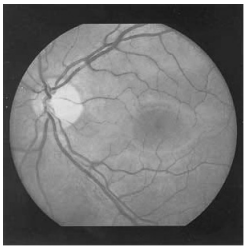
1) за статичними ознаками — те, що практично не змінюється з часом, починаючи з народження людини (фізіологічні характеристики);

2) за динамічними ознаками — поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів у завданнях ідентифікації користувача комп'ютерних систем використовуються такі:

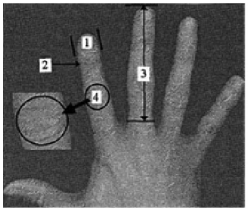
1. Ідентифікація за відбитком пальця. В основу цього методу покладена унікальність малюнка папілярних узорів на пальцях. Ідентифікація побудована таким чином: за допомогою сканера одержують зображення відбитка, потім це зображення за складним алгоритмом перетворюється на спеціальний цифровий код. Далі цей код порівнюється з еталонними кодами, які зберігаються в базі даних.

2. Ідентифікація за розташуванням вен на долоні. Прилад, який прочитує інформацію в цьому випадку, — інфрачервона камера. У результаті на вході програми при формуванні цифрового коду з'являється малюнок вен на руці людини. Не потребує контакту людини з пристроєм для сканування. Має високі показники надійності і достовірності.

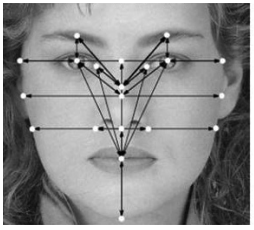


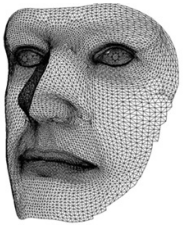
3. Ідентифікація за сітківкою ока. У цьому випадку сканується малюнок кровоносних судин очного дна, який має нерухому структуру, незмінну в часі. Зрозуміло, що цей малюнок спостерігається тільки за певних умов: при скануванні людина дивиться на віддалене світлове джерело і спеціальна камера сканує її очне дно, що у свою чергу може викликати неприємні відчуття у людини. Вважають одним з найнадійніших біометричних методів.

4. Ідентифікація за райдужною оболонкою ока. Малюнок райдужної оболонки ока — унікальний для кожної людини. У цьому методі важлива не лише спеціальна камера, але і надійне програмне забезпечення. Адже саме за допомогою програмного забезпечення із зображення виділяється малюнок потрібної нам райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів.




5. Ідентифікація за формою кисті руки. Цей метод ґрунтується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. При аналізі цього малюнка виконуються вимірювання, за допомогою яких формується відповідний цифровий код.





6. Ідентифікація за формою обличчя. На практиці використовується як двовимірне, так і тривимірне зображення. Причому двовимірне розпізнавання обличчя сьогодні — один з найнеефективніших методів біометрії, тому має обмежене коло застосування або викорис-

товується тільки в сукупності з іншими методами. Розпізнавання за тривимірним зображенням обличчя чимось схоже на метод ідентифікації за формою кисті руки. Тут так само будується тривимірний образ обличчя. Спеціальне програмне забезпечення виділяє з цього образу контури очей, губ та інших частин обличчя. Далі проводяться точні вимірювання між цими контурами. Саме за цими даними будується цифровий код.

Серед динамічних методів, які використовуються для ідентифікації особи користувача, можна назвати такі:

1. Ідентифікація за голосом [15]. Зараз існує безліч програм з розпізнавання голосу. У методі ідентифікації за голосом важливі частотні характеристики голосу людини. Саме за частотними характеристиками і будується цифрова модель.

2. Ідентифікація за почерком. При ідентифікації цим методом звичайно досліджується підпис людини. Перевіряються такі динамічні характеристики, як: графічні параметри, сила натиску на поверхню, швидкість нанесення підпису. За цими характеристиками і будується цифровий код.

3. Ідентифікація за клавіатурним почерком [16]. Цей метод аналогічний ідентифікації за почерком, але замість того, щоб ставити автограф, людині необхідно надрукувати кодове слово. Цифровий код будується за динамікою набору певного слова.

При всьому теоретичному різноманітті можливих біометричних методів тих, що застосовуються на практиці, серед них небагато. Основних методів три — розпізнавання за відбитком пальця, за зображенням особи (двомірному або тривимірному) і за райдужною оболонкою ока.

Сьогодні всі біометричні технології є імовірносними і нерідко ця обставина служить основою для не дуже коректної критики біометрії.

Важко не погодитися, що біометричні технології надійніші і зручніші ніж ті засоби захисту, які широко застосовувалися до теперішнього часу [17]. Але, незважаючи на активну діяльність протягом останніх років у напрямку розробки та вдосконалення методів ідентифікації користувачів з метою управління доступом до ресурсів інформаційних систем, надійність та стійкість існуючих систем недостатня для потреб сьогодення.

## 7.6. Комплексна (або багатофакторна) ідентифікація

Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку [18].

Сьогодні існують комбіновані системи таких типів:

– системи на базі безконтактних смарт-карт і USB-ключів;

– системи на базі гібридних смарт-карт;

– біоелектронні системи.

Таблиця 7.4

**Основні функції комбінованих систем**

| Функція | Комбіновані системи | | |
|---|---|---|---|
| | На базі безконтактних смарт-карт і USB-ключів | На базі гібридних смарт-карт | Біоелектронні системи |
| Ідентифікація і аутентифікація комп'ютерів | Є | Є | Є |
| Блокування роботи комп'ютерів і розблокування при пред'явленні персонального ідентифікатора | Є | Немає | Є |
| Ідентифікація і аутентифікація співробітників при їх доступі в будівлю, приміщення (з нього) | Є | Є | Немає |
| Зберігання конфіденційної інформації (ключів шифрування, паролів, сертифікатів і т. д.) | Є | Є | Є |
| Візуальна ідентифікація | Немає | Є | Є |

*Безконтактні смарт-карти і USB-ключі.* У корпус брелока USB-ключа вбудовується антена і мікросхема для створення безконтактного інтерфейсу. Це дозволить організувати управління доступом у приміщення і до комп'ютера, використовуючи один ідентифікатор. Ця схема використовування ідентифікатора може виключити ситуацію, коли співробітник, покидаючи робоче місце, залишає USB-ключ

у роз'ємі комп'ютера, що дозволить працювати під його ідентифікатором. У разі ж, коли не можна вийти з приміщення, не використовуючи безконтактний ідентифікатор, цієї ситуації вдасться уникнути.

Сьогодні найбільш поширено два ідентифікатори подібного типу:

– RfiKey — компанія Rainbow Technologies;

– eToken PRO RM — компанія Aladdin Software Security R.D.

Виріб RfiKey підтримує інтерфейс USB 1.1/2.0 і функціонує зі зчитувачем HID Corporation (PR5355, PK5355, PR5365, MX5375, PP6005) і російської компанії Parsec (APR-03Hx, APR-05Hx, APR-06Hx, APR-08Hx, H-Reader).

eToken RM — USB-ключі і смарт-карти eToken PRO, доповнені пасивними RFID-мітками.

RFID-технологія (Radio Frequency Identification, радіочастотна ідентифікація) є найпопулярнішою сьогодні технологією безконтактної ідентифікації. Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом так званих RFID-міток, що несуть ідентифікаційну і іншу інформацію.

З сімейства USB-ключів eToken RFID-міткою може бути доповнений тільки eToken PRO/32K. При цьому треба враховувати обмеження, обумовлені розмірами ключа: RFID-мітка повинна бути не більше 1,2 см в діаметрі. Такі розміри мають мітки, що працюють на частоті 13,56 МГц, наприклад, виробництва Ангстрем або HID.

*Гібридні смарт-карти.* Гібридні смарт-карти містять різнорідні чипи. Один чип підтримує контактний інтерфейс, інший — безконтактний. Як і в разі гібридних USB-ключів, гібридні смарт-карти вирішують два завдання: доступ у приміщення і доступ до комп'ютера. Додатково на карту можна нанести логотип компанії, фотографію співробітника або магнітну стрічку, що робить можливим повністю замінити звичайні пропуски і перейти до єдиного «електронного пропуску».

Смарт-карти подібного типу розробляють багато компаній: HID Corporation, Axalto, GemPlus, Indala, Aladdin Knowledge Systems та ін.

У Росії компанією Aladdin Software Security R.D. розроблена технологія виробництва гібридних смарт-карт eToken PRO/SC RM. У них мікросхеми з контактним інтерфейсом eToken PRO вбудовуються в безконтактні смарт-карти. Смарт-карти eToken PRO можуть бути доповнені пасивними RFID-мітками виробництва HID/ISOProx II, EM-

Marine (частота 125 кГц), Cotag (частота 122/66 кГц), Ангстрем / КИБИ-002 (частота 13,56 МГц), Mifare і інших компаній. Вибір варіанту комбінування визначає замовник.

*Біоелектронні системи.* Як правило, для захисту комп'ютерних систем від несанкціонованого доступу застосовується комбінація з двох систем — біометричної і контактної на базі смарт-карт або USB-ключів.

Найчастіше як біометричні системи застосовують системи розпізнавання відбитків пальців. При збігу відбитку з шаблоном дозволяється доступ. До недоліків такого способу ідентифікації можна віднести можливість використовування муляжу відбитку.

Досягти підвищення надійності та точності автоматизованих систем ідентифікації користувачів можна за рахунок об'єднання використання біометричних характеристик разом з класичними способами ідентифікації користувачів (наприклад, парольний захист, PIN-код, використання різноманітних карт і т. д.) [19].

Актуальною вбачається проблема розробки і дослідження комплексних систем, що використовують для прийняття рішення щодо доступу до інформаційних систем кілька біометричних характеристик користувача (наприклад, використовувати разом особливості клавіатурного почерку, голосу, динаміки роботи користувача з маніпулятором «миша» або використання відбитків декількох пальців і т. д.) [20; 21]. Деякі виробники вже розпочали інтеграцію двох методів розпізнавання облич, включаючи дво- і тривимірні зображення.

## 7.7. Висновки

На основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів інформаційних систем, можна впевнено сказати, що парольний захист сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах світового масштабу. Проте без використання інших механізмів захисту парольний захист сам по собі не є надійним, оскільки не може

забезпечити серйозного захисту. Досить поширеними як ідентифікатори є також різноманітні електронні ключі (токени, карти тощо). Але слід зауважити, що останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні завдання доступу до інформаційних систем.

Таким чином, розглянувши технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі в міру зростання обчислювальних потужностей все більш запитаним буде саме вживання систем комплексної (або багатофакторної) ідентифікації та аутентифікації, що дозволить уникнути людських помилок, пов'язаних із застосуванням слабких паролів, і посилити вимоги до парольної аутентифікації.

Щодо вибору системи ідентифікації безпосередньо у кожній окремій ситуації користувач повинен: об'єктивно оцінити співвідношення цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації/аутентифікації, яке він обирає (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від «кого» потрібно захищати). Але безперечною порадою є обов'язкове використання комплексної системи ідентифікації, яка поєднує кілька підходів до вирішення завдання доступу до інформаційних ресурсів комп'ютерних систем.

# РОЗДІЛ 8

# НАУКОВІ Й ТЕХНОЛОГІЧНІ АСПЕКТИ ПОБУДОВИ КОМП'ЮТЕРНОЇ МЕРЕЖІ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЮРИДИЧНА АКАДЕМІЯ УКРАЇНИ ІМЕНІ ЯРОСЛАВА МУДРОГО»

Трансформації комунікаційного поля (частиною якого є, наприклад, віртуальні інформаційні середовища), темп яких має виразну тенденцію до зростання, представляють певний виклик для сучасної педагогіки. Так, світоглядна картина студентів у сучасних умовах (на відміну від ситуації, що мала місце ще кілька десятиліть тому) переважно визначається інформацією, яку одержують з джерел, не пов'язаних із вищою школою. Вплив трансформацій комунікаційного поля на навчальний процес є різноманітним; він виявляється на різних рівнях. Відомим будь-якому педагогу прикладом є імітація самостійної роботи з літературою методом «Copy-Paste». Цей приклад показує, що сучасне комунікаційне середовище істотно знижує ефективність багатьох педагогічних прийомів, що склалися в індустріальну фазу розвитку цивілізації, тобто її вплив на навчальний процес є амбівалентним. Надаючи величезні можливості для пошуку потрібної інформації, це середовище в той же час багато в чому обмежує ефективність традиційних стимулів для її засвоєння. «Все знає Google» — роль вищої школи як «джерела знань» падає, і ця тенденція здатна тільки зміцнюватися. Постіндустріальна концепція вищої освіти неминуче прийде до необхідності змістити акцент з поняття «компетентність» на поняття «креативність», бо немає сенсу прищеплювати

навички, які застаріють через кілька років. Набагато важливіше прищепити студентам навички вчитися самостійно, в тому числі навички роботи зі значними обсягами інформації, включаючи її пошук, критичний аналіз і переосмислення. Тобто на перший план при підготовці за будь-якою спеціальністю повинні виходити дисципліни, які навчають навичкам «існування» в сучасному інформаційному середовищі. Однією з таких навичок, наприклад, є використання добре розвинених методів перевірки достовірності інформації та оцінки її якості, що внаслідок значних обсягів доступної інформації можна здійснити практично в будь-якому випадку. Раніше такого роду методи використовувалися переважно фахівцями в галузі розвідки і контррозвідки, але з розвитком сучасних інформаційних теорій їх використання стає інструментом представників практично будь-якої професії. Проектування віртуальних середовищ саморозвитку вимагає, на нашу думку, доповнення, поновлення і збагачення цього ряду такими медіаторами, як, скажімо, Web-сайт, Internet, соціальні мережі, мережеве співтовариство, яке утворилося в соціальній мережі, блозі, групі дистанційного навчання тощо. Всі ці інтерактивні знаряддя безумовно відіграють роль медіаторів, а саме в посередницькому акті і прихована таємниця розвитку, таємниця перетворення реальної форми в ідеальну. Вона, у свою чергу, є плинною, рухливою, такою, яка багато в чому залежить від суб'єкта розвитку, і тому цей процес набуває рис саморозвитку. Вкажемо на деякі принципові психолого-педагогічні проблеми, вирішення яких необхідне для проектування віртуального середовища саморозвитку. Так, специфіка віртуального освітнього простору сприяє поляризації навчальної діяльності від абсолютно несамостійної до повного взяття учнями на себе функцій управління навчальною діяльністю. В останньому випадку всі психологічні механізми навчання працюють інакше, що, у свою чергу, веде до принципової зміни сучасної парадигми освіти [1]. Очевидно, з одного боку, що в умовах дистанційного навчання віддаленість і часова асинхронність заважають поточному контролю за процесом. З другого боку, готовність до навчання і відповідна мотивація психологічно обґрунтовано будуються на основі проблематизації і потребують додаткової постійної підтримки. Навчальні співтовариства і комунікація в них

вимагають «багаторівневої інтерактивності» і психологічно обґрунтованого балансу синхронності — асинхронності спілкування, коректно вибудуваної діалогової взаємодії.

