

Стрімкі зміни у сфері сучасних комп'ютерних технологій призводять до того, що недавня реальність і прогнози сьогодні здаються смішними. «Я думаю, що на світовому ринку може знайтися попит на 5 комп'ютерів» — висловився у 40-х роках минулого століття Том Ватсон, засновник фірми IBM. «Немає ніяких підстав вважати, що хто-небудь захоче мати комп'ютер у себе вдома» — 1977 року був упевнений Кен Олсон, засновник корпорації Digital Equipment. «640 кілобайт пам'яті більш ніж досить для будь-кого» — був переконаний у 1981 році засновник і голова корпорації Microsoft Біл Гейтс.

Комп'ютерна ера почалась 1951 року. Тільки через 11 років фірма IBM запропонувала на ринку перший вінчестер, і лише в 1970 році було розроблено дискету. А сьогодні комп'ютерна грамотність є настільки важливою частиною освіти кожної людини, як вміння читати і писати. Але мінімального набору знань і навичок роботи на персональному комп'ютері замало для того, щоб вижити у світі, де інформація перетворюється на зброю, а економіка стає електронною, поширюється дистанційна освіта та інформаційний кримінал, будуються інформаційні міста та кіберпростір, інформаційно-комунікаційні технології впливають на державне управління і змінюють повсякденне життя кожного громадянина.

Суспільство стає інформаційним — підвищується роль інформації і знань, збільшується частка інформаційних продуктів і послуг у валовому внутрішньому продукті, удосконалюється вже розвинута інформаційно-комунікаційна інфраструктура, формується глобальний інформаційний простір. Це виклик для кожного.

Фахівці практично всіх сфер сьогодні працюють в умовах інформаційних перенавантажень. Єдиний спосіб впора-

тися з ними полягає у використанні нових інформаційних технологій, які змінюють не тільки процеси створення, передавання, оброблення інформації та прийняття рішень на її основі, а й усю діяльність підприємства, організації чи установи.

Очевидно, що правознавець повинен знати, як можна застосувати інформаційні технології у своїй роботі та які правові інформаційні системи вже створено й упроваджено. Але незалежно від майбутнього місця роботи йому необхідні знання про комп'ютерні технології загалом, про тенденції комп'ютеризації та інформатизації, про інформаційні системи підприємницьких фірм, банків, органів державної влади та ін. Без цього юрист не може ефективно виконувати свої функції, завдання.

Більш того, інформатизація викликає принципово нові проблеми, що потребують правового регулювання. Юридичні питання електронного документообігу та мережі Інтернет, застосування криптографічних засобів і цифрової готівки, забезпечення секретності електронного листування та охорони авторських прав на програмне забезпечення, боротьби з кіберзлочинністю та ін. зумовили появу того, що називають «інформаційне право», «комп'ютерне право» або «право з інформаційних технологій», «телекомунікаційне право». Це сфера діяльності кваліфікованих, талановитих юристів, готових до найнеймовірнішого майбутнього.

Пропонований навчальний посібник має за мету допомогти студентам засвоїти основи інформаційних систем і технологій, а також підходи до їх використання в діяльності органів законодавчої та судової влади, прокуратури, Міністерства юстиції і Міністерства внутрішніх справ. Перелік джерел, використаних під час підготовки посібника та рекомендованих для більш поглибленого вивчення дисципліни, наведено наприкінці кожного розділу.



ОСНОВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

1.1. КОНЦЕПЦІЯ ІНФОРМАТИЗАЦІЇ В УКРАЇНІ

Інформатизація — сукупність взаємозв'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що мають на меті створити умови для задоволення інформаційних потреб громадян і суспільства завдяки розробці, розвитку й використанню інформаційних систем, мереж, ресурсів та технологій, які базуються на застосуванні сучасної обчислювальної та комунікаційної техніки. Часто термін «інформатизація» вживається разом із терміном «**комп'ютеризація**», який позначає процес розвитку та впровадження комп'ютерів, що забезпечують автоматизацію інформаційних процесів і технологій у різних сферах людської діяльності.

Наприкінці XX століття інформатизація стала важливою галуззю економіки розвинених країн і визначальною сферою суспільного життя, оскільки дає змогу заощаджувати основні види ресурсів, забезпечувати ефективне адміністративне і господарське управління та знижувати соціальну напруженість. Із цього погляду інформатизація стає важливою функцією держави, фактором забезпечення її безпеки та суверенітету.

Нормативно-правове та нормативно-технічне забезпечення процесу інформатизації в Україні почалося після ухвалення 1998 року Законів України «**Про Національну програму інформатизації**», «**Про Концепцію Національної програми інформатизації**» та «**Про затвердження Завдань Національної програми інформатизації на 1998—2000 роки**». Окрім цього, було ухвалено низку інших нормативних актів Кабінету Міністрів України та Указів Президента України.

Закон України «**Про інформацію**» визначає (а деякі статті Конституції України посилюють) *основні принципи державної політики в галузі інформатизації*:

- інформаційна свобода — «Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір» (ст. 34 Конституції України);

- невтручання в особисте життя — «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди...» (ст. 32 Конституції України);

- відкритість і доступність інформації — «Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе...» (ст. 32 Конституції України), «Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення...» (ст. 57 Конституції України);

- інформаційна безпека — обмеження інформаційної свободи, відкритості й доступності інформації, режим використання персональних даних в інтересах національної безпеки, економічної доцільності й захисту прав інших людей (статті 32, 34 Конституції України);

- право власності на інформаційні ресурси та підтримка різних форм власності;

- відповідальність власників інформаційних ресурсів за якість інформації та порушення під час роботи з інформацією;

- роль держави у формуванні й реалізації політики інформатизації та інформаційної безпеки;

- гармонізація українського інформаційного законодавства із законодавством інших країн.

Згідно з відповідною Національною програмою *основні напрями інформатизації в Україні* такі: розроблення політики та організаційно-правове забезпечення інформатизації; формування національної інфраструктури інформатизації; інформатизація стратегічних напрямів розвитку державності, безпеки та оборони; інформатизація процесів соціально-економічного розвитку; інформатизація пріоритетних галузей економіки; інформатизація фінансової та грошової системи, державного фінансово-економічного контролю; інформатизація соціальної сфери; інформатизація в галузі екології та використання природних ресурсів; інформатизація науки, освіти і культури; міжнародне співробітництво.

Національна програма інформатизації передбачає виконання низки галузевих і регіональних програм та проектів. Зокрема, планується створювати й розвивати інформаційно-аналітичні, обчислювальні та автоматизовані системи, центри й мережі у правовій сфері.

Процес створення оптимальних умов щонайповнішого задоволення інформаційно-правових потреб органів суду, прокуратури, юстиції, Міністерства внутрішніх справ та інших правоохоронних органів завдяки ефективній організації та використанню

інформаційних ресурсів визначається як **правова інформатизація**. Часто це поняття охоплює також процес створення всіх необхідних умов для забезпечення правовою інформацією органів влади, організацій, суб'єктів господарської діяльності та громадян.

Отже, правова інформатизація — це інформатизація правотворчої та правореалізаційної діяльності, а також правове забезпечення процесів інформатизації.

Основні принципи реалізації проектів з інформатизації такі:

1) принцип відкритості політики — усі головні заходи в інформаційній сфері мають відкрито обговорювати фахівці, а їхні думки мають враховуватись під час прийняття рішень;

2) принцип рівності інтересів — інтереси всіх учасників інформаційної діяльності мають бути враховані однаковою мірою незалежно від їхнього суспільного стану, форми власності та державної приналежності;

3) принцип системності передбачає декомпозицію системи на складові (компоненти), кожен з яких можна автономно розробляти й упроваджувати, забезпечуючи єдність технічної політики;

4) принцип пріоритетності вітчизняного виробника — за однакових умов пріоритет віддається конкурентоспроможному вітчизняному виробникові інформаційно-комунікаційних засобів, продуктів і послуг;

5) принцип соціальної орієнтації — основні заходи мають бути спрямовані на забезпечення соціальних інтересів громадян України.

Засобами інформатизації є електронні обчислювальні машини (ЕОМ), програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їхні окремі елементи, інформаційні мережі та мережі зв'язку, що використовуються для реалізації інформаційних технологій. Саме інформаційні системи й технології є предметом подальшого розгляду.

1.2. РОЗВИТОК ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Інформаційна технологія (ІТ) — це комплекс методів і процедур, за допомогою яких реалізуються функції збирання, передавання, оброблення, зберігання та доведення до користувача інформації в організаційно-управлінських системах¹ з використанням обраного комплексу технічних засобів.

¹ Системами організаційного управління (організаційними, організаційно-управлінськими) називають системи, об'єктом керування яких є люди, колективи людей.

Розвиток технічних засобів протягом кількох мільйонів років зумовлював постійне вдосконалення ІТ. Тому виокремлюють кілька *етапів їхнього розвитку*:

- «ручна» інформаційна технологія (панувала до другої половини XIX століття) — оброблення інформації здійснювалось вручну, за допомогою пера, рахівниці, бухгалтерських книг, а зв'язок забезпечувався пересиланням листів і пакетів;
- «механічна» інформаційна технологія розпочалась із винайденням друкарської машинки та телефону, модернізацією системи поштового зв'язку. Така технологія стала базою формування організаційних структур в економіці;
- «електрична» інформаційна технологія (зародилась у 1940—1950-х роках) ґрунтувалась на широкому використанні електричних друкарських машинок, копіювальних машин, портативних диктофонів і т. ін.

З появою та повсюдним упровадженням ЕОМ і периферійної техніки настала ера комп'ютерної інформаційної технології, яка дістала також назву нової, сучасної, безпаперової. Основні принципи нової інформаційної технології (НІТ) — це інтегрованість, гнучкість та інформативність. Для неї характерні такі *особливості*:

- робота користувача в режимі маніпулювання даними (а не програмування);
- цілкова інформаційна підтримка на всіх етапах проходження інформації на основі інтегрованої бази даних, яка передбачає одну уніфіковану форму подання, зберігання, пошуку, відображення, відновлення та захисту даних;
- безпаперовий процес опрацювання документа, коли на папері фіксується лише його остаточний варіант, а проміжні версії та необхідні дані, записані на машинні носії, доводяться до користувача через екран дисплея комп'ютера;
- інтерактивний (діалоговий) режим розв'язування задач, що дає змогу користувачам активно впливати на цей процес;
- уможливлення колективної (групової) співпраці для підготовки документів і виконання завдань на базі кількох персональних комп'ютерів, об'єднаних засобами комунікацій;
- можливість адаптивної перебудови форм і способів подання інформації у процесі розв'язування задачі.

Існують *два способи впровадження НІТ*. Перший передбачає її пристосування до наявної організаційної структури з локальною модернізацією методів роботи. Другий спосіб полягає в тому, що вся організаційна структура модернізується з метою максимального розвитку комунікацій і розробки нових інформаційних вза-

ємозв'язків, які раніше були економічно недоцільними (див. підрозд. 4.2). Саме в разі застосування другого способу інформаційна технологія дає найбільший ефект, оскільки раціонально розподіляються архіви даних, знижуються обсяги інформації, що циркулює в системі, досягається збалансованість ефективності кожного управлінського рішення з обсягом розв'язуваних задач.

Сьогодні також залишаються два організаційні варіанти реалізації інформаційних технологій — **централізоване та розподілене оброблення інформації**. Перший варіант притаманний великим спеціалізованим організаціям (наприклад, регіональним обчислювальним центрам), де створюються підрозділи з оброблення інформації, працівники яких не є фахівцями в певній предметній галузі (оператори та системні адміністратори на противагу юристам і бухгалтерам). В умовах розподіленого оброблення інформації відповідні операції покладаються на працівників окремих функціональних підрозділів, які діють у межах своїх професійних обов'язків. Розподілене оброблення інформації ґрунтується на застосуванні персональних ЕОМ, які можуть бути відокремленими або пов'язаними в локальну чи глобальну мережу (див. розд. 2). Зауважимо, що за наявності великих і складних мереж ЕОМ деякі функції (підтримка мережі в дієздатному стані, супроводження програмного забезпечення і т. ін.) покладаються на персонал, який має спеціальну підготовку з комп'ютерної техніки.

За будь-якого варіанта реалізація інформаційної технології має ґрунтуватися на деяких *принципах*, найважливішими серед яких є зручність виконання операцій для користувача, мінімальні витрати ручної праці на оброблення інформації, можливість перевірки повноти та коректності розрахунків на ЕОМ, мінімальні витрати часу на поновлення інформації в разі її втрати, забезпечення захисту інформації від несанкціонованого доступу.

1.3. ПОНЯТТЯ ТА ЕТАПИ РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ

У літературі знаходимо кілька визначень терміна «інформаційна система». У загальному розумінні організаційні системи, в яких оброблення інформації відбувається за допомогою засобів обчислювальної техніки, називають (автоматизованими) інформаційними системами управління. Можна також керуватися одним із таких визначень:

інформаційна система (ІС) — це людино-машинна система, яка збирає, нагромаджує, зберігає, обробляє та видає за запитом або на замовлення користувача інформацію у вигляді даних і знань, необхідних для виконання функцій управління;

інформаційна система — це організаційно-технічна система, яка забезпечує вироблення рішень на основі автоматизації інформаційних процесів у різних сферах людської діяльності.

Початок створення ІС у нашій країні датують 1963 роком, коли на великих підприємствах почали використовувати ЕОМ для розв'язування задач економіко-організаційного управління. Відтоді компоненти ІС — дані та обчислення — зазнали істотних змін, що дає підстави виокремити *три етапи розвитку ІС*.

ІС 1-го покоління, які у вітчизняній літературі відомі під назвою «Автоматизовані системи управління (АСУ) — позадачний підхід», а в зарубіжній — «Системи (електронного) оброблення даних» (Data Processing System), обмежувались розв'язуванням деяких функціональних управлінських задач, зокрема задач бухгалтерського обліку. Для кожної такої задачі окремо готувались дані, створювалась математична модель і розроблялось програмне забезпечення. Крім процедур безпосереднього розв'язування задачі до програм вносились процедури формування та ведення необхідного інформаційного фонду. Такий підхід характеризувався інформаційною надмірністю (дані, сформовані для однієї задачі, не могли бути використані для розв'язування інших), математичною надмірністю (відомо, що математичні моделі різних задач мають спільні блоки), тривалістю та великою трудомісткістю розробки, недостатньою адаптованістю ІС до можливих змін.

В основу побудови ІС 2-го покоління (1972—1986 роки) було покладено концепцію централізовано керованої бази даних, яка за допомогою спеціального програмного продукту (системи керування базою даних) обслуговує всі прикладні програми. Інакше кажучи, забезпечувалось колективне використання даних. Згідно з цим системи 2-го покоління називали «АСУ — концепція бази даних» та «Управлінські (адміністративні) ІС» (Management Information System). Головна функція таких систем полягала в забезпеченні керівництва інформацією.

В ІС 3-го покоління було реалізовано концепцію єдиної централізовано керованої бази моделей — блоків обчислень, спільних для багатьох прикладних програм. Такі системи дістали назву **систем підтримки прийняття рішень** (СППР, Decision Support System). СППР — це інтерактивна комп'ютерна система, призначена для підтримки різних видів діяльності в разі прийняття рішень стосовно

слабоструктурованих або неструктурованих проблем. Сьогодні в різних галузях СППР розглядаються як перспективний напрям використання обчислювальної техніки та інструмент підвищення ефективності праці (див. докладніше підрозд. 1.7).



Проблеми прийняття рішень — класифікація Г. Саймона

Відомий американський учений Г. Саймон виокремив три класи проблем прийняття рішень:

▲ *добре структуровані (цілком формалізовані, кількісно сформульовані) проблеми — рішення приймаються в умовах добре визначених цілей і цілковитої доступності необхідної інформації; фактори, які потрібно врахувати, та наслідки дій або детерміновані (детерміновані ситуації), або стохастичні (ситуації прийняття рішень в умовах ризику). Прикладом є задачі бухгалтерського та складського обліку, підготовки статистичної звітності;*

▲ *неструктуровані (неформалізовані, якісно сформульовані) — рішення приймаються за неясних цілей, неповної вхідної інформації, невизначеності наслідків дій. Для проблем описано лише найважливіші характеристики та ознаки, а кількісні залежності між ними невідомі. Прикладом є задачі довгострокового прогнозування та організаційних перетворень;*

▲ *слабоструктуровані (змішані) проблеми — рішення приймаються в умовах неповної інформації, проблеми містять як кількісні, так і якісні елементи. Прикладом є задача вибору проекту проведення наукових досліджень.*

Існує певна відповідність між виділеними класами задач і категоріями працівників організаційного управління. Так, керівники (директори, головні адміністратори) переважно вирішують неструктуровані задачі, спеціалісти (начальники функціональних служб, головні спеціалісти) — слабоструктуровані, технічні робітники (касири, коректори, експедитори) — формалізовані. Таким чином, можна сказати, що СППР зорієнтовані на працівників вищої та середньої ланок управління.

1.4. СТРУКТУРА ІНФОРМАЦІЙНИХ СИСТЕМ

Комп'ютерні ІС належать до класу складних систем, які містять багато різноманітних елементів, що взаємодіють. Повної і загальноприйнятої класифікації елементів ІС досі не існує. Найчастіше у структурі ІС виокремлюють компоненти — елементи, які вважають неподільними. **Компонент (підсистема) ІС** — це частина ІС, виокремлена за зазначеною ознакою або сукупністю

ознак, що розглядається як самостійне ціле. За своїм призначенням компоненти поділяються на забезпечувальні та функціональні.

Забезпечувальні компоненти — види забезпечення — ІС:

- технічне — сукупність усіх технічних засобів, використовуваних під час функціонування системи;
- програмне (ПЗ) — сукупність програм на носіях даних і програмних документів, що призначені для відлагодження, функціонування та перевірки роботоздатності ІС;
- математичне — сукупність математичних методів, моделей і алгоритмів розв'язування задач, які застосовуються в ІС. До цього виду забезпечення включають моделі та алгоритми, які стають надалі інструментом розробки програмних засобів (моделі системи управління та об'єкта автоматизації відносять до організаційного забезпечення);
- організаційне — сукупність документів, що описують технологію функціонування ІС, методи, згідно з якими користувачі вибирають і застосовують технологічні прийоми для одержання конкретних результатів під час функціонування ІС;
- інформаційне — інформаційні ресурси як предмет праці, методи і засоби ведення інформаційної бази. До інформаційного забезпечення належать форми документів, нормативна база й реалізовані рішення щодо обсягів, розміщення та форм існування інформації, яка використовується в ІС під час її функціонування;
- лінгвістичне — сукупність засобів і правил формалізації природної мови, які під час функціонування ІС використовуються при спілкуванні користувачів та експлуатаційного персоналу ІС з комплексом технічних засобів;
- правове — сукупність правових норм, які регламентують правові відносини під час функціонування ІС та юридичний статус результатів такого функціонування;
- ергономічне — сукупність засобів і методів, які створюють найсприятливіші умови праці людини в ІС, умови для взаємодії людини та ЕОМ. Ергономічні вимоги визначаються властивостями людини та характеристиками середовища і встановлюються для підвищення ефективності, надійності та безпеки функціонування системи «людина — машина».

Функціональний підхід до структури ІС дає змогу виокремити її елементи за іншим принципом.

Функція ІС — це сукупність дій ІС, спрямована на досягнення зазначеної мети. Перелік функцій конкретної ІС залежить від сфери її діяльності, об'єкта управління, призначення і т. ін.



Складові ІС — ергономічне забезпечення та інтерфейс користувача

Робота користувача з ІС має бути зручною і комфортною. На емоційний, фізичний і розумовий комфорт людини впливають соціальні фактори, фактори фізичної та психологічної ергономіки — психологічний клімат, конструктивні особливості обладнання, доступність і надійність системи, чутливість системи, якість роботи діалогу «користувач — система».

Інтерфейс користувача — це комплекс апаратних і програмних засобів, що забезпечує взаємодію користувача з комп'ютером. Це поняття включає три головні аспекти:

- ▲ мову дій — що може робити користувач під час взаємодії з ІС;
- ▲ мову відображення — що бачить (чує) користувач у результаті роботи системи;
- ▲ базу знань — що необхідно знати користувачеві для роботи з ІС.

Близьким за змістом до терміна «функція ІС» є термін **«задача оброблення даних»** — функція або її частина, що являє собою формалізовану сукупність автоматичних дій, виконання яких приводить до результатів заданого виду.

Класифікація задач важлива для розуміння можливого призначення ІС і характеристик технології автоматизованого оброблення даних.

За *сферою розв'язування* задачі можна поділити на економічні, політичні, правові тощо. Основою розв'язування будь-якої правової задачі є те чи інше перетворення інформації. З огляду на це **правову задачу** (у широкому сенсі) можна визначити як ситуацію правового характеру, яка потребує виконання певного комплексу дій, що мають на меті знайти такі кількісні та якісні характеристики початкової інформації про об'єкт пізнання, які, у свою чергу, дали б змогу здобути нові знання про нього і використовувати їх для відшукування істини у виконуваному правовому дослідженні. Оскільки початкової інформації часто бракує для розв'язування задачі, то доводиться перетворювати й саму її постановку.

З погляду *можливості автоматизованого розв'язування* правові задачі, як і будь-які інші, можна поділити на кілька типів:

- такі, що їх може розв'язати тільки людина;
- такі, що людина може їх розв'язати, скориставшись технічними засобами для виконання тих чи інших операцій, що входять до задачі;
- такі, що людина може їх розв'язати, утворивши з машиною діалогову людино-машинну систему;
- такі, що машина може їх розв'язати без втручання людини.

Межа між названими типами задач розпливчаста, але спостерігається постійна тенденція до збільшення частки робіт, виконуваних автоматизовано або автоматично. Прикладом є поділ обов'язків між людиною та ЕОМ із судово-криміналістичної експертизи. На початку використання обчислювальної техніки судовий експерт працював з ЕОМ через посередника (оператора) — формував завдання та початкові дані, застосовував традиційні криміналістичні методи дослідження для контролю і поповнення машинних даних, зіставляв здобуті результати й формулював висновки. Згодом необхідність у посередникові відпала, а з повним визнанням надійності результатів, отримуваних за допомогою ЕОМ, відпала потреба в паралельних дослідженнях з використанням традиційних криміналістичних методів. Сьогодні виконання деяких видів криміналістичних експертиз (переважно ідентифікаційного характеру) повністю автоматизоване — від кодування початкової інформації до оцінювання здобутих результатів.

Спосіб взаємодії людини з ЕОМ, поділ обов'язків і відповідальності між ними багато в чому залежить від *ступеня формалізації алгоритму*. За цією ознакою розрізняють:

- формалізовані задачі — задачі, для яких визначено чіткий алгоритм розв'язування, описаний у вигляді математичних формул і залежностей. Такі задачі можуть розв'язуватись в автоматичному режимі;
- частково формалізовані — повний алгоритм розв'язування задачі невідомий, відомі тільки окремі його частини. Розв'язування задачі розбивається на окремі етапи, порядок виконання яких залежить від проміжних результатів, що їх має оцінити користувач. Для таких задач передбачається інтерактивний режим розв'язування;
- неформалізовані — неможливо визначити алгоритм обчислення заздалегідь. Для розв'язування таких задач існують спеціальні методи, за допомогою яких в інтерактивному режимі можна виконати певну дію, задавши початкові умови, що можуть постійно змінюватись. Якість розв'язку задачі цілком залежить від кваліфікації, таланту та інтуїції людини.

За *методом обчислення (математичною сутністю)* виокремлюють задачі прямого розрахунку, в яких виконуються звичайні арифметичні дії за чітко визначеним алгоритмом; оптимізаційні, які полягають у виборі одного (оптимального за визначеним критерієм) розв'язку серед багатьох можливих, та інформаційно-пошукові (типу «запитання—відповідь»). Для оптимізаційних задач характерні, як правило, невеликі обсяги вхідних даних і складні методики розрахунків з використанням різноманітних матема-

тичних моделей. Складні методики розв'язування притаманні й інформаційно-пошуковим задачам, які оперують значними обсягами інформації, що характерне й для задач прямого розрахунку, які є найпростішими стосовно алгоритму.

За *характером перетворення інформації* розрізняють задачі обчислювальні, імітаційні, прийняття рішень.

За *регулярністю розв'язування* бувають задачі систематичні, епізодичні та випадкові, а за *частотою виникнення і необхідною швидкістю розв'язування* — регламентовані та оперативні.

1.5. КЛАСИФІКАЦІЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Загальноприйнятої класифікації ІС досі не існує, тому для виокремлення класів таких систем беруть різні ознаки.

За *предметною сферою застосування* розрізняють економіко-організаційні АСУ, автоматизовані системи управління технологічними процесами (АСУ ТП) та проектно-конструкторські системи (САПР). Конкретні класи систем можна розглядати залежно від предметної галузі. **Предметна галузь** — це сукупність об'єктів, понять, зв'язків, відношень і способів перетворення та взаємодії цих об'єктів під час розв'язування задач, що стосуються певної сфери людської діяльності (наприклад, юридичної).



Інтеграція АСУ та АСУ ТП — два приклади

Відмінності між АСУ та АСУ ТП зумовлюються різницею в характері об'єкта управління (колективи людей і, відповідно, машини, прилади, обладнання) та формах передавання інформації (документ і, відповідно, сигнал). Водночас сьогодинішній етап розвитку ІС характеризується високим ступенем їхньої інтеграції — спосіб організації окремих компонентів в одну систему, яка забезпечує узгоджену та цілеспрямовану взаємодію цих компонентів.

Наприклад, Єдина автоматизована система керування міським пасажирським транспортом у м. Києві об'єднує чотири автономні системи — диспетчерське управління міським комунальним транспортом, управління маршрутками, автоматизоване управління дорожнім рухом і паркуванням. Для забезпечення роботи електронного регулювальника руху на перехрестях використовуватимуться камери стеження.

Особливістю юридичної діяльності є те, що здебільшого і «основне виробництво» (діяльність юриста за своєю сутністю), і система управління пов'язані з виробленням і переробкою інформації. Таким чином, у діяльності юридичних установ застосовуються тільки автоматизовані системи управління, але юрист може у своїй роботі використовувати інформацію, що надходить з АСУ ТП, так само як і з інших систем.

За ступенем централізації оброблення інформації виокремлюють централізовані ІС, децентралізовані, колективного використання.

За ступенем автоматизації процесів управління розрізняють інформаційно-пошукові, інформаційно-довідкові, інформаційно-управляючі системи, СППР, інтелектуальні ІС.

За рівнем розрізняють державні ІС, територіальні (регіональні), галузеві, об'єднань, підприємств або установ, технологічних процесів.

Державні ІС призначені для розв'язування найважливіших проблем країни. Це, наприклад, інформаційно-аналітичні системи Верховної Ради України, Кабінету Міністрів України, Адміністрації Президента України, Ради національної безпеки і оборони України, Конституційного Суду України, Верховного Суду України, Генеральної прокуратури України.

Територіальні ІС призначені для управління адміністративно-територіальним регіоном. Це ІС області, міста, району.

Галузеві ІС призначені для управління відомчими підприємствами та організаціями.

ІС управління підприємствами (організаціями, установами) становлять одну з найчисленніших категорій. Єдину характеристику таких систем подати неможливо, бо дуже різноманітні системи та об'єкти, де вони використовуються, — це банки і підприємства, суди і прокуратури, податкові органи і страхові компанії та багато інших. Але існують два терміни, актуальні для будь-якої предметної галузі, — «корпоративна ІС» (КІС) та «автоматизоване робоче місце» (АРМ).

Термін «корпоративна ІС» має різні тлумачення. Загалом можна визначити, що **корпоративна ІС** — це ІС масштабу підприємства¹, яка характеризується здатністю працювати в розподіленій структурі (корпорації) із множиною територіально розосереджених філій, а також повнофункціональністю. Схематично рівневу структуру КІС наведено в табл. 1.1.

Як правило, й інтегровані АСУ (ІАСУ) забезпечують автоматизацію всіх управлінських задач на всіх рівнях. Але це стосується лише задач оперативного обліку, формалізованих задач. Тому подібні системи позначаються як OLTP (On-line Transaction Processing, оперативне оброблення трансакцій²). Їх призначення — підвищувати продуктивність праці робітників та попереджувати технічні помилки й невідповідності, які можуть виникати через великий обсяг

¹ Термін в англomовній літературі — Enterprise Information System.

² У спеціальній літературі слово «transaction», яке має значення «операція», не перекладається.

оброблюваної інформації. Основною ознакою таких систем є прогнозованість запитів на оброблення інформації.

Оскільки аналізувати інформацію та генерувати звіти безпосередньо в OLTP-системах практично неможливо через розосередженість даних по різних джерелах (різномісних базах даних), їх інтегрують у сховище даних (див. підрозд. 1.7). Побудована на цій основі управлінська ІС нижнього рівня надає доступ до даних по підприємству (організації), структурованих згідно з вимогами середнього управлінського персоналу.

Корпоративне сховище даних є основою і для вирішення задач стратегічного рівня за допомогою СППР, зокрема OLAP-систем (On-Line Analytical Processing, оперативна аналітична обробка, див. підрозд. 1.7). Найчастіше такі системи не входять до класу ІАСУ, а є розробками третіх фірм. Головною ознакою таких систем є непрогнозованість запитів — неможливо заздалегідь визначити їх кількість, складність і час надходження.

Відфільтрована й агрегована інформація використовується для вироблення стратегічних рішень з управління та розвитку відповідно до описаної управлінської ідеології. Реалізація в КІС правил визначення бізнес-результату залежно від певних умов або дій становить ще одну відмінність таких систем.

Таблиця. 1.1

СТРУКТУРА КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Рівень	Системи	Користувачі	Інформація
Стратегічний	Корпоративна ІС	Вище керівництво	Стратегічний план розвитку
	Аналітичні ІС (СППР, OLAP-системи)	Інформаційно-аналітична служба	Аналітичні звіти на рівні підприємства (організації), прогнози, плани
Оперативний	Управлінська ІС нижнього рівня	Керівники середньої ланки	Корпоративне сховище даних, оперативні розпорядження, звіти на рівні підрозділу
	Системи оперативного обліку — OLTP (ІАСУ, АСУ ТП, САПР та ін.)	Виконавці нижньої ланки	Початкові облікові дані (база даних)

Отже можна сказати, що ІАСУ є основою для побудови КІС і входить до неї як органічна складова. Базовим структурним елементом таких систем є АРМ.

Автоматизоване робоче місце (АРМ) — це програмно-технічний комплекс, призначений для автоматизації діяльності певного виду. Основною характеристикою АРМ є орієнтація на людину, яка не має професійної підготовки з використання обчислювальної техніки, але професійно обізнана у конкретній предметній галузі. Залежно від категорії працівників організаційного управління, до якої належать користувачі, а також відповідно до характеру розв'язуваних задач розглядають *три класи типових АРМ*:

- АРМ керівника складається з підсистем забезпечення ділової діяльності (електронний записник, особистий архів, картотека доручень і т. ін.), прийняття рішень, рутинних робіт та комунікацій;
- АРМ спеціаліста. Основою такого АРМ є підсистема забезпечення професійної діяльності, яка звичайно містить розвинену базу даних, засоби електронного обчислення форм і ділової графіки, а також набір програмних засобів для проведення математичних розрахунків і моделювання;
- АРМ технічного та допоміжного персоналу. Основні функції, що автоматизуються, — це введення інформації, оформлення документів, ведення картотек і архівів, оброблення вхідної та вихідної документації, контроль виконавчої діяльності. Оскільки виконання таких операцій мало залежить від специфіки галузі, підприємства чи установи, можливий масовий випуск типових АРМ цієї категорії.

1.6. ПРАВОВА ІНФОРМАЦІЯ ЯК ОСНОВА ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВОВИХ ІС

Поняття «інформація» має центральне значення в контексті інформаційних систем і технологій. У загальному розумінні воно означає пояснення, викладання, повідомлення. У теорії інформаційних систем інформація ототожнюється з будь-якими відомостями (даними), тобто тлумачиться як сукупність відомостей про будь-що або будь-кого. Згідно з кібернетичним підходом інформацією є лише нові, корисні, вагомі для користувача відомості.

Відповідно до Закону України «Про інформацію» **інформація** — це документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навко-

лишньому природному середовищі. Як один із видів інформації цей Закон виокремлює **правову інформацію** — сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Джерелами правової інформації є Конституція України, інші законодавчі й підзаконні нормативні правові акти, міжнародні договори та угоди, норми й принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань. Отже, правова інформація поділяється на **нормативну і ненормативну**.

До ненормативної правової інформації можна віднести документи, які не містять правових норм, а отже, мають рекомендаційний та інформаційний характер. Її можна поділити на дві групи.

1. Інформація про стан законності та правопорядку.

- інформація про дотримання прав і свобод людини, що міститься у звітах Уповноваженого з прав людини, офіційні дані про стан виконання Україною своїх міжнародних зобов'язань, матеріали комісій з прав людини;

- інформація про стан законності й правопорядку, ефективності прокурорського нагляду, що міститься в публікаціях засобів масової інформації, у періодичних виданнях правоохоронних і правозастосовних органів, інформація про форми і способи захисту прав громадян, про вжиті заходи з відновлення законності.

2. Інформація, пов'язана з розкриттям і розслідуванням правопорушень:

- кримінологічна — дані про злочинність та інші правопорушення, а також ефективність карних заходів;

- криміналістична — інформація, що використовується при доведенні факту злочину та ідентифікації особи чи групи осіб, які вчинили злочин;

- судово-експертна — інформація, що використовується під час судових експертиз для доведення (або спростування) факту злочину і вини обвинуваченого;

- оперативно-розшукова — інформація, що відбиває хід і результати проведення оперативно-розшукових заходів з установлення та розшуку осіб, які вчинили кримінально карне діяння і переходять від правосуддя, а також інші відомості та матеріали.

Існують й інші підходи до класифікації правової інформації. Деякі з ознак класифікації є спільними для різних видів інформації.

Залежно від *стадії виникнення* розрізняють первинну інформацію, яка виникає безпосередньо у процесі юридичної діяльності, і вторинну, яка виникає в результаті оброблення первинної та (або) іншої вторинної інформації. До вторинної належить інформація проміжна і результатна. Одержання результатної інформації є метою функціонування ІС.

З позиції *технології розв'язування задач* розрізняють інформацію вхідну, проміжну і вихідну. Вхідною називають інформацію, що підлягає обробці — первинна і вторинна інформація, константи. Вихідна інформація є підсумком оброблення вхідних даних, але вона разом з результатною інформацією містить і деякі первинні дані. Проміжною є інформація, необхідна для розв'язування цих самих задач у наступних періодах.

За *стабільністю* інформація поділяється на постійну (сталу), яка не змінює своїх значень, умовно постійну, для якої це твердження може бути справедливим протягом тривалого періоду, та змінну, значення якої часто змінюються.

Різновиди інформації варто враховувати, організовуючи оброблення інформації, створюючи інформаційні системи, вибираючи варіанти технології розв'язування конкретних задач. Зазначимо також, правова інформація має бути вірогідною — об'єктивно відбивати реальність, повною — достатньою для розв'язування правової задачі, своєчасною — надходити до користувача тоді, коли той матиме в ній потребу.

Деякі властивості інформації є об'єктом правового регулювання. Зокрема, установлюється **правовий режим доступу до інформації** — передбачений правовими нормами порядок одержання, використання, поширення та зберігання інформації. За цією ознакою розрізняють:

- відкриту інформацію, доступ до якої забезпечується її систематичним публікуванням в офіційних друкованих виданнях («Офіційний вісник України», «Відомості Верховної Ради України», газета «Урядовий кур'єр»), поширенням її засобами масової комунікації, безпосереднім її наданням зацікавленим громадянам, державним органам та юридичним особам;
- інформацію з обмеженим доступом — конфіденційну і таємну. **Конфіденційна інформація** — це відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов. До **таємної інформації** належить

інформація, що містить відомості, які становлять державну чи іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству, державі.

Зазначимо, що конфіденційність (секретність) — це тільки одна з характеристик інформації, які мають розглядатись у контексті її автоматизованого оброблення. Вона є головною для важливої державної інформації. Для відкритої інформації не менш важливими вимогами є цілісність і доступність, у деяких випадках — захищеність від тиражування.

Організація процесів отримання, використання, поширення та зберігання інформації, тобто *інформаційної діяльності* — сукупності дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави, — істотно залежить від вибору носіїв та способу фіксації інформації на них. Одним з основних носіїв інформації, зокрема правової, є паперовий документ. Але з бурхливим зростанням обсягів правової інформації, яке почалося в розвинених країнах з другої половини XX століття разом з ускладненням завдань соціального управління і регулювання, постала невідкладна потреба в широкому використанні й інших носіїв. Сьогодні *документ* — це передбачена законом матеріальна форма одержання, зберігання, використання і поширення інформації фіксуванням її на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носіїві. Це визначення стосується не тільки рукописних чи друкованих матеріалів на папері чи у вигляді книг, журналів, діаграм, карт тощо, а й матеріалів недрукованого походження (машинозчитуваних записів, фільмів, звукових записів) і тривимірних об'єктів чи реалій.

У контексті інформаційних систем і технологій особливого значення набуває таке поняття, як *дані* — інформація, подана у формалізованому вигляді, придатному для обробки автоматизованими засобами за можливої участі людини. Сучасною формою організації даних на машинних носіях є автоматизовані банки даних.

Автоматизований банк даних — це система інформаційних, математичних, програмних, мовних, організаційних і технічних засобів, необхідних для інтегрованого нагромадження, зберігання, ведення, актуалізації, пошуку та видачі даних. Основними складовими автоматизованого банку даних є база даних і система керування базою даних (СКБД).

База даних — це іменована структурована сукупність взаємозв'язаних даних, що відбиває стан об'єктів та відношень між ними в певній предметній галузі. База даних призначається для ви-

користання багатьма користувачами у процесі розв'язування кількох прикладних задач і не залежить від окремих прикладних програм. База даних перебуває під управлінням **СКБД** — комплексу програмних і мовних засобів загального і спеціального призначення, необхідних для створення бази даних, підтримки її в актуальному стані, маніпулювання даними й організації доступу до них різних користувачів чи прикладних програм в умовах застосовуваної технології оброблення інформації.

Організація баз даних є необхідною передумовою для створення правових інформаційних систем і належного забезпечення правовою інформацією суспільства, але використання таких баз може призводити до нових проблем. Скажімо, нагромадження великого обсягу правової інформації в банку даних може призвести до монополізації, а згодом і до зловживань у вигляді приховування інформації, її незаконного оприлюднення чи використання з корисливою метою. Для запобігання таким зловживанням право власності на правову інформацію має належати державі, а використання даних регламентуватися законодавством. Іншим вкрай важливим питанням є забезпечення захисту інформації, про що йдеться в розд. 3.

1.7. СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Системами підтримки прийняття рішень називають інтелектуальні системи, за допомогою яких особи, що приймають рішення (ОПР), мають змогу аналізувати ситуації, формулювати задачі, виробляти, контролювати й оцінювати варіанти рішень, які забезпечують досягнення поставленої мети. Згідно з таким узагальненим визначенням можна тлумачити СППР як одну з категорій управлінських інформаційних систем. Проте останні найчастіше визначаються як системи підготовки управлінських звітів — періодичних структурованих документів. На противагу цьому СППР має бути дієвою інтерактивною системою, що реагує як на заплановані, так і на непередбачувані інформаційні запити, зорієнтована на специфічний тип рішень або на множину взаємозв'язаних рішень і застосовується там, де неможливо або небажано мати повністю автоматичну систему.

Сфера використання таких систем практично необмежена. Вони мають не лише суто економічне застосування, а й призначаються для правоохоронних органів, судового виробництва, органів виконання покарань, національної безпеки, служби охоро-

ни, військової розвідки, митниці, податкової поліції, міграційної служби та багатьох інших. Правоохоронна діяльність вирізняється в цьому списку, оскільки створення СППР у цій галузі можливе тільки в разі взаємодії математиків, юристів, практиків та фахівців з інформаційних технологій, причому готові системи мають працювати в умовах розподілених організаційних структур, що використовують різноманітні засоби автоматизації і не завжди забезпечені якісними каналами зв'язку.

Понад 25 років практичного використання СППР показали, що прийняття рішень можна підтримувати по-різному. Різні типи СППР надають різну допомогу ОПР — пропонуються можливості використовувати і маніпулювати великими базами даних або застосовувати правила і контрольні перевірки чи користуватися великими математичними моделями. Для позначення певних типів СППР (іноді із суто маркетинговою метою) вживають багато специфічних термінів. Основні категорії СППР розглядають залежно від того, який із головних компонентів системи взято за домінуючий. Проте зазначимо, що ІС можна віднести до класу СППР тільки за наявності в неї *родової структури* — підсистем керування базою даних, керування базою моделей та інтерфейсу користувача.

СППР, зорієнтовані на дані, — це тип СППР, який зосереджується передусім на доступі й маніпуляції великими базами структурованих даних. До цієї категорії відносять:

- системи підготовки управлінських звітів;
- **сховища даних** (Data Warehouse) — це особлива форма організації бази даних, призначена для зберігання в погодженому вигляді агрегованої інформації, одержуваної з баз даних різних OLTP-систем та зовнішніх джерел. Одна з найважливіших цілей створення сховищ даних — швидка реакція на інтерактивні запити. Сховища містять великі обсяги даних і мають такі характеристики, як предметна орієнтація, інтегрованість, підтримання хронології, незмінність, мінімальна надмірність, захищеність;
- системи аналізу даних (On-line Analytical Processing, **OLAP**) — це системи швидкого аналізу розподіленої багатовимірної інформації. Термін «OLAP» невіддільний від терміна «сховище даних». OLAP-системи забезпечують різні точки зору на дані та різні форми їх подання. Програмний продукт можна віднести до класу OLAP, якщо він має три головні особливості: багатовимірність даних, складні обчислення, швидка обробка;
- **виконавчі інформаційні системи** (Executive Information System, інформаційна система керівника) — автоматизовані системи, призначені для забезпечення необхідною актуальною інфор-

мацією менеджерів вищої ланки управління у процесі прийняття стратегічних рішень. Акцент робиться на графічні дисплеї та легкий у використанні інтерфейс, за допомогою яких подається інформація з корпоративної бази даних;

- **географічні ІС** (геоінформаційні системи, Geographic Information System, ГІС) або просторові СППР (Spatial DSS) — СППР, що дають змогу поєднувати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо). Прикладом таких систем є ГІС, що використовуються в роботі органів внутрішніх справ (див. підрозд. 9.6).



OLAP — кілька застосувань у діяльності правоохоронних органів

Засоби аналітичної обробки допомагають знизити витрати й заощадити час на пошук інформації, істотної для розкриття та розслідування злочинів. Сфери застосування таких систем різноманітні. Серед них можна виокремити:

- ▲ *розслідування фактів шахрайства — оперативне збирання та аналіз інформації з різних джерел (повідомлення, результати попереднього розслідування, банківська і фінансова інформація), установлення неявних зв'язків, часовий аналіз, що виявляє нестикування в подіях, виявлення нових слідів у справі і т. ін.;*

- ▲ *розвідувальний аналіз (комп'ютерна розвідка) — знімання інформації з радіоэфіру й телефонних ліній, нагромадження даних оперативної роботи (фіксація подій, де з'являються підозрювані, аналіз їхніх зв'язків і т. ін.); аналіз послідовності малозначущих на перший погляд подій (наприклад, регулярне перерахування невеликих сум різними особами на один рахунок) з метою виявлення прихованих закономірностей; а також планування цілей розвідки, формування і перевірка робочих гіпотез, організація збирання, тестування та інтерпретації даних із подальшим поданням результатів у вигляді діаграм, схем, таблиць, графіків;*

- ▲ *визначення потенційних об'єктів і суб'єктів кримінальної активності — профілактика злочинів, ідентифікація порушників закону, з'ясування цілей, часу та об'єктів можливого злочину, запобігання масовим злочинам і терористичним актам, прогнозування можливостей і напрямків промислового шпигунства, побудова картини обвинувачення і врахування всіх факторів;*

- ▲ *непроцесуальне використання даних — аналіз публікацій у відкритому друці, формування громадської думки, підготовка кон-трактів для комерційних структур і т. ін.*

Другу велику категорію становлять *СППР, зорієнтовані на доступ та маніпуляцію моделями* — статистичними, фінансовими, оптимізаційними і/або імітаційними. Здебільшого такі системи використовують дані й параметри, що їх надають ОПР, але, як правило, не потребують великих обсягів даних. Приклади таких СППР:

- засоби аналізу рішень, які допомагають ОПР розбити проблему на складові й структурувати її. Мета цих інструментальних засобів полягає в тому, щоб допомогти користувачеві застосувати такі моделі, як дерева рішень, моделі багатоатрибутної корисності, моделі Баєса, моделі аналізу ієрархій тощо;
- засоби лінійного програмування — засоби використання відповідних математичних моделей для пошуку оптимального розв'язку задач розподілу ресурсів і т. ін.;
- імітаційні засоби — засоби проведення певної кількості експериментів для перевірки результатів, що впливають з кількісної моделі системи.

Деякі OLAP-системи, що дають змогу виконувати складний аналіз даних, можуть бути класифіковані як гібридні СППР, що забезпечують і моделювання, і пошук та підсумковий аналіз даних. Гібридним підходом до СППР вважаються також технології **здобування даних** (Data Mining). Синонімами терміна «здобування даних» є «виявлення знань у базах даних» та «інтелектуальний аналіз даних». Мета здобування даних полягає у виявленні прихованих правил і закономірностей у наборах даних.

Засоби здобування даних та експертні системи становлять ще одну категорію СППР — *рекомендаційні СППР* (Suggestion DSS). Експертні системи (ЕС) як системи штучного інтелекту часто розглядають як окремий клас ІС, але останнім часом спостерігається тенденція реалізації їхніх модулів у складі СППР і виконавчих ІС. Докладніше ЕС розглянуто в підрозд. 1.8.

СППР, зорієнтовані на документи розробляються для управління неструктурованими документами і Web-сторінками (див. підрозд. 2.4). Такі СППР інтегрують різноманітні технології зберігання та оброблення гіпертекстових документів, зображень, звуків, відео тощо.

Групові СППР (комунікаційні СППР) — це інтерактивні автоматизовані системи, призначені для підтримки розв'язування неструктурованих і напівструктурованих проблем кількома ОПР, що працюють як група. Групові СППР є гібридними системами — вони підтримують електронні, візуальні та звукові комунікації, складання розкладів, спільне використання даних і моде-

лей, колективне генерування альтернатив, консолідацію ідей та інтерпретацію результатів. Крім цього, групові СППР мають можливість, які вже були розглянуті стосовно інших класів СППР.

Нині більшість використовуваних СППР є внутрішньоорганізаційними — їх розроблено для індивідуального або групового використання в межах окремої організації. На відміну від них *інтерорганізаційні СППР*, що належать до порівняно нової категорії систем, можуть мати серед своїх користувачів і зовнішніх щодо фірми осіб (акціонерів, споживачів, постачальників і т. ін.). Створити такі системи вдалося насамперед завдяки розширенню доступу до мережі Інтернет, яка забезпечує комунікаційні зв'язки різних типів, зокрема й необхідні для СППР. На базі Web-технологій створюються та використовуються системи, які дістали назву Web-зорієнтованих.

Усі зазначені типи СППР можна класифікувати залежно від ступеня їх спеціалізації. *Функціонально зорієнтовані системи* розробляються для підтримання специфічних бізнес-функцій або типів ділової діяльності. Такі системи можна назвати галузевими. Вони можуть бути зорієнтовані на маркетинг або фінанси, складання розкладів або встановлення діагнозів. Зазначені СППР можна придбати в «коробковому» варіанті або створити в результаті пристосування загальноорієнтованих систем, які в цілому підтримують ширші завдання, такі як управління проектами, аналіз рішень, бізнес-планування.

Очевидно, що в юридичній діяльності доводиться застосовувати численні як загально- так і функціонально зорієнтовані системи. Наприклад, аналітичні продукти англійської компанії i2 Group, що їх сьогодні Інтерпол та Європол прийняли як стандарт, використовують 1300 державних і комерційних організацій у 90 країнах світу. Технології i2 добре зарекомендували себе, коли йдеться про введення оперативно-слідчої інформації, аналіз даних, візуалізацію результатів і планування заходів, спрямованих на боротьбу з організованою злочинністю, незаконним обігом наркотиків та економічними злочинами. Системи забезпечують перевірку висунутих слідчих версій, аналіз результатів слідчих дій, виявлення прихованих зв'язків, формування напрямків дій слідчого, візуалізацію фактів, які свідчать про винність або невинність конкретної особи, контроль за розслідуванням кримінальних справ. Серед продуктів, що їх пропонує компанія, можна назвати такі:

- Analyst's Notebook — програма для відображення взаємозв'язків між особами, подіями, банківськими рахунками, номерами

ми телефонів, автомашин та іншими об'єктами, виявлення динаміки послідовності подій, діаграми дій у кожній події;

- IBase — програмне забезпечення для збирання, структуризації та зберігання даних із різних джерел;

- IBridge — інструментарій для вилучення та об'єднання інформації з усіх доступних джерел, зокрема СКБД Oracle, Microsoft Access і SQL Server, текстових файлів;

- Analyst's Workstation — продукт, який інтегрує всі технології від i2 Group, включаючи оброблення даних за допомогою системи візуальних запитів за принципом «намалюй запитання — отримай картинку-відповідь» і засоби інтеграції із зовнішніми додатками, наприклад із ГІС.

1.8. ПРАВОВІ ЕКСПЕРТНІ СИСТЕМИ

Експертні системи належать до класу інтелектуальних систем (систем штучного інтелекту), які виконують операції, імітуючи інтелектуальну діяльність людини — дії та розумові висновки людей у нестандартних ситуаціях, коли схема, алгоритм розв'язування задачі, що постала перед фахівцем, апіорі невідомі. Інтелектуальні системи забезпечують розв'язування неформалізованих задач користувача в деякій предметній галузі та організовують його взаємодію з комп'ютером у звичних поняттях, термінах, образах. Отже, можна подати таке визначення.

Експертна система — це інтелектуальна система, призначена для розв'язування задач у певній предметній галузі на основі знань, наданих експертами, яка містить базу знань і підтримує функції обґрунтування, пояснення та виправдання.

Застосовуються також такі терміни:

- **система на основі знань** — інтелектуальна система, в якій знання про предметну галузь подано в явному вигляді та відокремлено від інших знань системи;

- **дорадча система** — інтелектуальна система, що забезпечує формування рекомендацій про послідовність і перелік можливих дій користувача у процесі розв'язування задачі.

Основною відмінністю інтелектуальних систем від інших є те, що в них об'єктом нагромадження, зберігання, оброблення, передавання та використання є не дані, а знання. **Знання** — це сукупність фактів, закономірностей, відношень та евристичних правил, що відбиває рівень обізнаності з проблемами деяких предметних галузей. Специфічні особливості знань, що дають змогу відрізни-

ти їх від даних, такі: внутрішня інтерпретація, наявність ситуативних зв'язків, активність і форма подання.

Згідно з різними підходами виокремлюють такі *типи знань*:

- декларативні (предметні) знання — факти (тобто класи об'єктів і зв'язки між ними), які можна подати у вигляді множини тверджень, що не залежать від того, де і коли такі знання використовуються;

- процедурні знання (правила) — описи процедур, за допомогою яких ці знання можна здобути. У разі процедурного подання знань немає потреби зберігати інформацію про всі можливі стани предметної галузі, як тоді, коли використовуються декларативні знання, — достатньо мати опис початкового стану та процедур, що генерують на його основі потрібні наступні стани;

- евристичні знання — знання, які акумулюють неформальний досвід розв'язування задач у деякій предметній галузі;

- семантичні знання — знання про стан об'єктів предметної галузі та відношення між ними;

- прагматичні знання — знання про способи розв'язування задач у предметній галузі;

- каузальні знання — знання, в основу яких покладено причинно-наслідкові зв'язки.

Знання на відміну від даних, що відбивають кількісні характеристики і подаються здебільшого в цифровому вигляді, містять якісні характеристики у вигляді текстової інформації. Це також становить одну з відмінностей ЕС від систем оброблення даних. Відповідно, користувач ЕС одержує в результаті її роботи не документ у табличному вигляді, а інтелектуальну пораду у формі тексту.

Специфіка функціонування ЕС та інформаційного об'єкта для оброблення зумовлює особливості архітектури такої системи. У загальному випадку вона складається з розглянутих далі восьми блоків.

1. **База знань** — упорядкована сукупність правил, фактів, механізмів виведення та програмних засобів, що описує деяку предметну галузь та призначена для подання нагромаджених у ній знань. У базі знань мають бути присутні як загальновідомі факти, явища, закономірності, що визнані в даній предметній галузі й опубліковані (знання 1-го роду), так і набір емпіричних правил та інтуїтивних висновків, якими користуються спеціалісти, приймаючи рішення в умовах невизначеності за наявності неповної суперечливої інформації, і які найчастіше не опубліковані (знання 2-го роду). Очевидно, що результатом роботи розробника

ЕС — фахівця з ІТ, є порожня ЕС, в якій база знань не заповнена. Заповнює базу знань експерт — знавець предметної галузі — згідно з вибраною моделлю подання знань.

До основних **моделей подання знань** (моделей знань), що являють собою сукупності правил подання, опису та породження знань у базі знань, належать такі:

- логічна — модель подання знань, в основу якої покладено формальну логіку;
- фрейм — модель подання знань, яка під час заповнення її елементів — слотів — певними значеннями перетворюється на опис конкретного факту, події, процесу;
- семантична мережа — модель подання знань за допомогою мережі вузлів, сполучених дугами, де вузли відповідають поняттям чи об'єктам, а дуги — відношенням між вузлами;
- продукційна система — система, в якій знання подано у вигляді сукупності продукцій та правил їх застосування. Правило продукції можна подати так: **ЯКЩО** <умова> **ТОДІ** <висновок чи дія>.

Крім знань, здобутих від експертів, ЕС містить **метазнання** — знання про знання, що зберігаються в її базі знань, або про процедури, які можна здійснити з ними.

Можливість завантажувати базу знань та редагувати знання, які зібрані в базі, надає експертові блок нагромадження знань. Його функції охоплюють також формування емпіричних залежностей із неповних знань, тобто здобуття знань 1-го роду на основі знань 2-го роду. Але через складність реалізації цих функцій не всі ЕС містять такий блок.

2. Система керування базою знань — сукупність програмних та апаратних засобів для організації та ведення бази знань.

3. База цілей — компонент інтелектуальної системи, який містить інформацію про поведінку інтелектуальної системи в разі досягнення цілей у межах конкретної предметної галузі.

4. Розв'язувач задач — компонент інтелектуальної системи, призначений для формування на основі наявних знань логічних висновків, реалізація яких приводить до розв'язку задачі.

5. Інтелектуальний інтерфейс — сукупність програмних та апаратних засобів, які забезпечують взаємодію інтелектуальної системи з користувачем на основі звичних понять, термінів, образів, притаманних певній сфері інтелектуальної діяльності людини.

6. Система обґрунтування — компонент інтелектуальної системи, призначений для перевірки відповідності здобутого розв'язку знанням, що містяться в базі знань.

7. Система пояснення — компонент інтелектуальної системи, призначений для пояснення користувачеві способу, за допомогою якого знайдено розв'язок, а також самого розв'язку. Наявність цього блоку дає змогу використовувати ЕС не лише для прийняття рішень, а й як навчальну систему.

8. Система довіри — компонент інтелектуальної системи, призначений для підвищення рівня довіри користувача до здобутих результатів. Одним зі способів досягнення високої довіри може бути виправдання — функція обґрунтування деякого розв'язку із залученням наявних в інтелектуальній системі ціннісних чинників.

Використання систем штучного інтелекту в юридичній діяльності зумовлюється високим рівнем інтелектуальності, спеціалізації та професіоналізму, що притаманні розумовій діяльності юриста, судді, слідчого, криміналіста, судового експерта. Можна визначити такі напрями застосування інтелектуальних систем і технологій у галузі права: інтелектуалізація автоматизованих інформаційно-пошукових систем із законодавства; створення автоматизованих систем аналізу нормативних правових текстів; побудова консультативних систем із правотворення; створення експертних систем у сфері правозастосовної діяльності; розробка алгоритмів і програм ідентифікації за допомогою ЕОМ об'єктів при розслідуванні та розгляді судових справ (сфера криміналістики й судової експертизи).

Зарубіжні комерційні правові ЕС використовуються переважно в галузі управління фінансами. Наведемо кілька прикладів.

♦ ЕС «DSCAS» допомагає аналізувати юридичні аспекти позовів щодо відшкодування додаткових витрат, пов'язаних з відмінностями фізичних умов на місці передбачуваного будівництва від зазначених у контракті. Такі позови ґрунтуються на даних, які містяться в конкретних договорах. ЕС забезпечує посадову особу правовими знаннями для прийняття рішення щодо позову.

♦ ЕС «JUDITH» разом з юристом і з його слів засвоює фактичні та юридичні передумови цивільної справи, а далі пропонує розглянути різні варіанти підходів до її ведення.

♦ ЕС «LEGAL ANALYSIS SYSTEM» допомагає адвокатам аналізувати справи про навмисну образу дією з погляду права і практики його застосування.

♦ ЕС «LRS» надає допомогу стосовно добору й аналізу інформації про судові рішення та правові акти в галузі кредитно-грошового законодавства, пов'язаного з використанням векселів і чеків.

◆ ЕС «TAXMAN» допомагає дослідити логіку міркувань та аргументацію на прикладі законодавства про оподаткування корпорацій.

◆ ЕС «SAL» підтримує юристів при встановленні розмірів позовів, пов'язаних із професійними захворюваннями робітників, які працюють з азбестом.

◆ ЕС «LDS» допомагає юристам урегульовувати проблеми позовів про відшкодування збитків і компенсації за шкоду, пов'язану з випуском дефектної продукції. Система на основі опису справи висуває версію про винність відповідача, визначає ціну позову, розмір компенсації, який забезпечує інтереси сторін.

На російське трудове законодавство зорієнтована експертна довідково-консультаційна система «Ущерб», призначена для юридичного аналізу ситуації притягнення робітників і службовців до матеріальної відповідальності в разі, коли підприємству завдано матеріальних збитків. Система дає змогу розглядати таке коло питань: можливість притягнення особи до відповідальності за збитки, завдані підприємству або організації; встановлення виду й розміру матеріальної відповідальності з огляду на обставини конкретної ситуації; визначення орієнтовного розміру збитків і порядку їх відшкодування. Така структура базується на формулі, згідно з якою, приступаючи до розгляду конкретної справи (ситуації) по суті, необхідно встановити характер правовідносин, які виникають, і виокремити основні критерії для їх оцінювання. Це дає змогу правильно визначити нормативні акти, до яких потрібно звернутися для правильного вирішення справи, і розглянути порядок їх застосування. ЕС «Ущерб» містить контекстно залежний довідник із законодавства, а також посилання на використану юридичну літературу. Система призначена для використання судами, органами прокуратури при проведенні загальнонаглядових перевірок, при дослідженні діяльності підприємств та їхніх посадових осіб юридичними службами, керівниками і радами трудових колективів установ та організацій, професійними спілками при вирішенні спорів з адміністрацією, а також у навчальних закладах, де вивчається курс права.

Окремою сферою застосування експертних систем є прийняття рішення про напрямок розслідування і виконання слідчих дій. Сутність криміналістичних досліджень зводиться до встановлення закономірності у зв'язках, що існують між фактом злочину, особистістю злочинця, місцем і способом здійснення злочину, особливостями злочинної поведінки.

ЕС, що застосовуються в роботі слідчого, ґрунтуються на збиранні, класифікації та використанні узагальненого досвіду роз-

слідкування у вигляді знань окремих професіоналів. Такі знання, виражені у формі правил типу «Якщо існує такий факт, то, ймовірно, відбулася така дія або існував такий мотив цієї дії», придатні для автоматизованого оброблення і дають змогу імітувати процес оцінювання слідчим ситуації розслідування та забезпечувати в режимі діалогу консультативну підтримку прийняття ним рішень. Основними задачами, виконуваними за допомогою таких систем, є визначення можливих напрямків розслідування (формування версій про події з урахуванням, по змозі, різних джерел одержання інформації), вибір найбільш імовірних напрямків; надання користувачеві рекомендацій щодо подальших дій (призначення експертиз, проведення оперативно-пошукових заходів, перевірки та слідчі дії тощо).

Прикладом таких систем є «Маньяк» — ЕС підтримки прийняття рішень при розкритті серійних вбивств, здійснених на сексуальному ґрунті. Вона призначена допомагати співробітникам карного розшуку та слідчим прокуратури в розробці найбільш імовірної версії про тип можливого злочинця з обмеженням кола осіб, що підлягають перевірці на причетність до певного злочину. Основу системи становлять систематизовані взаємозв'язані набори найістотніших криміналістичних ознак, за якими виявляється зв'язок між подією злочину і вбивцею-маніяком. Використання системи сприяє збагаченню досвіду і знань працівників карного розшуку та слідчих прокуратури; установленню так званих прикордонних типів злочинців, розпізнати яких іншими методами надзвичайно важко або й зовсім неможливо; усуненню деякої частки суб'єктивізму під час формування версій за умов невизначеності; вирівнюванню знань неоднаково підготовлених співробітників.



Контрольні запитання і завдання

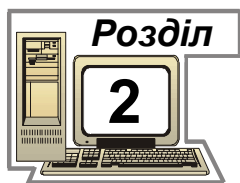
- 1. Які основні принципи державної політики в галузі інформатизації визначає законодавство України?*
- 2. Які особливості характерні для нової інформаційної технології?*
- 3. Схарактеризуйте три покоління ІС.*
- 4. Назвіть забезпечувальні компоненти ІС.*
- 5. Подайте визначення правової задачі і назвіть, за якими ознаками можна класифікувати задачі оброблення інформації.*

6. Схарактеризуйте концепцію побудови корпоративних інформаційних систем.
7. Що таке правова інформація? Назвіть види правової інформації.
8. Що таке правовий режим доступу до інформації і які види інформації за цією ознакою розрізняють?
9. Що таке система підтримки прийняття рішень? Поясніть концепцію їх класифікації та назвіть основні типи сучасних СППР.
10. Визначте напрямки використання СППР в юридичній діяльності. Наведіть приклади.
11. Чим відрізняються інтелектуальні інформаційні системи від систем оброблення даних?
12. Визначте напрямки використання ЕС в юридичній діяльності. Наведіть приклади правових ЕС.



Література

1. Береза А. М. Основи створення інформаційних систем: Навч. посібник. — К.: КНЕУ, 2001. — 214 с.
2. Гаврилов О. А. Основы правовой информатики. — М.: Академ. правовой ун-т при Ин-те государства и права РАН, 1998. — 42 с.
3. ДСТУ 2394-94. Інформація та документація. Базові поняття. Терміни та визначення. — К.: Держстандарт України, 1994. — 53 с.
4. ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення. — К.: Держстандарт України, 1994. — 55 с.
5. ДСТУ 2429-94. Система «людина—машина». Ергономічні та техніко-естетичні вимоги. Терміни та визначення. — К.: Держстандарт України, 1994. — 35 с.
6. ДСТУ 2481-94. Системи оброблення інформації. Інтелектуальні інформаційні технології. Терміни та визначення. — К.: Держстандарт України, 1994. — 72 с.
7. Єрьоміна Н. В. Проектування баз даних: Навч. посібник. — К.: КНЕУ, 1998. — 208 с.
8. Кісельов М. Про створення єдиної інформаційної системи органів юстиції України // Право України. — 1997. — № 3.
9. Компьютерные технологии в юридической деятельности: Учеб. пособие / Под ред. проф. Н. Полевого, канд. юрид. наук В. Крылова. — М.: Изд-во БЕК, 1994. — 304 с.
10. Матеріали сайту <http://dssresources.com/>.
11. Ситник В. Ф. та ін. Основи інформаційних систем: Навч. посібник. — К.: КНЕУ, 2001. — 420 с.
12. Ситник В. Ф. та ін. Системи підтримки прийняття рішень. — К.: Техніка, 1995. — 162 с.



Розділ

2

ОСНОВИ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

2.1. ОСНОВНІ ПОНЯТТЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Однією з базових вимог сучасності є вчасне забезпечення особи, яка приймає рішення, актуальною інформацією. Не в останню чергу це стало можливим завдяки тому, що називають тепер «другою комп'ютерною революцією» — поєднанню обчислювальних і комунікаційних технологій у рамках глобальної мережі з неосяжним обсягом і необмеженим потенціалом. Сьогодні термін «*телекомунікації*» (від грец. «tele» — далеко та «communis» — спілкуюся) позначає здатність передавати текст, голос, зображення і навіть нематеріальні активи (грошові кошти) через мережі разом із функціональною інформацією, призначеною для управління комп'ютерними системами.

Комп'ютерні мережі є одним з основних видів телекомунікацій. **Комп'ютерна мережа** — це сукупність каналів передавання даних і/або засобів комунікації, які з'єднують окремі ЕОМ і дають змогу використовувати спільні програмні й технічні засоби для організації зв'язку.

Основним призначенням комп'ютерних мереж є обмін даними; розподіл ресурсів — спільне використання обчислювальних потужностей (ресурсів процесора), периферійних пристроїв (принтерів, графопобудовників) та ін.; розподіл даних і програмних засобів.



Комп'ютерні мережі та мережі зв'язку

*Комп'ютерні мережі є одним із видів мереж зв'язку. Закон України «Про зв'язок» містить таке визначення: **мережа зв'язку** — сукупність засобів та споруд зв'язку, поєднаних в єдиному технологічному процесі для забезпечення інформаційного обміну. При цьому розрізняються електричний зв'язок і поштовий зв'язок. Електричний зв'язок — це передавання, випромінювання чи прийом знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах.*

Поштовий зв'язок — приймання, обробка, перевезення та доставляння письмових відправлень, матеріальних цінностей, виконання доручень фізичних та юридичних осіб щодо грошових переказів, банківських операцій.

Загалом мережні технології забезпечують скорочення витрат і підвищення продуктивності роботи, що є основним фактором їх поширення.

Існування та функціонування мереж визначається протоколами і стандартами. **Протокол** — це сукупність правил (визначень, домовленостей), які регламентують формат і процедури обміну інформацією між двома або більшою кількістю незалежних пристроїв чи процесів. Іншими словами, протокол — це опис того, як програми, комп'ютери або інші пристрої мають функціонувати у процесі взаємодії між собою — від порядку передавання бітів до формату повідомлень електронної пошти.

Створення протоколів диктується необхідністю організації повноцінної взаємодії технічних і програмних засобів різних вузлів мережі. З'єднати два комп'ютери кабелем — цього ще замало, аби забезпечити комунікації: кожен учасник зв'язку надсилатиме повідомлення, які не будуть зрозумілі одержувачам. Такий процес можна порівняти із засіданням, де немає головуючого і всі учасники говорять водночас, та до того ж різними мовами без перекладача. Із цього погляду, протокол, затверджений як **стандарт**, містить правила, дотримуватись яких неодмінно мають розробники мережного технічного та програмного забезпечення.

Роботи зі стандартизації проводять як національні, так і міжнародні організації. Серед найбільш впливових можна назвати такі: Міжнародна організація зі стандартизації (International Organization for Standardization, **ISO**), Міжнародний союз з телекомунікацій (International Telecommunication Union, **ITU**), Європейська асоціація виробників комп'ютерів (European Computer Manufactures Association, **ECMA**), Американський інститут національних стандартів (American National Standards Institute, **ANSI**), Інститут інженерів з електроніки і радіоелектроніки (Institute of Electronic and Electrical Engineers, **IEEE**).

З усвідомленням того, що передавання інформації між мережами різних країн матиме таке саме значення, як і з'єднання телефонних систем, Міжнародна організація зі стандартизації

почала розробку еталонної моделі взаємодії відкритих систем¹ (**Open System Interconnection, OSI**), яку сьогодні оформлено кількома стандартами. Модель OSI передбачає кілька рівнів, кожному з яких відводиться своя роль. Рівневе подання можна обґрунтувати за аналогією зі звичайним спілкуванням. Коли люди спілкуються, вони намагаються обмінятися ідеями. Якщо відправник *A* хоче передати повідомлення адресатові *B*, то він має перетворити ідею на слова, а згодом передати ці слова наявними засобами — поштою, за допомогою азбуки Морзе тощо. На цьому рівні ідея не істотна — важливо, які фізичні засоби можна застосувати для передавання символів. Отже, повідомлення проходить три рівні — когнітивний (рівень ідей), мовний (рівень слів) та фізичний. В адресата *B* проходження рівнів відбувається у зворотному порядку: він одержує лист, читає слова, а далі перетворює їх на ідею. Так само при передаванні даних через мережу повідомлення проходить *сім рівнів*: фізичний, канальний, мережний, транспортний, сеансовий, подання даних, прикладний. Рівні моделі OSI розроблено не повністю. Верхні три рівні реалізуються прикладними додатками й утворюють єдиний шар (його можна назвати логічним) над мережною інфраструктурою, яку утворюють нижні чотири рівні.

2.2. КЛАСИФІКАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Сьогодні у світі налічуються сотні тисяч обчислювальних мереж. Загальноприйнятої стійкої класифікації мереж не існує, тому в цьому розділі розглянуто класифікацію за найважливішими й найчастіше використовуваними ознаками.

За *розмірами* розрізняють локальні та глобальні мережі. **Локальна обчислювальна мережа (ЛОМ)**, як правило, зв'язує не більш ніж сотню вузлів в одній локальній зоні (не більш ніж кілька кілометрів). **Глобальна мережа** може охоплювати територію регіону, держави чи кількох країн, з'єднувати як окремі ЕОМ, так і локальні мережі. Проміжним класом є міські (муніципальні) мережі, зорієнтовані на географічні області невеликих розмірів. Відмінність між названими класами мереж полягає не тільки в розмірах охоплених ними територій, а й у

¹ Відкритими називають системи, що базуються на однакових стандартах. OSI — еталонна модель відкритих систем, використовувана як база для порівняння.

швидкості передавання даних — технології, які забезпечують більші швидкості, працюють на менших відстанях. Існують і інші відмінності щодо використовуваного обладнання та принципів побудови мереж.

За *типом з'єднуваних ЕОМ* розрізняють однорідні (гомогенні, з однотипним складом технічних засобів) та неоднорідні (гетерогенні) мережі. Вузли ЛОМ здебільшого комплектуються однотипним апаратним і програмним забезпеченням, що практично неможливо забезпечити у глобальних мережах.

Доступ до комерційних мереж та послуги їхніх сервісних служб є *платними*. У некомерційних мережах («умовно безплатних») користувач платить тільки за підімкнення, експлуатацію системи зв'язку, використання мережних служб. Комерційні мережі підтримуються професійними організаціями, які існують з метою надання мережних послуг, а некомерційні, як правило, — навчальними закладами, інформаційними структурами та громадськими організаціями.

Якщо всі ЕОМ мережі мають однакову продуктивність і рівні *права*, мережа називається одноранговою. Однак у процесі нарощування мережі один або кілька комп'ютерів роблять більш потужними, їм надаються додаткові права — створюється мережа з виділеним сервером.

Проблема визначення рангів тісно пов'язана з вибором *способу організації оброблення інформації*. За цією ознакою мережі поділяються на централізовані, розподілені, із серверами.

У розподіленій мережі всі вузли виконують подібні між собою функції, причому кожний окремий вузол може використовувати ресурси інших вузлів і надавати у спільне використання свої ресурси. Такий підхід забезпечує оптимальність використання ресурсів, стійкість мережі до відказів (вихід із ладу одного вузла не призводить до фатальних наслідків — його легко можна замінити), але при цьому постають проблеми забезпечення розподілу ресурсів, безпеки та прозорості.

Централізовані мережі (із хост-машиною) складаються з особливо надійного й потужного центральною вузла та неінтелектуальних терміналів. На центральному вузлі здійснюється обробка даних, виконуються функції керування мережею (діагностування, збирання статистики і т. ін.), установлюється зв'язок з іншими мережами. Термінали називаються неінтелектуальними, оскільки вони позбавлені обчислювальних можливостей, на них виконуються тільки функції введення і виведення інформації та керування

процесом її оброблення. Роль терміналів можуть виконувати персональні комп'ютери і навіть дисплейні станції. Нині централізовані мережі практично не застосовуються.

Проміжне місце між централізованими і розподіленими мережами посідають мережі із серверами. **Сервер** — це потужний комп'ютер, призначений для виконання певних завдань за допомогою відповідного ПЗ. Решта машин у мережі, які звертаються до послуг сервера, називаються клієнтськими (клієнтами), інша назва — робочі станції.

Залежно від виконуваних завдань розрізняють:

- принт-сервер (сервер друку) — активний мережний пристрій (комп'ютер), який дає змогу підмикати кілька принтерів для створення єдиного вузла друку та сортування документів у разі великого документообігу. До різних портів принт-сервера можна підмикати лазерні, матричні, струменеві принтери, копіри;

- файл-сервер (файловий сервер) — центральний вузол мережі, на якому зберігаються файли даних, доступні всім користувачам. Файл-сервер не бере участі у виконанні додатків — файл (або його частина) передається на робочу станцію, а після оброблення дані копіюються на файл-сервер. Він може не лише виконувати основні функції, а й бути засобом для спільного використання периферійних пристроїв. Мережі з файл-сервером мають два основні недоліки. По-перше, не забезпечується одночасний доступ кількох користувачів до одного набору даних (файл, з яким працює один користувач, блокується і стає недоступним для інших). По-друге, за великої кількості запитів до файл-сервера мережа швидко насичується і продуктивність системи різко знижується;

- клієнт-сервер — це спосіб не стільки організації мережі, скільки логічного подання й обробки інформації, згідно з яким сервери виконують оброблення даних, а клієнтські машини — функції формування запитів, відображення результатів та їх обробки. Окремим випадком організації такого середовища є використання серверів баз даних, які мають таке призначення: управління єдиною базою даних і доступом до неї багатьох користувачів; захист бази даних за допомогою засобів відновлення та створення резервних копій; контроль за дотриманням правил глобальної цілісності даних. Оскільки клієнт і сервер працюють спільно і розподіляють завантаження

(звідси термін «розподілена обробка»)¹, така система може забезпечити більшу продуктивність порівняно з файл-серверною. До того ж клієнтська частина додатка працює не з цілими файлами, а з невеликими наборами даних (рядками таблиць), що забезпечує паралельність роботи користувачів і мінімальний мережний трафік². Перевагами таких систем є також гнучкість, адаптованість до вимог додатків, оптимальне використання ресурсів, нарощуваність.

Залежно від *фізичного середовища передавання даних* розрізняють мережі на основі витвої пари, коаксіального кабелю, оптоволоконного кабелю, радіозв'язку, супутникового зв'язку.

За *способом використання каналу передавання даних* розрізняють мережі з комутацією каналів і мережі з комутацією пакетів. Комутація каналів — це процес з'єднання двох або більшої кількості станцій з монопольним використанням каналу до його роз'єднання. У разі комутації пакетів повідомлення розбивається на частини — пакети, канал зайнятий тільки на час пересилання окремого пакета, після чого звільняється для передавання інших пакетів.