## 8.1. Завдання інформаційної інфраструктури університету

Названі проблеми є відомими і такими, що мають впливати на розбудову засобів навчання в технічній і віртуальній сферах. Розглянемо, яким чином реалізуються ідеї навчання через інформаційні технології в Національному університеті «Юридична академія України імені Ярослава Мудрого».

Університет є відомим регіональним центром з впровадження комп'ютерних технологій навчання та наукової роботи. Матеріальну базу цього процесу становить об'єднання наявного парку з понад 800 персональних ЕОМ у локальну мережу університету та забезпечення їх виходу в глобальну мережу Internet. Це дало можливість створити і розвивати сучасну комп'ютеризовану бібліотеку, електронні читальні зали, комп'ютерні аудиторії, комп'ютеризувати робочі місця у навчальному відділі, деканатах, на кафедрах, у допоміжних підрозділах та використовувати наявні програмні й інформаційні ресурси, обсяг яких має тенденцію до динамічного зростання. Локальна мережа охопила всі навчальні корпуси, всі гуртожитки, спортивний комплекс, культурно-просвітницький центр — Палац студентів, пансіонати університету тощо. У своїй основі мережа має структуру територіально розгалужених оптоволоконних ліній зв'язку.

Мультисервісна оптоволоконна локальна мережа університету є комплексом програмного і технічного забезпечення, що призначений для підтримки автоматизації як навчального процесу, так і процесу управління університетом у цілому. Для реалізації цієї мети створені Центр інформаційних технологій (ЦІТ); Центр інформаційного та технічного забезпечення навчального процесу; уточнені завдання Лабораторії технічних засобів освіти; розбудовується перспективна

електронна бібліотека з рядом сучасних сервісів. У цілому поставлено завдання на створення інтегрованого простору знань для цілей навчання студентів спеціальності «правознавство» та інших, за якими йде підготовка в університеті. Цей простір знань має бути, безумовно, реалізований в електронному вигляді і спиратися на інфраструктуру мультисервісної оптоволоконної локальної мережі університету [2; 3; 4; 5].

Основними завданнями, що поставлені перед інформаційною інфраструктурою університету, є:

– організація, розвиток, підтримка роботоздатності локальної мережі університету;

– розвиток зовнішніх каналів зв'язку університету з Internet;

– організація та підтримка роботи серверів (поштових, доступу до каналів зв'язку, Web-серверів, ftp-серверів тощо);

– створення навчального інформаційного порталу університету;

– забезпечення зв'язку між усіма абонентами мережі за допомогою протоколу ICQ та файлообмінних послуг;

– надання послуг IP-телефонії, IPTV, електронної пошти та телефонного зв'язку для абонентів мережі;

– оперативний облік успішності та відвідувань студентів;

– автоматизація проведення модульного контролю знань;

– забезпечення доступу до сайту бібліотеки та бібліотечного каталогу;

– забезпечення доступу до електронних копій раритетних видань;

– доступ до інформаційної бази правових документів та інформації, яка накопичена в науково-дослідних інститутах Національної академії правових наук України;

– доступ до серверів наукової інформації за підпискою eLIBRARY.ru, правової бази даних «Мега-НаУ», електронних версій «Вісника Московського державного університету», бази наукових видань EBSCO Host Research тощо;

– підтримка сайту університету та створення Web-сторінок факультетів, кафедр, окремих викладачів та підрозділів;

– виконання навчальних функцій у комп'ютерних класах, під'єднаних до мережі;

– організація системи дистанційного навчання в університеті;

– проведення сеансів відеотелеконференцзв'язку з абонентами в інших країнах;

– надання доступу до Internet для пошуку і використання наукової і учбової інформації у навчальній і науковій діяльності;

– постійне вдосконалення концепції і методики подання інформації в електронному освітньо-науковому інформаційному просторі університету;

– поетапна автоматизація інформаційних зв'язків структурних підрозділів університету, які виконують основну навчальну та наукову роботу;

– перегляд зображень деяких Web-камер, встановлених в університеті;

– встановлення нормативних вимог до роботи користувачів мережі і контроль за їхнім дотриманням;

– забезпечення інформаційної безпеки мережі;

– ведення різноманітних обліків та багато інших завдань.

До складу Центру інформаційних технологій входять такі підрозділи: Лабораторія інформаційних технологій правової освіти; Лабораторія організації дистанційної освіти; Лабораторія розвитку інформаційно-освітнього середовища академії.

До складу Центру інформаційного та технічного забезпечення навчального процесу входять підрозділи: Лабораторія інформаційно-аналітичного забезпечення навчального процесу; Лабораторія локальних комп'ютерних мереж; Лабораторія технічних засобів навчання.

## 8.2. Апаратна складова локальної мережі

Центральною ланкою забезпечення та підтримки єдиного простору інформаційних ресурсів є апаратне забезпечення, що зосереджено в Центрі інформаційних технологій. У технічному плані магістраль є ієрархічною структурою з централізованим управлінням

і ефективним наданням інформаційних сервісів. Топологія мережі описується схемою «сніжинка». Це означає, що до центрального сервера під'єднано множину локальних мереж, виконаних за схемою «зірка», що територіально розміщені в різних навчальних корпусах і підрозділах.

Деякі вузли мережі винесені від головного корпусу на відстань до 20 км (з'єднання з ними виконано через проміжну мережу провайдера). Оптоволоконних (оптичних) кабелів прокладено загальною довжиною 11 500 м, кабелю «звита пара» категорії 5е прокладено 18 000 м, і ця довжина збільшується за рахунок розгалуження мережі в процесі її розвитку. Загальна кількість робочих станцій у мережі перевищує 800 одиниць і в подальшому ця кількість буде збільшуватись. На рис. 8.1 показана загальна інфраструктура мережі. До мережі університету під'єднані комп'ютерні класи, що є у всіх гуртожитках. Загальна довжина інформаційних магістралей перевищує 40 км.

У Центрі інформаційних технологій встановлений головний сервер мережі — це багатофункціональний двопроцесорний сервер HP ProLiant DL380 з двома процесорами Intel Xeon 3 GHz, виготовленими за технологією EM64T. Оперативний запам'ятовуючий пристрій має ємність 2 Gb, дисковий масив має ємність 504 Gb. Дисковий масив має перспективи нарощення своєї ємності до 1 Tb. У шафі сервера встановлені також оптобокс, чотири медіаконвертори D-Link, два керовані комутатори D-Link та один звичайний комутатор D-Link, патч-панель і модеми. У головному корпусі є також важливі вузли, до яких прокладені оптичні лінії і встановлені медіаконвертори, це бібліотека та АТС. У інших будівлях, до яких є оптичне підключення, встановлені свої медіаконвертори і виконано розгалуження до всіх комп'ютерів користувачів кабелем «звита пара». Взагалі у мережі встановлено понад 30 одиниць медіаконверторів D-Link та 60 комутаторів. Швидкість передачі даних за оптичними каналами становить 1 Gb/s, за лініями «звита пара» — до 100 Kb/s. На території головного корпусу університету функціонує три хот-споти, мережі Wi-Fi, що забезпечують бездротове підключення користувачів до локальної мережі університету [6].

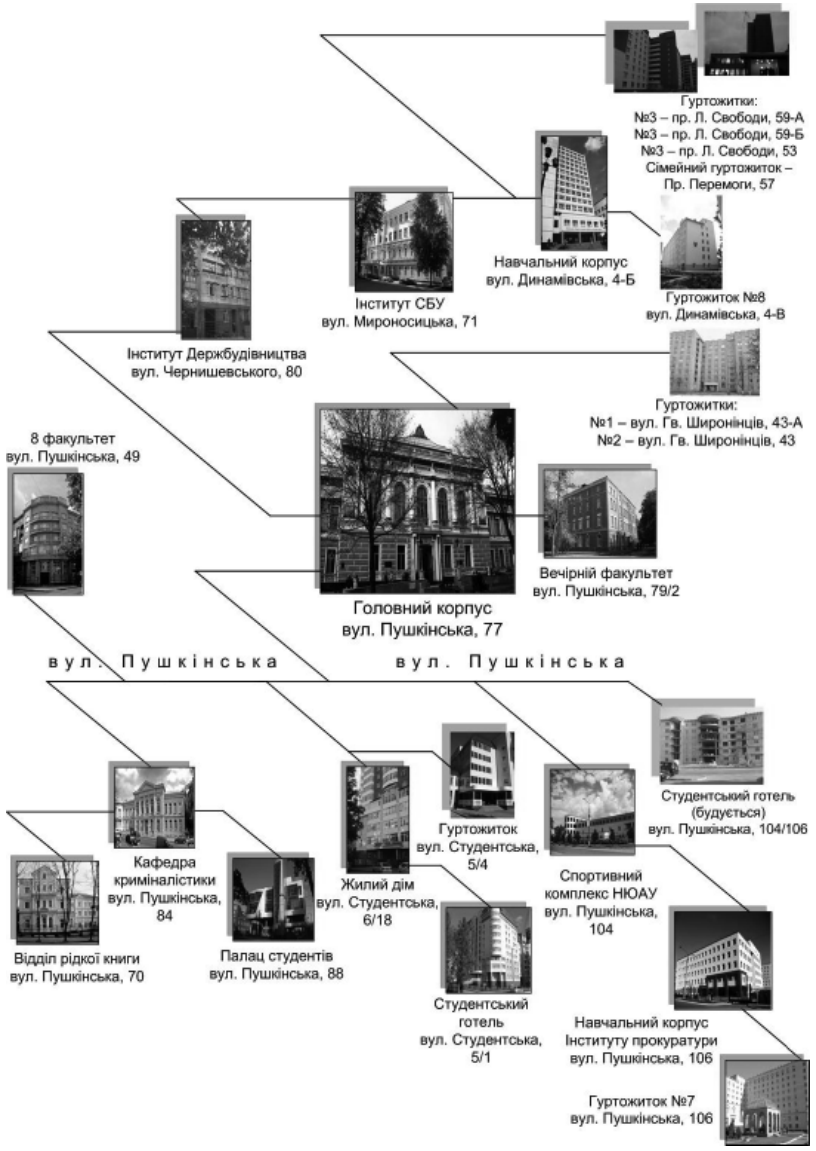



*Рис. 8.1.* Структура мультисервісної оптоволоконної інформаційної мережі університету

Інформаційна мережа академії є доменом глобальної мережі Internet jur-academy.kharkov.ua. Централізоване обслуговання мережі передбачає цілеспрямоване управління ресурсами та захист від несанкціонованого доступу та руйнівної дії зловмисних програм.

Створена мережа є універсальним середовищем передачі і збереження інформації, вона потенційно може забезпечити будь-які сучасні і перспективні інформаційні послуги і саме тому офіційно вона отримала назву «єдина мультисервісна оптоволоконна інформаційна магістраль».

## 8.3. Структура інформаційного простору

Привабливість інформаційної інфраструктури університету для користувачів у першу чергу зумовлена її наповненням. В інформаційному забезпеченні мережі можна виокремити кілька великих розділів: адміністративний; навчальний; дистанційної освіти; презентаційний. Вони містять ряд інформаційних ресурсів, що використовуються в поточній діяльності та навчанні. Для навчання (як традиційного, так і електронного) використовуються в першу чергу такі компоненти, як: інформаційні ресурси електронної бібліотеки ИРБИС; нормативна база документів серверу Верховної Ради, що оновлюється двічі на добу, доступ до якої існує завдяки сприянню Національної академії правових наук України; ftp-сервер навчальних ресурсів, розподілених за дисциплінами; навчальні електронні інформаційні комплекси в середовищі Moodle для е-освіти та дистанційної освіти; доступ до раритетних видань; знанняорієнтована навчально-консультаційна інформаційна правова система JURONT (юридична онтологія) [7; 8; 9]; навчальна підсистема АСУ університету з множиною навчальних ресурсів, у тому числі відеоресурсів та інші електронні джерела. Також передбачено, що на кожному робочому місці в мережі можна отримати весь спектр загальних інформаційних послуг: доступ до загальних ресурсів мережі Internet як навчальних, пізнавальних, так і розважальних; доступ до серверів наукової інформації у мережі

Internet; використання зон Wi-Fi в університеті; сервіс ICQ для обміну миттєвими повідомленнями; IP-телефонія та відеозв'язок через Internet із застосуванням програми «Skype»; огляд Web-камер, що встановлені в приміщеннях університету; цифрове телебачення в обсязі програм, що надає провайдер (на 2012 рік — це близько 100 каналів); використання досить об'ємних інформаційних ресурсів міської мережі провайдера — ресурсів піринговой мережі DC; захист інформації у мережі програмними та апаратними засобами, що забезпечує Центр інформаційного та технічного забезпечення навчального процесу; інші сервіси для управління навчальним процесом та господарською діяльністю. Названі послуги перекривають усі сучасні інформаційні потреби користувачів і розгорнуті на базі високопродуктивного устаткування. За необхідності при виникненні запитів користувачів у мережі будуть розгорнуті будь-які інформаційні сервіси, тому що апаратна інфраструктура побудована таким чином і з такою перепускною спроможністю, що здатна забезпечити всі існуючі і перспективні сервіси. Також слід зазначити, що користування всіма послугами локальної мережі є безкоштовним для всіх користувачів у навчальних корпусах і частково на платній основі (за ресурси мережі Internet) у гуртожитках університету.