Іншою важливою характеристикою мережі є її **топологія** — конфігурація з'єднання елементів. Від топології мережі багато в чому залежать такі її характеристики, як надійність, продуктивність і т. ін. Найпростішим способом організації мережі є безпосереднє з'єднання всіх вузлів, які мають взаємодіяти, за допомогою ліній зв'язку від пристрою до пристрою. Таку мережу називають **повнзв'язаною**. Але цей спосіб прийнятний тільки для небагатьох вузлів, оскільки має такі недоліки, як висока вартість і велика кількість каналів зв'язку. Тому основними видами топологій сучасних мереж є «зірка», кільцева, шинна, деревоподібна.

У мережі з **топологією у вигляді зірки** (рис. 2.1) центральний вузол (концентратор) має зв'язки з робочими станціями, не зв'язаними між собою безпосередньо. Уся інформація між периферійними робочими місцями проходить через центральний вузол. Пропускна здатність і продуктивність мережі визначаються потужністю центрального вузла, який є найбільш вразливим місцем мережі з погляду її надійності (з порушенням роботи центрального

¹ Крайнім випадком реалізації технології клієнт—сервер є використання «тонкого» клієнта — клієнтська машина має тільки пристрої вводу/виводу інформації (клавіатуру, «мишу», екран) та засоби підімкнення до мережі, усі додатки розміщені й виконуються на сервері.

² Трафік — потік даних у мережі.

вузла припиняється функціонування всієї мережі). Кабельне з'єднання досить просте, але для його прокладання потрібні значні витрати, особливо коли центральний вузол географічно розміщений не в центрі топології.

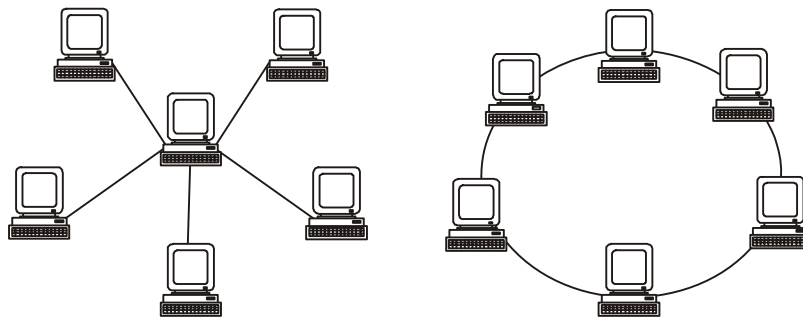


Рис. 2.1. Топології мереж «зіврка» і «кільце»

У випадку **кільцевої топології** (див. рис. 2.1) кожен вузол мережі має зв'язок з двома і тільки з двома іншими вузлами — перша робоча станція зв'язана з другою, друга з третьою і т. д., остання робоча станція зв'язана з першою. Повідомлення передаються по колу — на основі аналізу адресної і керуючої інформації, розміщеної на початку повідомлення, станція приймає рішення щодо його подальшого передавання на сусідній вузол. Кільцеві мережі різняться за способом керування. Тривалість передавання інформації збільшується пропорційно кількості станцій мережі. Основними недоліками кільцевої топології є складність і висока вартість прокладки кабелю у випадку географічної віддаленості вузлів та їх розміщення не за колом, а також уразливість — вихід з ладу хоча б однієї станції паралізує всю мережу.

Якщо мережа не замкнена у коло, в ній є тільки два прикінцеві вузли і довільна кількість проміжних, а між будь-якими двома вузлами є лише один шлях, то таку мережу називають **лінійною**.

Шинна топологія (рис. 2.2) передбачає наявність комунікаційної лінії, доступної для всіх робочих станцій, які до неї підімкнено. Будь-яка станція мережі може вступати в контакт з будь-якою іншою станцією. Основними перевагами такої топології є простота розширення мережі (робочі станції можуть бути підімкнені або відімкнені від мережі в будь-який час без порушення її роботи), простота методів управління, відсутність

необхідності в централізованому управлінні, мінімальні витрати кабелю, надійність (функціонування мережі не залежить від стану окремої робочої станції). Для підвищення надійності роботи мережі разом з основним кабелем прокладають запасний, на який станції перемикаються в разі несправності основного.

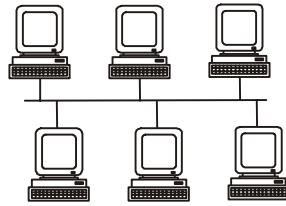


Рис. 2.2. Шинна топологія мережі

Окремо розглядають клас **чарункових мереж**, які містять принаймні два вузли, між якими є два чи більше шляхів.

Поряд із названими топологіями мереж застосовуються і комбіновані. Одним із прикладів є **деревоподібна топологія** (рис. 2.3), яку можна розглядати як розвиток шинної топології — за допомогою спеціальних пристроїв об'єднуються кілька шин — або топології типу «зірка» — один чи кілька термінальних вузлів можуть бути концентраторами іншої мережі.

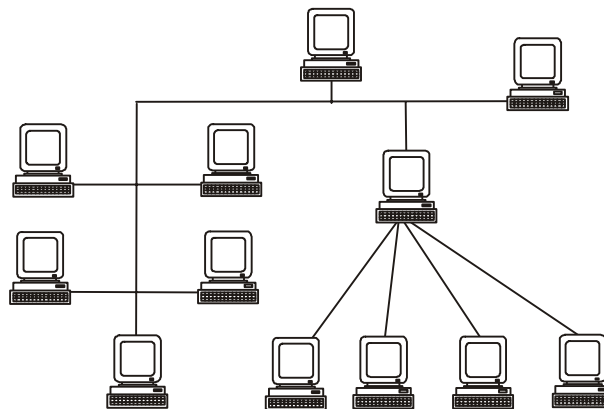


Рис. 2.3. Деревоподібна топологія мережі

Варто зазначити, що термін «топологія» застосовується здебільшого до ЛОМ — глобальні мережі будуються за довільними топологіями і найчастіше функціонують за специфічними протоколами.

Набори технічних засобів і правила їх з'єднання для організації мережі певної топології описано у відповідних стандартах. Таким чином регламентується припустима **мережна архітектура** — кабельна система мережі, кодування сигналів, швидкість передавання, формат мережних кадрів, топологія і метод доступу до каналу. Іншими словами, мережна архітектура визначає реалізацію фізичного і канального рівнів моделі OSI. Найпоширенішими архітектурами мереж є Ethernet та її модифікації, Token Ring (маркерне кільце), ARCnet, FDDI (інтерфейс передавання даних за оптоволоконними лініями) та її модифікації, ATM (технологія асинхронного передавання даних), ISDN (цифрова мережа з інтеграцією сервісу).

Мережі також можна класифікувати за *операційними системами*, які забезпечують їх функціонування. До найпоширеніших мережних операційних систем належать Microsoft Windows, Microsoft Windows NT, IBM OS/2 та UNIX-системи (BSD, LINUX та ін.).

Закони України «**Про зв'язок**» та «**Про Національну систему конфіденційного зв'язку**» визначають такі види мереж залежно від *кола користувачів та призначення*:

- мережа зв'язку загального користування — мережа зв'язку, яку експлуатують підприємства та об'єднання зв'язку для забезпечення потреб у послугах зв'язку всіх споживачів;
- мережа спеціального зв'язку (спеціальна мережа зв'язку) — мережа зв'язку, яка забезпечує обмін інформацією з обмеженим доступом;
- відомча мережа зв'язку — мережа зв'язку, яку експлуатує юридична або фізична особа для задоволення власних потреб;
- мережа технологічного зв'язку — відомча мережа зв'язку для обміну інформацією з метою забезпечення технологічних процесів у виробничій діяльності;
- мережа зв'язку подвійного призначення — мережа зв'язку, яку експлуатує юридична або фізична особа для задоволення власних потреб та надання (на умовах ліцензування) послуг зв'язку всім споживачам;
- спеціальна мережа зв'язку подвійного призначення — спеціальна мережа зв'язку, призначена для забезпечення зв'язку в інтересах органів державної влади та органів місцевого

самоврядування, з використанням частини її ресурсу для надання послуг іншим споживачам;

- Єдина національна система зв'язку — сукупність мереж зв'язку загального користування, відомчих та подвійного призначення, які забезпечують задоволення потреб споживачів (підприємств, установ, організацій, населення та ін.) у послугах зв'язку;

- Державна система урядового зв'язку — система спеціального зв'язку, яка забезпечує передавання інформації, що містить державну таємницю, і функціонує в інтересах управління державою в мирний та воєнний час;

- Національна система конфіденційного зв'язку — сукупність спеціальних систем (мереж) зв'язку подвійного призначення, які за допомогою криптографічних і/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та в разі впровадження надзвичайного і воєнного стану.

2.3. КОНЦЕПЦІЯ ПОБУДОВИ, АДМІНІСТРУВАННЯ ТА СЕРВІСИ ІНТЕРНЕТ

2.3.1. Ретроспектива та концепція побудови

Інтернет (Internet) стала явищем світового масштабу, яке має безліч визначень та епітетів — «мережа мереж», «Всесвітня павутина», «глобальна комп'ютерна мережа», «найбільша у світі мережа» або просто «Мережа».

Можна назвати дві причини, які зумовлюють існування Інтернет та об'єднання мереж загалом — одна мережа не може обслужити всіх користувачів, а користувачі потребують універсальної взаємодії. У 1960-х роках уряд США прийшов до розуміння величезної ролі комп'ютерів в освіті, дослідженнях і розробках у військовій галузі, а тому почав фінансування проекту створення експериментальної комп'ютерної мережі через Агентство перспективних

досліджень (US Advanced Research Project Agency, ARPA)¹. Відповідно, створену мережу, яка наприкінці 1969 року об'єднувала чотири комп'ютери, було названо **ARPAnet** (Advanced Research Projects Agency Network).

ARPAnet об'єднувала локальні мережі американських університетів, наукових лабораторій і військових баз². У 1983 році ARPAnet було поділено на дві частини: MILnet — військову мережу, яка залишилась у віданні Міністерства оборони, та ARPAnet, яку віддали для громадянських досліджень (вона припинила своє існування 1990 року).

Однією з головних цілей досліджень, що проводились в ARPAnet, було створення мережі, яка може зберігати роботоздатність у разі порушення зв'язку між її окремими частинами (зокрема, у разі ядерного нападу).



Інтернет-хребет — backbone

*Як і система автошляхів, Інтернет не є однорідною — у ній є свої магістралі та путівці. Магістраль Інтернет — **backbone** (хребет, опорна мережа) — високошвидкісна мережа, що об'єднує кілька потужних комп'ютерів. Першою backbone була NSFnet, створена у 1980-ті роки з ініціативи Національного наукового фонду (National Science Foundation, NSF, <http://www.nsf.gov>). NSFnet об'єднувала п'ять суперкомп'ютерних центрів, з'єднаних спеціальними телефонними лініями. В основу NSFnet було покладено IP-технологію ARPAnet (див. п. 2.3.2) і регіональний принцип побудови — зацікавлені заклади з'єднувались між собою, а одержана таким чином мережа в одній із своїх точок — із суперкомп'ютером. Зауважимо, що саме такий підхід зробив Інтернет доступною всім бажаючим.*

Це стало однією з головних характеристик Інтернет як наступниці ARPAnet — відсутність центрального вузла, який керує

¹ Із включенням агентства ARPA до структури Міністерства оборони США (DoD, Department of Defence) його назва змінилась на DARPA (Defence Advanced Research Project Agency).

² Першими у 1969 році до ARPAnet було під'єднано Каліфорнійський університет в Лос-Анджелесі, Стенфордський університет, Каліфорнійський університет Санта-Барбари та університет штату Юта. У 1972 році ARPAnet об'єднувала 40 комп'ютерів, а 1973-го було здійснено перше міжнародне підімкнення. Варто зазначити, що авторство щодо розробки Інтернет не можна віддати виключно США. Навіть на ранніх етапах побудови ARPAnet багато досліджень проводилось у Німеччині, Нідерландах (Амстердамі), Великобританії та інших країнах. Якщо спочатку велике значення для розвитку Мережі мали кошти, що їх виділяв уряд США, то згодом їх багаторазово перевищили інвестиції приватного сектора.

роботою мережі, унеможливилося її катастрофу. Інтернет справді є мережею мереж, які працюють за різними протоколами, пов'язують різні типи комп'ютерів, фізично передають дані по всіх доступних типах ліній. Кожна така мережа функціонує автономно і фінансується з окремих джерел. Не існує організації «Інтернет Inc.», яка збирає плату з усіх мереж або користувачів. Представники мереж збираються разом і вирішують, як їхні мережі будуть зв'язуватись і як підтримувати такі взаємозв'язки. Користувачі платять за доступ **провайдерів послуг Інтернет** (ISP, Internet Service Provider) — організації, яка надає доступ до Інтернет і може платити за свій доступ мережному власнику державного масштабу.

Нині кількість комп'ютерів і мереж у складі Інтернет точно невідома. Мережа перебуває у стані постійної перебудови і розвитку. Існують і різноманітні перспективні проекти. Триває розробка 2-го покоління Інтернет — «**Інтернет-2**» — проекту, започаткованого в 1996 році університетами США. Інтернет-2 буде повністю закритою мережею, яку реалізовуватимуть спеціальні консорціуми на основі високошвидкісної базової мережі Національного наукового фонду vBNS (Very high-speed Backbone Network Service). Головним призначенням Інтернет-2 є тестування нових технологій, які згодом переноситимуться на Інтернет.

У США Інтернет-2 розглядається як складова глобального державного проекту **NGI** (Next Generation Internet, Інтернет наступного покоління, <http://www.ngi.gov/>), для реалізації якого створено спеціальний Центр — глобальну безприбуткову промислову організацію, яка супроводжує, структурує та аналізує широкий діапазон Інтернет-додатків, забезпечує технічну, ринкову, промислову, освітню й користувацьку підтримку для широкої та ефективної взаємодії з урядовими колами на базі Інтернет, вживає заходів з прискорення її розвитку.



Інтернет — міжнародна взаємодія і розробка політики розвитку

*Найвища влада в Інтернет належить **ISOC** (Internet SOciety, Всесвітнє співтовариство Інтернет, <http://www.isoc.org/>) — міжнародній організації з добровільним членством, метою якої є сприяння глобальному обміну інформацією через Інтернет та розвитку всебічного використання Мережі — від комерції та освіти до соціальних питань.*

ISOC призначає раду старійшин, яка відповідає за технічну політику, підтримку та управління Інтернет, — **IAB** (Internet Architecture Board, Рада з архітектури Інтернет, <http://www.iab.org/>). Вирішення поточних експлуатаційних і технічних проблем покладається на іншу добровільну організацію — **IETF** (Internet Engineering Task Force, Цільова група з інжинірингу в Інтернет, <http://www.ietf.org/>), а зокрема — на її робочі групи. Останні мають різні функції: випуск документації, вироблення стратегії дій при виникненні проблем, стратегічні дослідження, розробка нових і доопрацювання вже існуючих стандартів і протоколів.

Також ISOC проводить міжнародні конференції INET (International NETworking conference) та інші форуми, навчальні курси, статистичні і маркетингові дослідження, здійснює публікації і торговельні операції, бере участь в ініціативах соціального, економічного, політичного, етичного і правового характеру.



Інтернет-етикет — netiquette

За відсутності регламентації та багатьох формальних правил, якими люди користуються в особистому спілкуванні, особливого значення в Інтернет набула етика — було вироблено правила хорошого тону, дотримання яких є обов'язком кожного цивілізованого користувача. З-поміж них можна виокремити такі:

- ▲ не думайте, що коли Ви можете щось зробити, то Ви маєте це робити;

- ▲ поважайте право інших користувачів на конфіденційність;

- ▲ розсилаючи електронне повідомлення, спитайте себе, чи бажаєте Ви, щоб його прочитав користувач-новачок, ваші батьки, діти, Ви самі 10 років потому;

- ▲ несіть відповідальність за свої слова та дії, тоді інші почуватимуться зобов'язаними нести таку саму відповідальність;

- ▲ пам'ятайте, що в Інтернет працюють люди різних соціальних прошарків і різних поглядів; не вважайте, що інші користувачі мають ті самі права і ті самі обов'язки, що й Ви;

- ▲ не перевантажуйте ресурсів Інтернет; перш ніж звертатись до її можливостей, зробіть все можливе на локальному комп'ютері.

Узагальнено можна назвати два постулати, які визначають усі правила: по-перше, вияви індивідуальності поважаються і заохочуються, а по-друге, Мережа — річ гарна, яку слід захищати.

В Європі ініціатива належить двом впливовим організаціям. Перша з них — **TERENA** (Trans-European Research and Education Networking Association, Транс'європейська мережна асоціація в галузі досліджень та освіти, <http://www.terena.org>)

була заснована 1994 року злиттям RARE (Reseaux Associees pour la Recherche Europeene, Європейське об'єднання дослідників) та EARN (European Academic and Research Network, Європейська академічна та дослідницька мережа). Місією TERENA є сприяння та участь у розробці високотехнологічної комп'ютерної мережної інфраструктури. Другою організацією є найбільша у світі асоціація Інтернет-провайдерів — EuroISPA (<http://www.euroispa.org>).



Перспективи Інтернет — IPN

У 1997 році Вінтон Серф (один із творців протоколу TCP/IP, «батько» Інтернет) висунув ідею міжпланетарного розширення Інтернет. Сьогодні IPN (InterPlaNetary Internet) — це проект, який фінансується NASA і реалізується спільними зусиллями урядових організацій та промислових груп. Метою проекту є підтримка космічних систем зв'язку, проектування роботів, створення в Сонячній системі аванпостів як із присутністю, так і з відсутністю людини. IPN стане «мережею об'єднань Інтернет» — звичайні глобальні мережі підмикатимуться до мережі верхнього рівня. Передавання даних здійснюватиметься за допомогою нового транспортного протоколу, зорієнтованого на великі відстані. Таким чином стане можливим передавання даних між Землею і, приміром, Марсом.

2.3.2. Адресація в Інтернет

Одним із найважливіших елементів спадщини, що перейшла до Інтернет, є протокол маршрутизованого доставляння пакетів TCP/IP, на який було переведено ARPAnet у 1983 році, що уможливило розширення мережі до світового масштабу.



Протоколи Інтернет — TCP/IP

TCP/IP — це набір протоколів, серед яких TCP і IP є основними.

TCP (Transmission Control Protocol) — протокол управління передаванням даних у вигляді пакетів — TCP-сегментів, які складаються із заголовків TCP і даних. Саме передавання здійснюється за допомогою протоколу IP. TCP забезпечує високу надійність передавання даних, оскільки передбачає використання контрольних сум для перевірки їх цілісності і відправлення підтверджень того, що передані дані було прийнято без перекручувань.

IP (*Internet Protocol, протокол Інтернет*) — протокол низького рівня, який відповідає за переміщення пакетів даних по окремих мережах, пов'язаних між собою маршрутизаторами. Дані передаються у вигляді пакетів, що називаються IP-датаграмами.

В основу маршрутизації в Інтернет покладено **IP-адресу**. IP-адреси — це 32-бітові числа, що розбиваються на октети (восьмибітові числа), які записують у вигляді десяткових чисел, наприклад 124.44.186.11. Перші три частини адреси позначають належність до певного класу мереж, а остання є унікальною для окремого комп'ютера. Коли формується мережа, їй присвоюється номер, який визначає кількість машин у межах цієї мережі¹. IP-адреси окремим машинам призначають із заданого так діапазону. Інформація, що передається, розбивається на пакети, у кожному з яких вказується адреса. Пакети доставляються незалежно один від одного і збираються у вузлі-одержувачі.

Для зручності користувачам надається інша система, що ґрунтується на символічних ідентифікаторах, — так звана **доменна адресація** — за таким шаблоном:

ім'я_користувача @ назва_системи . домен

Більшість імен короткі (до 8 символів), вони не можуть містити пропусків і звичайно записуються буквами в нижньому регістрі. Двоє користувачів, які працюють на одному комп'ютері, не можуть мати однакових імен. Домен, який вказується слідом за крапкою, може складатися з кількох піддоменів, назви яких також відокремлюються крапками, наприклад .kiev.ua або .com.ua.

Відповідність адреси, відомої користувачеві, IP-адресі, що її використовують внутрішні механізми передавання даних, забезпечується службою імен доменів **DNS (Domain Name System)**, яка виконує їх двосторонню трансляцію.



Символ сучасності — @

Перше електронне повідомлення по мережі надіслав 1971 року американський комп'ютерний інженер Рей Томлінсон. Саме він вибрав символ @ як розділовий знак, що не зустрічається в жодному імені і не може призвести до плутанини. Походження символу @ викликає суперечки серед лінгвістів і палеографів.

¹ Тепер активно впроваджується нова версія IP-адресації — 128-бітна, що пов'язано з очікуваним лавиноподібним збільшенням кількості користувачів Інтернет.

Дослідження показують, що він зародився у XV столітті в іспано-арабських та греко-романських мовах як комерційний символ для позначення одиниць виміру товару, зокрема амфори (anfora або arroba) — міри маси приблизно в 12,5 кг. Вимова «арроба» залишається за цим символом і в деяких сучасних мовах, але частіше для його позначення використовуються метафори: «собачка», «равлик», «черв'як», «мишеня», «булочка з корицею», «штрудель» та ін.

Доменна структура Інтернет є ієрархічною. Найвищий (кореневий) рівень не має назви. Далі йде обмежена кількість доменів верхнього рівня, в яких може бути практично необмежена кількість доменів 2-го рівня і т. д. Імена **доменів верхнього рівня** (Top Level Domains, TLDs) стандартизовані. Їх можна поділити на *два типи*: описові імена родових доменів (generic Top Level Domains, gTLDs) та імена, які визначають розміщення домену. Адреса комп'ютера може мати ім'я одного з цих типів (але не обидва разом).

Найпоширенішими є родові домени, які визначають прикладний напрямок мережі: .com — комерційні організації, .edu — освітні установи, .gov — урядові установи, .int — міжнародні організації, .mil — військові установи, .net — мережні організації, .org — організації, які не належать жодній іншій категорії.

З 1997 року було введено нові домени верхнього рівня, серед яких: .aero — авіатранспорт, .arts — культура і розваги, .biz — бізнес, .coop — кооперативи, .firm — бізнес (фірми), .info — інформаційні послуги, .museum — музеї, .name — приватні особи, .nom — персональні, .pro — професіонали (юристи, економісти і т. п.), .res — відпочинок і розваги, .shop — магазини, .web — WWW-діяльність.

Імена географічних доменів завжди подаються як двобуквене скорочення назви країни, зазвичай, згідно зі стандартом ISO-3166-1 (звідси їх позначення — ccTLDs, country-code Top Level Domains, домени верхнього рівня з кодами країн). Приклади: ua — Україна, ca — Канада, eu — Європейський Союз, uk — Великобританія, us — США.

Імена доменів верхнього рівня в конкретній адресі не завжди точні. Багато з постачальників мережних послуг не вказують своїм доменом верхнього рівня «net», комп'ютери з назвами домену «edu» можуть використовуватись для комерційних або військових цілей, а адреси географічного домену «ag» — належати німецьким бізнесменам.

Домени верхнього рівня можна класифікувати за ознакою «спонсорства». **Спонсор** — це організація, що представляє найбільш зацікавлену в цьому домені спільноту і якій ICANN (див. підрозд. 2.3.3) делегує повноваження з формулювання політики функціонування домену. Спонсор також відповідає за вибір оператора реєстру, повноваження реєстраторів та їх взаємовідносини. Домен, який не спонсорується, функціонує згідно з правилами, установленими глобальною Інтернет-спільнотою за посередництва ICANN.

За призначенням домени поділяють на **публічні (спільного користування)** — такі, що адмініструються в інтересах певної спільноти, та **приватні**, що адмініструються певною фізичною або юридичною особою у своїх власних інтересах. Так, домен .UA адмініструється в інтересах української **Інтернет-спільноти** — спільноти всіх громадян і/або резидентів України, фізичних та юридичних осіб, органів державної влади та управління України, органів місцевого самоврядування, які використовують мережу Інтернет та Інтернет-технології, незалежно від мети та способів такого використання.

У публічному домені можуть бути як публічні, так і приватні піддомени згідно з правилами публічного домену попереднього рівня, а у приватному домені публічні доменні імена неможливі.

2.3.3. Адміністрування доменних імен Інтернет

За загальну координацію та управління DNS, делегування доменів верхнього рівня та встановлення параметрів протоколів Інтернет тривалий час відповідала **IANA** (Internet Assigned Numbers Authority, Адміністрація адресного простору Інтернет, [http:// www.iana.org/](http://www.iana.org/)), а зокрема — призначена нею Служба реєстрації (Internet Network Information Center, **InterNIC**). IANA не є організацією в повному розумінні цього слова, це тільки назва контракту між Університетом Південної Каліфорнії та урядом США.

Безпосереднє керівництво IANA здійснював доктор Джон Постел, шанований у всьому світі висококваліфікований фахівець, який мав необмежений вплив на розвиток Мережі (за словами журналу «Економіст» — «бог Інтернет»). Зокрема, йому належить авторство **RFC**, створених під егідою IANA (RFC —

Request for Comments, Запит коментаріїв — серія документів, які описують різні технічні аспекти Інтернет).

В основу влади і повноважень IANA було покладено не закон або зобов'язання, а згоду провайдерів Інтернет на добровільну співпрацю. Збільшення та комерціалізація Інтернет, конкурентна боротьба за її простір, поява нових зацікавлених осіб, виникнення багатьох нетехнічних проблем (зокрема, юридичних) зумовили появу в 1999 році нової організації, відповідальної за розподіл адресного простору, управління системою доменних імен і адміністрування системи кореневого сервера — **ICANN** (The Internet Corporation for Assigned Names and Numbers, Інтернет-корпорація з присвоєння імен і номерів, <http://www.icann.org>).

Для розробки та реалізації програми розвитку системи родових доменів верхнього рівня спільним рішенням IANA та ISOC було утворено International Ad Hoc Committee (**IAHC**, Міжнародний спеціальний комітет). Сьогодні в рамках Меморандуму розуміння щодо gTLD (gTLD-MoU, The Generic Top Level Domain Memorandum of Understanding) працює Наглядовий комітет з політики (Policy Oversight Committee, **POC**). До складу POC входять представники IANA, ISOC, IAB, ITU, **CORE** (Council of Registrars, Рада Інтернет-реєстраторів, <http://www.core.gtld-mou.org>), INTA (International Trademark Association, Міжнародна організація з торгових марок, <http://www.inta.org>), WIPO (World Intellectual Property Organization, Всесвітня організація з охорони інтелектуальної власності, <http://www.wipo.int>, <http://www.wipo.org>). У своїй діяльності POC тісно взаємодіє з громадськістю, зокрема через опрацювання RFC.

Найбільші повноваження з адміністрування доменних імен у Європі належать Мережному координаційному центрові RIPE — **RIPE NCC** (The RIPE Network Coordination Centre, <http://www.ripe.net/>). RIPE NCC працює як Регіональний реєстр Інтернет у Європі — реєструє локальні (національні) реєстри Інтернет, які фактично фінансують його послуги; розподіляє для них блоки адресного простору IP, одержані від IANA; виконує інші обов'язки із забезпечення роботи Інтернет-провайдерів у Європі.

RIPE (Reseaux IP Europeens) — це організація вільної співпраці щодо європейських мереж, які діють за протоколом TCP/IP. Більшість робіт з адміністративної та технічної координації виконується у різноманітних робочих групах. Одним

із проєктів RIPE є **CENTR** (Council of European National Top level domain Registries, Рада європейських національних реєстрів верхнього рівня, <http://www.centri.org>), який з 1999 р. оформлено як незалежну організацію.

Права з безпосереднього адміністрування окремого домену (верхнього рівня) — управління простором імен у ньому — делегуються спеціально призначеному **адміністраторові** (координаторові), який, у свою чергу, може делегувати права з адміністрування доменів нижнього рівня третім особам. При цьому делегування публічних доменів третього та нижчих рівнів не рекомендоване.

Основною вимогою до адміністратора домену є його здатність виконувати необхідні обов'язки рівноправно, чесно і компетентно. Він повинен мати доступ до Інтернет, його персонал — бути доступним за електронною поштою. Призначений адміністратор домену верхнього рівня відповідає за управління доменом перед країною, якщо йдеться про домен країни, і перед співтовариством Інтернет. Сторони, вельми зацікавлені в домені, мають погодитись, що призначений адміністратор (вибраний за їхньою участю) їх задовольняє. IANA (ICANN) виступає арбітром з питань адресного простору Інтернет у випадках, коли сторони не можуть дійти згоди. Для піддоменів не висуваються додаткові вимоги, крім тих, що існують для доменів верхнього рівня.

Згідно з Правилами домену .UA адміністратор публічного домену має бути суб'єктом підприємницької діяльності, зареєстрованим в Україні. У процесі делегування доменного імені в публічному домені крім адміністратора беруть участь **реєстрант** — особа, що бажає користуватися та розпоряджатися певним доменним іменем в публічному домені, та **реєстратор** — зареєстрований в Україні суб'єкт підприємницької діяльності, який надає реєстрантові послуги, необхідні для технічного забезпечення делегування та функціонування доменного імені. Адміністраторові публічного домену забороняється виступати водночас реєстратором імен в цьому самому домені. Відносини між учасниками процесу делегування доменного імені будуються виключно на договірній основі. При цьому інтереси всіх членів української Інтернет-спільноти щодо системи доменних імен є рівними настільки, наскільки це не зачіпає законних інтересів інших членів української Інтернет-спільноти і/або будь-яких третіх осіб. Доменні спори розв'язуються компетентними судами в порядку, установленому чинним законодавством України.



Зона .UA — адміністрування і реформи

Український домен верхнього рівня .UA було зареєстровано у грудні 1992 року. Право адміністрування домену було надано ТОВ «Комунікаційні Системи», яке пізніше припинило свою діяльність. Упродовж понад восьми років адміністрування та реєстрація назв доменів виконувались добровільними зусиллями Групи координації домену .UA щодо розвитку системи адміністрування домену, утвореної з приватних осіб. У 1998 році розпочався процес реформування. Його учасниками стали компанії—оператори Інтернет, державні органи та установи (Мінекономіки, Держкомзв'язку, «Укртелеком», Міністерство закордонних справ, ДСТСЗІ¹ СБУ, Міністерство оборони та ін.). У 2000 році розпочала роботу Робоча група з питань реорганізації системи управління домену .UA та створення Регістру доменних імен України (UANIC WG). Робочою групою та її Експертною радою² було виконано підготовчу роботу зі створення ЗАТ «Український мережний інформаційний центр» (UANIC).

Доменні імена Інтернет є сферою, де стикаються суперечливі інтереси багатьох зацікавлених осіб і сил. Будь-яка фірма або користувач, які бажають мати своє «представництво» в Мережі, мають вирішити проблему вибору доменного імені.

Загальна практика показує, що існує два підходи до вибору назви сервера — більш професійний точний підхід з урахуванням функцій або розміщення сервера та витіюватий підхід, коли серверові присвоюється прізвище відомої людини, назва тварини, ім'я кіно- чи міфологічного героя тощо. У першому випадку назва полегшує сприйняття та роботу із сервером. Водночас довільно вибране ім'я може бути зручнішим за складний акронім, його можна залишити незмінним, навіть якщо функції змінились, а приховування їх у назві сервера певною мірою запобігає хакерським атакам.

У контексті Інтернет проблема набуває інших аспектів. Доменне ім'я пропонується зовнішньому світу, а тому воно має стосуватись або сфери діяльності фірми, або її назви, добре запам'ятовуватись, бути коротким і легко вимовлятись. Останнім часом з'явилась можливість зареєструвати доменне

¹ Департамент спеціальних телекомунікаційних систем та захисту інформації.

² До складу Експертної ради входять адміністратори доменів загального використання в зоні .UA, представники компаній-реєстраторів, юристи, патентні повірники.

ім'я верхнього рівня українською або російською мовою, наприклад «супермаркет.com» або «право.net». Оскільки в популярних публічних доменах вже не вистачає осмислених, інтуїтивно зрозумілих імен, така можливість доволі важлива. Очевидні й переваги для користувачів, які не дуже добре володіють англійською мовою. Що ж до проблем доменних імен, поданих кирилицею, то їх можна назвати, уявивши необхідність набрати ім'я, зареєстроване корейською, китайською або японською (ієрогліфами).

Вимагає уваги вибір домену вищого рівня — географічний проти негеографічного (наприклад, .ua чи .edu) — або домену нижчого рівня (.com.ua або kiev.ua). Альтернативою власному доменному імені є ім'я, пропоноване Інтернет-провайдером у комплексі послуг (типу «firma.provider.net»), що забезпечує менші витрати. Але використання власного імені домену має переваги, оскільки воно є коротшим, легше запам'ятовується і впізнається; показує, що фірма є серйозним учасником Інтернет-спільноти; захищає інвестиції в рекламу і залишається незмінним у разі зміни провайдера.



Реєстрація доменних імен — спосіб збагачення

Дуже популярним в Інтернет способом збагачення є кіберсквоттинг — реєстрація з метою наступного перепродажу доменних імен, які можуть знадобитись кому-небудь у майбутньому. За неперевіреними даними, Cineta.com було продано за 700 тис. дол. США, а WallStreet.com — за 1,03 млн. Міжнародний третейський суд WIPO, створений 1999 року, за час свого існування вже розглянув кілька тисяч справ за позовами компаній, які не бажають викупати у третіх осіб права на використання власного імені як домену. Очікується кількарізове зростання кількості таких справ у зв'язку з уведенням нових доменів, хоча CORE передбачає певний механізм розв'язання проблем — у разі задоволення її вимог товарний знак буде зареєстровано в кожному з доменів.

Ця проблема має й інший бік. За оцінками фахівців, 90 % доменних імен в Інтернет не використовуються — вони зареєстровані «про запас» або позначають проекти, які вже закрито. До того ж щоденно минає строк продовження реєстрації (оплати) близько 10 тис. доменних імен у всьому світі. Забудькуватість реєстранта може призвести до втрати доменного імені. Згадаймо найбільш масштабний прецедент: 37 тис. канадців втратили свої домени зі зміною національного оператора в 2000 році. А 2001 року в Мережі з'явилась нова

послуга служби SnapNames — відстеження доменних імен за базами реєстрів. SnapNames повідомляє про можливість подання заявки на реєстрацію імені, якщо воно звільнилось, або нагадує про наближення строку перереєстрації.

З метою захисту законних інтересів членів Інтернет-спільноти України щодо їхньої інтелектуальної власності в домені .UA приватні доменні імена 2-го рівня делегуються виключно в разі, якщо відповідне доменне ім'я повністю або його компонент 2-го рівня (до знака «.», але без нього) за написанням або вимовою збігається із зареєстрованим в Україні словесним знаком для товарів та послуг (торговою маркою), права на використання якого на території України належать відповідному реєстранту. Таке делегування відбувається незалежно від класів Міжнародної класифікації товарів і послуг, за якими зареєстровано торгову марку. Делегування відбувається виключно за умови надання належним чином завірених копій таких документів:

- Свідоцтва України на знак для товарів та послуг, виданого центральним органом виконавчої влади з питань правової охорони інтелектуальної власності;
- договору про передачу права власності на знак або ліцензійного договору (у разі, якщо реєстрант не є власником Свідоцтва);
- довідки бюро перекладів про те, що заявлене доменне ім'я або його частина за своїм написанням або вимовою збігається з відповідною торговою маркою.

Публічні домени 2-го рівня в домені .UA делегуються за власною ініціативою адміністратора домену .UA з метою побудови системи публічних доменів, організованої за принципом задоволення інтересів різних спільнот користувачів. Коли йдеться про вибір імен публічних доменів 2-го рівня в домені .UA, адміністратор домену .UA насамперед бере до уваги думки й пропозиції реєстраторів та української Інтернет-спільноти.

2.3.4. Сервіси Інтернет

Набір мережних протоколів TCP/IP, які дають змогу передавати інформацію, є основою для багатьох інших протоколів Інтернет, призначених для організації різноманітних служб (сервісів). Найбільш популярними сервісами є поштові (служби електронної пошти), пошукові (спеціальні пошукові

системи та підмережі), віддаленого доступу (Telnet), розподілених ресурсів (FTP, Archie, Gopher, WAIS), інформаційні (WWW).

Електронна пошта (E-mail, electronic mail) — це служба поштового зв'язку, в якій повідомлення передаються в електронному вигляді з використанням комп'ютерів і каналів зв'язку. Електронна пошта може пересилатись не тільки у глобальних мережах (зокрема, Інтернет), а й у локальних. Розрізняють *три варіанти організації електронної пошти*:

- проста (одне джерело — один одержувач);
- списки розсилки (одне джерело — багато одержувачів) — повідомлення розсилається всім зацікавленим особам за заздалегідь визначеним списком. Організуючи список розсилки, до відома потенційних учасників доводять тему, правила підписки (включення адрес до списку), правила внесення змін до підписки та її припинення, а також адресу, на яку потрібно надсилати свої листи. Списки можуть бути пакетними (дайджестними, коли пересилаються пакети певного розміру, що складаються з кількох повідомлень) або послідовної обробки;



Допомога новачкам — FAQ

Списки розсилки, телеконференції, окремі Web-сервери Інтернет мають розділи FAQ (Frequently Asked Questions) — запитання, які часто ставлять. Користувачеві-початківцю настійливо рекомендується ознайомитись із відповідями на ці запитання, щоб уникнути помилок і не відволікати адміністраторів.

- телеконференції і дискусії (багато джерел — багато одержувачів). Телеконференції являють собою варіант електронних дошок оголошень (Broadcast Bulletin System або Bulletin Board System, BBS) — повідомлення не розсилаються конкретним адресатам, а зберігаються на спеціальних серверах, де стають доступними для будь-якого користувача мережі. Електронні листи можна читати безпосередньо із сервера або замовляти їх на свою поштову скриньку через підписку. Через деякий час інформація із сервера конференції вилучається (вноситься до архіву).