Презентаційна частина інформаційних ресурсів представлена двома Web-сайтами — це офіційний сайт університету і сайт наукової частини. Обидва є досить розгалуженими, постійно підтримується їх актуальність завдяки своєчасному оновленню інформації. Сайт університету представлений трьома мовами.

## 8.4. Навчальна інформація в мережі

Щодо навчального розділу мережі, то слід зазначити, що у зв'язку з переходом до варіативної системи навчання з урахуванням кредитно-модульної складової в сучасних вищих навчальних закладах виникли значні зміни в процесі поширення та застосування навчально-методичної літератури — збільшились обсяги, ускладнилися зв'язки та збільшився темп оновлення навчальних матеріалів. При цьому ви-

никла потреба в оперативній та загальнодоступній інформаційній підтримці цих процесів.

Застосування Internet для інформаційного забезпечення університету є ефективним, тому що більшість студентів мають практичну можливість доступу до мережі Internet у гуртожитках і місцях свого проживання та мають досвід її використання. Окрім того, функціонування навчального розділу спирається на ресурси і можливості комп'ютерної мережі університету. Доступ до навчально-методичних матеріалів студенти можуть отримати із внутрішньої мережі університету. Також безумовну практичну цінність розділ навчально-методичної літератури інформаційної системи має для студентів заочної форми навчання. Відповідно до політики захисту авторських прав розробників навчально-методичних матеріалів доступ до всієї номенклатури матеріалів користувачі мають у локальній мережі академії, а із мережі Internet — частково, за наявності реєстрації користувача у внутрішній мережі [10; 11]. Ще одна болюча проблема інформаційних навчальних ресурсів — підтримка їх у актуальному стані. Це пов'язано з тим, що наповнення учбових дисциплін змінюється дуже швидко, й інформаційні ресурси у мережі необхідно приводити у відповідність до цих змін. Актуалізація наповнення потребує таких самих зусиль, як при створенні нових курсів. Але відповідна технологія ще не напрацьована і не підтримана нормативною документацією. Проблема полягає в іншій організації робочого часу викладачів і його обліку.

Основним джерелом навчальної інформації, що повністю відповідає програмі підготовки студентів та робочим планам дисциплін, є ftp-сервер навчальних ресурсів. Структура інформації на ftp-сервері складається з набору окремих папок, які названі в точній відповідності до найменувань дисциплін. До електронних папок може мати доступ кожен користувач мережі (адреса ftp://web.nlau.net.ua). У них розміщені електронні навчальні матеріали, підручники, методичні вказівки, тести, питання до заліків і екзаменів, теми курсових робіт тощо. Продовжується наповнення і оновлення цих ресурсів необхідною інформацією. Їх використання значно спрощує студентам можливість знайти і скористатися необхідними для навчання джерелами, що підвищує рівень підготовки спеціалістів.

## 8.5. Організація дистанційної та електронної освіти в Національному університеті «Юридична академія України імені Ярослава Мудрого»

Дистанційне навчання (англ. distant learning) — засіб реалізації процесу навчання, в основу якого покладено використання сучасних інформаційних та телекомунікаційних технологій, що дозволяють навчатися на відстані без безпосереднього, особистого контакту між викладачем і учнем.

Під терміном «дистанційне навчання» також розуміють:

– цілеспрямоване і методично організоване керівництво навчально-пізнавальною діяльністю осіб, що знаходяться на відстані від освітнього центру, яке відбувається завдяки електронним і традиційним засобам зв'язку;

– процес отримання знань і навичок за допомогою спеціалізованого освітнього середовища, яке засноване на використанні інформаційних технологій (ІТ), що забезпечує обмін навчальною інформацією на відстані і реалізує систему супроводу та адміністрування навчальним процесом.

Спочатку дистанційне навчання здійснювалось у формі писемного спілкування, тобто розв'язані завдання відсилались поштою. На сучасному етапі дистанційне навчання здійснюється за допомогою Internet, доступу до мережних баз даних тощо.

Сучасна дистанційна освіта ґрунтується на використанні таких елементів:

– середовища передачі інформації (пошта, телебачення, радіо, інформаційні комунікаційні мережі);

– методів, що реалізують передачу і засвоєння користувачем навчальної інформації, які залежать від технічного середовища обміну і відображення інформації.

Дистанційна освіта стає більш популярною у вищій школі, тому що вона має ряд незаперечних переваг. Зазначимо найбільш значущі [12; 13].

*Активізація позиції учня*. Дистанційне навчання передбачає гнучке й евристичне управління самостійною роботою студента, що дозволяє студенту активізувати особисту позицію за певним спектром проблем, самостійно планувати час, що відводиться на заняття, а також багато в чому визначати зміст навчального процесу.

*Підвищення мотивації учнів до самоосвіти та самовдосконалення.* Дистанційне навчання спрямоване на підвищення рівня професійної мотивації студентів, розширення їх загального світогляду.

*Формування навичок самостійної роботи з використанням сучасних комп'ютерних технологій*. Комп'ютеризація освітнього процесу, безперечно, формує комп'ютерну грамотність як одну з основних компетенцій випускника вищого навчального закладу.

*Підвищення ефективності організації навчально-виховного процесу в рамках класно-урочної системи.* Сучасні комп'ютерні інформаційні технології, зокрема дистанційне навчання, дозволяють багато в чому подолати такі недосконалості класно-урочної системи, як відсутність зворотного зв'язку між викладачем і студентом, складність організації самостійної роботи студентів, відсутність у викладачів можливості опитати кожного студента на занятті, дефіцит навчального матеріалу і т. д.

*Оптимізація процесу навчання для студентів-заочників.* Правильно організована система дистанційного навчання дозволить студентам ознайомитися або отримати навчальний матеріал безпосередньо з дому та/або у випадку неможливості приїзду на заняття автоматизувати систему контролю отриманих знань, надати гнучкий графік навчання та багато іншого.

*Поліпшення загального психологічного клімату на заняттях у класі.* При використанні елементів дистанційного навчання студенти можуть повною мірою продемонструвати свої знання, вміння, навички в режимі автономної роботи, що сприяє зниженню рівня тривожності і створенню ситуації успіху на занятті. Відносини між викладачем і студентом стають більш довірчими, бо про можливі помилки студента буде обізнаний тільки викладач, а не весь клас.

*Індивідуалізація та диференціація процесу навчання*. Впровадження елементів дистанційного навчання в навчально-виховний процес сприяє, з одного боку, індивідуалізації цього процесу, оскільки про-

грама багато в чому визначається відповідно до психолого-педагогічних характеристик особистості учня. З другого боку, в основі дистанційного навчання лежить принцип диференціації педагогічного процесу, тому що студентам пропонують різні способи самоконтролю.

*Розширення можливостей контролю зі зворотним зв'язком і діагностикою.* Дистанційне навчання передбачає комплексну діагностику та моніторинг процесу навчання, отримуваних знань, умінь і навичок із заданої теми.

*Здійснення самоконтролю і самокорекції.* Ця технологія дозволяє формувати й удосконалювати вміння та навички самостійної роботи студентів. Також системи дистанційного навчання істотно допомагають в організації процесу навчання студентів-інвалідів, які можуть отримати якісну освіту, не виходячи з дому. Нові інформаційні технології дозволяють таким студентам брати активну участь у громадському житті та долучатися до нових знань з можливістю постійних он-лайн консультацій і контролю сформованості цих знань.

Сьогодні найперспективнішим напрямком розвитку дистанційної освіти є інтерактивне спілкування викладача та студента засобами інформаційних комунікаційних мереж, у тому числі за допомогою Internet-технологій [13].

Уже сьогодні дистанційна освіта претендує на особливу форму навчання (поряд із денною, заочною, вечірньою та екстернатом) [14].

Використання інформаційних технологій при організації дистанційної освіти дозволяє:

– зменшити витрати на проведення навчання (не вимагає витрат на оренду приміщень, витрат на дорогу до місця навчання як викладачів, так і студентів, тощо);

– проводити навчання значної кількості людей одночасно;

– підвищити якість освіти за рахунок використання сучасних засобів, великих електронних бібліотек тощо;

– створити єдиний освітній простір, що дуже важливо для самого процесу дистанційної освіти, адаптації до неї, зручності користування тощо.

Дистанційне навчання з використанням комп'ютерних та інформаційно-комунікаційних технологій, як правило, реалізується в таких формах:

– телеконференції — листування електронною поштою (e-mail), засноване на списках розсилки як альтернативи звичайному листуванню. Для такої форми навчання є характерним досягнення лише базових завдань освіти;

– чат-заняття — навчальні заняття з використанням чат-технологій: обмін невеликими текстовими повідомленнями у реальному часі. Такі заняття проводяться одночасно, щоб усі учасники мали можливість спільного доступу до чату. Чат як засіб спілкування може використовуватися як окремо, так і разом з іншими формами навчання, доповнюючи їх;

– Web-заняття — це збірне поняття для дистанційних занять, які проводяться у вигляді конференцій, семінарів, ділових ігор, форумів, лабораторних та контрольних робіт, практикумів, он-лайн тестувань, опитувань й інших форм навчальних занять, що реалізуються за допомогою засобів та технологій Internet, а саме: за допомогою технологій World Wide Web (WWW) нового покоління, що забезпечують інтерактивність спілкування. Саме на таку форму навчання наразі покладають найбільші сподівання, як на дуже зручну, невибагливу до технічного устаткування, гнучку в управлінні та інтуїтивно зрозумілу у використанні особами різного віку та освіченості. Основним засобом інтерактивного спілкування учнів з викладачем та між собою під час використання Web-технологій є форум — технологія обміну текстовими повідомленнями. На відміну від чату, — більш простої форми спілкування, — форуми дозволяють обмінюватися повідомленнями асинхронно, а отже, є досить тривалими в часі; форуми і повідомлення в ньому можуть мати як приватний, так і публічний характер; організовуються за конкретними темами, у яких зручно задавати запитання та шукати відповіді на раніше задані запитання; дають можливість коментувати чиєсь запитання чи відповідь на нього, висловлюючи при цьому, наприклад, власну думку з тієї чи іншої проблеми. Форуми є перш за все джерелом практичних знань, на відміну від звичайних Web-занять, адже форуми створюються на «історії» живого спілкування з найбільш актуальних питань, що, як правило, мають практичних характер;

– аудіо-, відеоконференції (аудіокасти, Web-касти, вебінари) — форма навчання за допомогою найсучасніших технологій передачі звуку та зображення. Дозволяють проводити практичні «зустрічі» викладачів та слухачів на великій відстані, також дозволяють зібрати

значну аудиторію, але вимагають присутності слухача біля технічних засобів відтворення такого спілкування у певний, заздалегідь заданий час. Можуть організовуватися як в односторонньому порядку, так і з використанням зворотного зв'язку, тобто бути інтерактивними [15].

Отже, в Національному університеті «Юридична академія України імені Ярослава Мудрого» існує потенційна можливість реалізації всіх вищезазначених форм за допомогою створюваних у Центрі інформаційних технологій навчальних електронно-інформаційних комплексів (НЕІК) [16; 17] з дисциплін навчального плану, які наділені такими можливостями:

1) здатні забезпечити більш поглиблене вивчення студентом певної навчальної дисципліни, оскільки включають не лише текст підручника, а й інші джерела, які в цілому дають змогу це забезпечити;

2) виключають необхідність у використанні значного обсягу паперового матеріалу (підручників, коментарів, збірників постанов ВСУ, матеріалів судової практики тощо);

3) можуть використовуватись: а) при підготовці студентами рефератів, виконанні контрольних і написанні курсових робіт, наукових студентських доповідей; б) при відпрацюванні пропущених практичних занять, проведенні групових та індивідуальних консультацій; в) для індивідуальної роботи і самостійної перевірки отриманих у процесі вивчення НЕІК знань, підготовки для складання іспитів та заліків;

4) включають досить багато необхідної для отримання якісної освіти навчальної інформації, є дуже компактними і можуть постійно поповнюватися необхідними матеріалами без використання для цього досить громіздкого процесу опублікування підручників чи навчально-методичних посібників;

5) можуть використовуватись для перевірки знань студентів у процесі модульного контролю знань, поточного контролю знань та вибіркового контролю (ректорські перевірки);

6) доступ до них може бути забезпечений як шляхом використання існуючих у навчальному закладі комп'ютерних мереж, так і мережі Internet, у тому числі мобільних пристроїв — планшетів, смартфонів тощо.

Особливо хотілось би наголосити на такому: НЕІК можуть забезпечити найвищу актуальність навчальної інформації за рахунок того, що за змістом кожного розділу може слідкувати відповідальний ви-

кладач, і зміни до змісту він може вносити у НЕІК постійно (щоденно) з кафедральних або особистих комп'ютерів (через мережу Internet) [18; 19]. Це особливо актуально в ситуації постійної зміни нормативно-правової бази. На поточний момент кілька комплексів є повністю завершеними [20; 21].

Отже, можна констатувати, що Університет потенційно готовий до впровадження дистанційної форми навчання з використанням інформаційних технологій на базі створеної в Центрі інформаційних технологій (ЦІТ) мультисервісної оптоволоконної мережі та основних інформаційних послуг, що в ній надаються.

## 8.6. Інформація з раритетних джерел у мережі

Університет має унікальну підбірку раритетних видань, що зберігаються у Відділі рідкісних видань наукової бібліотеки. Одним із пріоритетних напрямів діяльності ЦІТ визначено завдання зі створення електронних копій раритетних видань університету для забезпечення в подальшому вільного доступу всіх охочих до цих видань. Складно перебільшити значимість можливості використання дослідниками цих джерел.

З огляду на масштаби проекту було розроблено стратегічний план із упровадження новітніх технологій у процес створення електронної бібліотеки, яка врешті має вмістити не лише всі оцифровані копії раритетних видань, але й найактуальніші, найважливіші сучасні праці науковців Університету, а згодом і весь навчальний та науковий фонд бібліотеки.

Таке амбіційне завдання вимагає залучення найкращих фахівців та використання найсучасніших інформаційних технологій, тому воно було доручене колективу ЦІТ, до числа співробітників якого також входять студенти університету.

Центр інформаційних технологій створив технологічну основу для створюваної бібліотеки, яка розмістилася на серверах ЦІТ [22].

Для роботи над Бібліотекою було використано більше 15 сучасних сканерів, які працювали і продовжують працювати щоденно з ранку до вечора, декілька фото- та відеокамер для роботи над дуже старими

та громіздкими книгами, які практично неможливо оцифрувати на планшетному сканері.

Окрім штатних співробітників ЦІТ, до роботи над книгами залучено охочих та відповідальних студентів, яким запропонували роботу у ЦІТ на волонтерській основі. Ці студенти отримують не лише безцінний досвід роботи із сучасною комп'ютерною технікою та надсучасною комп'ютерною мережею, але й мають змогу долучитися до перлів правової думки, до столітніх фоліантів, із якими їм довелося працювати. Захоплення від такого спілкування із «сучасним» та «минулим» притягує щоразу все більше нових охочих.

Отже, для впорядкування та обліку роботи над рідкісними виданнями та з метою підвищення контролю якості електронних версій книг було вирішено створити комплекс спеціалізованого програмного забезпечення.

До цього комплексу увійшло кілька модулів:

1) серверний модуль;

2) бази даних;

3) модуль адміністратора;

4) модуль для сканування рідкісного видання;

5) модуль для перевірки оцифрованого матеріалу;

6) модуль для автоматизованого графічного оброблення цифрового матеріалу;

7) модуль компіляції та контролю якості;

8) модуль для створення та редагування електронного каталогу;

9) модуль для завантаження електронної копії раритетного видання до серверу ЦІТ;

10) Web-модуль, який працює в режимі електронного каталогу та повнотекстової бази електронних копій раритетних видань.

Таким чином, розробивши повний комплекс програмних засобів для створення Бібліотеки електронних копій раритетних видань, ЦІТ перейшов на якісно новий рівень роботи над рідкісними фоліантами.

Із упровадженням новітніх технологій існує можливість створювати, оброблювати, зберігати та користуватися набагато кращими (ніж це біло раніше) електронними копіями книжок. Підвищення якості контенту електронної бібліотеки стало можливим завдяки використ-

танню сучасного обладнання та налагодженої технології отримання цифрових матеріалів.

Створення електронних копій видань — тривалий та кропіткий процес, виконання якого вимагає високої концентрації, зібраності, а також обережності та уважності при роботі із делікатними рідкісними виданнями.

Він починається у Відділі рідкісної книги, де відповідальні бібліотекарі після консультацій із кафедрами приймають рішення про необхідність оцифровування того чи іншого видання. Після чого книга розміщується у чергу та у визначений час потрапляє до ЦІТ.

Після цього всі книги оглядаються співробітниками ЦІТ та приводяться в стан, придатний до оцифровки (книги перевіряються на цілісність, підклеюються та готуються до процесу сканування (наприклад, розділяються сторінки, які були досі нерозділеними; це стосується, як правило, других примірників книжок, що зберігаються у відділі і не надаються користувачам), а також заносяться в реєстр отриманих книг, придатних та готових до оцифровки.

Наступний етап створення електронної копії є найголовнішим — це процес сканування рідкісного видання за допомогою створеного у ЦІТ спеціалізованого програмного забезпечення та використання сучасної електронної техніки різного профілю (сканерів різних форматів, фотоапаратів, відеокамер тощо).

Після створення «грубої» електронної копії рідкісного видання починається тривалий процес її обробки, до якого входять: 1) внесення бібліографічної інформації про фоліант до загальної бази даних електронних копій раритетних видань на сервері ЦІТ; 2) перевірка якості відсканованого матеріалу та його «звіряння» з оригіналом, з метою виявлення неякісно оброблених сторінок (помилки сканера, недостатнє притиснення книги до скла сканера, «розмиття» тексту, його «обірваність», випадково загнуті сторінки тощо), а також помилково пропущених чи двічі відсканованих сторінок; 3) виправлення виявлених недоліків; 4) графічне оброблення цифрових матеріалів: відскановані сторінки спочатку вирівнюються, потім на них виділяються ділянки із корисною інформацією (текст, малюнки), за якими сторінки врешті і «обрізуються», відсікаючи зайву інформацію для

естетичного впорядкування та зменшення обсягу інформації (для заощадження місця на сервері). Така обробка здійснюється спеціальним програмним забезпеченням під контролем оператора та є найтривалішим етапом в обробці книги.

Після остаточної обробки електронної копії раритетного видання, вона завантажується на сервер ЦІТ до каталогу Бібліотеки електронних копій раритетних видань. Така копія може бути переглянута на спеціальному сайті, створеному у ЦІТ, за адресою: http://oldlib.nulau.org.ua.

На фінальній стадії рідкісні видання, що пройшли процес оцифровки, знову переглядаються на цілісність. У разі виявлення порушень, які виникли під час процесу сканування, книги повторно підклеюються та приводяться у належний стан. І, нарешті, після завершення всіх робіт вони повертаються до Відділу рідкісної книги на зберігання.

У разі необхідності може бути проведена процедура створення електронної портабельної (переносної) версії книги для її збереження на електронному носії. У такому разі книга додатково оброблюється та зберігається в одному з популярних форматів, як-то: .djvu чи .pdf.

Слід зазначити, що у зв'язку зі створенням вищезазначеного Web-сайта Електронної бібліотеки раритетних видань, що зберігається на сервері ЦІТ, необхідність в останніх маніпуляціях із електронною копією раритетного видання практично відпадає, адже таку копію в разі необхідності та наявності доступу до Бібліотеки можна буде переглянути з будь-якого місця на планеті за допомогою мережі Internet.

Таким чином, за п'ять років роботи над рідкісними виданнями ЦІТ оцифрував більше 4 200 книг або більше ніж 1 653 000 сторінок. І на цьому робота не завершується: постійно обговорюються ідеї щодо вдосконалення тих чи інших програмних модулів, вдосконалюється технологія створення копій рідкісних видань, запроваджуються новітні інформаційні та комп'ютерні технології, які дозволять ще швидше і ще якісніше створювати безсмертні копії наукових здобутків, закарбованих на старовинному пожовклому папері. На рис. 8.2 показані перші сторінки деяких відсканованих і оброблених видань.

Це забезпечує необмежене використання цих видань у первісному вигляді без погіршення їх стану і збереження на необмежений строк.

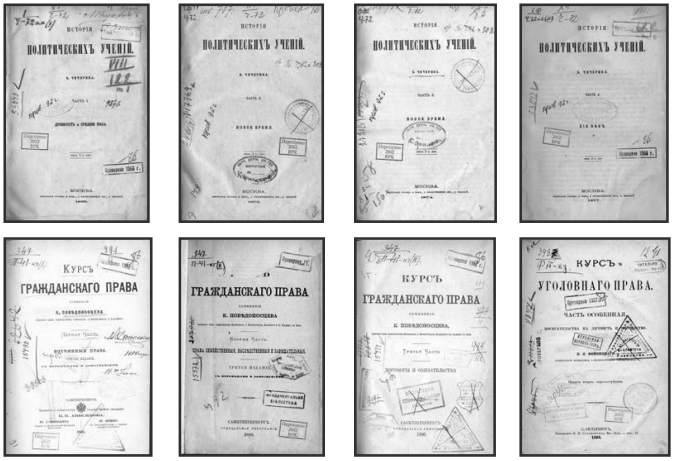



*Рис. 8.2.* Титульні сторінки деяких раритетних видань, які переведені в електронний формат і зберігаються на сервері ЦІТ

## 8.7. Інші інформаційні ресурси і сервіси

Вперше мережа Університету експериментально випробувала можливості цифрового телебачення. Цифровий сигнал зображення, який дає набагато чіткіше зображення ніж звичайний аналоговий сигнал, через мережу супутників передається у локальну мережу, де може відображатися на моніторах комп'ютерів. Завдяки застосуванню спеціалізованого обладнання такий сигнал може бути прийнятим звичайним телевізійним приймачем. Ця технологія використовує ту саму локальну мережу, за якою передаються всі інші дані. Тому вона дозволяє економити значні кошти на прокладення телевізійного кабелю та встановлення додаткового обладнання для потреб телебачення у всіх будівлях університету та у гуртожитках. На екрані монітора можна одночасно переглядати як програму цифрового телебачення, так і роботу в будь-якому додатку. За такою технологією у перспективі буде доступно більше 1 000 цифрових телевізійних каналів (зараз трохи менше 100), у тому числі призначених для навчального процесу і підготованих у різних країнах світу.

В університеті створена телевізійна студія, яка обладнана сучасним цифровим студійним обладнанням, завдяки цьому можлива трансляція телевізійних та авторських програм у локальну мережу ВНЗ. Ці передачі готуються досить професійно і за встановленим графіком передаються у мережу. Робота Палацу студентів, всі урочисті заходи, що відбуваються в ньому, також транслюються через мультисервісну мережу і сервер ЦІТ. Таким чином, на будь-якому комп'ютері, що під'єднаний до локальної мережі, без додаткового обладнання можна переглядати програми телебачення. Цей сервіс для користувачів мережі безкоштовний.

У Центрі інформаційних технологій розроблено Web-сайт університету та наукового відділу (рис. 8.3), які супроводжуються і підтримуються в актуальному стані. Слід зазначити високу інформаційну ємність цих Web-сайтів і наголосити, що продовжується розвиток їх структури й інформаційного наповнення. За дорученням проректора з наукової роботи А. П. Гетьмана відсканковані і впорядковані в електронному форматі всі випуски збірника «Проблеми законності», що були видані університетом впродовж часу його існування. А останнім часом започатковано збірник «Теорія і практика правознавства», який існує лише в електронному вигляді і доступний через згадану Web-сторінку.


*Рис. 8.3.* Стартова сторінка Web-сайта наукового відділу університету

Центр інформаційних технологій займається забезпеченням конференцій, круглих столів, олімпіад, що проводяться в університеті, особливо, коли йдеться про дистанційну участь і використання мультимедійних матеріалів. Крім того, ЦІТ забезпечує інформаційну підтримку всіх заходів і подій внутрішнього рівня, що відбуваються в навчальному закладі. Забезпечує технічно та інформаційно участь Університету в різноманітних виставках освітніх установ, що проводяться в Україні. Для впровадження і використання в практику навчальної діяльності новітніх інформаційних технологій у Центрі виконуються наукові дослідження, основна мета яких — підбір і обґрунтування існуючих, а також розробка елементів нових технологій для консолідації різноманітної за змістом і структурою інформації в інтергальний простір правових знань. З цією метою розроблений програмний комплекс «JURONT» (юридична онтологія), що становить знанняорієнтовану навчально-консультаційну інформаційну правову систему. Структурним підґрунтям подання інформації у «JURONT» є використання семантичної мережі знань у вигляді онтологічної структури [7; 8; 9]. Зараз продовжується подальший розвиток ідей, що використані в цій системі, для автоматизованої і навіть у деяких аспектах автоматичної обробки і впорядкування правової інформації.

У цілому ЦІТ університету вивчає та впроваджує нові можливості підвищення інформаційного рівня навчального закладу. Серед перспективних напрямків у 2012 році вивчаються можливості впровадження в нашій мережі «хмарових» обчислень і використання новітніх комунікаційних сервісів на платформі Microsoft.

Залучення широких верств викладачів, розробників інформаційного наповнення і користувачів інформаційних систем вимагає постійного інформування їх про існуючі можливості технологій, про запропоновані технічні і технологічні рішення, що знаходять своє відображення в інформаційних системах університету. Тому у 2008–2012 роках проведено цикл семінарів-тренінгів із застосування новітніх інформаційних технологій в освітній діяльності — для професорсько-викладацького складу, що задіяний у програмі підготовки і впровадження дистанційних методів освіти. Також усі викладачі і студенти університету мають можливість отримати особисті

індивідуальні консультації від фахівців Центру з питань використання інформаційних технологій.

Завдяки своєчасному та яскравому висвітленню подій на сайті Університету та в місцевих ЗМІ університет широко відомий як в Україні, так і за її межами.

Що стосується інформатизації адміністративного управління, то в міру розвитку інформаційних технологій й усвідомлення «вузьких місць» системи адміністративного управління вимальовується ідея корекції напрямків подальшого розвитку у бік реінжинірингу бізнес-процесів на платформі процесної моделі управління, створення системи управління потоками робіт, документів і знань як складової частини інтегрованого інформаційно-освітнього адміністративно-управлінського Intranet-порталу, у якому б відображалися вітрини даних традиційних інформаційно-управляючих систем.

## 8.8. Висновки

Таким чином, можна зробити кілька висновків. Сучасні студенти для підвищення ефективності навчання потребують розширення інформаційних послуг, у тому числі на робочих місцях у гуртожитках і вдома. Зростаючі обсяги і темпи збільшення доступної для навчання інформації в електронному вигляді поставили теоретичну і практичну проблеми управління інформаційним наповненням систем навчання і контролю знань. Реалізація положень Болонської декларації в системі вищої освіти і науки України вимагає більш глибокої стандартизації процесів навчання і рівня знань учнів.