Найвідоміша телеконференція Інтернет — Usenet — всесвітній «дискусійний клуб», який охоплює кілька десятків тисяч «форумів», що називаються групами новин (newsgroup).

Для полегшення вибору телеконференції в її назві зазначається категорія, до якої вона належить: alt — альтернативні погляди, biz — бізнес, comp — обчислювальна техніка, news — новини, rec — хоббі, розваги тощо, sci — наука, soc — соціальні теми, talk — дискусії різної тематики, misc — інші категорії. Наприклад, у групі новин news.newusers.questions можна поставити запитання про роботу Usenet.

І телеконференції, і списки розсилки можуть бути **модерованими** — відповідальна особа (група осіб) переглядає кожне повідомлення і дозволяє (забороняє) його розсилання. У немодерованих телеконференціях (списах розсилки) така перевірка не виконується.

Електронний лист має чітко визначену *структуру*:

- поштова адреса відправника («From»). Деякі програми надають можливість відправити лист від імені іншого користувача;
- поштова адреса одержувача («To»). У разі відправлення відповіді (reply) на одержаний лист у поле адреси одержувача заноситься адреса автора початкового листа, а в поле теми (див. далі) — та сама тема з приставкою «Re»;
- копія («CC») — додаткові адреси. Це необов'язкове для заповнення поле, вміст якого буде доступний усім одержувачам листа;
- невидима копія («BCC») — додаткові адреси, недоступні для решти адресатів;
- тема («Subject») — необов'язкове, але бажане для заповнення поле;
- текст листа.

Також користувач може задавати додаткові ознаки листа: пріоритет листа, який впливає на черговість його відправлення, необхідність автоматичного інформування про доставку та ін.



Електронні листи — специфіка спілкування

Електронне листування передбачає правила, які доповнюють вимоги до звичайної кореспонденції та машинописного тексту. По-перше, під час роботи з електронною поштою потрібно зважати на існування різних форматів і запобігати випадкам, коли адресат не може прочитати повідомлення. По-друге, потрібно обмежувати розмір електронного листа та вкладених у нього файлів. Ця вимога особливо важлива в разі, коли лист передається по ненадійних каналах зв'язку, і зумовлює мінімальність цитувань та появу усіляких скорочень. Останні слід

використовувати дуже обережно, оскільки вони варіюються від стриманого ІМНО (*In My Humble Opinion*, «на мою скромну думку») до неформального ROTFL («*Rolling On The Floor Laughing*», «качаюся по підлозі від сміху») і досить грубого (хоча, можливо, справедливого) RTM («*Read The Manual*», «читайте керівництво»). По-третє, слід пам'ятати, що відсутність невербальних форм в електронному спілкуванні вимагає додаткових зусиль для попередження непорозумінь. З цією метою використовуються «смайлики» (*emoticon, smiley*), які вказують на емоційний підтекст останньої фрази: :-) :- (:-) :- < :- o :- X B-) :-@. Як і скорочення, смайлики неприпустимі в офіційних листах.

Telnet — послуга віддаленого доступу. Користувач може працювати на віддаленому комп'ютері майже так само, як і в разі безпосереднього доступу. Комп'ютер користувача виступає терміналом віддаленого комп'ютера. Слово «telnet» також позначає протокол, який підтримує відповідну послугу, і програму, яка обслуговує сеанси роботи користувача.

FTP (*File Transfer Protocol*, протокол передавання файлів) — протокол, який визначає правила передавання файлів (а також цілих каталогів із вкладеними каталогами й файлами) з одного комп'ютера на інший. Таку саму назву має програма з відповідним призначенням. FTP також надає можливість шукати файли на віддаленому комп'ютері. В Інтернет існують численні FTP-сервери, які надають можливість скопіювати загальнодоступні файли (програмне забезпечення типу «freeware» або «shareware») анонімним користувачам (zareєстрованим як «anonymous» або як «guest» — «гість»).

Для пошуку і видачі інформації про розміщення загальнодоступних файлів на анонімних FTP-серверах призначена система **Archie**. Основою для пошуку може бути назва файла (каталога) або слова, що в ньому подаються. В останньому випадку пошук здійснюється серед заздалегідь нагромаджених описів файлів, що їх склали автори. Доступ до Archie здійснюється через Archie-сервери, наприклад archie.doc.ic.ac.uk.

Gopher — це інтегратор, який дає змогу користуватись усіма можливостями Інтернет (telnet, ftp, e-mail та ін.) завдяки Gopher-серверам. Оболонка Gopher організована як множина вкладених меню.

WAIS (*Wide Area Information Servers*, широкомасштабні інформаційні сервери) — діалогова система з віконним інтерфейсом для пошуку даних за ключовими словами, що вводяться у вікні

спеціальної клієнтської програми і передаються на WAIS-сервер для обробки. WAIS переглядає у зазначених базах даних і архівах усі тексти і підраховує, з якою частотою в них трапляються ключові слова. Ці відомості передаються користувачеві для вибору потрібних даних.

Серед багатьох інших можливостей Інтернет велику популярність здобули:

- чати (від англ. «to chat» — базікати) — спілкування в реальному часі двох і більшої кількості користувачів, коли текст, уведений з клавіатури одного з них, практично відразу відображається на моніторах інших учасників. Так створюються «кімнати нарад»;

- ICQ (від англ. «I seek you» — «я шукаю тебе») — комунікаційна програма, головною функцією якої є «миттєве доставляння повідомлень» між користувачами, кожний з яких має свій унікальний номер.

Поява нових протоколів, зокрема VRTP (Virtual Reality Transfer Protocol — протокол передавання даних віртуальної реальності) призведе до появи в Інтернет сервісів, досі невідомих.

2.4. ВИКОРИСТАННЯ SERVICE WORLD-WIDE WEB

World-Wide Web (WWW, Web, W3, Всесвітня павутина) є найбільш популярним сервісом Інтернет і дуже зручним способом роботи з інформацією. Автор — Тім Бернерс-Лі з Європейської лабораторії фізики елементарних частинок (Centre Europeen des Recherches Nucleaire, **CERN**) у Женеві (Швейцарія) — разом зі своєю командою розробляв систему WWW як спосіб організації інформації для наукових співробітників. В основу WWW покладено технологію гіпертексту, основні ідеї якої було розроблено ще на початку XX століття. Батьком концепції гіпертексту в сучасному розумінні вважають Теодора Хольма Нельсона. Сьогодні повноваження з реалізації можливостей Web належать Міжнародному консорціуму **W3C** (<http://www.w3.org/>). Пріоритетними напрямками діяльності W3C є розробка рекомендацій з безпеки, захисту інтелектуальної власності, конфіденційності, універсальності доступу. До кола членів W3C входять виробники апаратного й програмного забезпечення, телекомунікаційні та інші компанії. Рекомендації, вироблені W3C, не є обов'язковими стандартами, але приймаються як такі,

головним чином через відкритість — у їх розробці може взяти участь будь-яка зацікавлена особа.

Гіпертекст (гіпер- від англ. «hyper-» — «над-») — це звичайний текст, який містить посилання як на власні фрагменти, так і на інші тексти. Такий метод подання інформації дає змогу переглядати її незалежно від способу її початкової організації, за довільним маршрутом. Найпростішим прикладом гіпертексту є книга, зміст якої — це посилання на її розділи, користуючись якими можна не читати книгу від самого початку і до кінця, а відразу перейти на сторінку з потрібною інформацією.

У World Wide Web одиницею зберігання гіпертексту є **Web-сторінка** — електронний документ, підготовлений за допомогою мови розмітки гіпертексту HTML (HyperText Markup Language). Відповідно, базовий протокол для пересилання гіпертекстів — HTTP (HyperText Transfer Protocol).



Гіпертекст — приклад застосування

Прикладом гіпертекстової системи є он-лайнова ІС поліції Шотландії PINS (Police On-line Information System) — навчально-довідкова бібліотека, яка містить два головні керівництва, що використовуються шотландською поліцією, — закон про дорожній рух і кримінальний кодекс. Кожен із цих документів містить понад 3000 сторінок стислого тексту, з яких близько 1000 сторінок щорічно оновлюються з різних причин. Після автоматичного розпізнавання розділів і секцій пошуком абзаців, курсиву і т. ін. текст було розбито на окремі Web-сторінки, між якими встановлено ієрархічні зв'язки і визначено механізм навігації та повнотекстового пошуку. PINS було запущено Королевою Великобританії в червні 1998 року.

Web-сторінка може містити не тільки текст, а й графіку, звук, відеозображення, елементи програмного коду (наприклад, мовою Java) та ін. Тому такі документи називають **гіпермедійними**. До того ж за допомогою WWW можна дістати доступ до telnet, e-mail, ftp та інших сервісів Інтернет.

Комплекс пов'язаних за темою Web-сторінок називають **Web-сайтом** (від англ. «site» — місцезрештування). Часто, але не завжди файли, що входять до складу сайту, зберігаються на одному **Web-сервері** — комп'ютері, підімкненому до Інтернет, який має IP-адресу, зберігає Web-сторінки та інші файли і надає їх користувачам у відповідь на запити. Послуги з розміщення сайту в WWW називають **хостингом**.

Для запитування та відображення Web-сторінок призначено спеціальні прикладні програми — **Web-броузери** (або просто броузери¹, від англ. «browser», «browse» — перегорнути, переглянути). Найбільш популярними броузерами є Microsoft Internet Explorer, Netscape Communicator, Opera.

Кожна сторінка має свою адресу у форматі **URL** (Universal Resource Locator, універсальний координатор ресурсів): спочатку вказується протокол (тип зв'язку, який потрібно встановити — http://, ftp://, gopher://), далі йде доменне ім'я, що визначає місцезнаходження файлу (сервер/шлях/файл), наприклад, <http://www.informjust.kiev.ua/info.html>. У цьому контексті словосполучення «**домашня сторінка**» може позначати не тільки сторінку персонального характеру, а й «титильну», початкову сторінку Web-сайту, яку користувач одержує, вказуючи URL-адресу цього сайту.



Web — застосування фантастичне і реальне

Величезні можливості World Wide Web надихають на пошук нових сфер їх застосування. Вже пропонують продавати холодильники, які можуть самі відстежувати наявність продуктів і автоматично робити замовлення для поповнення запасів. За допомогою технологій WWW мікрохвильові печі зможуть одержувати інструкції з приготування страв від компанії-виробника, посилати в разі потреби замовлення на ремонт та виконувати інші функції. Але поки реальне застосування знайшли тільки Web-камери. Web-камера має можливості цифрового фотоапарата і відеокамери, але, на відміну від них, звичайно не може працювати без комп'ютера і має порівняно невисокі технічні характеристики. Ці недоліки можуть компенсувати додаткові можливості — миттєвий перегляд результатів зйомки на екрані монітора, збереження знімків і відеофільмів в електронному форматі, їх редагування за допомогою спеціального програмного забезпечення і, головне, передавання через Інтернет та розміщення на Web-сторінках. Останні дві можливості використовуються для організації відеоконференцій, створення кругових інтерактивних панорам, спостереження (камера-шпигун реагує на рух перед її об'єктивом і записує те, що відбувається; схоплені кадри можуть передаватись електронною поштою або завантажуватись на Web-сайт, що дасть змогу на відстані перевірити обстановку вдома або в офісі).

¹ Це запозичене слово має два варіанти написання — «броузер» і «браузер».

Найчастіше перехід між Web-сторінками здійснюється не зазначенням в адресному рядку броузера точної URL-адреси, а вибором на відкритій сторінці гіперпосилання (посилання, лінку) — виділеного фрагмента документа (тексту або рисунка), який містить вбудовані адреси URL. Під час наведення «миші» на гіперпосилання змінюється вигляд курсора — він набирає форми руки із вказівним пальцем, що натискає на вибраний елемент. Переміщення за гіперпосиланнями називають Web-серфінгом (Web-surfing).

World Wide Web у своїй роботі використовують і комерційні фірми, і громадські організації як для доступу до актуальної інформації, так і для подання відомостей про себе й свою діяльність. Це досягається за допомогою Web-серверів різних типів.

За *логікою навігації* в середовищі Інтернет розрізняють дві основні групи Web-серверів: сервери управління трафіком, мета функціонування яких — пошук ресурсів, необхідних користувачеві, та кінцеві сервери, що містять такі ресурси.

До першої групи належать:

- **пошукові системи**, призначені для пошуку ресурсів Інтернет за ключовими словами, які визначає користувач (див. розд. 5). Пошук здійснюється у спеціальній базі даних, що містить **індекси** пошукової системи — терміни, які описують зміст ресурсів Мережі. Шукає ресурси, переглядає їх і приписує їм терміни спеціальна програма — **робот-індексувальник**, якого називають спайдером (від англ. «spider» — павук) або кроулером (від англ. «crawler» — плазун). База індексів пошукової системи постійно оновлюється. Кожна пошукова система має власний особливий спайдер і специфічний спосіб пошуку даних у базі індексів, а тому результати пошуків у відповідь на один і той самий запит у різних пошукових системах можуть бути істотно різними. Класичним прикладом пошукових систем є AltaVista — <http://www.altavista.com/>;

- **каталоги**, які також пропонують користувачеві можливості щодо пошуку потрібних ресурсів, але не за допомогою ключових слів, а вручну за ієрархічно організованими тематичними рубриками. Королем каталогів вважається Yahoo! — <http://www.yahoo.com/>. Зауважимо, що нині дедалі більше пошукових служб поєднують у собі елементи пошукових систем і каталогів — користувач сам вибирає спосіб пошуку;

- ініціювальні сервери, які не лише здійснюють пошук, а й надають комплекс додаткових послуг своїм користувачам. Збіль-

шення кількості ініціювальних серверів є ще однією тенденцією розвитку пошукових служб Інтернет. Найбільші сервери такого роду дістали назву порталів (докладніше див. далі).

Другу групу Web-серверів становлять:

- сервери присутності, які забезпечують віртуальну присутність фірм (організацій, підприємств) у середовищі Інтернет. Їх називають рекламними, або інформаційними. Такі сервери можуть мати складну будову і для полегшення навігації пропонувати функції пошуку потрібної інформації на своїх Web-сторінках;

- інформаційні сервери, призначені для надання інформації за певною тематикою. Такі сервери можна поділити за ознакою платності доступу до інформації або її розміщення на Web-сервері. Власники Web-серверів із безплатними послугами можуть одержувати дохід за спонсорською (рекламною) моделлю — за рахунок продажу рекламного місця на своїх сторінках чи розміщення баннерів. Баннер — це прямокутний блок, найчастіше графічний, який містить гіперпосилання на сайт, що рекламується;

- інтерактивні магазини — Web-сервери, призначені для організації продажу товарів і надання послуг. Інтерактивний магазин поєднує елементи прямого маркетингу з функціями традиційного магазину. Основні завдання інтерактивного магазину — надавати клієнтові інформацію про товар або послугу, одержувати та обробляти замовлення, одержувати платню, а в разі торгівлі інформацією ще і відправляти оплачений товар.

Постановою Кабінету Міністрів України від 04.01.2002 р. № 3 затверджено Порядок обнародування в мережі Інтернет інформації про діяльність органів виконавчої влади. Щоб забезпечити гласність і відкритість, міністерства й відомства, а також державні адміністрації областей мають створити, починаючи із січня 2002 року, власні Web-сайти та постійно висвітлювати через них свою роботу. На таких сайтах мають бути представлені українською та англійською (у разі потреби — й іншими мовами) головні завдання та правові основи діяльності органів влади, їхня структура, керівництво, адреси й телефони, звіти та анонси подій, процедура видачі ліцензій і реєстрації, а також інформація про порядок оскарження рішень і т. ін. Облдержадміністрації також повинні розміщувати на своїх сайтах інформацію про виконання бюджету областей, рівень оплати енергоносіїв і комунальних послуг, тарифи та пільги, а також про сплату місцевих податків і зборів.

Секретаріат Кабінету Міністрів, Міністерство економіки, Держкомзв'язку та інформатизації і СБУ зобов'язані створити єдиний Web-портал Кабінету Міністрів, який об'єднає всі сайти органів виконавчої влади.



«Розкручування» сайту — кілька підходів

Один із міфів, пов'язаних з Інтернет, полягає в тому, що достатньо лише створити Web-сайт — і його відразу почнуть відвідувати зацікавлені користувачі. Насправді сайтпромоушен — «розкручування» сайту — це тривалий процес, який потребує чималих знань і зусиль. Основними шляхами реалізації є такі:

- ▲ реєстрація в каталогах;
- ▲ публікація інформації про сайт у розсилках, телеконференціях, групах новин, FFA (Free For All — «вільні для всіх», різновид каталогів, сховище посилань);
- ▲ баннерообмін;
- ▲ обмін посиланнями з аналогічними сайтами;
- ▲ участь у «кільцях» — «Web-рінгах» — тематичних об'єднаннях сайтів;
- ▲ розміщення адреси сайту в листах, електронних книгах і т. ін.;
- ▲ публікація інформації про сайт у журналах, газетах, рекламних проспектах тощо.

Портал — це Web-сайт, призначений для специфічної аудиторії, який об'єднує інформаційне наповнення і доставляння важливої інформації, забезпечує спільну роботу, надає персоналізований доступ до послуг і додатків. Кожний із порталів можна розглядати як відправну точку навігації в Інтернет, але повнота їхніх послуг часто виключає необхідність переходу на інші сайти.



Українські портали — кілька прикладів

AtlasUA (www.atlasua.net), Avanport (www.avanport.com), Bigmir.net (www.bigmir.net), «Воля» (www.volia.com), Gala.net (www.gala.net), <Meta> (www.meta-ukraine.com), «Нувсе» (www.nuvse.com), TopPing (www.topping.com.ua), Uaport (www.uaport.net), Український портал (www.uaportal.com), «Укроп» (Український об'єднаний портал, www.ukrop.com).

Найбільш поширеними елементами порталів є канали (категорії, за якими можна здійснювати пошук даних), електронна пошта, дискусії, розділ електронної купівлі. Усі портали мають аналогічну архітектуру, але за відмінностями між ними можна виокремити такі *категорії*:

- мегапортالي (горизонтальні портали) — це оригінальні портали Інтернет. Багато мегапорталів було започатковано як пошукові системи, наприклад Yahoo!, Lycos, America Online. Особливістю мегапорталів є їхня зорієнтованість на всіх користувачів Інтернет, а не на специфічну аудиторію;

- вертикальні портали («вортали», субпортали) — портали для специфічних ринкових ніш або груп користувачів. Діапазон діяльності вертикальних порталів малий — послуги з інвестиційного менеджменту, товари для спорту і т. ін. Можна сказати, що специфічний вертикальний портал існує практично для будь-якої аудиторії Інтернет і будь-який ринок має більш як один вертикальний портал. За прогнозами фахівців, кількість субпорталів з часом збільшуватиметься, тоді як мегапорталів ставатиме дедалі менше;

- портали типу B2B — електронні ринки для здійснення бізнес-операцій (закупки, проведення аукціонів і т. ін.);

- корпоративні портали (інтранет-портали, бізнес-портали, корпоративні інформаційні портали) створюються для потреб окремого підприємства або організації і можуть бути доступні як ізсередини (наприклад, для співробітників юридичного відділу), так і зовні (для клієнтів, постачальників, торгових партнерів, які потребують інформації або взаємодії). Корпоративні портали мають такі самі функції, як і звичайні Інтернет-портали, але вони є вікном доступу до корпоративної інформації, додатків і процесів. У разі внутрішньокорпоративного використання такі портали розглядають як 2-ге покоління інтранет-технологій (див. підрозд. 2.6). Як правило, термін «корпоративний портал» може визначати такі поняття, як «виконавчий портал», «портал управління», «портал розробників», «портал знань», «портал комерційної інформації».

Корпоративні портали можуть бути як горизонтальними (охоплювати весь обсяг інформації, додатків і процесів підприємства), так і вертикальними (зорієнтованими на окремий бізнес-процес, функцію або додаток). В останньому випадку на сервері порталу можуть існувати кілька логічних порталів, які обмежують доступні користувачам ресурси.

Корпоративні портали відіграють значну роль у створенні віртуальних організацій, оскільки надають доступ до додатків електронного робочого місця (починаючи від електронної пошти та календаря і закінчуючи засобами управління взаємовідносинами з клієнтами та автоматизацією продажу) (див. підрозд. 4.5);

- голосові портали пропонують інформаційне наповнення та Web-послуги на основі доступу за телефоном без використання комп'ютера — голосового інтерфейсу. Користувач набирає номер свого голосового порталу і за допомогою голосових команд або клавіатури телефону одержує інформацію та здійснює операції. Загалом, портали часто розглядаються як реалізація ідеології одноманітних (уніфікованих) комунікацій — усі види повідомлень (електронна пошта, телефонні повідомлення, факси) мають нагромаджуватись в єдиному місці, доступ до них має надаватись за допомогою універсального інтерфейсу. Із цього погляду голосовий доступ стає ще однією послугою будь-якого порталу. Проте завдяки голосовим порталам користувачі дістають принципово нові можливості. Одним із прикладів є організація презентацій, нарад або дискусій у вигляді телеконференцій. Ініціатор конференції подає у відповідному розділі порталу номери телефонів учасників, і система обдзвонює їх. Кожен з учасників може говорити і слухати решту своїх колег, а ініціатор — ще й контролювати хід дискусії (стежити за підімкненням учасників, заглушати їхні виступи, тимчасово припиняти їх участь у дискусії або повністю відмикати їх);

- персональні портали надають послуги індивідуальним споживачам. Серед таких послуг можуть бути електронна пошта, ведення календаря, персональний інформаційний менеджер. Деякі портали дають змогу виділяти в персональному просторі три «кімнати» — персональну, спільну та публічну. Якщо доступ до даних і додатків першої кімнати суворо обмежений, то аналогічними елементами спільної кімнати можуть користуватись усі запрошені. Це дуже зручно для проведення презентацій або Інтернет-лекцій. Вміст публічної кімнати (наприклад, електронна візитна картка власника) доступний для всіх, хто знає її адресу. Персональні портали можуть входити до складу мегапорталу (наприклад, MyYahoo!) чи бути незалежними.



Мобільний вхід до Інтернет

Один із напрямків розвитку Інтернет визначається тим, що власників мобільних телефонів сьогодні більше, ніж тих, хто використовує комп'ютер для роботи в Мережі. Для надання можливості користуватися послугами Інтернет за допомогою мобільного пристрою зв'язку розроблено протокол **WAP** (від англ.

Wireless Application Protocol). Розповсюдження мобільних телефонів з функцією WAP, пристроїв PDA¹, смартфонів² вже дало поштовх для розвитку нового різновиду електронної комерції — мобільної комерції, хоча її майбутнє залишається невизначеним і буде пов'язане насамперед з удосконаленням безпроводових мереж передавання даних.

2.5. ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ РОБОТИ В ІНТЕРНЕТ

Одна з найважливіших проблем, пов'язаних з Інтернет, полягає в тому, щоб забезпечити конфіденційність користувачів, тобто запобігти прихованому збиранню персональних даних, до якого вдаються переважно комерційні фірми, нагромаджуючи відомості про своїх споживачів (реальних і потенційних). Дані про здійснені покупки в сукупності з демографічною статистикою та іншою інформацією стають ключем до стимулювання продажу та підвищення прибутків. Захисники громадянських свобод вважають таку практику порушенням фундаментальних прав людини, оскільки здебільшого інформацію про користувачів збирають без їхньої згоди. З іншого боку, таких заходів вдаються й правоохоронні органи, розшукуючи хакерів, педофілів та інших злочинців. Щодо правової регламентації таких дій точаться гарячі суперечки. Але очевидно, що держава, яка забезпечує свободи громадян, саме тим насамперед відрізняється від тоталітарної, що правоохоронні органи в ній не мають вільного доступу до приватної інформації громадян.

У цьому контексті забезпечення **анонімності користувачів Інтернет**, під якою розуміється неможливість їх ідентифікації, перестає бути суто технологічною проблемою.

Насправді Інтернет за своєю суттю не передбачає забезпечення анонімності. Навпаки, сім'я комунікаційних протоколів TCP/IP базується на тому, що кожний підімкнений до Інтернет комп'ютер має постійний або тимчасовий ідентифікатор — IP-адресу, яка дає змогу відправляти і приймати інформацію. У разі звернення до будь-якого Web-сайту IP-адреса комп'ютера, з якого робиться запит, обов'язково заноситься до лог-файла — спеціального текстового файлу протоколу роботи серверу, на якому розміщено цей сайт, — звідки його легко можна вибрати.

¹ PDA (Personal Digital Assistant, персональний цифровий асистент) — портативний кишеньковий комп'ютер.

² Смартфон — гібрид мобільного телефону і PDA.

Ще одна проблема щодо забезпечення конфіденційності пов'язана з «cookies»¹ — невеликими файлами зі службовою інформацією, які на комп'ютер користувача без його дозволу може записати будь-який сервер Інтернет. Файли cookies не дають змоги встановити особу користувача, але під час їх використання можна відстежити його поведінку в Інтернет. Броузери мають опції відмови від одержання файлів cookies, але це унеможливує роботу з деякими сайтами.

Одним із підходів до вирішення зазначених проблем є встановлення контролю над чужим комп'ютером і робота в Інтернет від його імені. Це незаконний спосіб, до якого вдаються хакери під час своїх атак у Мережі. Але цим принципом можна скористатися й цілком легально.

Широко застосовується доступ до Інтернет з локальної мережі через **проксі-сервер** — посередник між комп'ютером користувача і сайтами, до яких він звертається. Однією з його функцій є анонімізація — персональна інформація не передається далі проксі-сервера. Крім проксі-серверів корпоративної ІС або Інтернет-провайдера можна використовувати спеціальні служби забезпечення анонімності. Використовуючи сервери таких служб як перший крок для входу в Інтернет, користувач дістає гарантії, що

всі сайти, які він відвідуватиме, одержуватимуть не його персональні дані, а характеристики сервера-«анонімайзера», який працює через власний проксі-сервер. Прикладами таких служб є [http:// www.anonymizer.com/](http://www.anonymizer.com/), <http://www.onion-router.net/>, <http://aixs.net/aixs/>, <http://www.rewebber.com/>, <http://www.private-server.com/>.

На жаль, як показують дослідження, зазначені служби не забезпечують абсолютної анонімності і можуть видати ІР-адресу у відповідь на спеціально зорієнтовану атаку. Найдосконаліший сервіс надає нині служба Freedom Network (Мережа свободи, <http://www.freedom.net/>). Клієнт має повідомити номер кредитної картки, з якої було здійснено оплату, а далі він може завантажити програму-клієнта, що дає можливість створити кілька псевдонімів для роботи. Усі пакети з даними надійно шифруються і передаються через множинну серверів, якими

¹ Основна мета використання файлів cookies — ідентифікація користувача і персональне налаштування Web-сторінок. Такі файли, одержані від певного Web-сервера, записуються на комп'ютер користувача і надсилаються цьому серверові під час подальших запитів інформації з нього. При цьому сервер точно знає, «хто до нього прийшов і що йому треба показати».

керують провайдери-партнери, приховуючи маршрути передавання.

2.6. ОРГАНІЗАЦІЯ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ. ІНТРАНЕТ

Характерною ознакою корпоративних (відомчих) комп'ютерних мереж є те, що для їх побудови слід з'єднати локальні (регіональні) обчислювальні мережі, а для деяких з них — ще й розв'язати задачу підімкнення віддалених користувачів.

Перша задача звичайно розв'язується за допомогою мостів і маршрутизаторів — пристроїв, що використовуються для з'єднання мережних сегментів. У разі централізованої структури (потоків інформації спрямовані або до центру, або від нього) перевага надається мостам, які дають можливість об'єднати різні ЛОМ у прозорому режимі і незалежно від застосовуваних мережних протоколів. Завдяки маршрутизаторам вдається обслуговувати довільні інформаційні потоки з можливістю вибору оптимального маршруту для передавання пакетів і підмикатись до глобальних мереж за відповідними протоколами.

За допомогою мостів і маршрутизаторів створюються і **віддалені вузли** мережі — локальна мережа нібито продовжується за допомогою телефонного каналу. Програмне забезпечення запускається безпосередньо на комп'ютері віддаленого користувача і через мережу звертається до файл-сервера, мережних принтерів та інших ресурсів. Цей підхід найбільш придатний для реалізації технологій «клієнт—сервер».

На відміну від технології віддаленого вузла технологія **«віддаленого управління»** полягає в тому, що програмне забезпечення функціонує на комп'ютері, який входить до складу ЛОМ організації, так званому **комунікаційному сервері** (сервері віддаленого доступу). Віддалений абонент працює в мережі організації, як і співробітники організації на місці, ресурси ЛОМ доступні для нього так само, як і в разі роботи за комп'ютером, безпосередньо підімкненим до мережі. Комп'ютер такого користувача перетворюється фактично на віддалений термінал, з'єднаний з комунікаційним сервером телефонним або іншим каналом. Технологія «віддаленого управління» зменшує трафік — по каналу зв'язку передаються тільки оновлення екрана на сервері, коди натиснутих клавіш та інші дії, виконані віддаленим користувачем.

Удосконалення технологій Інтернет і засвоєння їх широким колом користувачів сприяло їх упровадженню в корпоративні (відомчі) мережі навіть у тому разі, коли вони не підімкнені до Мережі.

З 1995 року почав застосовуватись термін «інтранет» (intranet, інтра-мережа). Узагальнюючи численні визначення, можна сказати, що **інтранет** — це внутрішньокорпоративна мережа, побудована на основі стандартних технологій Інтернет (TCP/IP, Web та ін.). Якщо організація (підприємство) здійснює електронний бізнес (див. підрозд. 4.3), то виникає змішана мережа, в якій підмножина внутрішніх вузлів становить інтранет, а для позначення решти (як прави-

ло, Web-серверів або просто вузлів, доступних ззовні) використовується термін **Extranet**¹ (екстранет, екстрамережа).

Концепція **повнофункціонального інтранет** (Full Service Intranet, FSI) передбачає в інтрамережі такі *сервіси*:

- користувачські — створення і публікація документів; координація робіт і взаємодія користувачів (системи електронної пошти і засоби підтримки колективної роботи); навігація (швидкий пошук і доступ до інформації); доступ до додатків;
- мережні — єдина довідкова служба (управління інформацією про людей та ресурси); реплікація (прозорий розподіл даних по мережі); безпека; управління.



Інтернет та інтранет — політика безпеки

Організація (підприємство) може втілювати в життя таку політику щодо взаємодії з Інтернет:

▲ **взаємодія без обмежень.** У цьому разі рекомендується зберігати й обробляти важливі та закриті дані відокремлено від решти;

▲ **внутрішні системи фізично відокремлені від зовнішніх мереж;**

▲ **типова політика.** Використання публічних каналів зв'язку ставить критичне завдання захисту даних, що передаються, та запобігання доступу до корпоративних вузлів зовні. Один із відповідних підходів полягає у створенні віртуальної приватної мережі

¹ Термін поки не є сталим.

(Virtual Private Network, VPN). **VPN** — це концепція захищеного передавання корпоративної інформації через Інтернет з використанням систем криптографічного захисту (див. підрозд. 3.4.3).

Інший підхід полягає в розмежуванні внутрішніх і зовнішніх мереж за допомогою брандмауера. **Брандмауер**¹ (firewall, «вогняна стіна») може бути маршрутизатором, персональним комп'ютером, сервером або групою серверів, призначених спеціально для захисту мережі або підмережі від зовнішніх мереж. Але насамперед, брандмауер — це підхід до безпеки, метод захисту мережі централізацією доступу до неї та контролем за ним апаратно-програмними засобами. Усі зовнішні з'єднання відбуваються через брандмауер, де вони аналізуються і пропускаються або блокуються.

Брандмауер також може приховувати уразливі внутрішні системи та важливу інформацію (топологія мережі, типи мережних пристроїв, ідентифікатори користувачів і т. ін.), протоколювати вхідний і вихідний трафік, забезпечувати більш надійну автентифікацію порівняно зі стандартними додатками.

Додатки FSI поділяють на *три групи*:

- 1) базові, що надаються інтранет як стандартні засоби (електронна пошта, засоби колективної роботи, телеконференції, комп'ютерна телефонія, зберігання і спільне використання інформації, навігація та пошук, довідники);
- 2) додатки, що їх розробляють незалежні виробники;
- 3) додатки, що розробляються спеціально для потреб конкретної організації (підприємства) — бази і сховища даних, кадрові і фінансові додатки та ін.

Інтранет як корпоративна мережа має такі *переваги*:

- уніфікований, простий і зручний доступ до інформації. І для перегляду загальнодоступних відомостей про компанію на Web-сервері в Інтернет, і для роботи з внутрішньою інформацією на Web-сервері інтранет потрібна одна програма — Web-броузер. Останні версії популярних броузерів можуть надавати доступ не тільки до звичайних Web-сторінок, а й до баз даних, тривимірних моделей тощо. Збільшення системи не вимагає від користувача додаткової підготовки, всі переваги Web-технологій залишаються в силі;

¹ Початкове значення запозиченого слова «брандмауер» — глуха стіна з вогнетривких матеріалів, що має запобігати поширенню пожежі з однієї будівлі на іншу.

- полегшення географічного розширення корпоративної мережі та збільшення обсягу доступних інформаційних ресурсів за рахунок природного сполучення інтрамережі з Інтернет. Вельми важливим фактором при цьому є те, що дедалі більша частка інформації від зовнішніх джерел надходить в електронному вигляді, що полегшує її обробку та інтеграцію з внутрішніми базами;

- кардинальні зміни внутрішніх комунікацій. Крім миттєвого доступу до повної актуальної інформації в масштабі всієї організації (підприємства) співробітники одержують можливість спілкуватись, проводити групові дискусії та колективний аналіз тощо. Усі офіційні комунікації підтримуються системою електронного документообігу на базі Web-серверу, а неофіційні — засобами електронної пошти і телеконференцій;

- порівняна простота проектів з упровадження інтранет, які є економічно вигідними і дають швидку віддачу, оскільки базуються на відкритих технологіях і стандартному інструментарії. Це знижує витрати як на створення та експлуатацію ІС, так і на навчання співробітників.



Контрольні запитання і завдання

1. Що таке комп'ютерна мережа? Яке призначення мають комп'ютерні мережі?
2. Для чого необхідні протоколи і стандарти?
3. Що таке топологія мережі та архітектура мережі? Які топології комп'ютерних мереж Ви знаєте?
4. Схарактеризуйте основні типи мереж, виділені за способом організації обробки інформації.
5. Назвіть види мереж, визначені Законами України «Про зв'язок» та «Про Національну систему конфіденційного зв'язку».
6. Схарактеризуйте підходи до управління та адміністрування, прийняті в Інтернет.
7. Які типи адресації застосовуються в Інтернет і в чому полягає відмінність між ними?
8. Як здійснюється адміністрування доменних імен Інтернет?
9. Визначте проблеми захисту інтелектуальної власності в адресному просторі Інтернет.
10. Визначте способи використання сервісів Інтернет у професійній діяльності юриста.

11. Як може бути організована корпоративна комп'ютерна мережа?

12. Що таке інтранет і які сервіси вона передбачає?

13. Яке призначення має брандмауер?



Література

1. ДСТУ 2229-93. Системи оброблення інформації. Локальні обчислювальні системи. Терміни і визначення. — К.: Держстандарт України, 1993.

2. ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення. — К.: Держстандарт України, 1994.

3. ДСТУ 3043-95. Системи оброблення інформації. Телеобробка даних і комп'ютерні мережі. — К.: Держстандарт України, 1995.

4. Матеріали сайтів <http://nic.net.ua>, <http://www.citforum.ru/Internet/>, <http://ua-nic.net>, <http://www.hostmaster.net.ua/>, <http://www.gtld-mou.org/>, <http://www.icann.org>, <http://www.infocity.kiev.ua/>, <http://www.osp.ru/cw/>, <http://www.uazone.org/>.

5. Ситник В. Ф., Козак І. А. Телекомунікації в бізнесі: Навч.-метод. посібник для самост. вивч. дисц. — К.: КНЕУ, 1999. — 204 с.



ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

3.1. ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ ІС

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення.

Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

Серед *причин комп'ютерних злочинів* і пов'язаних з ними викрадень інформації головними є такі:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп'ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Серед основних статей втрат варто виокремити такі:

- збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через нероботоздатність системи (мережі);
- вартість викрадених і скомпрометованих даних;
- витрати на відновлення роботи системи, на перевірку її цілісності, на доробку уразливих місць тощо.

Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників ІС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у держав-

ному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

Економічні та юридичні питання, приватна та комерційна таємниця, національна безпека — усе це зумовлює необхідність захисту інформації та ІС.

Згідно із Законом України «Про захист інформації в автоматизованих системах» *захист інформації* — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій».

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби і побудувати надійну систему захисту.

Базовими *принципами інформаційної безпеки* є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними *випадками порушення безпеки інформації* можна назвати такі:

- несанкціонований доступ — доступ до інформації, що здійснюється з порушенням установлених в ІС правил розмежування доступу;
- витік інформації — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації — дія, внаслідок якої інформація в ІС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;
- підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в ІС;
- блокування інформації — дії, наслідком яких є припинення доступу до інформації;
- порушення роботи ІС — дії або обставини, які призводять до спотворення процесу обробки інформації.

Причини настання зазначених випадків такі:

- збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);
- некоректна робота програмного забезпечення (втрати або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);
- навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи ІС, спричинення витоку інформації);
- помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);
- навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією).

Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або впливу інформації, але передбачають втручання в роботу системи.