Парадигма індустріальної освіти, яка передбачає навчання в рамках жорстких вимог «спеціальності», вже не відповідає поточним потребам людства. Для постіндустріальної освіти надбання студентом власне знань і конкретних предметних умінь є вторинним. На перший план виступає навчання здатності оперувати в суспільстві, що трансформується в інформаційному полі, комунікувати, ширше — «існувати в постіндустріальному комунікаційному просторі».

Запропонована ієрархічна модель централізованої системи електронної освіти, яка заснована на розподілі освітніх сервісів і контента за декількома функціональними рівнями, що відповідають структурі навчальних ресурсів для освіти в університеті, що дозволяє здійснювати електронну освітню політику і мінімізувати витрати на розгортання та експлуатацію системи електронної освіти.

Реалізована в Національному університеті «Юридична академія України імені Ярослава Мудрого» інноваційна модель віртуального інтегрального інформаційного середовища навчання забезпечує:

– необмежений доступ до інформаційних навчальних ресурсів, що зосереджені в мережі;

– сучасне середовище комунікацій, спілкування й обміну інформацією;

– електронне спілкування за ланцюжком: студент — викладач — кафедра — деканат — бібліотека — ректорат;

– доступ до глобальної мережі Internet і всіх її інформаційних ресурсів;

– розвиток творчих здібностей студентів, вмінь і навичок роботи в інформаційному просторі;

– адаптацію студентства до сучасного інформаційного світу та майбутньої професійної діяльності.

Перспективні дослідження передбачається виконати в напрямку створення онтологічних структур подання знань і нечітких зв'язків між поняттями в галузі правознавства, залежно від ступеня впевненості в наявності взаємозв'язків між ними. Також передбачається дослідження впливу принципів самоорганізації на якість створюваної множиною користувачів онтології в предметній області правознавства.

У поточний момент продовжується розвиток науково-освітньої мережі Національного університету «Юридична академія України імені Ярослава Мудрого».

# Список використаної літератури

**Список літератури до розділу 1**


1. Роговский, Е. А. США. Информационное общество. Экономика и политика [Текст] / Е. А. Роговский. – М. : Международные отношения, 2008. – 408 с.
2. Авдеев, Р. Ф. Философия информационной цивилизации [Текст] / Р. Ф. Авдеев ; ред. : Е. С. Ивашкина, В. Г. Деткова. – М. : Владос, 1994. – С. 96–97.
3. Воронина, Т. П. Информационное общество: сущность, черты, проблемы [Текст] / Т. П. Воронина. – М., 1995. – 111 с.
4. Белл, Д. Социальные рамки информационного общества [Текст] / Д. Белл ; сокр. пер. Ю. В. Никулевича // Новая технологическая волна на западе / под ред. П. С. Гуревича. – М., 1988.
5. Окинавская Хартия глобального информационного общества [Электронный ресурс] : принята 22.07.2000 лидерами стран «Большой Восьмерки». – Режим доступа: http://www.mcbs.ru/iles/documents/documents/charter_inf_obschestvo.pdf.
6. Кастельс, М. Информационная эпоха. Экономика, общество и культура [Текст] ; пер. с англ. / под науч. ред. О. И. Шкаратана. – М. : ГУВШЭ, 2000. – 608 с.
7. Мартин, У. Дж. Информационное общество (реферат) [Текст] / У. Дж. Мартин / Теория и практика общественно-научной информации : ежеквартальник / АН СССР. ИНИОН. – М., 1990. – № 3. – С. 115–123.
8. Основи інформатики та обчислювальної техніки [Текст] : підручник / В. Г. Іванов, В. В. Карасюк, М. В. Гвозденко ; за заг. ред. В. Г. Іванова. – Х. : Право, 2012. – 312 с.
9. Глушков, В. М. О кибернетике как науке [Текст] / В. М. Глушков // Кибернетика, мышление, жизнь. – М., 1964. – 512 с.
10. Винер, Н. Кибернетика [Текст] / Н. Винер. – М. : Наука, 1958. – 215 с.
11. Колин, К. К. Природа информации и философские основы информатики [Текст] / К. К. Колин // Открытые системы. – 2005. – № 2. – С. 43–51.
12. Терещенко, Л. Глобальная сеть: пробелы в праве [Текст] / Л. Терещенко // Рос. юстиция. – 2000. – № 2. – С. 49 –51.
13. Дутов, М. Правовое обеспечение развития электронной коммерции [Текст] / М. Дутов // Господарське право. – 2001. – № 4. – С. 33–34.
14. Степанов, Теоретико-правовая оценка развития сферы информационно-электронных технологий [Текст] / О. А. Степанов // Право и политика. – 2001. – № 2. – С. 12–15.

15. Трофименко, А. Сетевые публикации: понятие и правовое регулирование [Текст] / А. Трофименко // Рос. юстиция. – 2000. – № 3. – С. 49–50.
16. Закон України «Про концепцію загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу» [Текст] // Відом. Верхов. Ради України. – 2003. – № 3. – Ст. 12.
17. Ершов, А. П. Информатика: предмет и понятие [Текст] / А. П. Ершов // Кибернетика. Становление информатики. – М. : Наука, 1986.
18. Колин, К. К. О структуре и содержании образовательной области «Информатика» [Текст] / К. К. Колин // Информатика и образование. – 2000. – № 10. – С. 5–10.
19. Колин, К. К. Становление информатики как фундаментальной науки и комплексной научной проблемы [Текст] / К. К. Колин // Системы и средства информатики : сб. науч. тр. ; спецвып. : Научно-методологические проблемы информатики / под ред. К. К. Колина. – М. : ИПИ РАН, 2006.
20. Колин, К. К. Фундаментальные проблемы информатики [Текст] / К. К. Колин // Системы и средства информатики : сб. науч. тр. – Вып. 7. – М. : Наука, 1995.
21. Норенков, И. П. Информационные технологии в образовании [Текст] / И. П. Норенков, А. М. Зимин. – М. : Изд-во МГТУ им. Н. Э. Баумана, 2004.
22. Урсул, А. Д. Информатизация общества: Введение в социальную информатику [Текст] / А. Д. Урсул. – М. : Акад. общественных наук при ЦК КПСС, 1990.
23. Колин, К. К. Информатика как фундаментальная наука [Текст] / К. К. Колин // Информатика и образование. – 2007. – № 6.
24. Информатика для юристов и экономистов [Текст] / С. В. Симонович и др. – СПб. : Питер, 2001. – 688 с.
25. Фридланд, А. Я. Информатика: процессы, системы, ресурсы [Текст] / А. Я. Фридланд. – М. : БИНОМ ; Лаборатория знаний, 2003. – 232 с.
26. Правова інформатика [Текст] : підручник : у 2 т. / за ред. В. Я. Тація, Я. Ю. Кондратьєва, М. Я. Швеця. – К. : Парлам. вид-во, 2004. – Т. 1. – 416 с.
27. Глушков, В. М. Основы безбумажной информатики [Текст] / В. М. Глушков. – М. : Наука, 1982. – 552 с.
28. Правова інформація та комп'ютерні технології в юридичній діяльності [Текст] : навч. посіб. / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін. ; за заг. ред. В. Г. Іванова. – Х. : Право, 2010. – 240 с.
29. Шепітько, В. Ю. Вибрані твори / Избранные труды [Текст] / В. Ю. Шепітько. – Х. : Видав. агенція «Апостиль», 2010. – 576 с.
30. Шепитько, Ю. Тактика расследования преступлений, совершаемых организованными группами и преступными организациями [Текст] / Ю. Шепитько. – Харьков, 2000.

31. Белкин, Р. С. Криминалистическая энциклопедия [Текст] / Р. С. Белкин. – 2-е изд., доп. – М., 2000.
32. Кузьмічов, В. С. Криміналістичний аналіз розслідування злочинів [Текст] : монографія / В. С. Кузьмічов. – К. : НАВСУ – НВТ «Правник», 2000. – 450 с.
33. Коновалова, В. Е. Убийство: Искусство расследования [Текст] : монография / В. Е. Коновалова. – Х. : Факт, 2001. – 312 с.
34. Шепитько, В. Ю. Криминалистика XXI века: предмет познания, задачи и тенденции в новых условиях [Текст] / В. Ю. Шепитько // Современное состояние и развитие криминалистики : сб. науч. тр. / под ред. Н. П. Яблокова и В. Ю. Шепитько. – Х. : Апостиль, 2012. – С. 41–54.
35. Бірюков, В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів [Текст] : монографія / В. В. Бірюков ; Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2009. – С. 627–660.
36. Компьютерные технологии в криминалистической фотографии: теоретические и прикладные вопросы [Текст] : учеб. пособие / А. А. Сафонов, С. М. Колотушкин, А. В. Кочубей. – Волгоград : ВА МВД России, 2005. – 140 с.
37. Шинкаренко, І. Р. Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія [Текст] : монографія / І. Р. Шинкаренко, В. О. Голубєв, М. В. Карчевський, І. Ф. Хараберюш. – Донецьк : РВВ ЛДУВС, 2007.
38. Семенов, Г. В. Расследование преступлений в сфере мобильных телекоммуникаций [Текст] / Г. В. Семенов. – М. : Юрлитинформ, 2006. – 336 с.
39. Грабовский, В. Д. Фоноскопия. Теория и практика использования звуковых следов в расследовании преступлений [Текст] : учеб. пособие / В. Д. Грабовский, О. Н. Кравчук. – Н. Новгород : Нижегородская академия МВД России, 2001. – 108 с.
40. Шепитько, В. Ю. Кодирование и обработка изображений в криминалистических информационных системах [Текст] / В. Ю. Шепитько, В. Г. Иванов, Ю. В. Ломоносов // Спеціальна техніка у правоохоронній діяльності : матеріали міжнар. наук.-практ. конф. – К. : Нац. акад. внутр. справ України, 2005. – Ч. 1 – С. 209–218.
41. Шепитько, В. Ю. Технико-криминалистическое исследование цифровых изображений документов [Текст] / В. Ю. Шепитько, В. Г. Иванов, Ю. В. Ломоносов, Л. И. Керик // Питання боротьби зі злочинністю. – Х. : Кроссроуд, 2006. – Вип. 12. – С. 194 –203.
42. Баранов, А. Электронное правительство в Украине? Будет! Когда? [Текст] / А. Баранов // Зеркало недели. – 2002. – № 1.

43. Григор, О. О. Формування інформаційного суспільства в Україні в контексті інтеграції в Європейський Союз [Текст] : автореф. дис. … канд. наук з держав. упр. / О. О. Григор. – Львів : Львів. регіонал. ін-т держ. упр. Нац. акад. держ. упр. при Президентові України, 2003. – 16 с.
44. Приймак, Ю. Ю. Методи та принципи організації електронного уряду [Текст] /Ю. Ю. Приймак // Університетські наукові записки. – Хмельницький : Вид-во Хмельниц. ун-ту упр. та права, 2008. – № 1. – С. 328–333.
45. Ємельяненко, О. Традиційний та електронний уряд: концептуальні відмінності [Текст] /О. Ємельяненко // Віче. – 2008. – № 2. – С. 20–22.
46. Миланко, О. Питання доступу до інформації та проблеми «електронного урядування» [Текст] / О. Миланко // Юрид. вісн. України. – 2004. – № 49. – 4 –10 груд. – С. 12.
47. Масарік, В. Застосування новітніх технологій у місцевих органах влади [Текст] /В. Масарік // Аспекти самоврядування : часоп. Укр.-амер. прог. «Партнерство громад». – 2006. – № 5. – С. 53–60.
48. Лебедева, Н. Н. Доступ граждан к информации о деятельности органов государственной власти [Текст] /Н. Н. Лебедева // Вестн. Моск. ун-та. Сер. 11, Право. – 2005. – № 5. – С. 76 –84.
49. Буренко, Т. О. Особливості адаптації в Україні Європейського досвіду функціонування інституту публічних послуг [Текст] /Т. О. Буренко // Вісн. Акад. митної служби України. Сер. «Державне управління». – Д. : Акад. митної служби України, 2010. – № 2010. – № 1(2). – С. 28–34.
50. Литвинов, Г. Модель електронного уряду для України: досвід Словенії [Текст] / Г. Литвинов, В. Сіряченко // Вісн. Нац. акад. держ. управління при Президентові України. – 2004. – № 4. – С. 422–434.
51. Сітко, І. Уряд – бізнес: від єдиного вікна до єдиного електронного офісу [Текст] / І. Сітко // Вісн. Нац. акад. держ. упр. при Президентові України. – 2007. – № 4. – С. 268–278.
52. Титаренко, О. Аналіз реалізації концепції електронного уряду в Японії [Текст] / О. Титаренко // Актуальні проблеми державного управління. – Д. : ДРІДУ НАДУ, 2006. – Вип. 4 (26). – С. 99–105.
53. Семенов, А. Досвід зарубіжних країн щодо розробки та реалізації програми електронного урядування: уроки для України [Текст] / А. Семенов // Вісн. Нац. акад. держ. управління при Президентові України. – 2006. – № 2. – С. 407–415.

**Список літератури до розділу 2**

1. Воробьев, В. И. Теория и практика вейвлет-преобразования [Текст] / В. И. Воробьев, В. Г. Грибунин. – СПб. : Изд-во ВУС, 1999. – 208 с.

2. Daubechies, I. Ten Lectures on Wavelets [Текст]. – SIAM, 1992.
3. Ричардсон, Ян. Видеокодирование. H. 264 и MPEG-4 – стандарты нового поколения [Текст] / Ян Ричардсон : пер. с англ. – М. : Техносфера, 2005. – 368 с.
4. Сэломон, Д. Сжатие данных, изображений и звука [Текст] / Д. Сэломон. – М. : Техносфера, 2004. – 368 с.
5. Шлезингер, М. Десять лекций по статистическому и структурному распознаванию [Текст] / М. Шлезингер, В. Главач. – Киев : Наукова думка, 2004. – 535 с.
6. Шепитько, В. Ю. Кодирование и обработка изображений в криминалистических информационных системах [Текст] / В. Ю. Шепитько, В. Г. Иванов, Ю. В. Ломоносов // Спеціальна техніка у правоохоронній діяльності : матеріали міжнар. наук.-практ. конф. – К. : Нац. акад. внутр. справ України, 2005. – Ч. 1 – С. 209–218.
7. Шепитько, В. Ю. Технико-криминалистическое исследование цифровых изображений документов [Текст] / В. Ю. Шепитько, В. Г. Иванов, Ю. В. Ломоносов, Л. И. Керик // Питання боротьби зі злочинністю. – Х. : Кроссроуд, 2006. – Вип. 12 – С. 194–203.
8. Иванов, В. Г. Многоэтапный алгоритм сжатия мультимедийных данных [Текст] / В. Г. Иванов, Ю. В. Ломоносов // Радиоэлектроника и информатика : науч.-техн. журн. ХГТУРЭ. – 2000. – № 4 (13). – С. 87–89.
9. Иванов, В. Г. Алгоритм сжатия данных на основе вычислений точек перегиба в структуре сигнала [Текст] / В. Г. Иванов, Ю. В. Ломоносов // Системный анализ, управление и информационные технологии : вестн. ХГПУ. – 2000. – № 94. – С. 25–29.
10. Вінцюк, Т. Мовленнєві інформаційні технології в Україні – на шляху до європейського співробітництва Схід-Захід [Текст] / Т. Вінцюк // Пр. Сьомої Всеукр. міжнар. конф. «Оброблення сигналів і зображень та розпізнавання образів (УкрОБРАЗ 2004)». – К. : Кіберн. центр Нац. акад. наук України, 2004. – С. 9–17.
11. Цуркан, Є. Ю. Інтелектуальні голосові технології в портативних телекомунікаційних пристроях [Текст] / Є. Ю. Цуркан // Пр. Сьомої Всеукр. міжнар. конф. «Оброблення сигналів і зображень та розпізнавання образів (УкрОБРАЗ 2004)». – К. : Кіберн. центр Нац. акад. наук України, 2004. – С. 249–250.
12. Ричардсон, Ян. Видеокодирование. H. 264 и MPEG-4 – стандарты нового поколения [Текст] / Ян Ричардсон : пер. с англ. – М. : Техносфера, 2005. – 368 с.
13. Назаров, М. В. Методы цифровой обработки и передачи речевых сигналов [Текст] / М. В. Назаров, Ю. Н. Прохоров. – М. : Радио и связь, 1985. – 176 с.

14. Аблазов, В. И. Преобразование, запись и воспроизведение речевых сигналов [Текст] / В. И. Аблазов, В. И. Гупал, А. В. Згурский. – К. : Лыбидь, 1991. – 208 с.
15. Фланаган, Дж. Анализ, синтез и восприятие речи [Текст] / Дж. Фланаган : пер. с англ. ; под ред. А. А. Пирогова. – М. : Связь, 1968. – 396 с.
16. Рабинер, Л. Р. Цифровая обработка речевых сигналов [Текст] / Л. Р. Рабинер, Р. В. Шафер : пер. с англ. ; под ред. М. В. Назарова, Ю. Н. Прохорова. – М. : Радио и связь, 1981. – 495 с.
17. Прохоров, Статистические модели и рекурентное предсказание речевых сигналов [Текст] / Ю. Н. Прохоров. – М. : Радио и связь, 1984. – 240 с.
18. Винцюк, Т. К. Анализ, распознавание и интерпретация речевых сигналов [Текст] / Т. К. Винцюк. – Киев : Наукова думка, 1987. – 264 с.
19. Ковалгин, Ю. А. Цифровое кодирование звуковых сигналов [Текст] / Ю. А. Ковалгин, Э. И. Вологдин. – СПб : Корона-Принт, 2004. – 234 с.
20. Лабутин, В. К. Модели механизмов слуха [Текст] / В. К. Лабутин, А. П. Молчанов. – М. : Энергия, 1973. – 200 с.
21. Артюшенко, В. М. Цифровое сжатие видеоинформации и звука [Текст] / В. М. Артюшенко, О. И. Шелухин. – М. : ИФК «Дашков и Ко», 2004. – 426 с.
22. Вакулюк, Б. Как и зачем сжимают звук [Текст] / Б. Вакулюк // Компьютерное обозрение. – Киев : Изд-во ООО «ІТС», 1998. – № 34. – С. 20–26.

**Список літератури до розділу 3**

1. Криницкий, И. А. Автоматизированные информационные системы [Текст] / И. А. Криницкий, Г. А. Миронов, Г. Д. Фролов. – М., 1982. – 384 с.
2. Полевой, Н. С. Криминалистическая кибернетика [Текст] / Н. С. Полевой. – 2-е изд. – М. : Изд-во МГУ, 1989. – 328 с.
3. Автоматизированные системы управления и приборы автоматики [Текст] // Харьк. гос. техн. ун-т радиоэлектроники (ХТУРЭ) : всеукр. междувед. науч.-техн. сб. тр. – 2003. – Вып. 113.
4. Информатика [Текст] : базовый курс / С. В. Симонович и др. – СПб. : Питер, 2001. – 640 с.
5. Правовая кибернетика [Текст] : сб. науч. тр. – М. : Наука, 1973. – 253 с.
6. Теорія та практика судової експертизи і криміналістики [Текст] : зб. наук.-практ. матеріалів (до 55-річчя видання роботи С. М. Потапова «Введение в криминалистику») / М-во юстиції України ; Харк. н.-д. ін-т суд. експертиз ім. Засл. проф. М. С. Бокаріуса ; редкол. : М. Л. Цимбал, Е. Б. Сімакова-Єфремян, В. М. Шерстюк та ін. – Х. : Право, 2001.

7. Теорія та практика судової експертизи і криміналістики [Текст] : зб. матеріалів міжнарод. наук.-практ. конф. / М-во юстиції України ; Харк. н.-д. ін-т суд. експертиз ім. Засл. проф. М. С. Бокаріуса ; Акад. правов. наук України ; Нац. юрид. акад. України імені Ярослава Мудрого ; редкол. : М. Л. Цимбал, М. І. Панов, Е. Б. Сімакова-Єфремян та ін. – Х. : Право, 2002. – Вип. 2.
8. Иванов, В. Г. Кодирование и поиск изображений в криминалистических информационно-аналитических системах [Текст] / В. Г. Иванов // Актуальні проблеми криміналістики : матеріали міжнар. наук.-практ. конф. (Харків) 25–26 вересня 2003 р. / редкол. : М. І. Панов (голов. ред.), В. Ю. Шепітько, В. О. Коновалова та ін. – Х. : Гриф. 2003. – С. 215–217.
9. Иванов, В. Г. Фурье и вейвлет-анализ изображений в плоскости JPEG технологий [Текст] / В. Г. Иванов, М. Г. Любарский, Ю. В. Ломоносов // Проблемы управления и информатики. – 2004. – № 5. – С. 111–124.
10. Ахмед, Н. Ортогональные преобразования при обработке цифровых сигналов [Текст] / Н. Ахмед, К. Р. Рао. – М. : Связь, 1980. – 248 с.
11. Иванов, В. Г. Повышение информативности дискретных данных на базе ортогональных преобразований и адаптивных алгоритмов [Текст] / В. Г. Иванов // Автоматизированные системы управления и приборы автоматики: респ. междуведомств. науч.-техн. сб. – Харьков : Вища школа, изд-во при Харьк. ун-те, 1983. – Вып. 67. – С. 63 –65.
12. Иванов, В. Г. Сложность и эффективность вычислений коэффициентов и рядов Хаара [Текст] / В. Г. Иванов // Изв. вузов СССР. Приборостроение. – 1985. – № 3. – Т. XXVIII. – С. 10 –13.
13. Иванов, В. Г. Синтез сигналов рядами Хаара произвольной размерности [Текст] / В. Г. Иванов // Изв. высш. учебн. заведений. Радиоэлектроника. – К., 2001. – № 4.
14. Иванов, В. Г. Многоэтапный алгоритм сжатия мультимедийных данных [Текст] / В. Г. Иванов, Ю. В. Ломоносов // Радиоэлектроника и информатика. – 2000. – № 4 (13). – С. 87–89.
15. Миано, Дж. Форматы и алгоритмы сжатия изображений в действии [Текст] / Дж. Миано. – М. : Триумф, 2003. – 336 с.
16. Методические рекомендации по использованию алгоритмов графических идентификационных при исследовании фотоизображений в целях отождествления личности [Текст] / под ред. Л. Н. Лихачева, Н. С. Полевого. – Рига, 1966.
17. Эльбур, Р. Э. Использование аппарата проективной геометрии в процессе идентификации личности по фотоснимкам [Текст] / Р. Э. Эльбур // Вопросы кибернетики и право. – М. : Наука, 1967.

18. Игнациус, Г. И. Проективная геометрия [Текст] / Г. И. Игнациус. – М., 1966.
19. Ефимов, И. В. Краткий курс аналитической геометри [Текст] / И. В. Ефимов. – М., 1967.
20. Колдин, В. Я. Идентификация и ее роль в установлении истины по уголовным делам [Текст] / В. Я. Колдин. – М., 1969.
21. Селиванов, И. А. Актуальные теоретические вопросы криминалистической идентификации [Текст] / И. А. Селиванов // Вопросы борьбы с преступностью. – М., 1971. – Вып. 14. – С. 144.
22. Юрапе, В. Ю. Некоторые вопросы теории идентификации объектов с использованием аппарата прективной геометри [Текст] / В. Ю. Юрапе // Вопросы кибернетики и право. – М., 1968.
23. Договор о научно-творческом сотрудничестве № 57/434 от 15.05.2000 г. с Научно-исследовательским экспертно-криминалистическим центром при УМВД в Харьковской области «Создание и внедрение автоматизированной системы кодирования и поиска изображений печатей и штампов АС “Клише”».
24. АС «Клише», затверджена постановою Президії АПрН України від 14 лютого 2002 р. № 19. № ДР 0102U002194 в Інституті вивчення проблем злочинності АПрН України «Проблеми криміналістичного забезпечення діяльності правоохоронних органів».

**Список літератури до розділу 4**

1. Cox, I. J. Secure spread spectrum watermarking for multimedia [Текст] / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Proceedings of the IEEE International Conference on Image Processing. – 1997. – Vol. 6. – P. 1673–1687.
2. Piva A. A watermarking technique for the protection of digital images IPR [Текст] / A. Piva, M. Barni, F. Bartolini, V. Cappellini // Proceedings of European Multimedia, Microprocessor System and Electronic Commerce Conference and Exhibition: Advances in Information Technologies: The Business Challenge. – 1997. – P. 636–643.
3. Chae, J. J. Robust Techniques for Data Hiding in Images and Video. Ph thesis, CA, USA, 1999.
4. Fridrich, J. Combining low-frequency and spread spectrum watermarking [Текст] / J. Fridrich // Proceedings of the SPIE Symposium on Optical Science, Engineering and Instrumentation. – 1998.
5. Cox, I. J. Secure spread spectrum watermarking for multimedia [Текст] / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Technical report, NEC Research Institure, USA, 1996.

6. Cox, I. J. A secure, robust watermark for multimedia [Текст] / I. J. Cox, J. Kilian, T. Leighton, T. G. Shamoon // Information hiding: first international workshop. Lecture Notes in Comp. Science. – 1996. – Vol. 1174. – P. 183–206.
7. Barni, M. A DWT-based technique for spatio-frequency masking of digital signatures [Текст] / M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva // Proceedings of the 11th SPIE Annual Symposium, Electronic Imaging '99, Security and Watermarking of Multimedia Contents. – 1999. – Vol. 3657.
8. Хорошко, В. О. Основи комп'ютерної стеганографії [Текст] : навч. посіб. для студ. і асп. / В. О. Хорошко, В. Д. Азаров, М. С. Шелест, Ю. Є. Яремчук. – Вінниця : Вінниц. держ. техн. ун-т, 2003. – 143 с.
9. Каханович, Г. Ф. Компьютерная стеганография. Теория и практика [Текст] / Г. Ф. Каханович, А. Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.
10. Грибунин, В. Г. Цифровая стеганография [Текст] / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-Пресс. 2002. – 272 с.
11. Швидченко, И. В. Анализ криптостеганографических алгоритмов [Текст] / И. В. Швидченко // Проблемы управления и інформатики. – 2007. – № 4. – С. 149 –155.
12. Chae, J. J. A robust embedded data from wavelet coeffcients [Текст] / J. J. Chae, D. Mukherjee, B. S. Manjunath // Proceedings of SPIE, Electronic Imaging, Storage and Retrieval for Image and Video Database. – 1998. – Vol. 3312. – P. 308–317.
13. Kundur, D. A robust digital image watermarking method using wavelet-based fusion [Текст] / D. Kundur, D. Hatzinakos // Proceedings of the IEEE International Conference on Image Processing. – 1997. – Vol. 1. – P. 544–547.
14. Lewis, A. S. Image compression using the 2-d wavelet transform [Текст] / A. S. Lewis, G. Knowles // IEEE Transactions on Image Processing. – 1992. – № 1. – P. 244–250.
15. Eggers, J. J. A blind watermarking scheme based on structured codebooks [Текст] / J. J. Eggers, J. K. Su, B. Girod // IEE Colloqium: Secure images and image authentication. – UK, 2000.
16. Costa, M. Writing on dirty paper [Текст] / M. Costa // IEEE Transactions on Information Theory. – 1983. – № 29(3). – P. 439–441.
17. Chen, B. Digital watermarking and information embedding using dither modulation [Текст] / B. Chen, G. W. Wornell // Proceedings of the IEEE Workshop on Multimedia Signal Processing. – 1998. – P. 273–278.
18. Schuchman, L. Dither signals and their effect on quantization noise [Текст] / L. Schuchman // IEEE Transaction on Communication Technology. – 1964. – № 12. – P. 162 –165.