Порушення безпеки ІТ — несанкціоноване використання ресурсів

За результатами розслідування, яке тривало 6 місяців, Центральне розвідувальне управління США (<http://www.cia.gov>) звільнило чотирьох співробітників за створення і використання таємного чата безпосередньо в мережі розвідувального підрозділу. Звільнених було визначено як неблагонадійних, щоб їх не могли прийняти на роботу аналогічні організації. Один із них обіймав високу посаду в американській розвідці. Ще 96 осіб понесли різного роду стягнення.

Чат, який було створено в середині 1980-х років, відвідували близько 160 співробітників, щоб пофліртувати, пожартувати або просто побазікати в обхід систем безпеки. В офіційній заяві ЦРУ цей факт було названо «волаючим порушенням цілісності мережі». Цей скандал ще раз засвідчив не лише існування проблем щодо інформаційної безпеки у ЦРУ, а й серйозне ставлення до них. Можна згадати, що наприкінці 1996 року за зберігання секретних матеріалів на домашньому комп'ютері, підімкненому до Інтернет, було звільнено Джона Дейча, директора Управління.

Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту.

Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви: сторонні, які не знають фірму; сторонні, які знають фірму, та колишні співробітники; співробітники-непрограмісти; співробітники-програмісти.

Межа між програмістами та простими користувачами з погляду небезпечності останнім часом стирається. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку і можуть скористатися спеціальним програмним забезпеченням, яке має дружній інтерфейс і доступне на піратських CD-ROM, у спеціальних розділах BBS і на сайтах Інтернет та FidoNet. За твердженнями експертів, тільки чверть співробітників цілком лояльна, чверть настроєна до фірми вороже і не має моральних обмежень, лояльність решти залежить від обставин. Тому нелояльні співробітники, які мають доступ до комп'ютерів і знайомі з системою, становлять серйозну загрозу¹. Передусім це організаційна проблема, технологія тут може відігравати тільки допоміжну роль.

Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники».

Хакери (хекери) — це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» — за однією з легенд, слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проекту, який не має видимого практичного значення і виконується виключно заради задоволення від самого процесу роботи. У більш вузькому розумінні слово «хакер» позначає тих, хто одержує неправомочний доступ до ресурсів ІС тільки для самоствердження (див. приклад). Останнє відрізняє хакерів від професійних зламувачів — *кракерів* (або «крекерів», не плутати з печивом!), які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень.

Найбільш криміногенною групою є *пірати* — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може

¹ За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів.

зосередитись на кредитних картках (таких називають «кардерами»), банківських рахунках, телефонному зв'язку (так звані «фрікери», «частотники») і т. ін., але в усякому разі його мотивацією є матеріальні інтереси, а не цікавість чи пустощі.



Хакери: погоня за славою, розваги чи самореалізація?

У січні 2001 року на сайті Хакер.ru з'явилося повідомлення про злом сайту ФБР (www.fbi.gov). За неперевіреними зі зрозумілих причин даними, хакери змінили структуру сайту і стерли директорію «wanted» (список найбільш небезпечних злочинців, яких розшукує ФБР), зробивши дублювальні копії файлів, про що й повідомили адміністратора сайту. Один з авторів зламу, московський програміст galblch, прокоментував свої дії так: «У принципі, злам був дрібницею — там була дірка... Першою ідеєю було просто написати адміну (адміністратору) про дірку без зламу як такого, але у зв'язку з іменитістю відомства, якому належить сайт, вирішили все ж таки розважитись». При цьому galblch вважає, що «писати програми більш цікаво, ніж шукати в них дірки, але й дірки цікаві...»

Шкідники (вандали) намагаються реалізувати у кіберпросторі свої патологічні схильності — вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без якої-небудь вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль.

Слід також зупинитись ще на одній групі, яка посідає проміжне місце між хакерами і недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш тяжких наслідків, ніж сплановані атаки професіоналів). Ідеться про *експериментаторів* («піонерів»). Найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів Мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема й законотворці.

Отже, одними з основних причин порушення безпеки інформації є незапитаність творчого потенціалу в поєднанні з неусвідомленням усіх наслідків протиправних дій. Цей фактор існує незалежно від національності або сфери професійної діяльності. Звичайно, жодна з особистих проблем не може стати приводом

для протиправної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп'ютерних злочинців. Стають відомими колосальні збитки від їхньої діяльності. Розвінчується міф про хакера як про комбінацію Гудіні і Фантомаса, адже часто своїми успіхами вони завдячують не своїм навичкам, а банальним пропускам у захисті систем (звідси і нове прізвисько — «ламери»). Поширюється думка про те, що комп'ютерний злочин легше попередити, ніж потім розслідувати. Однак це не вирішує проблему повністю, адже, крім бажання розважитись і самоствердитись існує ще недбалість, холодний комерційний розрахунок, прояви садизму та хворобливої уяви. Тому комп'ютерні злочини залишаються об'єктом уваги фахівців.



Хакерство — загроза чи невинна гра?

Секретні служби США поінформували комітет з озброєнь сенату про загрозу безпеці США № 1. Її становив хакер, який близько 200 разів зламав системи безпеки різного рівня і скопіював десятки секретних файлів, включаючи подробиці досліджень і розробок балістичних ракет. На те щоб його піймати, знадобилось 13 місяців. Хакером виявився англійський 16-річний хлопець, комп'ютерні навички котрого шкільний учитель оцінив у 4 бали. У ході судового засідання адвокат стверджував, що неповнолітній хакер не мав злого наміру і перебував під враженням від фільму «Іери патріотів».

Такі ігри можуть загрожувати виникненням реального військового конфлікту. Комп'ютерна атака на Пентагон у 1998 році збіглась у часі з черговим загостренням американо-іракських відносин у районі Перської затоки. Американське командування вважало, що атаку заподіяв Ірак з метою завадити висадці американських військ. До спеціального розслідування під кодовою назвою «Solar Sunrise» (http://www.sans.org/newlook/resources/IDFAQ/solar_sunrise.htm) було залучено агентів ФБР, представників відділу спеціальних розслідувань Військово-повітряних сил США, Міністерства юстиції, ЦРУ, Агентства національної безпеки та деяких інших урядових структур США. А справжніми винуватцями виявились двоє американських підлітків, якими керував 21-річний ізраїльський хакер.

3.2. ОСНОВНІ ВИДИ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем. У першому випадку правопорушення можна кваліфікувати за звичайними нормами права (крадіжка, грабіж, розбій і т. ін.). В інших випадках, коли

комп'ютер виступає і як інструмент, і як об'єкт, злочин відносять до окремої категорії (див. розділ XVI Кримінального кодексу України). Далі описано найбільш поширені види комп'ютерних злочинів.

Несанкціонований доступ до інформації, що зберігається у комп'ютері, та її розкрадання. Розрізнити ці дві категорії дуже важко. Найчастіше присвоєння машинної інформації та програмного забезпечення відбувається копіюванням, що зменшує ймовірність виявлення факту крадіжки. Можливі шляхи здійснення злочину:

- використання чужого імені або пароля («маскарад»). Одержати коди та паролі законних користувачів можна придбанням (звичайно з підкупом персоналу) списку користувачів з необхідними відомостями, знаходженням подібного документа в організаціях, де контроль за їх збереженням недостатній; підслуховуванням через телефонні лінії. Відомі випадки, коли секретна інформація, і не тільки приватного характеру, відпливала через дітей;
- незаконне використання привілейованого доступу;
- «зламування» системи;
- знаходження слабких місць у захисті системи чи недоробок у програмному забезпеченні;
- використання збоїв системи;
- крадіжка носіїв інформації;
- читання інформації з екрана монітора;
- збирання «сміття»;
- встановлення апаратури підслуховування та запису, підімкненої до каналів передавання даних;
- віддалене підімкнення;
- модифікація програмного забезпечення.

Підробка комп'ютерної інформації. Цей злочин можна вважати різновидом несанкціонованого доступу з тією різницею, що скоїти його може і стороння особа, і законний користувач, і розробник ІС. В останньому випадку може підроблятися вихідна інформація з метою імітування роботоздатності ІС і здачі замовнику свідомо несправної продукції. До цього самого виду злочинів можна віднести підтасування результатів виборів, голосувань і т. ін.

Уведення у програмне забезпечення «логічних бомб» — невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Різновидом логічної бомби є «часова бомба», яка спрацьовує в певний момент часу. Ще одним способом модифікації про-

грамного забезпечення є таємне введення у програму (чужу або свою) «троянського коня» — команд, які дають можливість зі збереженням роботоздатності програми виконати додаткові, не задокументовані функції, наприклад переслати інформацію (зокрема паролі), що зберігається на комп'ютері. В останньому випадку «троянський кінь» є засобом реалізації «прихованого каналу». Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру. Завдання ускладнюється, коли у програму вставляється не власне «троянський кінь» (див. вище визначення), а команди, які його формують і після досягнення поставленої мети — знищують. Також можна зазначити, що «троянські коні» можуть перебувати не тільки у програмах, а й в інших файлах, наприклад в електронних листах.



«Троянський кінь» — найкращий засіб попередження порушень авторського права?

Один із перших завантажувальних вірусів для IBM-PC (заражав дискети 360 Kb), який стрімко розповсюдився на Заході, був написаний у Пакистані власниками компанії з продажу програмних продуктів, які хотіли з'ясувати рівень піратського копіювання у своїй країні. Автори залишили у тілі вірусу текстове повідомлення зі своїми іменами, адресами і навіть номерами телефонів. Незважаючи на появу інших різноманітних методів захисту авторських прав, за минулий час цей приклад неодноразово наслідувався.

Розробка і поширення комп'ютерних вірусів. Напевне, сьогодні не має жодного користувача ІС, який у своїй роботі не стикався б із комп'ютерними вірусами. Прояви вірусів можуть бути різноманітними — від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів з жорсткого диска. У будь-якому разі це означає порушення цілісності ІС. Сьогодні фахівці очікують появи вірусів для програмованих мікросхем і мобільних телефонів. Більш докладно загрозу зараження комп'ютерними вірусами розглянуто в підрозд. 3.3.

Злочинна недбалість у розробці, виготовленні й експлуатації комп'ютерної техніки та програмного забезпечення. Необережне використання комп'ютерної техніки аналогічне недбалому поводженню з будь-яким іншим видом техніки, транспорту і т. ін. Його особливістю є те, що безпомилкових програм не буває у принципі. Якщо помилка призвела до наслідків, які вимагають покарання винуватців, про винність розробників свідчать:

- наявність у технічному завданні вказівок на те, що в системі може виникнути ситуація, яка призводить до збою (аварії);
- можливість створення контрольного прикладу з даними, які імітують ситуацію, що призвела до збою (аварії).



Великі наслідки невеликих похибок — атаки «салями»

Принцип атак «салями» полягає в тому, що грошові суми обробляються з певною точністю (гривня та сота частка — копійка, долар і сота частка — цент), яка звичайно перевищується в разі нарахування відсотків та виконання деяких інших операцій. Якщо розробник (або користувач) передбачає округлення суми 0,958652 грн до 0,94 грн, то в разі виконання 10 000 операцій на день його щорічний «прибуток» становитиме понад 30 000 грн. При цьому справжній власник може списати помилку на неточності обробки і не висуватиме претензій.

Окремим випадком недбалості програмістів є створення і залишення без контролю «люків» («чорних ходів») — прихованих, не задокументованих точок входу у програмний модуль, які часто використовуються для відлагодження програми та її підтримання у процесі використання. Але «люк» може бути використаний і для зламування системи сторонньою особою, і для таємного доступу до програми самим розробником. Для виявлення «люків» слід проводити ретельний аналіз початкових текстів програм.

До тяжких непередбачуваних наслідків можуть призвести й дії користувачів. Визначити їх як халатні можна за таких ознак:

- користувач мав у своєму розпорядженні інформацію про можливі наслідки порушення інструкцій;
- виконати вимоги інструкції було можливо фізично і психологічно.

Комп'ютерні злочини в мережі Інтернет. Виокремлення цієї категорії диктується реаліями використання глобальної мережі. По-перше, Інтернет стає інструментом здійснення «звичайних» злочинів. Це промисловий шпіонаж, саботаж, поширення дитячої порнографії і т. ін. Понад третина користувачів Мережі страждає від шахрайств. Продавці еквадорської нерухомості, нафтових свердловин в Антарктиді і кокосових плантацій в Коста-Ріці, будівельники фінансово-інвестиційних пірамід і брокери, які просувають акції певних фірм і наживають на продажу цих акцій у період ажіотажу, — їхні сайти та розсилки наздоганяють сотні

тисяч людей, серед яких не так вже й мало легковірних. Одним із ключових аспектів багатьох «схем» подібного роду є доступ до персональних даних користувача (див. приклад). Заповнивши анкету, людина стає потенційним об'єктом шахрайства в майбутньому, а найбільш довірливі, зокрема ті, хто надає інформацію про свою кредитну картку, страждають відразу. Відомо, що більшість шахрайств пов'язана з використанням пластикових кредитних карток і здійснюється на сайтах, що спеціалізуються на купівлі-продажу товарів.



Шахрайство в Інтернет — розсилання фальшивих листів

Типовим прикладом такого злочину є акція, заподіяна проти відомого Інтернет-аукціону eBay компанією Reverse Auction.com у 2000 році. Схема шахрайства доволі проста: користувачам розсилаються фальшиві листи з проханням оновити свої дані на сторінці, яка відкривається за гіперпосиланням у листі. Сторінка виглядає дуже схожою на сторінку eBay, але розміщена не на сайті компанії. У відповідь на позов eBay та Федеральної торгової комісії США суд присудив компанії ReverseAuction.com заплатити eBay 1,2 млн дол.

По-друге, стає все більше злочинів, пов'язаних із самим існуванням Інтернет. Крім розповсюдження вірусів та зламування сайтів можна назвати такі:

- «нюкання» (від англійського «nuke», ядерна зброя) — програмна атака на іншого користувача Інтернет, у результаті якої його комп'ютер втрачає зв'язок з мережею або «зависає»;
- «спам» (від англійського «spam»¹) або «junk mail» (пошта з мотлохом, непотрібна кореспонденція) — варіант багаторівневого маркетингу в мережі. Спаммерів можна поділити на дві групи. Першу становлять новачки, які тільки-но одержали доступ до Мережі та усвідомили, що можуть розсилати повідомлення куди завгодно і кому завгодно. Другу групу утворюють професіонали, які заробляють гроші на заздалегідь неправдивій рекламі типу «Отримай премію...», «Розбагатій...», «Швидко зароби...» і т. ін. Про нечесність таких «бізнесменів» говорить хоча б їх небажання вказати свої справжні ім'я та координати;
- «винюхування» («sniffing») — сканування пакетів, які передаються в мережі для одержання інформації про користувача (-ів);

¹ Назва «spam» пішла від скетчу комік-групи «Літаючий цирк Монті Пайтона», в якому відвідувачі ресторану, які безуспішно намагалися зробити замовлення, були змушені слухати хор, що прославляв консервованій ковбасний фарш — spam.

- «серверний трикутник» (Web-spoofing, Web-мистифікація) — зловмисник, який проникає на сайт, змінює механізм пошуку так, що вся інформація, що її запитують користувачі, передається через якийсь інший сайт, де її, до того ж, можуть певним чином «обробити»;

- мережні атаки, спрямовані на «зависання» серверів («Denial of service attack», DOS-attack, атака, що спричинює відмову від обслуговування) або уповільнення їхньої роботи різними способами («повені»). Найчастіше для реалізації таких атак використовуються пакети технологічної інформації та самі правила взаємодії серверів за мережними протоколами. Конкретні назви атак з'являються за назвами програм, що їх реалізують («persi»), позначеннями пакетів технологічної інформації («SYN», «UDP») або як похідні від інших слів («smurfing», перекручене «surfing» — серфінг, пересування за гіперпосиланнями).

Фактично єдиний спосіб створити систему, абсолютно стійку до зовнішніх впливів, — припинити будь-які її зв'язки із зовнішнім світом. А мінімальним із погляду заходом є заборона доступу до Інтернет не для службових цілей.

3.3. КОМП'ЮТЕРНІ ВІРУСИ ЯК ЗАГРОЗА ІНФОРМАЦІЙНИМ СИСТЕМАМ

Вважають, що перші прототипи «електронних інфекцій» з'явилися наприкінці 1960-х — на початку 1970-х років у вигляді програм-«кроликів», які швидко розмножувалися і займали системні ресурси, знижуючи таким чином, продуктивність комп'ютерів. «Кролики» не передавалися між системами і були результатом пустощів системних програмістів. Термін «комп'ютерний вірус» уперше вжив американський студент Фред Кoen у 1984 році. Він поділив віруси на дві великі групи. До першої він відніс ті, які написані для певних наукових досліджень у галузі інформатики, а до другої — «дикі» віруси, вироблені з метою заподіяння шкоди користувачам.

Сьогодні написання вірусів набуває ознак промислового виробництва, їх кількість вимірюється десятками тисяч, і розуміння цієї загрози має стати необхідною вимогою для кожного користувача.

Комп'ютерний вірус — спеціально написана невелика за розмірами програма, яка може створювати свої копії, впроваджуючи їх у файли, оперативну пам'ять, завантажувальні області і т. ін. (заражати їх), та виконувати різноманітні небажані дії.

Небезпечність вірусу зростає через наявність у нього латентного періоду, коли він не виявляє себе. Для маскування вірус може використовуватися разом з «логічною» або «часовою бомбою».



Кілька ознак зараження ІС вірусами:

- ▲ припинення роботи або неправильна робота програм, які раніше функціонували успішно;
- ▲ неможливість завантаження операційної системи;
- ▲ зменшення вільного обсягу пам'яті;
- ▲ уповільнення роботи комп'ютера;
- ▲ затримки під час виконання програм, збої в роботі комп'ютера;
- ▲ раптове збільшення кількості файлів на диску;
- ▲ зникнення файлів і каталогів або перекручування їхнього вмісту;
- ▲ незрозумілі зміни у файлах;
- ▲ зміни дати і часу модифікації файлів без очевидних причин;
- ▲ незрозумілі зміни розмірів файлів;
- ▲ видача непередбачених звукових сигналів;
- ▲ виведення на екран непередбачених повідомлень або зображень.

Варто враховувати, що зазначені явища можуть бути наслідком й інших причин.

Віруси можна класифікувати за різними ознаками.

За *середовищем існування* розрізняють файлові, завантажувальні, комбіновані (файлово-завантажувальні), пакетні та мережні віруси.

Файлові віруси звичайно заражають файли з розширеннями .com та .exe. Однак, деякі їх різновиди можуть інфікувати файли й інших типів (.dll, .sys, .ovl, .prg, .bat, .mnu), при цьому вони, як правило, втрачають здатність до розмноження. У свою чергу, за *способом зараження середовища існування* файлові віруси поділяють на резидентні та нерезидентні. Останні починають діяти тільки під час запуску зараженого файлу на виконання і залишаються активними обмежений час. Резидентні віруси інсталиують свою копію в оперативній пам'яті, перехоплюють звертання операційної системи до різних об'єктів і заражають їх. Деякі віруси здатні перехоплювати досить багато різних функцій переривань, у результаті чого файли можуть заражатись у процесі перейменування, копіювання, знищення, змінювання атрибутів, перегляду каталогів, виконання, відкривання та здійснення інших операцій.

Резидентні віруси зберігають активність весь час до вимикання комп'ютера.

Порівняно новою групою можна назвати макровіруси, які використовують можливості макромов, вбудованих у текстові редактори, електронні таблиці і т. ін. Нині поширені макровіруси у Microsoft Word і Excel. Вони перехоплюють деякі файлові функції в разі відкриття чи закриття зараженого документа і згодом інфікують решту файлів, до яких звертається програма. У певному сенсі такі віруси можна назвати резидентними, оскільки вони активні тільки у своєму середовищі — відповідному додатку.

Окрему категорію файлових вірусів становлять віруси сім'ї DIR, які не впроваджуються у файли, а виконують реорганізацію файлової системи так, що під час запуску будь-якого файла управління передається вірусу.

Завантажувальні віруси відрізняються від файлових резидентних вірусів тим, що вони переносяться із системи в систему через завантажувальні сектори. Комп'ютер заражається таким вірусом після спроби завантаження системи з інфікованого диска, а дискета — при читанні її «змісту».

Комбіновані віруси можуть поширюватись як через завантажувальні сектори, так і через файли.

Пакетні віруси — це порівняно прості і старі віруси, написані мовою управління завданнями операційної системи.

Мережні віруси («черв'яки») розмножуються по комп'ютерній мережі, зменшуючи тим самим її пропускну здатність, уповільнюючи роботу серверів і т. ін. Вони посідають перше місце за швидкістю поширення. Найбільш відомим є так званий «черв'як Морріса». Останні моделі «черв'яків» упроваджуються у різні архіви (arj, zip та ін.) і зменшують вільний простір на диску.

За *ступенем деструктивності* віруси можна поділити на такі групи:

- порівняно безпечні, нешкідливі — їх вплив обмежується зменшенням вільної пам'яті і графічними або звуковими ефектами. Варто зазначити, що зменшення пам'яті в деяких випадках може призвести до збою системи, а ефекти — відволікти користувача, у результаті чого він припуститься помилки;

- небезпечні — віруси, які можуть призводити до збійних ситуацій;

- дуже небезпечні — дії вірусів можуть призвести до втрати програм, знищення даних, стирання інформації в системних областях тощо.

За *особливостями алгоритму* віруси важко класифікувати через їх різноманітність. Можна виокремити найпростіші, «вульгар-

ні» віруси, написані єдиним блоком, який можна розпізнати в тексті програми-носія, та віруси «роздроблені» — поділені на частини, що нібито не мають між собою зв'язку, але містять інструкції комп'ютерів, як їх зібрати в єдине ціле і розмножити вірус.

З погляду *прийомів маскування* розрізняють віруси-невидимки (стелс-віруси, stealth) та поліморфні віруси. Перші перехоплюють функції операційної системи, відповідальні за роботу з файлами, і коригують результати звернень. Механізм «невидимості» в кожному з цих вірусів реалізується по-своєму, однак можна виокремити кілька загальних принципів:

- для приховування збільшення довжини заражених файлів вірус передає програмі перегляду каталогів зменшене значення їхньої довжини;

- для того щоб користувач не виявив код вірусу під час перегляду файла, вірус виліковує його в момент відкриття і заново заражає у процесі закриття;

- для того щоб замаскувати свою присутність у пам'яті комп'ютера, вірус стежить за діями резидентних моніторів пам'яті, у разі спроби перегляду коду вірусу система зависає.

Поліморфними називають віруси, які застосовують різноманітні способи шифрування власного тіла. У разі зараження чергового файла алгоритм шифрування змінюється випадковим чином. При цьому дуже важко виділити **сигнатуру** — характерну послідовність байтів у коді вірусу.

3.4. ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

3.4.1. Класифікація засобів захисту інформації

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

Морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи

осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США.

Правові засоби захисту — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ.

Перехід до інформаційного суспільства вимагає удосконалення кримінального і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проекту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи (див. матеріали сайту <http://www.coe.int>), було внесено зміни, оскільки його розцінили як такий, що суперечить положенням про права людини і надає урядам і поліцейським органам зайві повноваження.

Загальною тенденцією, що її можна простежити, є підвищення жорсткості кримінальних законів щодо комп'ютерних злочинців. Так, уже сьогодні у Гонконгу максимальним покаранням за такий злочин, якщо він призвів до виведення з ладу ІС або Web-сайту, є 10 років позбавлення волі. Для порівняння, у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

Адміністративні (організаційні) засоби захисту інформації регламентують процеси функціонування ІС, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки. Вони охоплюють:

- заходи, які передбачаються під час проектування, будівництва та облаштування об'єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.);
- заходи, що здійснюються під час проектування, розробки, ремонту й модифікації обладнання та програмного забезпечення

(сертифікація всіх технічних і програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін тощо);

- заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б не вигідно або неможливо припускатися зловживань і т. ін.);

- розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень і т. ін.; розробка адміністративних норм та системи покарань за їх порушення тощо).

Адміністративні засоби є неодмінною частиною захисту інформації. Їх значення зумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації (див. приклад), а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються).



Комп'ютерні злами у вільний від роботи час — справа Ван де Глессена проти Getronics

Нідерландський хакер Димитрій Ван де Глессен, який зламав сайт Microsoft (<http://www.microsoft.com>) у листопаді 2000 року, незабаром був звільнений з роботи у компанії Getronics (<http://www.getronics.nl>). Однак у Нідерландах не існує закону, який би дозволяв звільняти співробітника за те, що він зламував сайти у вільний від роботи час. Тому справу було розглянуто в суді.

За словами хакера, формальним приводом його звільнення була його відмова від обслуговування конференції через небажання звертати до себе увагу журналістів. Він стверджує, що його прийняли на роботу саме через його хакерські вміння, а звільнення пояснюється тим, що він повідомив про злам керівництво Getronics вже після інформування Microsoft та оголошення зламу у пресі. Таким чином, Getronics, комерційний партнер Microsoft, втратила козирі у переговорах щодо контракту на забезпечення безпеки серверів цієї корпорації.

Представники Getronics заявили, що компанія справді потребувала професійних навичок Димитрія, але його злами інших компаній створювали проблеми для Getronics, і керівництво неодноразово вимагало від хакера припинити таку діяльність. Злам сайту Microsoft став останньою краплею.

Суд постановив, що компанія має виплатити Димитрію вихідну допомогу у розмірі заробітної плати за три місяці, що становить 10 тис. голландських гульденів (приблизно 4300 доларів).

Засоби **фізичного (технічного) захисту інформації** — це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів ІС, стихійних лих, саботажу, диверсій і т. ін. До цієї групи відносять:

- засоби захисту кабельної системи. За даними різних досліджень саме збої кабельної системи спричиняють більш як половину відказів ЛОМ. Найкращим способом попередити подібні збої є побудова **структурованої кабельної системи (СКС)**, в якій використовуються однакові кабелі для організації передавання даних в ІС, сигналів від датчиків пожежної безпеки, відеоінформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержувати вимог міжнародних стандартів;

- засоби захисту системи електроживлення. Американські дослідники з компанії Best Power¹ після п'яти років досліджень проблем електроживлення зробили висновок: на кожному комп'ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності ІС можливе використання аварійного електрогенератора або резервних ліній електроживлення, підімкнених до різних підстанцій;

- засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізова-

¹ Димитрієв А. Сторож для Storage. — <http://www.infocity.kiev.ua/hard/content/hard114.shtml>.

ний сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);

- засоби захисту від впливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо.

До цієї самої групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні мітки, що наносяться на документи і предмети (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього.

Як було вже сказано, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними.

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів (див. підрозд. 3.4.4), розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо (див. докладніше далі).

Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «**стеганографія**» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування тайнопису датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту — так вносились шифрована інформація про умови складання контракту.

Комп'ютерна стеганографія базується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Методи стеганографії дають можливість замінити несуттєві частки даних на конфіденційну інформацію. Сімейна цифрова фотографія може містити комерційну інформацію, а файл із записом сонати Гайдна — приватний лист.

Але найчастіше стеганографія використовується для створення **цифрових водяних знаків**. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

Щодо впровадження засобів програмно-технічного захисту в ІС, розрізняють два основні його способи:

- додатковий захист — засоби захисту є доповненням до основних програмних і апаратні засобів комп'ютерної системи;
- вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів ІС або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності засобів захисту між собою та з програмно-технічним комплексом ІС. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

3.4.2. Захист від комп'ютерних вірусів

Для виявлення, знищення та попередження «електронних інфекцій» можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Останніми роками з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивірусні плати, які вставляються у стандартні слоти розширення комп'ютера. Але найбільш поширеним методом залишається використання **антивірусних програм** — спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів.

Антивірусні програми поділяють на кілька видів.

Програми-детектори здійснюють пошук сигнатур вірусів. Недоліком детекторів є те, що вони можуть знаходити тільки ті віруси, які відомі їхнім розробникам, а отже, вони швидко заста-

рівають. Деякі програми-детектори можна налаштовувати на нові типи вірусів, проте неможливо розробити програму, яка могла б виявити будь-який заздалегідь невідомий вірус. Отже, негативний результат перевірки програмою-детектором не гарантує відсутності вірусів. Багато детекторів мають режими лікування або знищення заражених файлів — функції докторів.

Програми-доктори («фаги») не тільки знаходять заражені вірусами файли, а й «лікують» їх (видаляють з файла тіло програми-вірусу), повертаючи їх у початковий стан. Перед лікуванням файлів програма очищує оперативну пам'ять. Серед фагів виокремлюють поліфаги — програми-доктори, призначені для пошуку і знищення великої кількості вірусів. Як і детектори, програми-доктори потребують постійного оновлення.

Програми-ревізори запам'ятовують початковий стан програм, каталогів і системних областей, коли комп'ютер не заражений вірусом, а згодом, періодично або за бажанням користувача, порівнюють поточний стан системи з початковим. Як правило, перевірка здійснюється відразу після завантаження операційної системи — контролюються довжина файла, його контрольна сума, дата і час модифікації та інші параметри. Деякі програми-ревізори можуть при цьому виявляти і стелс-віруси. Гібриди програм-ревізорів і докторів можуть не тільки виявляти зміни, а й повертати файли і системні області до початкового стану. Вони є більш універсальними, оскільки можуть захистити і від вірусу, не відомого на час їх створення, якщо він використовує стандартний механізм зараження.

Програми-фільтри («сторожа», «монітори») — резидентні програми, призначені для виявлення підозрілих дій при роботі комп'ютера. Після одержання відповідного повідомлення користувач може дозволити або відмінити виконання операції. Деякі програми-фільтри перевіряють програми, які викликаються до виконання, та файли, що копіюються. Недоліком подібних програм є їх «набридливість», можливі конфлікти з іншим програмним забезпеченням, а перевагами — виявлення вірусів на ранній стадії, що мінімізує втрати.

Програми-вакцини («імунізатори») модифікують програми і диски таким чином, що це не відбивається на роботі програм, але вірус, від якого проводиться вакцинація, вважає їх інфікованими. Це вкрай неефективний спосіб захисту. Вакцини мають обмежене використання — їх можна застосовувати тільки проти відомих вірусів.

Як видно з наведеного опису, жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержува-

ти загальних правил (див. вставки) і користуватись останніми розробками антивірусних лабораторій.



Основні заходи з антивірусного захисту

1. Комплексно використовуйте сучасні антивірусні програми та оновлюйте їх версії.
2. Регулярно перевіряйте комп'ютер (системні області, пам'ять, файли), завантаживши ОС із захищеної від запису дискети (диска).
3. Перевіряйте на наявність вірусів дискети, записані на інших комп'ютерах.
4. Перевіряйте на наявність вірусів файли, що надходять із комп'ютерних мереж.
5. Завжди закривайте свої дискети від запису під час роботи на інших комп'ютерах, якщо на них не записується інформація.
6. Не залишайте у дисководі дискети під час вмикання комп'ютера або перезавантаження комп'ютера чи ОС.
7. Обов'язково робіть архівні копії цінної інформації на змінних носіях.



Чотири правила поведінки при зараженні комп'ютерної системи вірусом

1. Не поспішайте і не приймайте необачних рішень.
2. Слід негайно вимкнути комп'ютер, щоб вірус не продовжував своєї руйнівної дії.
3. Усі дії з виявлення вірусу і лікування системи обов'язково слід виконувати після завантаження комп'ютера із захищеної від запису чистої від вірусів дискети (диску) з ОС.
4. Якщо Ви не маєте досить знань і досвіду для лікування комп'ютера, скористайтесь досвідом фахівців.

Надати повну характеристику конкретних антивірусних програм і зробити рекомендації щодо вибору з-поміж них майже неможливо. Швидкість появи нових вірусів (близько 2000 на рік) приводить до постійного оновлення антивірусного програмного забезпечення. Це означає не тільки поповнення антивірусних баз, а й удосконалення евристичних аналізаторів, зміну конфігурації програм і т. ін. Тому для одержання актуальної інформації рекомендується звертатися до фахівців, розробників і періодичних видань. Відповідну інформацію можна також знайти в мережі Інтернет (див. вставку).

Нині найбільшого поширення в Україні набули російськомовні антивірусні програми:

- поліфар Dr.Web і резидентний сторож SpIDer Guard, розроблені антивірусною лабораторією Ігоря Данилова — <http://www.drweb.ru>;



Інтернет — допомога авторам вірусів і системним адміністраторам

Інтернет відіграє свою роль як у поширенні вірусів (і навіть у процесі їх появи), так і в боротьбі проти цих «електронних інфекцій». У Мережі існують сайти, де кожний бажаючий може одержати вичерпну інформацію про те, як написати власний вірус, як обійти антивірусний захист і т. ін. Більш того, доступні початкові тексти вірусів, доданням команд до яких можна створити свій вірус.

Водночас за допомогою конференцій та спеціалізованих сайтів (наприклад, <http://www.Dshield.org>) системні адміністратори одержують оперативну інформацію про нові віруси і засоби боротьби з ними. Також в Інтернет існують безплатні антивірусні служби, де можна у режимі on-line перевірити будь-який файл з локальної машини або одержати нову версію антивірусу.

Також можна назвати приклади серверів, присвячених проблемам комп'ютерної безпеки:

<http://csrc.ncsl.nist.gov> — Центр обміну інформацією щодо комп'ютерної безпеки NIST (NIST Computer Security Resource Clearinghouse);

<http://www.first.org/first> — Форум груп з боротьби з комп'ютерними злочинами (The Forum of Incident Response and Security Teams, FIRST);

<http://www.cert.org/> — Група надзвичайного комп'ютерного реагування (Computer Emergency Response Team, CERT);

<http://www.info-war.com/> — Портал з інформаційної безпеки та інформаційної війни (InfoSec and InfoWar™ Portal);

<http://www.iss.net/> — «Системи Інтернет-безпеки» (Internet Security Systems, ISS);

<http://www.ssl.stu.neva.ru/> — Спеціалізований центр захисту інформації у Санкт-Петербурзі (Saint-Petersburg Software Security Laboratory, SSL).

- поліфар Antiviral Toolkit Pro (AVP) Євгена Касперського — <http://www.avp.ru>;
- антивірусний пакет Norton Antivirus компанії Symantec — <http://www.symantec.com>.

За прогнозами експертів, у недалекому майбутньому очікується підвищення кількості вірусів, залучення у процесі їх створення нових технологій (див. приклад) та розширення «анти-антивірусних» дій. Прикладом останнього є скандал, який відбувся у 1996 році у зв'язку з наявністю «троянського коня» у фаль-

шивому доповненні до Dr.Web, який знищував файли на дисках. Однією з причин цього є двозначне положення розробників антивірусів — за деякими оцінками, кожний вірус приносить антивірусній індустрії не менш як 15 тис. доларів доходу щорічно протягом багатьох років.



Написання вірусів — сфера впровадження нових технологій

Улітку 1992 року було випущено перший конструктор вірусного коду для IBM-сумісних комп'ютерів, який дозволяє вибрати тип вірусу, об'єкти для зараження, наявність або відсутність саморозшифрування, протидію відлагоджувачеві, до 10 ефектів, які супроводжують дії вірусу і т. ін. Конструктор навіть мав стандартний віконний інтерфейс.

У 2000 році з'явилося нове покоління вірусів, здатних до самооновлення через Інтернет.

3.4.3. Методи криптографічного захисту

Криптографічний захист (шифрування) інформації — це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Методи криптографії поділяють на дві групи — підставлення (заміни) і переставлення. Підстановний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення може використовуватись певне слово або фраза — ключ. У загальному випадку у криптографії **ключ** — це послідовність бітів, що використовуються для шифрування та розшифрування даних. Наприклад, якщо використати слово ЮРИСТ як ключ за допомогою підстановної таблиці (див. нижче), то слово ЗЛОМ буде виглядати як ГИЙІ.

А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О
					А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Ї	Й
Ю	Р	И	С	Т													

Подібний шифр дуже швидко можна розкрити, вивчивши повторюваність символів та короткі слова «і», «або», «за» і т. ін.

У разі використання перестановного алгоритму змінюються не символи, а порядок їх розміщення в повідомленні.

Залежно від доступності ключів розрізняють:

- **симетричне шифрування** — для шифрування і розшифрування використовується один ключ. Такі системи із закритим ключем реалізовані, наприклад, в архіваторах даних. Це зручно для шифрування приватної інформації, але під час передавання повідомлення по каналах зв'язку слід забезпечити таємне передавання ключа, щоб одержувач міг здійснити розшифрування. У принципі, якщо можна таємно передати ключ, то можна передати і таємну інформацію, тоді відпадає необхідність у шифруванні, а якщо такої можливості немає, шифрування даремне;

- **асиметричне** — для шифрування використовується один, **відкритий** (публічний, загальнодоступний) ключ, а для дешифрування — інший, **закритий** (секретний, приватний). Це робить непотрібним таємне передавання ключів між кореспондентами. Відкритий ключ безплідний для дешифрування, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком моделі є необхідність адміністративної роботи — ключі (і відкриті, і закриті) треба десь зберігати і час від часу оновлювати.

Сьогодні існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є стандарт шифрування даних DES (Data Encryption Standart) та алгоритм RSA, названий за першими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970-х роках. Обидва алгоритми є державними стандартами США. DES є симетричним алгоритмом, а RSA — асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.

Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення **електронних (цифрових)¹ підписів (ЦП)** — сукупностей даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала.

Цифровий підпис передбачає вставляння в повідомлення сторонньої зашифрованої інформації. При цьому, якщо не застосо-

¹ Звичайно терміни «електронний підпис» і «цифровий підпис» застосовуються як синоніми, але перший з них має ширше значення, оскільки позначає будь-який підпис в електронній формі («оцифрований» не означає «цифровий»). Отже, електронні підписи не обов'язково базуються на криптографічних методах і можуть бути створені, наприклад, за допомогою засобів біометрії (див. п. 3.4.4).

вустється додаткове шифрування, сама інформація, що передається, ніяк не захищається. Сторонньою інформацією може бути **контрольна сума** (наприклад, CRC, Cyclic Redundancy Check, циклічний надлишковий код) — значення, яке автоматичне обчислюється за певним алгоритмом і широко використовується для перевірки цілісності інформації. Вимогою до відповідного алгоритму є неможливість створення відмінних текстів з однаковою сумою.

Більш поширеним методом є створення ЦП за допомогою асиметричного шифрування. При цьому накладання підпису виконується за допомогою закритого ключа, а перевірка підпису — за допомогою відкритого (відмінність створення ЦП від шифрування інформації). Публічний ключ та додаткові відомості (ім'я відправника, серійний номер ЦП, назва уповноваженої фірми та її ЦП) передається разом з підписом. Таким чином, послати зашифроване повідомлення і перевірити підпис може будь-хто, а розшифрувати або підписати повідомлення — тільки власник відповідного секретного ключа.

Криптографічний захист може бути організований як програмно, так і з використанням апаратно-програмних і апаратних засобів. Сьогодні фактичним стандартом для електронного листування в усьому світі завдяки своїй популярності й безплатному поширенню стала програма Філіпа Циммермана «**Pretty Good Privacy**» (**PGP**). У PGP застосовується так звана модель рівної довіри — відправник знає одержувача і довіряє йому ключ шифру, звідки і пішла назва «pretty good» (у буквальному перекладі — досить гарна). Перевагами PGP є висока надійність (єдиний метод зламування — «лобова атака»), потужний механізм обробки ключів, велика швидкодія. PGP можна інтегрувати в усі популярні поштові програми.

Загалом для забезпечення належного рівня захищеності інформації потрібна **криптографічна система (криптосистема)** — сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (зокрема й такої, що визначає заходи безпеки).

Уразливість криптографічних систем пов'язана з тим, що вони базуються на задачах, які визнані умовно нерозв'язуваними — для жодної з них не знайдено ефективного розв'язання, але й не доведено, що воно не існує. Від добору ключа методом перебирання криптосистема захищена поки що недостатнім рівнем швидкодії комп'ютерів. А численність типів можливих атак на криптографічні системи («на спосіб реалізації», «на паролі», «на користувача», «на

моделі довіри» і т. ін.) підтверджує той факт, що захист є надійним і безпечним доти, доки не розпочинаються спроби його зламування. І нарешті, головним обмеженням криптосистем є те, що при одержанні повідомлення зашифрованого парним ключем, не можна взнати напевне, хто саме його відправив (див. п. 4.3.1).

Останній недолік можна виправити за допомогою засобів біометричного захисту (див. наступний пункт) та **методом двофакторної аутентифікації** «Я маю» + «Я знаю» (використовується й однофакторна аутентифікація, але вона є менш надійною). Наприклад, користувач повинен мати пластикову картку (картку з магнітною смужкою або смарт-картку) і знати PIN-код.

Отже, розвиток криптосистем і підвищення надійності цифрових підписів створює необхідні передумови для заміни паперового документообігу електронним і переходу до здійснення електронних операцій.

3.4.4. Біометричний захист інформації

Системи біометричного захисту використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною **аутентифікацією**. Його суть — визначити, чи справді індивід є тією особою, якою він або вона себе називає. Це відрізняє аутентифікацію від ідентифікації та авторизації¹. Мета **ідентифікації** — перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а **авторизація** полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи.

Біометричні системи забезпечують найбільш точну аутентифікацію, оскільки перевіряють параметри, які дуже важко або неможливо змінити або підробити. Їхні переваги очевидні, оскільки традиційні системи захисту не здатні з'ясувати, наприклад, хто саме вводить код або вставляє смарт-картку.

Слід зазначити, що біометричні технології мають один суттєвий недолік. Вони спрацьовують завдяки тому, що системі відомі унікальні, конфіденційні характеристики кожної конкретної людини. Однак прибічники біометрії стверджують, що насправді вона забезпечує вищий рівень секретності, оскільки під час аутентифікації не залучається інформація про адресу людини, домашній телефон, банківський рахунок тощо.

¹ Слід визнати, що у літературі терміни «аутентифікація» та «ідентифікація» часто застосовуються як синоніми.

Донедавна біометрія вважалась атрибутом фантастичних романів і військових систем, але сьогодні відповідні технології доросли до загального застосування і далі швидко розвиваються. З удосконаленням біометричних пристроїв можна очікувати їх застосування не тільки у промисловості, а й у приватному секторі — проведення он-лайн операцій, доступ до банкоматів і засобів роздрібної торгівлі, вхід та вихід до будинків та багато іншого.

Протягом тривалого часу здійснювались спроби вибрати різні фізичні характеристики як індивідуальний штамп, що його можна було б постійно розпізнавати з високою точністю. Результати таких спроб втілено в сучасних технологіях:

- розпізнавання відбитків пальців. Основою цієї технології, започаткованої у кримінології в XIX столітті, є сканування відбитку пальців людини і порівняння їх з тими, що були попередньо записані у систему. Засоби захоплення варіюються від стандартних сканерів до складних пристроїв, які вимірюють дрібні заряди між складками шкіри. З огляду на зрілість цієї технології за допомогою подібних пристроїв можна досягнути високої точності. Подальший розвиток технології вимагає врахування можливих змін поверхні шкіри і навіть погодних умов. Для користувачів ця технологія приваблива через її простоту і швидкість;

- розпізнавання голосу. Цей підхід використовує стандартні засоби для запису модуляцій індивідуального мовлення. Рівень точності при цьому дещо нижчий, оскільки залежить від акустичного середовища та якості пристрою аудіозапису;

- аналіз геометрії руки передбачає вимірювання фізичних характеристик руки і пальців користувача. Рівень точності ідентифікації прямо пропорційний до кількості точок у записаному зразку. Новітні пристрої дають можливість створити тривимірну карту руки користувача;

- сканування сітківки ока. Ця технологія передбачає сканування системи кровоносних судин на сітківці. Точність розпізнавання дуже висока, на рівні розпізнавання відбитків пальців;

- сканування райдужної оболонки. Основою цього підходу є порівняння унікальних рисунків райдужної оболонки ока. Сканування виконується за допомогою спеціальної камери. На сьогодні точність ідентифікації не дуже висока, але очікується її збільшення з удосконаленням технології;

- розпізнавання обличчя. Для запису тривимірної геометричної карти обличчя людини застосовується стандартна цифрова

камера. Залежно від конкретного варіанта технології рівень точності розпізнавання коливається від низького до середнього;

- розпізнавання динаміки підпису. Під час аналізу підпису, який робиться спеціальною ручкою з перетворювачем прискорення по осях X і Y, враховується не тільки написання літер, а й швидкість і ступінь натискування;

- розпізнавання стилю набирання символів на клавіатурі. Під стилем тут розуміється швидкість натискання на клавіші, ритм ударів і тиск, який здійснюється на клавіші. За даними маркетингових досліджень, користувачі довіряють більше системам розпізнавання відбитків пальців, а не стилю введення даних. Але слід зазначити, що останні будуть готові до масового впровадження значно раніше завдяки своїй дешевизні. Так, у 2001 році на ринку з'явилося біометричне програмне забезпечення для захисту мереж Windows NT — «BioPassword LogOn». Для роботи не потрібне додаткове обладнання. Єдине, що вимагається від користувача, — створити власний шаблон, 15 разів ввівши своє ім'я і пароль. Точність розпізнавання становить 98 %. Початкова вартість пакета — від 20 до 90 дол. залежно від розмірів мережі.



Реальні біометричні системи — досвід США

Проект ФБР «Інтегрована автоматизована система ідентифікації відбитків пальців (Integrated Automated Fingerprint Identification Systems, IAFIS) має на меті заміну карток з відбитками пальців на базу даних з відсканованими зображеннями та супроводжувальною текстовою інформацією, яка буде доступна агентствам забезпечення законності та правопорядку в усьому світі. IAFIS розглядається як наріжний камінь Підрозділу інформаційних послуг кримінальної юстиції (Criminal Justice Information Services Division, CJIS).

Служба імміграції та натуралізації США (U.S. Immigration and Naturalization Service) використовує засоби аналізу геометрії руки для зменшення напруги на обмежувальних переходах. Дубльовані Системи прискореного обслуговування пасажирів (INS Passenger Accelerated Service System, INSPASS) встановлюються у найбільших аеропортах США. Мандрівник, інформацію про якого вже записано, вставляє видану йому картку у блок системи, йому ставляться кілька запитань і, нарешті, йому пропонується внести руку у спеціальний зчитувач. Якщо порівняння записаних даних і щойно відсканованих відбувається успішно, особу направляють до митного інспектора, а якщо ні — до імміграційного. Типовий процес займає 15—20 с.

Описані щойно технології можна розбити на дві групи залежно від того, як у них реалізується процес «захоплення» елементів людської анатомії. Технології, які не передбачають будь-якого зіткнення з людиною, наприклад, розпізнавання голосу, більш прийнятні для користувачів, але менш надійні. Але, з огляду на широке поле застосування біометричних технологій, можна передбачити, що всі вони будуть запитані. Швидкість їх поширення залежатиме від темпів удосконалення відповідних пристроїв та програмного забезпечення і зниження їхньої вартості. Також велике значення матиме законодавча підтримка і розробка промислових стандартів.

3.5. ОРГАНІЗАЦІЯ ЗАХИСТУ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Захист інформації неможливо регламентувати через різноманітність існуючих ІС та видів інформації, що обробляється. Конкретні заходи визначаються виробничими, фінансовими та іншими можливостями підприємства (організації), обсягом конфіденційної інформації та її значущістю. Можна назвати тільки *загальні правила*:

- створення та експлуатація системи захисту інформації є складною і відповідальною справою, яку мають робити професіонали;
- не слід намагатись організувати абсолютно надійний захист — такого просто не існує. Система захисту має бути достатньою, надійною, ефективною та керованою. Ефективність захисту інформації вимірюється не витратами на її організацію, а її здатністю адекватно реагувати на всі загрози;
- заходи із захисту інформації повинні мати комплексний характер, об'єднувати різні засоби;
- систему захисту слід будувати, виходячи з того, що основну загрозу становлять співробітники підприємства (організації, установи).

Необхідність залучення кваліфікованих фахівців до організації захисту інформації диктується тим, що тільки вони можуть визначити всі загрози і знайти ефективні засоби протидії. Сьогодні захист інформації стає однією з галузей, для якої розробляються спеціальні інструментальні засоби, призначені для генерації тестів, імітації загроз, аналізу текстів програм. Створюються експертні системи для формування вимог до безпеки ІТ та оцінки рівня їх виконання.

відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою. Цей Закон доповнюють інші закони та нормативні акти, однак слід зазначити, що для ефективного захисту інформації потрібне не тільки вдосконалення правової бази, а й комплексні заходи з втілення державної політики в цій галузі в життя (див. вставку).



Боротьба з кіберзлочинністю — справа державна

Наприкінці 2000 року уряд Великобританії (<http://www.number-10.gov.uk>) повідомив про виділення 25 млн фунтів стерлінгів на створення у 2001 р. спеціального елітного поліцейського підрозділу з боротьби зі злочинністю у сфері високих технологій (National Hi-Tech Crime Unit). До підрозділу запрошені спеціально підготовлені детективи з поліції, митниці, Національного управління з розслідування карних злочинів (National Crime Squad) і Національної кримінальної поліції (NCIS — National Criminal Intelligence Service) — всього 40 осіб у Лондоні і 46 слідчих у підрозділах на місцях. Об'єктами кібер-копів є шахраї, педофіли, хакери, автори вірусів та інші шкідники. На виділені гроші також фінансується цілодобова «гаряча лінія», яка інформує про можливі атаки та інші загрози.

Федеральне бюро розслідувань США запустило у 2001 році програму попередження комп'ютерних злочинів InfraGuard, розроблену Центром захисту національної інфраструктури (National Infrastructure Protection Center, NIPC, <http://www.nipc.gov/>). Однією з цілей програми є створення захищеної від вторгнення ззовні мережі для обміну інформацією між компаніями та органами забезпечення правопорядку про здійснені атаки та надання відомостей, які можуть попередити такі зазіхання. Однак деякі експерти вважають, що контроль з боку ФБР спричиняє недоступність інформації іншим учасникам. Це зумовлює появу інших подібних програм. Так, американські комп'ютерні корпорації Microsoft, Oracle, AT&T, Intel та 15 інших компаній створили центр обміну інформацією по боротьбі з комп'ютерною злочинністю (Information Technology Information Sharing and Analysis Center).

За твердженнями експертів, з усієї кількості комп'ютерних злочинів бувають своєчасно розкриті і покарані тільки 10—17 %. У 90 % випадків виявлення злочину завдячує випадковості. Основною причиною такого становища є особливості

комп'ютерних злочинів, які ускладнюють їх виявлення та доведення:

- незначні зовнішні прояви злочину — викрадена інформація може залишитись на місці, зчитування інформації може тривати частки секунд, занесення комп'ютерного вірусу списується на недосконалість антивірусного програмного забезпечення, а втрата даних — на збій технічних засобів;

- складність точного визначення втрат та їх оцінювання у грошовому еквіваленті;

- часто розслідування комп'ютерних злочинів є дуже дорогим, що обмежує можливості його проведення. А оскільки виявлені зловмисники часто здобувають легке покарання, потерпілі не бачать сенсу витратити додаткові кошти на їх розшук;

- небажання постраждалих звертатись до правоохоронних органів, оскільки це може призвести до обнародування секретної інформації, втрати клієнтів, партнерів або акціонерів, конфліктів усередині організації. Деякі постраждалі побоюються, що у процесі розслідування будуть виявлені незаконне ведення ними операцій або інші протиправні дії. Одним з аспектів цієї проблеми є те, що потерпіла особа зазвичай сприймається громадськістю як жадібна і дурна;

- складність доведення злочинного наміру або необережності. Найчастіше злочинець не в змозі передбачити повністю наслідки своїх дій — вони залежать від багатьох суб'єктивних і об'єктивних факторів, зокрема від стану ІС, її захищеності та кількості зв'язків з іншими системами;

- високі вимоги до слідчого, який повинен мати підготовку на рівні професійного програміста або системного адміністратора. Щонайменше слідчий повинен вміти користуватись відповідним програмним забезпеченням, але критичним для нього є розуміння внутрішніх механізмів роботи систем і мереж. Останнє необхідне вже при виконанні таких звичайних слідчих дій, як обшук і збір речових доказів. Інформацію, зчитану або роздруковану з машинних носіїв, можна прийняти як доказ тільки за гарантованої неможливості її змінювання у процесі виконання цієї операції. Таку гарантію може дати використання сертифікованих програмних засобів, перевірених на відсутність незадокументованих можливостей. Але це не вирішує проблему повністю, оскільки залишається питання, хто буде контролювати застосування слідчим подібних програм — запрошені на обшук поняті навряд чи зможуть це зробити. Отже, ці питання потребують додаткових досліджень і детальної регламентації у кримінально-процесуальному

законодавстві. Як не парадоксально, допомогти правоохоронним органам можуть і хакери (див. вставку).



Роль хакерів у захисті ІС — тестування на проникнення

Тестування на проникнення є заходом, який має на меті перевірку відсутності в ІС простих шляхів обійти механізми захисту для неавторизованого користувача. Для цього можна скористатися професійними засобами тестування. Відповідні програми існують для всіх операційних систем. Їх доцільно застосовувати хоча б тому, що вони можуть стати інструментом справжньої атаки. Недоліком подібних програм є те, що вони аналізують тільки вже відомі вразливі місця.

Кращим способом атестації безпеки системи є надання можливості спеціально запрошеним хакерам зламати її без попередження адміністраторів і користувачів. Результатом має стати конфіденційний звіт з оцінкою рівня доступності інформації та рекомендаціями щодо вдосконалення системи захисту.

Цей метод використовують і виробники програм комп'ютерного захисту. Прикладом є щорічний конкурс хакерів OpenHack, який проводить журнал eWeek. Компанія-розробник пропонує грошові призи у кілька десятків тисяч доларів тим, хто за два тижні зламає систему.

Однак, і тут можна зробити зауваження. Подібний конкурс не можна вважати ідеальною перевіркою. Професійні пірати не будуть рекламувати свої здібності, а залишать їх для «власного користування». OpenHack швидше можна назвати конкурсом молодих талантів, оскільки досвід минулих змагань показав, що серед переможців є особи, надто малі, щоб водити автомобіль.

Проте залучення юних хакерів до суспільно корисної роботи може стати одним із заходів з попередження комп'ютерних злочинів і розкриття вже скоєних. Сьогодні хакерів активно залучають у спеціальні поліцейські підрозділи. Прикладом є індійська національна кібер-поліція (National Cyber Cop Committee), «співробітниками» якої стали у 2000 році 19 хакерів у віці від 14 до 19 років.



Контрольні запитання і завдання

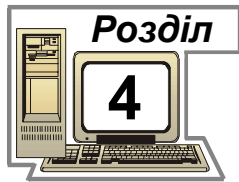
1. Обґрунтуйте визначення дії з втручання у роботу ІС або функціонування комп'ютерної мережі як злочину.
2. Назвіть основні шляхи порушення безпеки інформації.

3. Які основні види комп'ютерних злочинів?
4. Визначте відповідність між джерелами загрози для інформації та засобами її захисту.
5. Прокоментуйте такі міфи про віруси:
 - віруси можуть заражати захищені від запису диски;
 - деякі віруси абсолютно безпечні;
 - тільки піратські програми містять віруси;
 - антивірусні програми забезпечують повний захист від вірусів;
 - віруси можуть руйнувати комп'ютери;
 - вірус може вразити користувача комп'ютера;
 - вірус можна знищити тільки форматкуванням жорсткого диска.
6. Прокласифікуйте комп'ютерні віруси за відомими Вам ознаками.
7. У чому полягає відмінність між симетричними та асиметричними системами криптографії?
8. У чому полягає відмінність процесу створення цифрового підпису від шифрування інформації?
9. Які технології біометричної аутентифікації Ви знаєте?
10. Обґрунтуйте необхідність комплексного застосування засобів захисту інформації.



Література

1. Вакка Дж. Секреты безопасности в Интернет. — К.: Диалектика, 1997. — 512 с.
2. Жельников В. Криптография от папируса до компьютера. — М.: АБФ, 1996. — 336 с.
3. Коваленко М. М. Комп'ютерні віруси і захист інформації. — К.: Наук. думка, 1999. — 262 с.



СИСТЕМИ АВТОМАТИЗАЦІЇ ДІЛОВИХ ПРОЦЕСІВ ТА УПРАВЛІННЯ ДОКУМЕНТАМИ. ЕЛЕКТРОННА КОМЕРЦІЯ

4.1. СИСТЕМИ АВТОМАТИЗАЦІЇ ДІЛОВОДСТВА І ДОКУМЕНТООБІГУ

Сьогодні на ринку систем автоматизації роботи з документами представлено велику кількість продуктів з різноманітними назвами. Через чисельність і часте змішування термінів оцінити ту чи іншу систему досить важко. Головним при цьому є правильне визначення об'єкта автоматизації та функцій системи.

Об'єктом автоматизації може бути діловодство або документообіг. **Діловодство** — це діяльність зі створення документів та організації роботи з ними. Під організацією роботи з документами розуміють створення умов, що забезпечують рух, пошук і збереження документів. Рух документів в організації з моменту їх одержання або створення до завершення виконання або відправлення позначається як **документообіг**. Документообіг становить близько 15—20 % діловодства.

Діловодство і документообіг є окремими випадками більш загального поняття **управління документами**, яке, окрім них, включає ведення великих архівів документів, їх перетворення з однієї форми в іншу (наприклад, сканування і розпізнавання або публікація в Інтернет), розмежування і контроль доступу, координацію дій співробітників, а також тісну інтеграцію з офісними і прикладними програмами, що є інструментами обробки документів.

Сучасне українське діловодство здебільшого є спадком радянської системи. Залежно від виконуваних функцій розрізняють організаційно-розпорядницьке, бухгалтерське, нотаріальне, кадрове, технічне, медичне, військове та інші види діловодства. Кожний з них має свої відмітні риси, але спільним для будь-якої галузі та функції управління є організаційно-розпорядницьке (адміністративне) діловодство. Тому в разі впровадження системи автоматизації найчастіше йдеться про цей вид.

Організаційно-розпорядницькі документи такі:

- організаційні — положення, статути, інструкції, правила;

- розпорядничі — постанови, розпорядження, накази, вказівки, рішення;
- довідково-інформаційні — листи, доповідні і пояснювальні записки, протоколи, акти, огляди, звіти, стенограми, списки, переліки, реєстраційно-контрольні картки, графіки і т. ін.

Щодо системи управління розрізняють потоки вхідних (тих, що надходять), вихідних (тих, що відправляються) та внутрішніх документів.

Кожен документ у процесі свого життєвого циклу проходить певні стадії, які мають бути автоматизовані: створення, візування та узгодження, підписання та затвердження, реєстрація, розгляд, виконання, списання у справу, збереження, знищення. На етапі створення документ не має юридичної сили і є лише проектом. Після завершення підготовки, погодження, підписання, затвердження, проставлення печатки і штампів проект стає власне документом, набуває юридичної чинності і може використовуватися для доказу в суді і т. ін. Усе сказане стосується паперових документів, оскільки в національній правовій системі процедура експертизи справжності, доказу в суді, система реєстрації підписів (підпису фізичної особи на паспорті) і печаток застосовуються поки тільки до паперових документів. Можливість застосування такої процедури і відрізняє документ від простого тексту на папері чи будь-якому іншому носії.

Таким чином, необхідною умовою переходу до автоматизованого документообігу є надання правового статусу електронним документам. За відсутності правової регламентації в національному масштабі можливе використання тільки закритої (не зв'язаної із системами інших установ) корпоративної системи електронного діловодства. В Україні ця проблема вирішується з ухваленням Закону

«Про електронні документи та електронний документообіг», згідно з яким *електронний документ* — це документ, інформація в якому подана в електронній формі, що містить необхідні реквізити, зокрема електронний цифровий підпис. ЦП відрізняє електронний документ від звичайних файлів, дає змогу встановити його автентичність — підтвердити, що змістовна інформація документа не зазнала змін з моменту його підписання і документ підписаний певною особою. Отже, після накладання електронного підпису документ набуває юридичної сили. За винятком випадків, передбачених законом, електронний документ і звичайний документ на папері, які є ідентичними за змістом та реквізитами, мають однакову юридичну

силу. При цьому кожний з електронних примірників вважається оригіналом електронного документа.

За *реалізованою концепцією* розрізняють автоматизовані системи, зорієнтовані на вітчизняне і західне діловодство. Вітчизняне діловодство характеризується вертикальною спрямованістю — документ, що надходить в організацію, після реєстрації передається керівникові, який після розгляду документа накладає резолюцію із зазначенням відповідального виконавця. Далі документ надходить до відповідального виконавця, який або виконує документ, або направляє його на виконання своїм підлеглим. Після виконання документ передається у зворотному напрямку з нижнього рівня ієрархії до верхнього, де приймається звіт про виконання. На Заході звичною є горизонтальна схема — документи відразу направляються виконавцям без доповіді вищим керівникам. Ще однією важливою відмінністю нашої практики є наявність органу, що контролює виконання документа — перед відправленням документа відповідальному виконавцеві він ставиться на контроль. Таким чином, третя особа — діловод — завжди знає, у кого перебуває документ на виконанні і коли він має бути виконаний. Такі відмінності у веденні діловодства спричиняють суттєву різницю між системами західних і вітчизняних та російських розробників.

Стосовно *завдань управління документами і застосування ІТ* чіткої класифікації систем не існує. Можна навести такий загальний розподіл.

Засоби автоматизації офісної діяльності (Office Automation) — текстові редактори для підготовки і коригування документів, процесори електронних таблиць, програми генерації запитів за зразком з різних БД, мережні планувальники для призначення робочих зустрічей і нарад, засоби розробки і демонстрації презентацій, словники і системи порядкового перекладу, програми посилки і прийому факсів, електронна пошта для обміну повідомленнями і пересилання файлів. Це можуть бути окремі пакети (Word, WordPerfect, Excel, Lotus 1-2-3 тощо), інтегрований пакет програм (MS Works) або узгоджений набір пакетів (Microsoft Office або Corel Perfect Office). Для створення додатків на основі цих пакетів використовують макромови чи діалекти Basic (Word Basic, Excel Basic та ін.) або єдину мову для розширення додатків, наприклад Visual Basic for Applications для продуктів Microsoft. Для багатьох пакетів характерне використання так званих «майстрів» (Wizard), які в режимі діалогу допомагають користувачеві виконати складну процедуру.

Автоматизовані системи контролю виконання документів (АСКВД) призначені для обліку всієї документації установи, поставлення на контроль і контролю за виконанням документів (нагадування про наближення строків закінчення виконання документа, повідомлення про прострочені документи тощо). З цією метою у системах передбачається ведення журналу реєстрації і контролю або реєстраційно-контрольних карток документів. Такі системи побудовані на основі персональних СКБД і використовуються персоналом з діловодства і групами контролю.

Електронні архіви — системи автоматизації, призначені, насамперед, для фізичного збереження електронних копій документів та їх пошуку. Основою таких систем є персональна або клієнт-серверна СКБД. Документи зберігаються або у базі даних, або у файловій системі. Недоліком першого варіанта є прив'язка до конкретної СКБД і складність відновлення після збоїв, а другого — низький рівень захищеності інформації. Електронні архіви забезпечують пошук як за атрибутами, так і за змістом документів і можуть включати функції з контролю за виконанням документів.

Якщо в АСКВД реалізується традиційний облік документів із заміною паперових журналів обліку на електронні, то електронні архіви передбачають принципово новий погляд на документообіг — у системі зберігаються не тільки реєстраційні та контрольні картки, а й повний текст документа і його зображення. При цьому полегшується пошук і відновлення документа, його тиражування і розсилання, заповнення полів карток і посилення на документ (дані автоматично розпізнаються з образу документа і переносяться в картку або новий документ). Водночас такий підхід вимагає більше ресурсів (насамперед, пам'яті ЕОМ) і додаткового обладнання (сканер, лазерний принтер), система працює ефективно лише в умовах комп'ютерної мережі, її експлуатація ускладнюється, що підвищує вимоги до користувачів та обслуговуючого персоналу.



Носії інформації — проблема вибору

Паперовий (неавтоматизований) документообіг пов'язаний з багатьма проблемами: великий обсяг документів; складні процеси нагромадження і реєстрації документів; труднощі щодо контролю виконання доручень, визначення поточного місцезнаходження документів та пошуку архівних документів; залежність ефективно-

сті роботи з документом від особистих якостей співробітників; втрати документів. Однак вибір носія інформації має бути обґрунтований на підставі таких факторів:

▲ *вартість збереження інформації* — прямо пропорційна кількості документів і вартості збереження одного документа;

▲ *вартість (час) пошуку необхідної інформації* — прямо пропорційна кількості збережених документів, якщо відсутня система індексації. Остання, наприклад, у вигляді каталога, дозволяє прискорити пошук. Найбільші можливості у цьому плані має система повнотекстового пошуку, але вона можлива тільки для електронних документів;

▲ *вартість колективного використання інформації* — залежить від кількості копій документа, необхідних для колективного використання в разі одночасного доступу;

▲ *вартість (час) передавання документа від одного робочого місця до іншого*. За цією ознакою електронні документи є безперечними фаворитами.

З розвитком технологій зробити вибір все важче, оскільки пропонується використовувати «інтелектуальний папір» та «електронний папір». Вже сьогодні штрих-коди забезпечують зв'язок між папером та електронним обладнанням, яке може перевірити вид товару та його ціну. Хімічні мітки можуть допомогти в разі ідентифікації документа, а радіочастотні ідентифікатори — ще й визначити його місцезнаходження. Цифровий водяний знак у друкованому виданні може бути сприйнятий Web-камерою, а на екрані комп'ютера з'явиться знайдена в Інтернет додаткова інформація. Електронний папір, у свою чергу, матиме характеристики звичайного, але інформацію на ньому можна за бажанням оновлювати.

Системи організації групової роботи (групове забезпечення, groupware) зорієнтовані на автоматизацію роботи невеликих колективів і підтримують коректне спільне використання інформації групою користувачів. Основним призначенням цих систем є автоматизація офісної діяльності, документообігу, координації користувачів під час виконання поточних проектів і відстеження їх здійснення. В основу покладено електронну пошту, яка «знає» належність користувача до тієї чи іншої групи, структуру проекту та склад робочих груп і «вміє» розсилати повідомлення належним чином згідно з їхнім призначенням. При цьому відсутня структуризація проведення робіт — правила їх виконання у системі не визначаються. До цієї категорії відносять такі системи, як Microsoft Exchange, Lotus Notes (див. п. 8.2.3), Novell GroupWise.



Groupware — приклад застосування

Припустимо, що робоча група складається з п'яти учасників. З них три громадянина України працюють у Києві в одній фірмі на різних посадах. Завданням керівника є аналіз ситуації, розробка і коригування концепції діяльності, контроль її втілення у конкретних договорах. Юрист відповідає за правильність оформлення договорів, їх узгодження з чинними юридичними нормами. Третій учасник групи — виконавець, як і четвертий учасник, що перебуває у Львові. Вони безпосередньо укладають договори з клієнтами. Умови і тексти договорів визначаються керівником та юристом. Останній учасник групи — громадянин Великобританії — працює в Лондоні. Для нього договори, що укладаються в Україні, становлять інтерес, оскільки кожний з них передбачає замовлення обладнання у деякій міжнародній компанії, яка здійснює постачання з Великобританії. Усіх учасників групи пов'язує єдиний бізнес-процес з пошуку клієнтів, укладання договорів, їх опрацювання і відстеження виконання, постачання та багатоетапних оплат. У такій системі доречним буде ще один «учасник» — програмна система з функціями архіваріуса, секретаря та кур'єра. При цьому взаємодія учасників відбуватиметься так.

У базі даних договорів діючі особи (керівник та юрист) створюють специфічні документи, які можна назвати шаблонами або формулюваннями пунктів договорів. Дійсно, кожний пункт договору може мати альтернативне формулювання, наприклад, форс-мажор. На основі шаблонів виконавці укладають договори, будучи впевненими в їхній юридичній коректності і відповідності стратегії фірми. Ступінь автоматизації складання договорів може бути досить високою. Підготовлений документ передається спочатку юристу, а потім керівнику. Оскільки база даних договорів доступна всім учасникам, то фізично документ не переміщується, а відбувається поштове нагадування учаснику групи про необхідність завізувати або затвердити документ. У повідомленні, як правило, встановлюється посилання на договір, що спрощує навігацію у базі даних. Після укладення договору на його основі автоматично (за вимогою) створюється специфікація — документ, доступний британському учаснику групи. Для забезпечення конфіденційності його доступ до бази даних документів обмежується специфікацією. Документи можуть бути структурованими, тобто складатися з багатьох полів, наприклад, як договір та специфікація. Інші — додаток до договору — складаються з одного-двох полів, куди можна розмістити довільний текст з обґрунтуванням знижок, таблицею розрахунку собівартості товару і т. ін.

Діапазон застосувань groupware сягає від описаних договірних систем до розробки та експлуатації вузлів Інтернет, від роздрібної торгівлі за зразками до класичної канцелярії установи.

Системи автоматизації ділових процесів (САДП, системи автоматизації управління потоками робіт, workflow-системи, Workflow Management System) застосовуються, насамперед, для автоматизації документообігу і рутинних багатокрокових офісних операцій. Серед найбільш відомих розробок можна назвати системи Staffware, ActionWorkflow System, «OPTiMA-WorkFlow». Будь-яка САДП ґрунтується на комбінації таких технологій, як електронна пошта, управління проектами, робота з базами даних, об'єктно-орієнтоване програмування, CASE-технології.

Дуже часто терміни «groupware» та «workflow» використовуються як синонімічні. Однак, «groupware» є загальним терміном, який охоплює широкий спектр специфічних додатків групової роботи (календарне групове планування, спільне використання інформації, «дошки оголошень», форуми дискусій тощо). САДП є складовою цієї групи додатків. Із суто технічного погляду workflow-системи одночасно обслуговують множинну працівників і множинну задач, тоді як groupware-додатки паралельно обслуговують множинну користувачів і тільки одну задачу. Інші відмінності САДП такі:

- специфічність систем, зумовлена специфікою ділових процесів. Наприклад, на відміну від додатків календарного групового планування, які є стандартними для будь-якої організації, автоматизація ділових процесів — це технологія, яка допомагає користувачеві створювати додатки, необхідні саме йому;
- докладне визначення маршрутів, правил і ролей. Додаток колективного використання інформації стає додатком автоматизації управління потоками робіт тоді, коли визначений специфічний маршрут (наприклад, від А до В, від В до С), встановлені ролі (наприклад, А — організатор, В — юрист, С — ОПР) і зазначені певні правила («Контракт дійсний, якщо його схвалив С; якщо С його відхилив, контракт повертається до А, який вносить необхідні зміни»).

Докладніше workflow-системи розглянуто в наступному підрозділі.

Системи керування (електронними) документами (Electronic/Enterprise Document Management System) вважаються універсальними (див. раніше наведене поняття «управління документами») і мають забезпечувати:

- ведення довідника користувачів на основі організаційно-штатної структури організації;
- ведення журналів реєстрації і контролю виконання документів;

- контроль термінів виконання документів, оповіщення виконавця і діловода про наближення термінів контролю та про документи, не виконані вчасно;
- збереження документів у системі;
- підтримку шаблонів документів, складених документів, версій і підверсій, перехресних посилань між документами;
- відстеження документів поза системою, виписування документів із системи;
- пошук документів за атрибутами, повнотекстовий та нечіткий пошук;
- розробку документів, включаючи колективну розробку;
- візування, узгодження та затвердження документів;
- документообіг — усі види маршрутизації, автоматичне розсилання повідомлень, обмін повідомленнями і дорученнями усередині системи, формування реєстрів відправлення до зовнішніх організацій;
- ведення класифікаторів документів (за типом, видом тощо), довідників зовнішніх і внутрішніх організацій та ін.;
- суворе розмежування повноважень у системі, підтримку ролей, протоколювання та аудит дій користувачів;
- шифрування, цифровий підпис;
- ведення справ документів, списання документів у справу, передачу справ на збереження в архів;
- формування необхідних звітів, зокрема статистичних звітів з діловодства організації.

Системи керування документами ґрунтуються на промислових СКБД (Oracle, Informix, MS SQL Server, Sybase). Документи можуть зберігатись як у БД, так і у файловій системі. Обмін документами між користувачами здійснюється підсистемою обміну і маршрутизації документів, найчастіше роль цієї підсистеми виконують workflow-системи. Часто у складі систем присутні редактори довідників, реєстраційно-контрольних карт для задання атрибутів різних видів документів. Широко відомими прикладами таких систем є DOCS Open и Excalibur EFS.

Загальні *вимоги до системи автоматизації діловодства/документообігу* з будь-якої названої категорії такі:

- зручність і простота в адмініструванні та користуванні;
- масштабовуваність — система має підтримувати будь-яку кількість користувачів, її здатність нарощувати свою потужність має визначатись тільки потужністю відповідного апаратного забезпечення;

- розподіленість — система має підтримувати роботу з документами у територіально-розподілених організаціях, а також взаємодію з віддаленими користувачами;
- модульність — система має складатись з окремих модулів, інтегрованих між собою, що дає можливість замовникові вибирати й упроваджувати компоненти згідно зі своїми потребами;
- відкритість — система повинна мати відкриті інтерфейси для можливої доробки та інтеграції з іншими системами;
- переносимість — можливість використання на різних апаратних платформах у середовищі різного системного програмного забезпечення.

4.2. СИСТЕМИ АВТОМАТИЗАЦІЇ ДІЛОВИХ ПРОЦЕСІВ

Автоматизація завжди розглядалась як засіб підвищення ефективності управління. Але позитивного результату неможливо досягти в разі використання комп'ютерів як друкарських машинок, а ЛОМ — для тривіального обміну файлами. Водночас варто враховувати, що вигоди від автоматизованого виконання операцій (прискорення, спрощення і т. ін.) далеко не завжди компенсують необхідні витрати. Розуміння такої ситуації призвело до появи в 1990 році принципово нової концепції підвищення ефективності функціонування компаній — **бізнес-процес реінжинірингу** (Business Process Reengineering, BPR). За визначенням, BPR — це фундаментальне переосмислення і радикальне перепроєктування бізнес-процесів¹ для досягнення докорінного покращення основних показників діяльності — вартості, якості, послуг, швидкості. При цьому новітні ІТ розглядаються як інструмент реконструкції існуючих бізнес-процесів.

ІТ за своєю сутністю створюють умови для вдосконалення бізнес-процесів. Так, електронні комунікації дали змогу перебороти обмеження в розподілі та оновленні інформації, притаманні «паперовій» технології, а технології «клієнт-сервер» створили передумови для децентралізації прийняття рішень, залишивши проте практично без змін процеси комунікацій і координації. У цьому контексті особливого значення набувають workflow-системи, які

¹ Бізнес-процес (організаційно-виробничий процес) — це логічна серія взаємозв'язаних дій, яка використовує ресурси підприємства для створення або одержання в майбутньому корисного для замовника виходу, такого як продукт або послуга.

слід розглядати не як окремі додатки, а як засоби інтеграції ділових процесів підприємства.

Діловий процес («потік робіт» від англ. «workflow») — це логічно завершений набір операцій (ділових процедур), що підтримують структуру підприємства і реалізують його політику, спрямовану на досягнення поставленої мети. Ідеологія САДП ґрунтується на твердженні, що здебільшого ділові процеси мають такі характеристики:

- складаються зі скінченного набору завдань, що виконуються заданим чином;
- до їх виконання залучено численних працівників з різним ступенем відповідальності;
- вони полягають у вивченні, створенні, обробленні та передаванні інформації у різних формах (не тільки у формі документів);
- мають деяку мету, можливо, не очевидну всім учасникам.