19. Chu, C.-J. H. Luminance channel modulated watermarking of digital images [Текст] / C.-J. H. Chu, A. W. Wiltz // Proceedings of the SPIE Wavelet Applications Conference. – 1999. – P. 437–445.
20. Hsu, C.-T. Multiresolution watermarking for digital images [Текст] / C.-T. Hsu, J.-L. Wu // IEEE Trans. on Circuits and Systems II. – 1998. – № 45(8). – P. 1097 –1101.
21. Chae, J. Robust Techniques for Data Hiding in Images and Video [Текст] / J. Chae // Ph thesis, Department for Electrical and Computer Engineering, University of California, Santa Barbara, CA, USA, 1999.
22. Bas, P. A geometrical and frequential watermarking scheme using similarities [Текст] / P. Bas, J.-M. Chassery, F. Davoine // In SPIE Conference on Security and Watermarking of Multimedia Contents. – 1999. – № 3657. – P. 264–272.
23. Hartung, F. Spread Spectrum Watermarking: Malicious Attacks and Counterattacks [Електронний ресурс] / F. Hartung, J. Su, B. Girod. – Режим доступу: http://www.cs.vcla.edu/~miodrag/cs259-security/hattung99spread.pdf.
24. Petitcolas, F. Attacks on Copyright Marking Systems [Текст] / F. Petitcolas, R. Anderson, M. Kuhn // Lecture Notes in Computer Science. – 1998. – P. 218–238.
25. Кошкина, Н. В. Обзор спектральных методов внедрения цифровых водяных знаков в аудиосигналы [Текст] / Н. В. Кошкина // Проблемы управления и информатики. – 2010. – № 5. – С. 132–144.

**Список літератури до розділу 5**

1. Доктороу, К. Лекция, прочитанная в Microsoft 17 июня 2004 года // Компьютерра Online.
2. Зайцев, А. П. Технические средства и методы защиты информации [Текст] / А. П. Зайцев и др. – М. : Машиностроение, 2009. – 508 с.
3. Barry, Mark. Cryptography in Home Entertainment – A look at content scrambling in DVDs (июнь 2004 г.) [Електронний ресурс]. – Режим доступу: http://www.math.ucsd.edu/~crypto/Projects/MarkBarry/index.htm
4. Stevenson, Frank A. Cryptanalysis of Contents Scrambling System (8 ноября 1999 г.). [Електронний ресурс]. – Режим доступу: http://www.cs.cmu.edu/~dsf/DeCSS/FrankStevenson/analysis.html.
5. Final AACS Content Protection Specifications Include Managed Copy, Analog Sunset. CDRinfo (9 июня 2009г.) [Електронний ресурс]. – Режим доступу : http://www.cdrinfo.com/Sections/News/Details.aspx?NewsId=25479.

6. Marechal, Sander (January 9, 2007). DRM on audio CDs abolished [Електронний ресурс]. – Режим доступу : http://lxer.com/module/newswire/view/78008/index.html.
7. Конституція України [Текст] : прийнята 28.06.1996 р. // Відом. Верхов. Ради України. – 1996. – № 30. – Ст. 141.
8. Цивільний кодекс України [Текст] : прийнятий 16.01.2003 р. // Відом. Верхов. Ради України. – 2003. – № 40–44. – Ст. 356.
9. Про авторське право і суміжні права [Текст] : Закон України від 23.12.1993 р. № 3792-XII // Відом. Верхов. Ради України. – 2001. – № 43. – Ст. 214.
10. Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних [Текст] : Закон України від 23.03.2000 р. № 1587-III // Відом. Верхов. Ради України. – 2004. – № 7. – Ст. 46.
11. Цивільне право [Текст] : підручник : у 2 т. / за ред. В. І. Борисової. – Х. : Право, 2011. – Т. 1. – 656 с.
12. http://community.winsupersite.com/blogs/paul/archive/2008/06/19/msn-music-store-support-notification.aspx
13. Грибунин, В. Г. Цифровая стеганография [Текст] / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 261 с.
14. Конахович, Г. Ф. Компьютерная стеганография. Теория и практика [Текст] / Г. Ф. Конахович, А. Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.
15. Хорошко, В. О. Основи комп'ютерної стеганографії [Текст] : навч. посіб. для студ. і асп. / В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчик. – Вінниця : Вінниц. держ. техн. ун-т, 2003. – 143 с.
16. Алексеев, А. П. Методы внедрения информации в звуковые файлы формата MIDI [Текст] / А. П. Алексеев, А. А. Аленин // Инфокоммуникационные технологии. – Т. 9. – № 1. – 2011. – С. 86–89.
17. Аленин, А. А. Пространственное распределение информации в звуковых файлах [Текст] / А. А. Аленин, А. П. Алексеев // XVI РНТК ПГУТИ. – Самара, 2009. – С. 171 –172.
18. Кошкина, Н. В. Обзор спектральных методов внедрения цифровых водяных знаков в аудиосигналы [Текст] / Н. В. Кошкина // Проблемы управления и информатики. – 2010. – № 5. – С. 132 –144.
19. Кустов, В. Н. Методы встраивания скрытых сообщений [Текст] / В. Н. Кустов, А. А. Федчук // Защита информации. Конфидент. – 2002. – № 3. – С. 34 –37.
20. Хорошко, В. А. Введение в компьютерную стеганографию [Текст] / В. А. Хорошко, М. Е. Шелест. – Киев : НАУ, 2002. – 140 с.

21. Швидченко, И. В. Анализ криптостеганографических алгоритмов [Текст] / И. В. Швидченко // Проблемы управления и информатики. – 2007. – № 4. – С. 149 –155.
22. Іванов, В. Г. Захист авторських прав мультимедійних даних [Текст] / В. Г. Іванов, М. Г. Любарський, В. В. Карасюк, Ю. В. Ломоносов // Правове забезпечення оперативно-службової діяльності : актуальні проблеми та шляхи їх вирішення : матеріали постійно діючого науково-практичного семінару, 27 травня 2011 р., м. Харків. – Х. : ТОВ Оберіг, 2011. – Вип. 2. – С. 292–301.
23. Fridrich, J. Steganalysis of LSB encoding in color images [Текст] / J. Fridrich, R. Du, M. Long // ICM. – 2000. – P. 83–91.
24. Schyndel R. G. van. A Digital Watermark [Текст] / R. G. van Schyndel, A. Z. Tirkel, C. F. Osbome // Proc. of the IEEE Int. Conf. on Image Processing. – Vol. 2. – P. 86–90. – Austin, Texas, Nov 1994. – V.1174, 1996. – P. 347–350.
25. Wu, T. Selective encryption and watermarking of MPEG video [Текст] / T. Wu, S. Wu // International Conference on Image Science, Systems and Technology. – 1997. – P. 114–127.
26. Алексеев, А. П. Стеганографические и криптографические методы защиты информации [Текст] : учеб. пособие / А. П. Алексеев, В. В. Орлов. – Самара : Изд-во ПГУТИ, 2010. – 330 с.
27. Барсуков, В. С. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации [Електронний ресурс] / В. С. Барсуков, А. П. Романцов. – Режим доступу : http://st.ess.ru/publications/articles/barsukov.pdf.

**Список літератури до розділу 6**

1. Баранов, А. Н. Лингвистическая экспертиза текста: теория и практика [Текст] : учеб. пособие / А. Н. Баранов. – М. : Флинта ; Наука, 2007. – 592 с.
2. Бринев, К. И. Теоретическая лингвистика и судебная лингвистическая экспертиза [Текст] / К. И. Бринев. – Барнаул, 2009.
3. Россинская, Е. Р. Настольная книга судьи: судебная экспертиза [Текст] / Е. Р. Россинская, Е. И. Галяшина. – М. : Проспект, 2011.
4. Осадчий, М. А. Модельный метод в судебной лингвистической экспертизе (на примере авторoведческой экспертизы) [Текст] / М. А. Осадчий // Современные проблемы науки и образования (приложение «Филологические науки»). – 2011. – № 6. – С. 5.

5. Зайцева, Ю. В. Об автороведческой экспертизе формализованных текстов [Электронный ресурс] / Ю. В. Зайцева // V Международная научно-практическая конференция по криминалистике и судебной экспертизе «Криминалистические средства и методы в раскрытии и расследовании преступлений», 2–3 марта 2011 г., ЭКЦ МВД. – Режим доступа: http://www.textology.ru/article.aspx?aId=235.
6. Хмелев, Д. В. Как определить писателя? [Текст] / Д. В. Хмелев // Компьютера. – 2000. – № 9. – 14 марта.
7. Хмелев Д. В. Распознавание автора текста с использованием цепей А. А. Маркова [Текст] / Д. В. Хмелев // Вестн. МГУ. Сер. 9, Филология. – 2000. – № 2. – С. 115-126.,
8. Денисенко, В. Н. Типовая методика судебной лингвистической экспертизы [Текст] : метод. рекомендации / В. Н. Денисенко, Е. Ю. Чеботарева. – М. : ЭКЦ МВД России, 2007.
9. Нестеров, А. В. Основы экспертной деятельности [Текст] : учеб. пособие / А. В. Нестеров. – М. : Изд. дом Гос. ун-та Высшей школы экономики, 2009.
10. Галяшина, Е. И. Современное состояние и актуальные проблемы судебной лингвистической экспертизы в России и за рубежом [Электронный ресурс] / Е. И. Галяшина // Рос. право в Интернете. – 2008. – № 3. – Режим доступа: rpi.msal.ru/piints/200803galyashina.html.
11. Аверьянова, Т. В. Криминалистика [Текст] : учеб. для вузов МВД в 3 т. / Т. В. Аверьянова, Р. С. Белкин, И. А. Возгрин, А. Ф. Волынский / под ред. Р. С. Белкина и др. – М. : Инфра-М, 2007. – 580 с.
12. Кобзарь, С. И. Организация назначения криминалистических экспертиз и использования их результатов в расследовании преступлений [Текст] : учеб. пособие / С. И. Кобзарь ; МВД Украины, Луган. гос. ун-т внутр. дел им. Э. А. Дидоренко. – Луганск : РИО ЛГУВД, 2007. – С. 249–251.
13. Галяшина, Е. И. Возможности судебных речеведческих экспертиз по делам о защите прав интеллектуальной собственности [Текст] / Е. И. Галяшина //Интеллектуальная собственность. Авторское право и смежные права. – 2005. – № 9. – С. 50–59.
14. Голощапова, Т. И. Лингвистическая экспертиза [Текст] / Т. И. Голощапова, А. М. Полосина // Судебная экспертиза. – 2005. – № 4. – С. 12–15.
15. Баранов, Ю. Н. Теоретические основы применения лингвистических знаний в криминалистике при производстве фоноскопических и автороведческих экспертиз [Текст] : учеб. пособие / Ю. Н. Баранов. – Челябинск : Челяб. юрид. ин-т МВД России, 2004.

16. Судебная лингвистическая экспертиза [Текст] / И. В. Галактионова, И. М. Кобозева, Т. В. Коломийцева и др. // Бюл. М-ва юстиции РФ. – 2004. – № 9. – С. 63–70.
17. Галяшина, Е. И. Понятийные основы судебной лингвистической экспертизы [Текст] / Е. И. Галяшина // Теория и практика лингвистического анализа текстов СМИ в судебных экспертизах и информационных спорах : материалы науч.-практ. семинара. – М. : Галерия, 2003. – Ч. 2. – С. 48–64.
18. Ощепкова, Е. С. Идентификация пола автора по письменному тексту (лексико-грамматический аспект) [Текст] : дис. … канд. филолог. наук : 00.00.00 / Е. С. Ощепкова. – М., 2003. – 140 с.
19. Баранов, Ю. Н. Лингвистические исследования в криминалистике [Текст] / Ю. Н. Баранов // Судебная экспертиза на рубеже тысячелетий : материалы межведомственной науч.-прак. конф. в 3 ч. (21–22 мая 2002 г.). – Саратов : Сарат. юрид. ин-т МВД России, 2002. – Ч. 2. – С. 115–118.
20. Галяшина, Е. И. Использование специальных лингвистических знаний в судопроизводстве [Текст] / Е. И. Галяшина // Цена слова. Из практики лингвистических экспертиз текстов СМИ в судебных процессах по защите чести, достоинства и деловой репутации. – М. : Галерия, 2002. – С. 244–252.
21. Баранов, А. Н. Авторизация текста: пример экспертизы [Текст] / А. Н. Баранов // Введение в прикладную лингвистику : учеб. пособие. – М. : Эдиториал УРСС, 2001. – С. 43–51.
22. Кукушкина, О. В. Определение авторства текста с использованием буквенной и грамматической информации [Текст] / О. В. Кукушкина, А. А. Поликарпов, Д. В. Хмелев // Проблемы передачи информации. – 2001. – Т. 37. – № 2.
23. Огорелков, И. В. Современное состояние диагностических исследований в автороведении [Текст] / И. В. Огорелков // Криминалистика. XXI век : материалы науч.-практ. конф. 26–28 февраля 2001 года. – М. : ГУ ЭКЦ МВД России, 2001. – Т. 1. – С. 89–96.
24. Белкин, Р. Криминалистическая энциклопедия [Текст] / Р. Белкин. – М. : Мегатрон XXI, 2000.
25. http://sud-expertiza.ru/
26. http://mir-ekspertiz.info/osobennosti-avtorovedcheskoj-ekspertizy/
27. http://www.rusexpert.ru/magazine.htm
28. http://rusf.ru/cgi-bin/fr.cgi