Ділова процедура — це логічний етап ділового процесу, який необхідно реалізувати для його завершення. Наприклад, діловий процес «Обробка вхідного документа» складається з процедур реєстрації документа, видачі резолюції, постановки на контроль, виконання резолюції, контролю виконання, перевірки результатів.

Для відокремлення понять «виконання документа» і «виконання доручення» використовується термін **«робота»**, який позначає конкретне доручення, що виконується в рамках ділового процесу і складається з певних процедур. Опис роботи містить формулювання завдання, деяку інформацію у вигляді коментарів і, можливо, один чи кілька прикріплених документів, необхідних для виконання поставленого завдання. Робота складається з окремих етапів, для кожного з яких задається часовий інтервал, протягом якого він має бути завершений, і режим виконання. Очевидно, що тут поняття роботи є ширшим, ніж «документ», а поняття руху робіт ширше за «рух документів». Іншими словами, workflow за своєю суттю охоплює документообіг як окремий випадок.

Конкретні процедури виконуються за правилами. **Правило оброблення процедури** — це деяка умова, дотримання або недотримання якої викликає визначені дії. Такі правила можна поділити на правила оброблення даних і правила маршрутизації. **Правила маршрутизації** визначають сценарій реалізації ділового процесу, послідовність виконання його процедур. Прикладом різної маршрутизації одного об'єкта може бути правило розгляду вхідних документів і накладання резолюцій на них: «Документи, що належать до групи особливо важливих, розглядає і розписує керівник, а решту — його заступники, відповідно до кола питань, якими вони відають».

Залежно від *визначеності порядку виконання процедур* розрізняють жорстку і вільну маршрутизацію. Жорстка маршрутизація задається у випадку, коли порядок виконання процедур відомий заздалегідь і не залежить від результату виконання попередньої процедури. Іншими словами, завершення однієї процедури приводить до автоматичного запуску іншої (-их). Вільна маршрутизація (умовна або *ad hoc*-маршрутизація) визначається умовами, виконання або невиконання яких з'ясовується тільки після завершення попередньої ділової процедури. У цьому разі не можна сказати заздалегідь, яку процедуру буде запущено після виконання поточної, це визначає учасник ділового процесу з відповідними правами.

Залежно від *порядку проходження процедур* розрізняють послідовну і паралельну маршрутизацію. Послідовна маршрутизація передбачає виконання ділових процедур одну за іншою. Чергова процедура розпочинається тільки після завершення попередньої. Таким чином, у певний момент часу може виконуватись тільки одна процедура. За паралельної маршрутизації відбувається кілька ділових процедур одночасно. Це можливо, якщо такі процедури незалежні і їх виконання не вимагає результатів виконання інших.

Маршрути можуть бути складнішими, ніж прості послідовні чи паралельні. У деяких випадках задаються комбіновані маршрути з послідовних і паралельних елементів, а в деяких — умовні, з переходами залежно від стану тих чи інших змінних. Маршрутизація також може передбачати **контроль виконання**. Це поняття охоплює контроль доставки завдання, контроль ознайомлення із завданням, власне контроль виконання, моніторинг завдання, повідомлення про порушення термінів виконання, історію виконання завдань, контроль якості виконання.

Ще одним важливим компонентом опису ділового процесу є розподіл ролей між його учасниками. **Роль** визначає набір дій у рамках ділового процесу, який учасник має виконати для досягнення мети процесу. Під час визначення ролі закріплюються місце її розташування, функції, права доступу. Учасник може бути членом певної робочої групи, тоді на нього поширюються всі характеристики цієї групи. Існують *три типи ролей*:

- ініціатор роботи — це учасник ділового процесу, який формулює зміст роботи, описує її, запускає на виконання, здійснює контроль і приймає результати;
- виконавець роботи — це учасник ділового процесу, який виконує роботу, а також звітує і несе відповідальність за її результати. За наявності відповідних прав виконавець може створювати

нову роботу як частину тієї, що доручена йому, і призначати нових виконавців. Таким чином він сам стає ініціатором робіт, — створюється традиційна ієрархічна структура управління з кількома рівнями підпорядкованості;

- спостерігач — це учасник ділового процесу, який відстежує виконання роботи.

Формалізований опис ділового процесу та ділових процедур, що входять до його складу, правил їх виконання і ролей учасників процесу називають *моделлю процесу*. Модель процесу є результатом ретельного обстеження та аналізу об'єкта автоматизації на предмет оптимізації його діяльності. Із цією метою застосовуються традиційні методології системного аналізу, такі як SADT (Structured Analysis and Design Technique) чи DFD (Data Flow Diagram). Існують і спеціалізовані методології, що підтримуються окремими САДП, наприклад Action Workflow в Action Workflow System.

Модель ділового процесу вводиться у САДП під час впровадження системи за допомогою спеціалізованих формальних мов (скриптів) або графічних засобів (рис. 4.1). Одержана **карта ділового процесу** зберігається в базі даних. Зафіксована модель може змінюватись у процесі використання системи. Ця процедура не потребує перепрограмування, її виконує безпосередньо користувач.

У процесі використання САДП керівник або його секретар оформляє розпорядження у вигляді роботи, для якої описуються строки її початку, завершення та інші характеристики. Якщо виконання роботи вимагає ознайомлення з тим чи іншим документом, представленим в електронній формі, він може бути прикріплений до опису роботи для передавання користувачеві.

САДП дає змогу значно підвищити рівень обґрунтованості рішень завдяки своєчасному інформуванню керівництва про стан справ.

Таким чином, функціонування САДП дозволяє створити і підтримувати чітку технологію життєдіяльності всього апарата управління. Воно сприяє належній організації робіт, удосконалює зворотні інформаційні зв'язки, зміцнює трудову дисципліну і підвищує організаційну культуру. Поєднання технологій workflow з Web-технологіями дає змогу розширити комунікації та координацію у середовищі розподіленого прийняття рішень за межі окремої установи у рамках систем електронної комерції та віртуальних підприємств.

4.3. СУТНІСТЬ, СИСТЕМИ ТА УЧАСНИКИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

4.3.1. Поняття та учасники електронної комерції

Термін «електронна комерція» (ЕК) виник наприкінці 1950-х — на початку 1960-х років, практично відразу після появи ЕОМ. Найчастіше він позначає придбання чи продаж товару за допомогою електронних носіїв або через комп'ютерну мережу, зокрема Інтернет. Але сьогодні визначення дещо змінилось. **Електронна комерція** — це будь-яка форма бізнес-процесу, будь-який вид операцій, під час виконання яких взаємодія між суб'єктами відбувається електронним способом замість фізичного обміну або безпосереднього фізичного контакту. Крім продажу товарів, таке визначення охоплює маркетинг, фінансовий аналіз, інвестиційну діяльність, банківські послуги, страхування, консалтинг, представницькі функції, пошук співробітників, підтримку партнерських стосунків тощо. Для того щоб відбити таке розуміння, поряд з терміном ЕК використовується термін **електронний бізнес (e-business)**.

Основними учасниками системи ЕК є покупець (клієнт), підприємство торгівлі (торговець, продавець), банк, процесинговий центр, оператор, центр сертифікації. Спільним для всіх учасників системи ЕК є підімкнення до мережі, яка пов'язує їх між собою.

Ролі перших трьох учасників у системі очевидні. Покупець «входить» до електронного магазину за допомогою стандартного Web-броузера, переглядає перелік представлених товарів (варіант здійснення операції залежить від пропонованого способу навігації) і вибирає ті, які він бажає купити, — формує «кошик». Після цього йому надається форма замовлення зі списком обраних то-

варів, їх цінами та підсумковою вартістю. У деяких магазинах можливе інтерактивне обговорення та узгодження цін. Заповнена форма замовлення надсилається торговцю. Торговець, у свою чергу, зв'язується з банком клієнта, який має засвідчити платоспроможність покупця. Після одержання відповідного підтвердження торговець підтверджує замовлення, передає товар (або надає послуги) і одержує платіж.

Як і створення звичайного магазину, розробка його електронного варіанта є складним завданням, для виконання якого може залучатись стороння організація, яка здійснює функції оператора:

- надає торговцю програмні засоби для введення, модифікації та адміністрування інформації про товари і послуги, а також статус та обсяги замовлень;
- приймає від торговця дані, які становлять вміст електронних каталогів;
- цілодобово підтримує діяльність електронного магазину і надає торгові, платіжні, криптографічні та адміністративні послуги;
- забезпечує безпечний зв'язок між покупцем, фінансовою установою та торговцем під час здійснення покупки та її оплати.

Процесинговий центр — спеціалізований інформаційно-обчислювальний центр, який виконує функції збирання, оброблення, зберігання та передавання інформації між учасниками платіжної системи.

Оплата товарів у системі ЕК, як і в разі використання пластової картки у звичайному магазині, може здійснюватись із залученням банків. Кількість фінансових установ, що залучаються у процесі виконання платіжних операцій, та їхній склад залежать від організації платіжної системи, фінансових інструментів, що використовуються (більш докладний опис див. у п. 4.3.3), та від осіб покупця і торговця (наприклад, вони можуть бути клієнтами одного банку).

Уведення до системи ЕК такого учасника, як центр сертифікації, пов'язано з нагальною необхідністю забезпечення захисту інформації, що передається між усіма учасниками. Адекватний захист можна організувати застосуванням криптографічних засобів (див. підрозд. 3.4).

Одним із завдань організації системи криптографічного захисту є забезпечення правильної ідентифікації власника відкритого ключа. Часто такі ключі зберігаються на спеціалізованих серверах, де вони вільно доступні всім бажаючим, що робить можливою атаку на криптосистему типу «посередник» — зловмисник розміщує на сервері фальшивий ключ від імені потенційного адресата, а згодом

перехоплює повідомлення, що передається, і розшифровує його за допомогою власного закритого ключа. Проблема знімається, коли власник відкритого ключа вручає його своєму кореспондентові прямо в руки, але зрозуміло, що цей спосіб не прийнятний для систем ЕК, учасники яких не вступають у безпосередній контакт. Тому єдиним прийнятним способом є сертифікація.

Цифровий сертифікат — це інформація, яка включається до публічного ключа певної особи і допомагає іншим пересвідчитись, що цей ключ має силу і є справжнім. Цифровий сертифікат містить публічний ключ, сертифікуючу (розпізнавальну) інформацію, один або кілька цифрових підписів. Цифровий підпис у цьому разі не засвідчує сертифікат в цілому, а тільки підтверджує, що сертифікуючу інформацію було перевірено деякою особою або установою — центром сертифікації.

Центри сертифікації існують у *двох формах*. **Довідкові сервери** (directory servers, інша назва — сертифікаційні сервери, сервери ключів) — це бази даних, які надають користувачам можливість вносити та одержувати цифрові сертифікати. Сервер ключів може надавати також деяку адміністративну допомогу. Наприклад, сервер ключів PGP (PGP Keyserver) дозволяє записувати тільки ті ключі, що відповідають певним вимогам до сертифікатів.

Інфраструктури публічних ключів (Public Key Infrastructures), крім послуг зберігання сертифікатів, надають сервіси і протоколи управління публічними ключами — випуску, анулювання та надання довіреності. Основними компонентами інфраструктури публічних ключів є адміністрація сертифікації (Certification Authority, CA) та адміністрація реєстрації (Registration Authority). **Адміністрація сертифікації** — це програмна система, яка створює сертифікати і накладає на них свій цифровий підпис. За допомогою відкритого ключа CA будь-хто може перевірити цифровий підпис, а отже, цілісність сертифіката. **Адміністрація реєстрації** — це люди, які за допомогою відповідних засобів підтримують реєстрацію користувачів і виконують функції з адміністрування. Головне завдання адміністрації реєстрації — перевірити, чи належить публічний ключ особі, яка на це претендує. Таким чином, функціонування інфраструктури публічних ключів можна порівняти з роботою паспортного відділу.

Криптографія з відкритими ключами забезпечує захист даних, що передаються, але не приховує сам факт передачі і не може завадити визначенню учасників операції. Тому у системах ЕК шифрування доповнюється технологією «**сліпого підпису**». Її суть полягає в тому, що посередник («цифровий банк» або «цифровий

нотаріус») може завірити факт надходження певного повідомлення від певної особи у певний момент часу, не одержуючи доступу до змісту цього повідомлення. При цьому технологічно гарантується анонімність платника, але він може ідентифікувати себе сам і довести факт здійснення оплати. Інформація про особу одержувача платежу залишається відкритою.



Електронна комерція — ризики

Порушення приватності — велика кількість Web-сайтів запитує персональну інформацію для надання доступу, завершення операції або в маркетингових цілях. Відомості про Вас також можуть передаватися іншим організаціям. По суті, існує ризик неправомірного використання цих даних.

Фінансове шахрайство — дані про кредитні картки повинні захищатись від несанкціонованого доступу під час передавання та протягом їх зберігання на сервері одержувача як від хакерів, так і від недобросовісних службовців.

Нечесні або безвідповідальні продавці. Легкість створення Web-сайтів дає можливість поставити пастку — відкрити фіктивний електронний магазин (можливо, від імені особи з гарною репутацією), і одержувати оплату за неіснуючий товар. Можливі також неправильний опис товарів і невиконання умов поставки.

З урахуванням сказаного, е-покупцю слід звертати увагу на:

▲ *рівень захищеності інформації. Не слід вважати, що Вам за замовчуванням пропонується найкращий захист. Ви самі повинні оцінювати, яку інформацію про Вас збирають і як її можуть використати. Рекомендується віддавати перевагу заходам захисту інформації, які відповідають прийнятим стандартам;*

▲ *доступність інформації про учасника ЕК — місце його фізичного розташування, контактні телефони, інші реквізити, його репутація;*

▲ *повноту інформації про пропозицію (вид товару або послуги, його характеристики, ціни з урахуванням вартості доставки та сум податків) та про умови здійснення операції (термін поставки, спосіб оплати, гарантійні умови).*

4.3.2. Класифікація систем електронної комерції

Для класифікації систем електронної комерції можуть застосовуватись різні підходи. Так, залежно від *об'єкта купівлі-продажу* розрізняють торгівлю інформацією і торгівлю товарами. Загалом, до окремої категорії, крім інформації, можна віднести й інші товари, що можуть бути представлені в електронній формі — програмне забезпечення, відеопродукція, аудіозаписи,

комп'ютерні ігри тощо. За аналогією з прийнятим протиставленням технічного і програмного забезпечення (англомовні терміни — «hardware» і «software») подібні товари називають «м'якими», а решту (речові товари) — «жорсткими». Визначальною особливістю торгівлі «м'якими» товарами є те, що повний цикл комерційної операції, включаючи доставляння, можна здійснити через одну і ту саму мережу.

Більш значущими для класифікації є *типи суб'єктів*, які взаємодіють електронним способом. У процесі визначення учасників системи ЕК у попередньому пункті було прийняте припущення, що клієнтом є фізична особа, яка купує товари в електронному магазині. Отже, розглядався роздрібний сектор ЕК. На відміну від нього, у секторі «бізнес—бізнес» відбувається електронна взаємодія бізнес-організацій, наприклад, взаємодія постачальників матеріалів, виробника товару, дистриб'юторів і дилерів.

Участь у системах електронної комерції фінансових установ дає змогу виділити фінансовий сектор ЕК. Сьогодні банки вибирають один з трьох способів присутності в Мережі:

- присутність в інформаційних і маркетингових цілях — свої Web-сторінки має більшість сучасних банків;

- **Інтернет-банкінг** — використання Інтернет для надання звичайних послуг — віддалене управління рахунком (перевірка стану рахунка, платіжні операції, купівля-продаж валюти тощо), надання клієнтові інформаційної підтримки і супутніх послуг. Традиційно ці послуги надаються за телефоном, за допомогою повнофункціональних банкоматів, віддаленого модемного доступу і т. ін. Крім перерахованих вище послуг юридичним особам (у рамках системи «Клієнт—Банк») і фізичним особам (звідси термін — «home banking», домашній банкінг), до цієї категорії можна віднести віртуальних інкасаторів — системи розрахунків між банками;

- перенесення в мережне середовище таких інструментів, як чеки і платіжні картки, а також експерименти зі специфічними мережними розрахунковими і платіжними засобами (див. п. 4.3.3).

Крім банків і торговельних закладів, свої послуги в Інтернет пропонують й інвестиційні посередники. **Інтернет-брокерідж** охоплює послуги з купівлі-продажу цінних паперів і валюти в реальному часі через Мережу. В Україні подібні послуги поки що не надаються.

Більш узагальнено в ЕК виділяють категорії, основними (найпоширенішими) серед яких є такі:

- «**бізнес—бізнес**» (Business-to-Business, B2B),

- «**бізнес—споживач**» (Business-to-Customer, B2C).

Ця класифікація відбиває не тільки і не стільки тип учасників ЕК, як спосіб їх взаємодії. У системах В2В взаємодія бізнес-процесів цілком автоматизована. Іншими словами, обмін даними між системами не вимагає виконання ручних операцій — з ІС одного учасника дані без перешкод надходять через мережу до ІС іншого учасника. Така «безшовна» інтеграція стає можливою завдяки дотриманню єдиного стандарту повідомлень, що передаються (наприклад, стандарту UN/EDIFACT). Іншою особливістю систем В2В є рівноцінність усіх учасників, яких у системі може бути довільна кількість.

На відміну від В2В у системах «бізнес—споживач» передбачається тільки два учасники, при цьому обидва вони можуть бути бізнес-організаціями. Відмінність між системами полягає в тому, що хоча б в одній з організацій ІС не пов'язана напряму із зовнішніми системами (з Інтернет). Менеджер одержує (наприклад, електронною поштою) або сам вибирає (наприклад, у вікні броузера) потрібну йому інформацію від зовнішньої організації і вводить дані до власної бази. При цьому він виступає в ролі споживача. Якщо такий користувач є приватною особою, це буде випадок роздрібною торгівлі. До категорії В2С відносять і системи ЕК, в яких обидві організації взаємодіють через ручні операції.

Нові тенденції в електронній комерції пов'язані з появою нових абревіатур — В2G, G2C, C2G, G2G (x2G). Вони позначають нові сфери бізнесу, в які так чи інакше залучаються державні установи (Government). Їх розглянуто в підрозд. 4.4.

Зауважимо, що системи ЕК в цілому розвиваються двома шляхами. Перший шлях передбачає перехід до електронних операцій як розширення традиційного бізнесу. При цьому, строго кажучи, присутність в Мережі в рекламних цілях (створення Web-сторінки з метою інформування потенційних клієнтів або контрагентів) не означає участь в ЕК. Другий шлях передбачає переведення всієї діяльності у віртуальний режим. Уже сьогодні деякі компанії (торговельні організації, комерційні банки) обмежуються віртуальним бізнесом. Але будь-який електронний магазин повинен мати за собою і реальні структурні підрозділи — склад, відділ доставки та ін.

4.3.3. Платежі через Інтернет

Завершальним етапом процесу купівлі-продажу є оплата товару. У найпростішому випадку оплата в ЕК, за аналогією з покупками за каталогом, здійснюється за допомогою такого «архаїчного» засобу, як поштовий переказ. Сьогодні в Україні цей спосіб використовується

найбільш часто, хоча він неоперативний і незручний. Спосіб, який можна визнати адекватним вимогам електронного бізнесу, передбачає виконання *всіх!* необхідних операцій через персональний комп'ютер.

Існуючі засоби розрахунків в Інтернет можна поділити на кілька категорій.

Першу категорію становлять так звані сурогатні засоби — цифрові купони та жетони. Клієнт купує за готівку або за безготівковим розрахунком у банку певну унікальну послідовність символів, для якої банк гарантує нетривіальність алгоритму генерування, наприклад, «NetCash US\$ 0.05 B362646R725776X». Продавець приймає цю послідовність символів як оплату, а згодом передає до банку в обмін на ту ж грошову суму за відрхуванням комісійних. Правовий статус подібних операцій залишається розпливчастим, як і статус емітентів подібних засобів.

В Україні набув поширення такий вид сурогатних платіжних засобів, як «Інтернет-картки» (віртуальні картки). Віртуальна пластикова картка подібна до звичайної — клієнтові відкривається цільовий картковий рахунок, його картці присвоюється номер відповідно до стандартів платіжної системи (наприклад, VISA), проте картка у звичайному розумінні не видається, що означає меншу вартість її відкриття та обслуговування.

Більш поширеним у світі є *другий напрямок* — використання в ЕК таких традиційних платіжно-розрахункових засобів, як чеки та банківські пластикові картки. Використання різних типів карток, по суті, аналогічне, хоча смарт-картки мають більші можливості — за допомогою мікросхеми, розміщеної у картці, виконуються всі необхідні обчислення.

Платіжні системи на основі пластикових карток також відрізняються за рівнем безпеки операцій та необхідним програмним забезпеченням. Якщо клієнт передає відомості про кредитну картку безпосередньо продавцеві, то він тим самим покладається на порядність останнього. При цьому шифрування забезпечує захист від перехоплення інформації, але не гарантує, що вона надійде саме до продавця (а не до того, хто видає себе за продавця). Інший підхід започаткувала компанія CyberCash, яка пропонує спеціальне програмне забезпечення, призначене тільки для організації безпечного передавання інформації про кредитну картку, — «електронний гаманець». Реальні розрахунки при цьому виконуються процесинговими компаніями. Недоліки цього підходу такі:

- необхідність перевірки кредитоспроможності клієнта та авторизації картки, що підвищує витрати на проведення операцій, а

отже, цей спосіб є непідходящим для так званих мікроплатежів — платежів на невеликі суми;

- відсутність анонімності;
- обмежена кількість магазинів, які приймають кредитні картки (з часом цей недолік втрачає силу);
- неприйнятність цього способу для клієнта, який не має кредитної картки і не планує активно нею користуватись; до того ж у значної кількості людей зберігається психологічний бар'єр щодо передавання даних картки по Мережі.

На користь електронних гаманців свідчить існування стандартів їх застосування, найбільш відомий серед яких стандарт SET. SET дає можливість виконувати авторизацію за допомогою цифрових підписів і водночас захищає покупців, забезпечуючи механізм передавання номера картки для перевірки безпосередньо емітентові, минаючи проміжні ланки.

Якщо платіжні системи з використанням платіжних карток найчастіше є кредитними¹, то системи застосування електронних еквівалентів паперових чеків є дебетовими — під час відкриття рахунка клієнтові видається електронний документ, який містить його ім'я, назву фінансової структури, номер рахунка, ім'я (назву) одержувача платежу та суму. Основна частина інформації не кодується. Електронний чек повинен мати електронний підпис власника рахунка, а перед його оплатою він підписується й одержувачем платежу. Розрахунки електронними чеками стають невід'ємною частиною послуг домашнього банківського обслуговування, що пропонуються банками всього світу, хоча в таких системах поки не виключена можливість виписування чека без забезпечення.

Нарешті, *третю категорію платіжних засобів* складають «електронні гроші» («цифрові гроші», «цифрова готівка») — числа або послідовності символів, які є грошами і можуть використовуватись як такі. Створення електронних грошей вимагає вирішення суперечливості — з одного боку, гроші є штучними знаками з унікальною нумерацією і реалізуються зі специфічних матеріалів, а з іншого — послідовність символів є інформацією, що її можна скопіювати, так що буде неможливо відрізнити оригінал від копії. Вирішенням проблеми є поєднання інформації з апаратно-програмним комплексом (спосіб фізичної прив'язки), наприклад, з мікропроцесорною карт-

¹ Кредитні картки, на відміну від дебетових, дають тримачу можливість одержати кредит під час купівлі товарів чи оплаті послуг (згідно з умовами договору між клієнтом і банком сума платежу може перевищувати суму залишку коштів на рахунку). Клієнт повинен повернути кредит до визначеного терміну.

кою (Mondex), або із суто програмними засобами захисту (Digicash, Netcash, CyberCoin) — спосіб логічної прив'язки.

В основу технології цифрових грошей покладено методи криптографічного захисту з відкритими ключами та сліпого підпису. Емітент застосовує кілька пар ключів: одна з них аутентифікує його, а інші — певні номінали цифрових валют. Цифрові гроші, куплені в емітента, при оплаті передаються продавцеві, який, у свою чергу пересилає їх у банк для перевірки та погашення¹. Банк також стежить за тим, щоб кожна «монета» використовувалась клієнтом тільки один раз.

У принципі емітентом цифрових грошей може виступати як банк, так і продавець або посередник. Проблема полягає в тому, що поки не реалізовано механізми конвертування цифрових валют — цифрові гроші приймаються лише їхніми емітентами. Також поки що не передбачається конвертування електронних грошей в реальні, але їх приймає все більша кількість електронних магазинів.

Перевагою систем оплати за допомогою цифрових грошей є їх підхожість для мікроплатежів та анонімність платежів, а недоліками — необхідність попередньої купівлі купюр і неможливість одержання кредиту (системи цифрової готівки є дебетовими за своєю сутністю).

Системи електронної готівки вважають конкурентом платіжним системам на основі стандарту SET. Важливим аспектом під час вибору технології є правова неврегульованість систем розрахунків в Інтернет. Для України не менш значущими факторами є неплатоспроможність більшої частини населення, відсутність широкого доступу до Інтернет та безграмотність щодо нових технологій.

4.4. ДЕРЖАВА ЯК УЧАСНИК ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Можна визначити три взаємозв'язані напрями використання ЕК у роботі державних органів — участь в електронній торгівлі (B2G), електронна взаємодія з громадянами (G2C, C2G) і впровадження нових форм організації своєї діяльності (G2G, створення віртуальних підприємств, див. підрозд. 4.5).

Системи «*бізнес—уряд*» (Business-Government, B2G) створюються у першу чергу для укладання договорів і оформлення по-

¹ Насправді цифрові «монети» потрібного номіналу формуються за допомогою спеціального програмного забезпечення — електронного гаманця — самим платником, вони захищаються його закритим ключем і відкритим ключем банку, а далі передаються до банку. Після виконання необхідних перевірок і зменшення залишку на рахунку клієнта банк завіряє «монету» і надсилає її до електронного гаманця клієнта. Процес оплати здійснюється автоматично після того, як покупець вибрав потрібний товар і дав згоду на його оплату.

ставок матеріалів та обладнання. При цьому держава користується тими самими *перевагами ЕК*, що й решта замовників: глобальний вибір, персоналізація та підвищення якості послуг, швидке одержання товарів за потенційно нижчими цінами. Останнє можна вважати вирішальним фактором, оскільки йдеться про економію коштів платників податків на утримання і фінансування діяльності держапарату. Істотним фактором є і те, що електронна комерція може стати інструментом подолання бюрократії та хабарництва — будь-який претендент на одержання контракту може ознайомитись на відповідному сайті з вимогами, які він має задовольнити, і подати свої пропозиції у відповідь.



Державний сектор електронної комерції — досвід США

Обсяг ринку урядових інформаційних і товарних операцій у США оцінюється експертами на суму від 3 до 50 трильйонів доларів. Тільки на закупівлі необхідних товарів уряд витрачає більше 225 млрд дол. щорічно, з яких 40 млрд припадає на продукцію дрібного і середнього бізнесу — від скріпок до продуктів харчування.

За даними дослідження аналітичної компанії GartnerGroup витрати федеральних служб, служб штатів і місцевих органів влади через систему електронної комерції до 2005 року зростуть до 6,2 млрд дол. щорічно, а витрати на розвиток ринкового сегменту G2C — до 2,2 млрд дол.

У системі ЕК держава може виступати не тільки покупцем, а й постачальником. Із цього погляду головним завданням є забезпечення вільного доступу громадян до всієї необхідної державної інформації у рамках системи «**уряд—громадяни**» (Government-to-Citizens, G2C). Її доповнює система «**громадяни—уряд**» (Citizens-to-Government, C2G), в якій ініціатива проведення тієї чи іншої операції відходить від громадянина.



Держава в ролі постачальника. Цікавий приклад — компанія Unicor

Unicor — це ринкова марка американської державної Федеральної тюремної промислової корпорації, заснованої 1934 року. Її основною задачею є навчання та працевлаштування ув'язнених. Побічний продукт діяльності компанії — товари і послуги, вироблені в'язнями: офісні меблі, військова форма, електронне устаткування, захисні окуляри, послуги з уведення даних та оброблення пошти. Unicor перебуває на самозабезпеченні і щорічно здійснює до 250 000 операцій. У середньому одна операція обходилась компанії в 77 доларів. Сайт Unicor.gov — це електронний магазин, через

який ця державна організація реалізує свої товари і послуги. Результатом його впровадження стало зниження собівартості кожної операції вдвічі. Отже, можна підрахувати сумарну щорічну економію: $250\,000 \times 77/2$. Результат — 9,625 млн дол.!

Поділ на зазначені системи є абсолютно умовним, оскільки всі операції здійснюються через єдиний Web-портал. Для громадян такий портал дає можливість цілодобово сім днів на тиждень у режимі реального часу:

- замовляти комунальні та інші послуги. Запити автоматично передаються до відповідних департаментів (відділів). І керівники служб, і громадяни можуть відстежувати стан виконання замовлення, а перші — й впливати на процес його розгляду і виконання;
- переглядати рахунки за комунальні та інші послуги, перевіряти та оплачувати їх, оплачені квитанції автоматично нагромаджуються і зберігаються на сервері;
- сплачувати податки, збори, штрафи;
- робити внески;
- купувати квитки;
- переглядати плани роботи та протоколи нарад державних органів, ознайомлюватись з проектами та ініціативами (можливо, представленими у вигляді презентацій) і брати участь в їх обговоренні;
- переглядати персональну інформацію про державних службовців (відомості, що не є приватними, — біографія, особисті або офіційні заяви, контактна інформація тощо);
- ознайомлюватись з новинами життя міста, регіону або держави, з календарем майбутніх подій;
- переглядати закони, законопроекти, нормативні акти, муніципальні постанови;
- ознайомлюватись із результатами проведення виборів, референдумів тощо;
- вивчати звіти про роботу органів державної влади та про реалізацію окремих проектів;
- реєструвати скарги та ставити запитання. Такі можливості є додатковим засобом боротьби з корупцією. Скажімо, уряд Пакистану закликає громадян повідомляти анонімно про випадки хабарництва політиків, чиновників і бізнесменів через Web-сайт Національного бюро звітності (National Accountability Bureau);
- переглядати доступні робочі вакансії;

- ознайомлюватись зі звітами щодо дорожніх і транспортних пригод;
- реєструвати об'єкти, що підлягають обліку, наприклад засоби автотранспорту;
- робити запити на одержання або продовження терміну дії дозволів і ліцензій, виконувати відповідні платежі й одержувати необхідні документи;
- перевіряти списки виданих ліцензій;
- підписуватись до списків розсилки та одержувати електронною поштою рахунки, строк оплати яких настав або пройшов, з гіперпосиланнями до процедур їх оплати; попередження про тимчасову недоступність окремих послуг; анонси нових послуг на сайті; інші повідомлення згідно з вибраними користувачем налаштуваннями.

У правоохоронних органах усього світу добре зарекомендувала себе практика прийому повідомлень від громадян через електронну пошту та оголошення розшуку через спеціалізовані Web-сайти, на яких розміщуються записи та фотороботи злочинців, описи невпізнаних трупів, осіб, які пропали безвісти, а також орієнтировки щодо злочинів, фотографії та описи предметів антикваріату, що розшукуються, тощо. Користувач може подивитись архів фотографій, заповнити форму заяви, якщо він упізнав злочинця, повідомити про злочин, який готується, одержати рекомендації щодо забезпечення безпеки («56 способів захистити дитину від злочину», «Be e-wise» — «Будь е-досвідченим» та ін.). Існують і міжнародні проекти такого роду (див., наприклад, сайт Інтерполу <http://www.interpol.int/> або сайт з розшуку педофілів <http://www.pedowatch.org/>).

Адміністрування будь-якого Web-сайту дає змогу державним службовцям аналізувати звернення громадян і дії, що вони їх виконують, відвідуючи сайт.

Фахівці прогнозують, що незабаром цей список продовжить дистанційне навчання з предметів загальноосвітнього курсу, реєстрація шлюбів, голосування. Останнє може змінити саму природу державної влади. Наприклад, можна уявити прийняття важливих законів шляхом загального таємного волевиявлення в режимі реального часу на урядовому сайті або автоматичне подання законопроекту на розгляд законотворців (включення розгляду певної проблеми до порядку денного) після того, як за це проголосувала певна кількість виборців. Поява таких процедур може призвести до переростання концепції електрон-

ного уряду (е-уряду) в концепцію електронної демократії (е-демократії).



Е-уряд — реальність чи метафора?

Донедавна словосполучення «електронний уряд» сприймалось як метафора, що позначає інформаційну взаємодію органів державної влади і суспільства з використанням інформаційно-комунікаційних технологій. Однак, розвиток технологій у галузі штучного інтелекту дає підстави думати, що фантастичні романи не такі вже й нереальні. Так, у 2000 році в США з'явився перший у світі віртуальний кандидат у президенти країни — 55-річна випускниця Оксфорда Джекі Страйк (<http://www.jakie-strike.com/>). У деякому сенсі це ідеальний кандидат — завжди здоровий і доступний для виборців, непідкупний і з бездоганною репутацією. Той факт, що Джекі Страйк є колективним твором програмістів, публіцистів і відвідувачів сайту, підтверджує не тільки те, що реальним кандидатам можна не побоюватись суперництва, а й можливість зміни форм державного управління в майбутньому.

А поки можна говорити про такі *переваги* від упровадження систем ЕК у роботу державних органів:

- зменшення витрат на операції і підвищення ефективності їх проведення та обліку;
- більша відкритість і прозорість органів державної влади;
- своєчасний та зручний доступ громадян до послуг державних установ і необхідної інформації;
- розширення і підвищення ефективності внутрішніх та зовнішніх комунікацій;
- прискорення та поліпшення реагування на запити громадян;
- виключення необхідності для громадян проходити кілька адміністративних рівнів під час розв'язання своїх питань;
- зменшення штатів і спрямування їх до більш творчих задач;
- перехід до модернізованого безпаперового документообігу;
- своєчасне одержання платежів від населення.

Такі можливості особливо корисні для осіб, яким важко з тих чи інших причин звернутись до державних установ у приймальний час (зокрема, таких, що працюють) і громадян, які тимчасово виїхали з місця постійного проживання.

Найбільш суттєвою хибою подібних проектів (і реалізованих, і тих, що тільки розробляються) є те, що їх втілення у життя збільшить уже існуючий **інформаційний розрив у суспільстві** — вони торкаються лише тих громадян, які мають доступ до комп'ютера, підімкненого до Інтернет. Тому систе-

ми ЕК мають упроваджуватись із забезпеченням рівних можливостей з доступу до інформаційних ресурсів, що передбачає ліквідацію комп'ютерної неграмотності, роз'яснювальну роботу, надання пільгового доступу до Мережі. Останнє можна забезпечити організацією муніципальних Інтернет-центрів, які надаватимуть безкоштовний доступ до регламентованих ресурсів. Подібні центри можуть створюватись на базі шкіл або публічних бібліотек. Безумовно, подібні заходи повинні бути складовими продуманої державної політики, в якій передбачатимуться підходи до розв'язання фінансових, соціальних, юридичних та інших питань.

Цілий ряд проблем виникає і при організації державного Web-порталу на основі **ASP** (Application Service Providing) — перспективної технології спільного використання багатьма користувачами програмного забезпечення, встановленого на віддаленому Web-сервері. Сутність ASP полягає у розробці програмної заготовки (програмного додатка, який користується попитом) і здавання її в оренду. На основі цієї заготовки орендатор легко може створити власний проект. Будь-яке ASP-рішення складається з фронт-офісу — частини, яку бачать і з якою працюють відвідувачі, та бек-офісу — системи адміністрування, доступної тільки користувачеві ASP-рішення (орендатору).

На ринок ASP-рішень виходять як спеціалізовані компанії, так і диверсифіковані корпорації. Вони мають пропозиції і для державних установ. Основною перевагою ASP-рішень є їхня низька вартість — плата за користування ASP-рішенням і за послуги підімкнення до Інтернет замінює інвестиції в технічне забезпечення, а також витрати на розробку, адміністрування, підтримку і модернізацію програмного забезпечення. Водночас при виборі ASP-провайдера особливої уваги потребують юридичні документи, які регулюватимуть відносини між розробником і орендатором, зокрема функціональні можливості ASP-рішення та супутніх послуг, його характеристики, відповідальність сторін, ситуації, які можуть виникнути у процесі користування ASP-рішенням. Так, серйозні ASP-розробники, коли йдеться про разовий платіж за користування ASP-рішенням, передають право власності на нього з можливістю перенесення на інший сервер. У разі надання посередницьких послуг при комунікаціях між урядом і громадянами виникають також політичні та етичні питання — забезпечення секретності інформації, що передається, регулювання доступу провайдерів до приватної інформації громадян, залежність держави від приват-

них компаній, деякі з яких цілком можуть перейти у власність іноземних інвесторів.

4.5. ВІРТУАЛЬНЕ ПІДПРИЄМСТВО І ВІРТУАЛЬНИЙ ОФІС

Сьогодні Інтернет не тільки надає будь-якому індивіду можливість обмінюватись інформацією з будь-якою людиною у будь-якому куточку світу, що робить неістотною відстань (а на цьому, зокрема і базується електронна комерція). Новітні інформаційні технології дають змогу розширити бізнес-процеси за межі компаній і з'єднати їх через Мережу.

Необхідність співпраці економічних суб'єктів диктується сучасними реаліями:

- нові продукти стають дедалі складнішими і містять все більше високотехнологічних компонентів, тому компанії не можуть розробляти їх поодиночі;
- у процесі спільного виробництва нових продуктів компанія може дістати доступ до новітніх технологій і знань;
- нові ринки можуть досліджуватись колективно;
- співпраця зменшує ризик кожного окремого учасника.