**Список літератури до розділу 7**

1. Галатенко, В. А. Основы информационной безопасности [Текст] : учеб. пособие / В. А. Галатенко ; под ред. акад. РАН В. Б. Бетелина. – 4-е изд. – М. : Интернет-Университет Информационных технологий ; БИНОМ ; Лаборатория знаний, 2008. – 205 с.
2. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем [Текст] : підруч. для студ. вищ. навч. закл., які навчаються за напрямами «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною безпекою» / М. В. Грайворонський, О. М. Новіков. – К. : BHV, 2009. – 608 с.
3. Воронова, В. А. Системы контроля и управления доступом [Текст] / В. А. Воронова, В. А. Тихонов. – М. : Горячая линия – Телеком, 2010. – 272 с.
4. Щеглов, А. Ю. Защита компьютерной информации от несанкционированного доступа [Текст] / А. Ю. Щеглов. – СПб. : Наука и техника, 2004. – 384 с.
5. Хорошко, В. А. Методы и средства защиты информации [Текст] / В. А. Хорошко, А. А. Чекатков. – Киев : Юниор, 2003. – 504 с.
6. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] / П. Б. Хорев. – М. : Академия, 2006. – 256 с.
7. Джхунян, В. Л. Электронная идентификация [Текст] / В. Л. Джхунян, В. Ф. Шаньгин. – М. : NT Press, 2004. – 695 с.
8. Голубев, Г. А. Современное состояние и перспективы развития биометрических технологий [Текст] / Г. А. Голубев, Б. А. Габриелян // Нейрокомпьютеры: разработка, применение. – 2004. – № 10. – С. 39–46.
9. Завгородний, В. И. Комплексная защита информации в компьютерных системах [Текст] : учеб. пособие / В. И. Завгородний. – М. : Логос ; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.
10. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин / под ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М. : Радио и связь, 2001. – 376 с.
11. Даклин, П. Простые советы по более разумному выбору и использованию паролей [Электронный ресурс] / П. Даклин. – Режим доступа: http://www.infosecurity.ru/_gazeta/content/060525/article01.shtml.
12. Безмалый, В. Парольная защита: прошлое, настоящее, будущее [Электронний ресурс] / В. Безмалый // КомпьютерПресс. – 2008. – № 9. – Режим доступа: http://www.compress.ru/article.aspx?Id=20509&iid=901.

13. Конахович, Г. Ф. Захист інформації в мережах передачі даних [Текст] : підручник / Г. Ф. Конахович, О. Г. Корченко, О. К. Юдін. – К. : Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.
14. Кухарев, Г. А. Биометрические системы: методы и средства идентификации личности человека [Текст] / Г. А. Кухарев. – СПб. : Политехника, 2001. – 240 с.
15. Коновалов, Д. Н. Технология защиты информации на основе идентификации голоса [Электронный ресурс] / Д. Н. Коновалов, А. Г. Бояров. – Режим доступа: http://www.fact.ru/archive/07/voice.shtml.
16. Шарипов, Р. Р. Идентификация и аутентификация пользователей по клавиатурному почерку [Текст] / Р. Р. Шарипов // Электронное приборостроение : науч.-практ. сб. – Казань : ЗАО «Новое знание», 2005. – Вып. 3(44).
17. Голубев, Г. А. Современное состояние и перспективы развития биометрических технологий [Текст] / Г. А. Голубев, Б. А. Габриелян // Нейрокомпьютеры: разработка, применение. – 2004. – № 10. – С. 39–46.
18. Галатенко, В. А. Информационная безопасность: практический подход [Текст] / В. А. Галатенко. – М. : Наука, 1998. – 301 с.
19. Шрамко, В. Н. Комбинированные системы идентификации и аутентификации [Электронный ресурс] / В. Н. Шрамко // PCWeek/RE. – 2004. – № 45. – Режим доступа: http://www.pcweek.ro/themes/detail.php?ID=69114.
20. Десятчиков, А. А. Об объединении дистанционных биометрических методов распознавания человека [Текст] / А. А. Десятчиков, В. В. Лобанцов, И. А. Матвеев, А. Б. Мурынин // Современный экстремизм в Российской Федерации: особенности проявления и средства противодействия : материалы всерос. науч.-практ. конф. в Акад. упр. МВД России. – М. : Акад. упр. МВД РФ, 2006. – С. 374 –379.
21. Десятчиков, А. А. Синхронная биометрическая многофакторная идентификация [Текст] / А. А. Десятчиков, А. Б. Мурынин, Ю. П. Тресков, В. Я. Чучупал // Тр. ИСА РАН. Динамика неоднородных систем. – М. : УРСС, 2005. – Вып. 9 (1). – С. 188 –194.

**Список літератури до розділу 8**

1. Бершадский, М. Е. Возможные направления интеграции образовательных и информационно-коммуникативных технологий [Текст] / М. Е. Бершадский // Педагогические технологии. – 2006. – № 1. – С. 29–50.
2. Getman, A. Informative providing of modern education [Текст] / A. Getman, S. Ivanov, V. Karasiuk // Scientific Information for Society – from today to

the Future. Abstracts. 21st International CODATA Conference. October 5–8, 2008., Ukraine. – Kyiv : National Technical University of Ukraine «Kyiv Polytechnic Institut», 2008. – P. 89–90.

3. Семантичний інформаційно-освітній портал Національної юридичної академії України імені Ярослава Мудрого (СІОП) / група моніторингу проекту: В. В. Комаров, В. Г. Іванов, С. М. Іванов, В. В. Карасюк, Н. П. Пасмор. – Х. : Нац. юрид. акад. України, 2009. – 19 с.
4. Tatsyi, V. Віртуальний інформаційний простір у правознавстві на основі онтологічної моделі знань = Virtual information environment in science of law based on ontological knowledge model [Електронний ресурс] / V. Tatsyi, A. Getman, O. Sokolov, M. Shvets, S. Prylypko, S. Ivanov, V. Karasiuk, O. Lugoviy // Інформаційні технології і електрична інженерія – прибори і системи, матеріали і технології для майбутнього : пр. 54 Міжнародного наукового колоквіума = Information Technology and Electrical Engineering – Devices and Systems, Materials and Technologies for the Future: Conference Proceedings 54. Internationales Wissenschaftliches Kolloquium, 07–10 September 2009 / Ilmenau University of Technology. – Ilmenau: Germany: Impressum,Verlag ISLE, Betriebsstatte des ISLE e.V., 2009. – Флеш носій, 2 Гб. – 8 С. Бібліогр. у кінці ст.
5. Дорошенко, А. Распределённая платформа для управления ресурсами гетерогенного кластера [Текст] / А. Е. Дорошенко, К. А. Рухлис, А. С. Мохница // Проблеми програмування. – 2008. – № 2–3. – Спец. вип. – С. 150 –156.
6. Тацій, В. Інформаційна підготовка сучасного юриста: проблеми і перспективи [Текст] / В. Я. Тацій, С. М. Іванов, В. В. Карасюк // Професіоналізм педагога в контексті Європейського вибору України : матеріали міжнарод. наук.-практ. конф. «Професіоналізм педагога в контексті Європейського вибору України», 18–20 вересня 2008 р., Ялта. – Ялта : РВВ КГУ, 2008. – Ч. 3. – С. 72–76.
7. Іванов, С. М. Онтологічні моделі в корпоративному юридичному інформаційному просторі [Текст] / С. М. Іванов, В. В. Карасюк, О. С. Луговий, О. Ю. Соколов // Правова інформатика. – 2009. – № 3 (23). – С. 52 –58.
8. Tatsyi, V. Семантична мережа знань у правознавстві = Semantic network of knowledge in science of law / V. Tatsyi, A.Ge tman,, S. Ivanov, V. Karasiuk, O. Lugoviy, O. Sokolov // Автоматика, управління і інформаційні технології: Праці IASTED Міжнародної конференції = Automation, Control, and Information Technology (ACIT 2010): Proceedings of the IASTED International Conference on Automation, Control, and Information Technology, held June 15 – 18 2010 in Novosibirsk, Russia / The International

Association of Science and Technology for Development. – Anaheim, USA, Calgary, Canada, Zurich, Switzerland : ACTA Press 2010. – P. 218 –222.
9. Норенков, И. Интеллектуальные технологии на основе онтологий [Текст] / И. П. Норенков // Информационные технологии. – 2010. – № 1. – С. 17–23.
10. Иванов, С. Н. Учебные сервисы в локальной компьютерной сети [Текст] / С. Н. Иванов, В. В. Карасюк, В. Я. Таций // Образование и виртуальность : сб. науч. тр. 12-й Международной конф. Украинской ассоциации дистанционного образования / под общ. ред. В. А. Гребенюка и В. В. Семенца. – Харьков – Ялта : УАДО, 2009. – С. 59–66.
11. Іванов, С. М. Модель інформаційного середовища для підготовки юристів [Текст] / С. М. Іванов, В. В. Карасюк // Інформатика та системні науки (ІСН-2010) : матеріали Всеукр. наук.-практ. конф. 18–20 берез. 2010 р. / за ред. О. О. Ємця. – Полтава : РВВ ПУСКУ, 2010. – С. 75 –78.
12. Ибрагимов, И. М. Информационные технологии и средства дистанционного обучения [Текст] : учеб. пособие для студ. высш. учеб. заведений / под ред. А. Н. Ковшова. – М. : Изд. центр «Академия», 2005. – 336 с.
13. Батура, М. П. Новые образовательные технологии на основе высококачественной видеоконференцсвязи [Текст] / М. П. Батура, Б. В. Никульшин, В. Ю. Цветков // Развитие информатизации и государственной системы научно-технической информации (РИНТИ 2010) : доклады IX Международной конф. (Минск, 18 нояб. 2010 г.). – Минск : ОИПИ НАН Беларуси, 2010. – С. 122 –127.
14. Карпенко, М. Непрерывное образование на основе информационно-коммуникационных технологий [Текст] / М. Карпенко // Высшее образование в России. – 2005. – № 6. – С. 8–18.
15. Можаева, Г. В. Автоматизированная система дистанционного обучения «Электронный университет» [Текст] / Г. В. Можаева, Е. В. Рыльцева, В. И. Скрипка // Открытое и дистанционное образование. – 2008. – № 3 (31). – С. 68 –74.
16. Інструктивні матеріали щодо підготовки навчальних електронних комплексів (для розробників НЕІК) [Текст] / Комаров В. В. [та ін.]. – Х. : 2011. – 16 с.
17. Створення електронних навчальних дисциплін у віртуальному навчальному середовищі Львівської політехніки [Текст] : посібник / укл. : Д. В. Федасюк, Л. Д. Озірковський, В. М. Якубенко. – Л. : Вид-во Національного університету «Львівська політехніка», 2009. – 60 с.
18. Мясникова, Т. С. Система дистанционного обучения MOODLE [Текст] / Т. С. Мясникова, С. А. Мясников. – Харьков, 2008. – 232 с.

19. Анисимов, А. М. Работа в системе дистанционного обучения Moodle [Текст] : учеб. пособие / А. М. Анисимов. – 2-е изд. испр. и дополн. – Харьков : ХНАГХ, 2009. – 292 с.
20. Свідоцтво про реєстрацію авторського права на твір № 37621 // База даних «Навчальний електронно-інформаційний комплекс (НЕІК) з кримінального права України» авторів: В. Я. Тацій, В. І. Тютюгін, В. І. Борисов, С. М. Іванов, В. В. Карасюк, О. Ю. Соколов. Дата реєстрації 28 березня 2011 року.
21. Свідоцтво про реєстрацію авторського права на твір № 40293 // База даних «Навчальний електронно-інформаційний комплекс (НЕІК) з трудового права України» авторів: С. М. Прилипко, О. М. Ярошенко, Т. А. Занфірова, В. О. Гончаров, С. М. Іванов, В. В. Карасюк, Ю. С. Іванова. Дата реєстрації 21 вересня 2011 року.
22. Тацій, В. Я. Центр інформаційних технологій як технологічна база бібліотеки електронних копій раритетних видань [Текст] / В. Я.Тацій, С. М. Іванов, В. В. Карасюк, С. В. Глинянський // Питання вдосконалення діяльності відділів рідкісних книг бібліотек в інформаційному забезпеченні науково-освітнього процесу : матеріали виступів учасників «круглого столу» (м. Харків, 29 берез. 2012 р.) / за заг. ред. Н. П. Пасмор ; Нац. ун-т «Юрид. акад. України ім. Ярослава Мудрого», наук. б-ка. – Х. : Нац. ун-т «Юрид. акад. України ім. Ярослава Мудрого», 2012. – С. 3–7.

*Наукове видання*

# ІНТЕГРАЦІЯ ПРАВА ТА ІНФОРМАТИКИ: ПРИКЛАДНИЙ І ЗМІСТОВНИЙ АСПЕКТИ

**Монографія**

За загальною редакцією
*В. Г. Іванова, В. Ю. Шепітька, В. В. Карасюка*

Редактор *К. К. Гулий*
Коректори: *Н. Ю. Шестьора, О. М. Нещеретна*
Комп'ютерна верстка *О. І. Лагози*

Підписано до друку з оригінал-макета 09.10.2012.
Формат 60×84 $^{1}/_{16}$. Папір офсетний. Гарнітура Times.
Ум. друк. арк. 14,4. Обл.-вид. арк. 11,5. Вид. № 798.
Тираж 500 прим.

Видавництво «Право» Національної академії правових наук України
та Національного університету «Юридична академія України
імені Ярослава Мудрого»
Україна, 61002, Харків, вул. Чернишевська, 80а
Тел./факс (057) 716-45-53
Сайт: www.pravo-izdat.com.ua
E-mail для авторів: verstka@pravo-izdat.com.ua
E-mail для замовлень: sales@pravo-izdat.com.ua

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників і розповсюджувачів
видавничої продукції — серія ДК № 4219 від 01.12.2011 р.

Виготовлено в друкарні СПДФО Білетченко
Тел. (057) 758-35-98