У відповідь на вимогу часу поряд із традиційними формами міжорганізаційного співробітництва (спільні підприємства, стратегічні об'єднання тощо) з'являються нові, зокрема — віртуальні підприємства.



Віртуальність — різні виміри

Слово «віртуальний» вживається часто і з різними значеннями. Віртуальним називають об'єкт, який не існує в реальному фізичному просторі, але виявляє себе як справжній. В ідеалі, віртуальну реальність (образи і звуки), що породжується комп'ютером, не можливо відрізнити від дійсності, оскільки відповідні технології впливають безпосередньо на наші відчуття. Користувач взаємодіє зі штучним світом за допомогою різних сенсорів, таких як шолом і рукавички. Створення віртуальних світів може стати юридичною проблемою — наприклад, чи можна вважати злочином (і карати як злочин) вбивство, скоєне у віртуальності, і чи можна засуджувати людину, що скоїла реальний злочин, якщо вона була впевнена, що перебуває у віртуальному середовищі?

Водночас прикметник «віртуальний» може і не пов'язуватись з іншою реальністю, а означати певне штучне утворення. «Віртуальний світ» — це явища і процеси, що моделюються на екрані комп'ютера, — будинки і комунікаційні лінії, наукові й освітянські

проекти тощо. Віртуальність економіки означає проведення економічних операцій в електронному просторі. «Віртуальне співтовариство» — об'єднання в Інтернет користувачів зі спільними інтересами. Аналогічно віртуальність підприємства слід сприймати як метафору — підприємство, яке не має базових структур у фізичному просторі, не може існувати. Тут віртуальність передбачає взаємодію реальних фахівців та організаційних структур за допомогою новітніх інформаційних і комунікаційних технологій.

Віртуальне підприємство являє собою сукупність незалежних економічних суб'єктів, що об'єднуються для досягнення певної мети (виконання певного завдання), і має такі характеристики:

- тимчасовість;
- гнучкість, можливість швидкого утворення, реструктурування і розформування у потрібний час;
- невелика інфраструктура або її відсутність;
- сильна залежність від телекомунікацій — організація групової взаємодії фахівців у середовищі комп'ютерних мереж і програмного забезпечення колективної роботи різних класів;
- розподіленість центрів відповідальності, прийняття рішень на всіх рівнях управління;
- здатність реагувати в режимі реального часу на зміни в середовищі, умовах конкуренції або в потребах споживачів.

Варто зазначити, що віртуалізації підлягають не лише комерційні підприємства, а й державні організації та установи.

Законодавчі та політичні питання, економічний розвиток, охорона здоров'я, соціальний захист громадян, забезпечення законності і правопорядку, розбудова ринкової інфраструктури — усі ці та багато інших проблем потребують взаємодії різних гілок влади, міністерств і окремих органів державного управління. Вони узгоджують між собою окремі заходи, спільно приймають рішення, разом реалізують проекти і програми, обмінюються досвідом. Водночас можна спостерігати потоки управляючої інформації від центральних органів влади до місцевих і передавання звітів та даних спостережень у зворотному напрямку.

У цілому можна констатувати, що концентрація на обробці різного роду інформації у процесі державного управління створює передумови для впровадження нових технологій. У свою чергу, автоматизація бізнес-процесів та інтеграція даних і спільне їх використання набувають все більшого значення для адміністрування, прийняття рішень і надання послуг і стають критичними

для організації зв'язків між урядовими та іншими організаціями з одного боку, між державою та громадянами — з іншого. Глобалізація зумовлює справедливість вищесказаного і для міждержавного рівня хоча б у сфері боротьби зі злочинністю і тероризмом.

Із цього погляду створення **«віртуального уряду»** («електронного уряду», «е-уряду», системи G2G) є адекватним технологічним рішенням, яке доповнює інші види участі держави в електронній комерції.

Очевидно, що створення віртуального підприємства розпочинається з автоматизації бізнес-процесів окремої структури або кількох рівнів управління. При цьому наголос робиться на інтеграції даних з різних баз. Інтегровані дані стають доступними не тільки для співробітників, а й для зовнішніх користувачів, які одержують доступ до них через Web. Відповідні додатки надають доступ до інформації згідно зі встановленими бізнес-правилами і подають її у вигляді, прийнятному для користувачів. Бізнес-правила і визначають тип взаємодії. Так, центри електронної торгівлі для державних установ, які дають змогу постачальникам і покупцям збиратись в он-лайнному режимі і купувати/продавати необхідні товари, можна вважати і прикладом системи B2G, і прикладом створення простих віртуальних підприємств.

Головними перевагами віртуальних підприємств як форми міжорганізаційного співробітництва є їх динамічність, незалежність від галузевих або відомчих бар'єрів, поєднання географічно віддалених суб'єктів. Завдяки своїй здатності створювати та експлуатувати більш новаторські та цілеспрямовані служби за менших капіталовкладень, в більш стислі строки і зі значно меншим фінансовим ризиком, вони мають величезні перспективи поширення. Одним із наслідків цього процесу стане нестабільність економічних суб'єктів — передбачаються часті випадки створення і ліквідації підприємств зі швидким переміщенням працівників з одного підприємства на інше. Затребуваність і підприємств, і окремих працівників на ринку буде прямо пов'язана зі здатністю ефективно надавати і просувати спеціалізовані послуги з постійним їх удосконаленням. Очевидною стає неминучість зміни психології і діяльності персоналу. Уже сьогодні ця тенденція чітко виявляється під час створення **віртуальних офісів**.

Віртуалізація офісу, тобто залучення «віддалених» співробітників, які взаємодіють через Інтернет, є наступним кроком після створення інтранет із внутрішньофірмовими чатами, дошками оголошень, внутрішніми дискусійними форумами тощо. На спеціальному сервері, який надає послугу «віртуальний офіс», ство-

рюється модель фірми — розміщуються певні ресурси і встановлюються правила доступу до них співробітників і, можливо, сторонніх осіб (клієнтів, замовників, постачальників і т. ін.). Таким чином простір офісу поділяється на «кімнати», в яких співробітники спілкуються, обговорюють проблеми, консультуються один з одним, користуються службовою інформацією з бази даних. У всіх «кімнатах» створюються спеціальні форми, які полегшують процес діловодства — заповнюючи їх, співробітники можуть надавати стислий опис документа, вказувати строки виконання, визначати область його дії і статус. Для кожної «кімнати» призначається менеджер, який має координувати роботу інших і контролювати документообіг в цілому.

Для створення віртуального офісу існують серйозні передумови:

- економічна вигода — віртуалізація передбачає зменшення деяких накладних витрат — на орендну плату за приміщення, оргтехніку, відрядні, міжміські переговори тощо;
- підвищення ефективності роботи — співробітники не витрачають час на переїзди, скорочуються невиробничі витрати часу, прискорюється вирішення проблем (консультації, наради, переговори відбуваються в он-лайнному режимі).

У свою чергу, працівники можуть раціонально планувати свій час і працювати за сумісництвом, не виходячи з дому, при кращих можливостях працевлаштування (географічна віддаленість роботодавця вже не має значення).

Така модель організації праці у першу чергу приваблива для компаній і фахівців, професійна діяльність яких пов'язана з комп'ютерами і телекомунікаціями: програмістів і Web-дизайнерів, рекламних контор і дизайн-бюро, маркетингових агентств і мережних мас-медіа.

Водночас масове поширення такої практики гальмується певними *проблемами*. По-перше, далеко не всі потенційні вітчизняні «віддалені» працівники забезпечені комп'ютерною технікою, а недосконалість і дорожнеча зв'язку ставить під сумнів економічну ефективність подібних проектів. По-друге, перехід до віртуального офісу вимагає зміни всієї політики фірми — дистанційна форма трудового процесу вимагає або повної довіри до співробітників (якщо вони зарекомендували себе як висококваліфіковані і дисципліновані фахівці), або жорстко регламентованої системи управління. По-третє, віртуалізація вимагає продуманої системи комунікацій — керівник має чітко і повно формулювати завдання, перевіряти його виконання своїми підлеглими, вказувати на помилки і недоробки в «письмовій» формі. Вчетверте, віддалена

взаємодія висуває виключні вимоги до розвитку колективної мотивації, самоконтролю, ініціативності, відповідальності, спроможності самостійно виробляти і приймати рішення. По-п'яте, відсутність безпосередніх контактів, спілкування, обміну інформацією (навіть якщо вона не стосується безпосередньо службових обов'язків) негативно впливає на мотивацію людини, її ставлення до роботи, а можливо, і на якість результатів.

Очевидно, кожен підприємець і працівник має сам вибирати варіант своєї зайнятості — або вдома, або в офісі, або проміжний варіант, наприклад 30—40 % часу на роботу вдома, а решта часу — в офісі.



Контрольні запитання і завдання

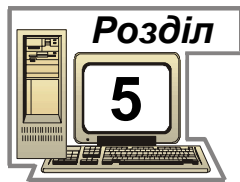
1. Назвіть класи систем автоматизації роботи з документами залежно від задач та технологій, що застосовуються.
2. Порівняйте концепції організації автоматизованих систем контролю виконання документів та електронних архівів.
3. Назвіть завдання, що їх автоматизують системи керування електронними документами.
4. Чим відрізняються системи groupware від workflow-систем?
5. Що таке модель ділового процесу і як вона використовується у workflow-системах?
6. Як розвиток електронної комерції впливає на економіку, управління, повсякденне життя пересічного громадянина?
7. Назвіть учасників електронної комерції і визначте роль кожного з них.
8. Як у системах електронної комерції використовуються методи криптографії?
9. Визначте напрямки участі держави в електронній комерції.
10. Визначте підходи до організації роботи юристів у режимі віртуального офісу.
11. Визначте проблеми і перспективи розвитку електронної комерції в Україні.



Література

1. Береза А. М. та ін. Електронна комерція: Навч. посібник. — К.: КНЕУ, 2002. — 236 с.

2. Діденко А. Н. Сучасне діловодство: Навч. посібник. — К.: Либідь, 1998. — 256 с.
3. Ефимова О. Средства workflow в рамках общей концепции управления предприятия. — www.cbit.kiev.ua/Docs/wf_line.html.
4. Козье Д. Электронная коммерция: Пер. с англ. — М.: Русская редакция, 1999. — 272 с.
5. Матеріали сайтів <http://www.aspbusiness.ru/>, <http://www.emoney.ru/>, <http://www.enterworks.com/>.
6. Рогач І. Ф., Сендзюк М. А., Антонюк В. А. Інформаційні системи у фінансово-кредитних установах: Навч. посібник. — К.: КНЕУ, 2001. — 239 с.



ПРАВОВІ ІНФОРМАЦІЙНО-ПОШУКОВІ СИСТЕМИ

5.1. КОНЦЕПЦІЯ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ

Вирішення великої кількості правових задач залежить від якості результатів **інформаційного пошуку** — вибору з усієї відомої сукупності документів, текстів, відомостей, фактів і даних тих елементів, які відповідають інформаційним потребам. За умов великих обсягів інформації, серед якої здійснюється пошук, стає доцільним і навіть необхідним використання інформаційно-пошукових систем.

Інформаційно-пошукова система (ІПС) — це сукупність методів і засобів, призначених для зберігання та пошуку документів, відомостей про них чи певних фактів.

За **тематикою** виділяють галузеві ІПС, полі- та вузькотематичні. Залежно від **типу інформації**, що зберігається, розрізняють документальні системи, в яких об'єктом зберігання і пошуку є документ, та фактографічні, в яких зберігаються і розшуковуються окремі дані, що характеризують деякі факти — події, процеси, явища.

За **режимом функціонування** виокремлюють:

- системи з вибіркоким пошуком — ІПС, в яких пошук виконується за постійним набором запитів для певного контингенту користувачів у масиві поточних надходжень документів чи даних, які надходять через певні інтервали часу. При цьому змінюється вміст системи, а запити залишаються без змін;
- системи з ретроспективним пошуком, які обслуговують разові запити, що змінюються залежно від інформаційних потреб користувачів, у нагромадженому інформаційному фонді зі значною хронологічною глибиною.

Найефективнішим способом пошуку інформації є перегляд кожного документа і визначення його відповідності **інформаційному запиту** — тексту певною мовою, що відбиває деяку інформаційну потребу. Проте такий пошук є дуже тривалим. Тому насправді пошук здійснюється не за текстами документів, а за їх стислими описами інформаційно-пошуковою мовою — **пошуковими образами**.

Процедура визначення пошукового образу документа (ПОД) називається **індексуванням**. Найбільш популярною моделлю створення ПОД є векторна модель. За цією моделлю кожному документу приписується вектор розмірності, що дорівнює кількості термінів, якими можна скористатися при пошуку. Елементами вектора є деякі числа (ваги), які визначають адекватність даного терміна документа (у найпростішому випадку — 1, якщо термін присутній, 0 — якщо термін у документі не трапляється).

Взаємодія користувача з ІПС охоплює такі *операції*:

- введення в систему пошукових образів документів і самих документів;
 - зберігання інформації в системі;
 - формування запитів, опис і введення у систему **пошукових розпоряджень** — інформаційних запитів, викладених інформаційно-пошуковою мовою і доповнених допоміжною інформацією;
 - пошук — порівняння пошукових образів документів з пошуковими розпорядженнями;
 - прийняття рішення про видачу знайденої інформації залежно від критерію пошуку, визначеного користувачем;
 - видача інформації, що відповідає інформаційному запиту.
- Функціонування ІПС можна оцінити за кількома *критеріями*:
- повнота — здатність відшукувати та видавати релевантні документи, тобто такі, що відповідають запиту користувача;
 - точність — здатність відсіювати та затримувати нерелевантні документи;
 - економічна ефективність — окупність витрат на функціонування системи вигодами від її використання, серед яких важливе значення мають підвищення оперативності та зменшення трудомісткості пошуку.



Якість роботи ІПС — релевантність і партинентність

Релевантність — характеристика ступеня відповідності змісту документа, знайденого в результаті інформаційного пошуку, змісту інформаційного запиту. Очевидно, що релевантність відрізняється від **партинентності** — характеристики ступеня відповідності змісту документа, знайденого в результаті інформаційного пошуку, інформаційній потребі, вираженій в інформаційному запиту.

ІПС може видати документ навіть якщо його ПОД не повністю відповідає пошуковому розпорядженню. У цьому разі резуль-

татом пошуку може бути не один якийсь документ, а їх множина, з якої користувач має вибрати ті, які відповідають його потребам найбільше. Це залежить від критерію пошуку, який може змінюватись за бажанням користувача. А загалом ефективність взаємодії користувача з ІПС та робота самої ІПС прямо залежить від якості *інформаційно-пошукової мови* (ІПМ) — спеціалізованої штучної мови, призначеної для опису центральних тем і формальних характеристик документів, а також опису інформаційних запитів і наступного виконання пошуку. З цією метою не може бути використана жодна з природних мов через їх неструктурованість, велику кількість граматичних винятків, неоднозначність та надмірність.

Основні елементи ІПМ такі:

- 1) алфавіт — система графічних знаків, що використовуються для утворення слів і словосполучень;
- 2) лексика — сукупність слів, що використовуються в мові;
- 3) граматики — сукупність засобів та правил побудови висловлювань;
- 4) парадигматичні (базові, аналітичні) відношення — відношення, які не залежать від контексту використання і спричинені не мовними, а логічними зв'язками. Наприклад, поняття «магнітний диск», «магнітна стрічка», «лазерний диск», «паперовий документ» утворюють тематичну групу «носії інформації», усередині якої можна виділити лексико-семантичні парадигми «паперові носії інформації» та «машинні носії»;
- 5) правила побудови індексів та їх ідентифікації.

Розрізняють ІПМ таких *видів*:

- передкоординатні (класифікаційного типу), в основу яких покладено систематичну класифікацію понять, що відбивають певні парадигматичні відношення. Класифікація може бути ієрархічною, фасетною, алфавітно-предметною;
- посткоординатні, в основу яких покладено принцип координатного індексування — зміст документів і запитів виражається набором ключових слів, вибраних з індексованого тексту.

Ключові слова — це слова, найбільш характерні для даного тексту або тематики. Пошук і вибір ключових слів є окремою складною проблемою, яка вимагає творчого підходу. Для правової ІПС таку роботу може виконати тільки висококваліфікований юрист широкого профілю. Але навіть повне визначення ключових слів недостатньо для організації ефективного пошуку, оскільки:

- ключові слова можуть мати різні варіанти написання та синоніми. Тоді документ, індексований за допомогою певного терміна, не буде виданий у відповідь на запит, складений з використанням терміна-синоніму;

- ключове слово може мати різні значення (проблема омонімічності). Запит, в якому присутні омоніми, призведе до видачі документів, які не стосуються вибраної користувачем теми;

- набір ключових слів не визначає родово-видові відношення між поняттями, а це звужує пошук.

З метою вирішення названих проблем для різноманітних тематик розробляються **тезауруси** — структуровані списки ключових слів, призначених для однозначного подання концептуального змісту документів і запитів. Тезаурус упорядковується так, щоб встановити прозорі еквівалентні, гомографічні, ієрархічні та асоціативні зв'язки між термінами.

Тезаурус містить:

- 1) **дескриптори** — слова та словосполучення, які однозначно позначають поняття з теми тезаурусу;

- 2) **недескриптори** — слова та словосполучення, які у природній мові позначають ті самі поняття, що і дескриптори, або еквівалентні поняття;

- 3) **семантичні зв'язки** (зв'язки на основі значень) між дескрипторами і не-дескрипторами, а також між самими дескрипторами.

Проблема омонімічності у тезаурусі вирішується тим, що кожне ключове слово ставиться у контекст, який робить це слово однозначним. Для вирішення проблеми синонімічності один із синонімів обирається, більш-менш довільно, як дескриптор, а синонімам надається статус не-дескрипторів. Тільки дескриптори можуть використовуватись при індексуванні та формулюванні запитів, при цьому не-дескриптори допомагають користувачам вибрати дескриптор. Якщо встановлено відповідність між ідентичними поняттями в різних мовах, користувач багатомовного тезауруса може формулювати запити рідною мовою і шукати документи незалежно від мови, якою вони були індексовані.

Прикладом спеціалізованого тезауруса є багатомовний політематичний інформаційно-пошуковий тезаурус **EUROVOC**, визнаний як міжнародний термінологічний стандарт. Він реалізований відповідно до стандартів ISO 2788-1986 «Guidelines for the establishment and development of monolingual thesauri» («Керівництво з введення і розробки одномовних тезаурусів») та ISO 5964-1985 «Guidelines for the

establishment and development of multilingual thesauri» («Керівництво з введення і розробки багатомовних тезаурусів»).

EUROVOC використовується для індексування та пошуку даних в ІПС офіційних документів органів, установ, інститутів і деяких держав — членів ЄС. Цей тезаурус охоплює всі теми, важливі для діяльності європейських інституцій: політика, міжнародні відносини, європейські співтовариства, законодавство, економіка, торгівля, фінанси, соціальні питання, освіта і комунікації, наука, бізнес і конкуренція, зайнятість та умови праці, транспорт, навколишнє середовище, сільське господарство, лісництво і рибна ловля, виробництво, технології та дослідження, енергія, промисловість, географія, міжнародні організації. Деякі теми у EUROVOC розроблені детальніше порівняно з іншими, оскільки вони важливіші для роботи ЄС. Наприклад, тезаурус містить назви областей кожної держави — члена ЄС, а назви регіонів інших країн відсутні.

Слід відзначити, що однією з характеристик політематичних тезаурусів взагалі і EUROVOC зокрема є досить довільне групування дескрипторів за темами. Фактично, деякі дескриптори можуть торкатися двох або більше тем, але для спрощення управління тезаурусом та обмеження його розміру прийнято уникати поліієрархії. Іншими словами, дескриптор включають не до всіх тем, до яких він може належати, а тільки до тієї теми, яка здається найбільш природною для користувачів.

EUROVOC реалізований офіційними мовами Європейського Союзу. Усі мови реалізації мають однаковий статус — кожен дескриптор в одній мові обов'язково має відповідний дескриптор в іншій мові. Однак, між не-дескрипторами у різних мовах не існує еквівалентності, оскільки багатство мов різниться для різних тем.

EUROVOC має дворівневу ієрархію. Верхній рівень складають теми, які мають двохсимвольні коди, наприклад, 12 — «LAW», «Право». Нижній рівень організовано як сукупність мікротезаурусів, позначених чотирма цифрами, перші дві з яких визначають тему, до якої належить цей мікротезаурус: 1216 — «criminal law» («кримінальне право»). Нумерація тем і мікротезаурусів єдина для всіх мов.

На екрані EUROVOC одночасно представлені дві панелі, які ілюструють вибраний рівень ієрархії: логотип EUROVOC і список тем і мікротезаурусів, або список мікротезаурусів і зміст вибраного мікротезауруса (рис. 5.1), або мікротезаурус і його окремий дескриптор.

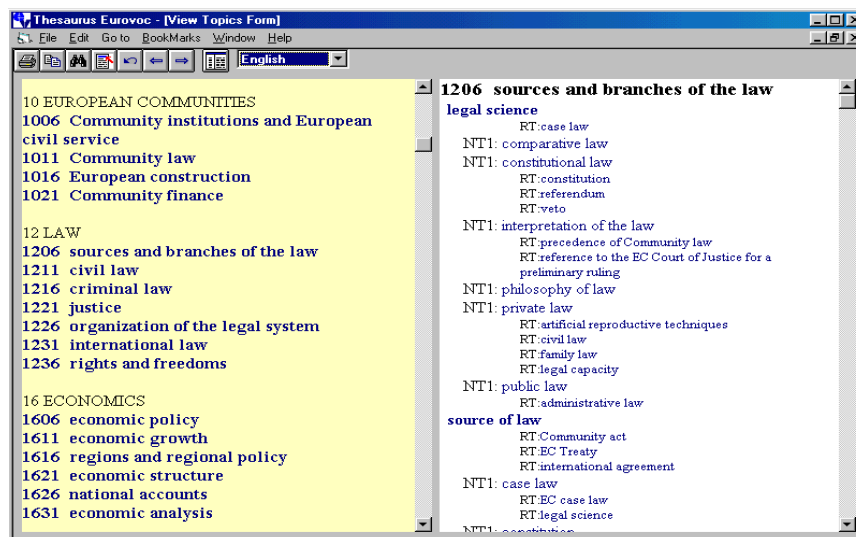


Рис. 5.1. Вікно тезауруса EUROVOC:
на лівій панелі — список мікротезаурусів за темами
«Європейські співтовариства», «Право», «Економікс»,
на правій — вміст мікротезауруса «Джерела та галузі права»

На рівні окремих дескрипторів і не-дескрипторів структура EUROVOC залежить від семантичних відношень, встановлених між ними. Передбачено такі їх *типи*:

1) «SN» (Scope Note, примітка щодо можливих значень) — визначення, що уточнює значення дескриптора, або вказівка, як використовувати дескриптор при індексуванні документа та формулюванні запитів;

2) «MT» (Microthesaurus, мікротезаурус) — посилання на мікротезаурус, до якого належить дескриптор (недескриптор);

3) «UF» (Used For, використаний для) та «USE» (використовує) — зв'язок еквівалентності між дескриптором і не-дескриптором (-ами), що він їх подає (UF), або між недескриптором і дескриптором, який замінює цей недескриптор (USE). Фактично зв'язок еквівалентності охоплює кілька типів зв'язків:

- повної синонімічності або ідентичного значення;
- близької синонімічності або схожого значення;
- антонімії або протилежного значення;
- включення, коли дескриптор охоплює одне або більше понять, яким надано статус недескрипторів, оскільки вони рідко використовуються;

4) ієрархічні зв'язки між дескрипторами:

- «BT» (Broader Term, ширший термін) — між певним дескриптором і родовим (більш узагальненим) дескриптором — зазначається з числом, яке показує кількість кроків за ієрархією між ними. При цьому дескриптори, для яких не існує ширших термінів, називаються термінами верхнього рівня. Деякі дескриптори з тем 72 «Географія» та 76 «Міжнародні організації» є поліієрархічними, іншими словами, для них існує більше одного ширшого терміна на наступному вищому рівні;

- «NT» (Narrower Term, більш вузький термін) — між родовим і видовим (більш вузьким) дескриптором — зазначається з числом, яке показує кількість кроків за ієрархією між ними;

5) «RT» (Related Term, взаємозв'язані терміни) — асоціативні зв'язки між дескрипторами. Асоціативний зв'язок показує особі, що проводить індексування, або користувачеві, що існує інший, настільки ж або навіть більш релевантний дескриптор. Передбачено асоціативні зв'язки таких *типів*: причини та наслідку; органу або інструменту; ієрархії (оскільки, як сказано вище, поліієрархія не припускається, втрачені ієрархічні зв'язки можна замінити асоціативними); супроводження; послідовності у часі або просторі; входження до складу; характерної риси; об'єкта дії або процесу; розташування; подібності (в разі, коли два майже синонімічні терміни включено як дескриптори); антонімії.

Асоціативні зв'язки мають такі *істотні характеристики*:

- вони симетричні;
- вони несумісні з ієрархічними зв'язками — якщо два дескриптори пов'язані ієрархією, між ними не можна встановити асоціативний зв'язок і навпаки;
- між дескрипторами, які мають спільний термін верхнього рівня, не може бути встановлено асоціативні зв'язки.

Навігація за тезаурусом здійснюється за допомогою посилань. Дескриптор можна вибрати, набравши на клавіатурі першу літеру його назви дескриптора. Також реалізовані повнотекстовий пошук і пошук за ключовими словами.

5.2. КОМП'ЮТЕРНА ПРАВОВА СИСТЕМА ЛІГА:ЗАКОН

Однією з найбільш популярних комп'ютерних правових систем в Україні є спеціалізована інформаційно-пошукова система «ЛІГА:ЗАКОН» (розробка інформаційно-аналітичного центру «Ліга», <http://www.liga.kiev.ua>). Система складається з

програмної оболонки, яка забезпечує пошук документів, та інформаційного ядра — *текстових баз даних нормативних документів*:

- «Загальне законодавство» — документи, прийняті вищими органами влади України: Верховною Радою України з 1990 р., Кабінетом Міністрів України з 1991 р., Президентом України з 1991 р., а також документи міністерств і відомств, які зареєстровані Міністерством юстиції України з 1993 р.;

- «Кодекси» — усі чинні кодекси України в контрольному стані;

- «Податки в Україні» — роз'яснення, листи, накази та інструкції Державної податкової адміністрації; листи, телеграми та інші документи НБУ та Міністерства фінансів; документи фінансового права, прийняті вищими органами влади, міністерствами і відомствами;

- «Міжнародні угоди» — міжнародні договори, угоди, конвенції;

- «Митне право» — документи, що регламентують митне право, видані Державною митною службою, вищими органами влади, міністерствами і відомствами;

- «Різне» — документи про кадрові перестановки;

- «ЛПГА:Столиця» — довідкова база нормативних документів, що регламентують ділове життя м. Києва;

- «Регіони» — документи, прийняті регіональними органами влади;

- «Консультації» — актуальні матеріали у вигляді анотацій статей, коментарів, відповідей на запитання з більше ніж 30 економічних видань із проблем оподаткування, підприємництва, зовнішньоекономічної діяльності, валютного регулювання, починаючи з 1999 р.;

- «Типові договори і форми» — систематизовані посилання на нормативні документи, якими затверджені різні типові статuti, договори, форми тощо; зразки цивільно-правових договорів і процесуальних документів;

- «Довідники» — довідково-аналітичні матеріали за різними напрямками (державні класифікатори, плани рахунків, ставки зборів, тарифи тощо), оформлені у вигляді систематизованих посилань на нормативні документи чи зведених таблиць; курси валют, індекси інфляції тощо з можливістю побудови динамічних графіків та їх масштабування;

- «Термінологічний словник» — терміни і поняття, що вживаються у нормативно-правових актах;

- «Моніторинг законодавства» — анотації фахівців ІАЦ «ЛІГА» до нових документів, що надходять у систему.

Система «ЛІГА:ЗАКОН» поставляється у версіях «Стандарт» і «Професіонал», які різняться за повнотою функцій та інформаційним наповненням.

На основі ППС «ЛІГА:ЗАКОН» розроблено тематичні комп'ютерні довідники, які містять у собі стандартний програмний комплекс і спеціалізоване інформаційне ядро — нормативні документи, консультації фахівців, огляд преси та довідкову інформацію з певних питань:

- «ЛІГА:Консультант БУХГАЛТЕРА» — бухгалтерський облік, оподаткування, деякі особливості підприємницької діяльності;

- «ЛІГА:Консультант ЗЕД» — зовнішньоекономічна діяльність, валютне і митне регулювання, валютний контроль;

- «ЛІГА:ПРАКТИК-керівник» — підприємництво, бухгалтерський облік, оподаткування, зовнішньоекономічна діяльність, валютне і митне регулювання, валютний контроль, антимонопольне законодавство, ліцензування, сертифікація, торгівля і побутове обслуговування.

Спільні *особливості* систем такі:

- зберігання текстів документів у форматах, близьких до поліграфічних, з наявністю гіпертекстових посилань і графічно зображених зв'язків між документами;

- розміщення всіх редакцій документів у хронологічній послідовності; контрольний стан документів, відстеження всіх змін і доповнень;

- систематизація документів за 35 тематичними напрямками;

- доступ до еталонних редакцій нормативних документів, що ідентичні внесеним до Єдиного державного реєстру нормативних актів;

- двомовний (український/російський) інтерфейс і пошук, можливість автоматичного підрядкового перекладу;

- можливості ведення власних добірок документів з їх інтеграцією у папки, створення 4 типів простих закладок (примітка, коментар, питання, увага), побудови власних зв'язків між документами (закладки-посилання); збирання, систематизації і пошуку власних документів користувача;

- відкритий інтерфейс — спеціальні засоби, що дають можливість здійснювати виклик системи «ЛІГА:ЗАКОН» з інших додатків;

- технологія «клієнт—сервер».

Системи оновлюються залежно від вибору абонента — щодня через Інтернет або за адресою ІАЦ «ЛІГА», або кур'єрською доставкою один раз на тиждень по м. Києву чи один раз на два тижні по Україні.

У системах реалізовано такі *основні види пошуку нормативних документів*:

1. Пошук за реквізитами. У системі ведуться такі реквізити документів: вид документа, видавець, слова з назви, дата прийняття документа, номер документа, статус документа («Чинний», «Втратив чинність», «Дію призупинено»), дата і номер реєстрації документа в Міністерстві юстиції, ключові слова, опублікування (неофіційні джерела). Цей вид пошуку слід використовувати тільки за умов, коли відомі точні значення реквізитів (одного або кількох). Пошук може відбуватись як у межах всієї бази (опція «Всі документи»), так і у вибраному діапазоні (опція «Нормативні», реквізит «Наявність у базах»).

Під час введення реквізитів «Вид документа», «Видавець», «Статус документа», «Ключові слова», «Опублікування» можна скористатись **довідником значень**. Довідник значень містить повний список тих значень пошукового реквізиту, які зустрічаються в інформаційних картках документів всієї бази системи. У відповідному діалоговому вікні присутні інструменти пошуку потрібного елемента (за першими літерами слова) і побудови пошукового виразу. За замовчуванням при виборі кількох значень з довідника між ними встановлюється логічне сполучення «АБО» («OR»). За допомогою спеціальних кнопок можна встановити сполучення типу «ТА» («AND»), «НІ» («NOT»), «ТОЧНО» («!»). На рис. 5.2. наведено вид екрана «Пошук за реквізитами» з відкритим діалоговим вікном роботи з довідником значень ключових слів.

Щодо реквізитів, для яких не існує довідника значень («Слова з назви», «Номер документа», «Номер реєстрації в Мін'юсті»), теж можна встановити складні умови пошуку — у контекстному меню для конкретного реквізиту послідовно вибрати пункт «Логічні операції» і сполучник.

Для введення реквізитів «Дата прийняття» і «Дата реєстрації в Мін'юсті», крім довідника значень, пропонуються календарі. Дати вводяться за шаблоном «rrrr/мм/дд».

Слова, що вводяться з клавіатури, рекомендується вказувати без закінчення.

Після одержання відповіді на запит можна скористатися опцією «Пошук у межах пошукового списку».

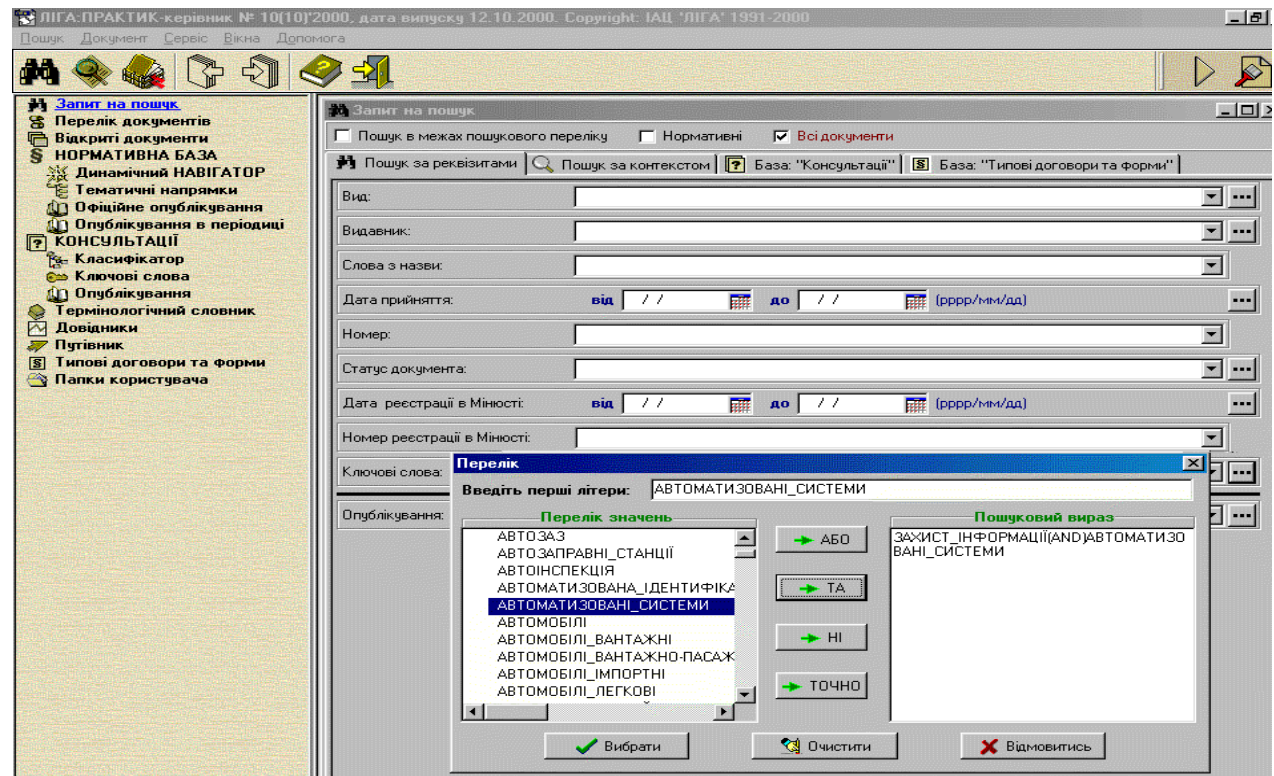


Рис. 5.2. Вікно пошуку за реквізитами

2. Пошук за ключовими словами, які визначають юристи ІАЦ «ЛІГА» на основі аналізу кожного документа, що надходить до системи «ЛІГА:ЗАКОН». Якщо до бази надійшов документ з новим ключовим словом, воно відразу попадає у загальний список. Правила роботи з довідником значень ключових слів не відрізняються від щойно наведених. Пошук за ключовими словами можна комбінувати з пошуком за іншими реквізитами.

3. Пошук за контекстом — пошук заданого набору слів безпосередньо у текстах документів. У цьому режимі можна задати пошук чотирьох різних словосполучень, кожне з яких може містити до чотирьох слів. Під час заповнення полів, розміщених по горизонталі, між відповідними словами встановлюється сполучник «ТА», під час введення слів у поля по вертикалі між ними встановлюється сполучник «АБО». У разі задання пошукових словоформ можна використовувати спеціальні символи, які можна додати до основи слова праворуч: * — будь-яке закінчення; ? — будь-яка буква; ! — точний пошук. Наприклад, задання у вигляді «подат» або «подат*» призведе до пошуку слів «податок», «податку», «податковий» та ін., а якщо запит буде сформульований як «податок!», то будуть знайдені тільки ті документи, в який трапляється слово «податок».

Можна варіювати близькість розміщення слів — опції «Слова в документах» і «Слова в абзацах». Останній вид пошуку досить тривалий, тому рекомендується обмежувати максимальну кількість документів, що їх слід знайти.

Діставши результати, можна скористатись кнопками «Наступний абзац з пошуковими словами» і «Попередній абзац з пошуковими словами».

4. Пошук за допомогою «Динамічного НАВІГАТОРА». Динамічний навігатор — дерево добірок документів, кожному вітку якого користувач може налаштовувати за видами документів, за видавцями, за датою прийняття або за тематичним напрямком. Якщо для вітки верхнього рівня існує чотири варіанти впорядкування, то для вітки наступного рівня — на один варіант менше, і т. д.

5.3. ПРАВОВА ІНФОРМАЦІЙНО-ПОШУКОВА СИСТЕМА «НОРМАТИВНІ АКТИ УКРАЇНИ»

Особливістю ІПС «*Нормативні акти України*» (НАУ, <http://www.nau.kiev.ua/>) є реалізація трьома мовами — українською, російською, англійською.

База даних НАУ має такий склад:

1) повна **нормативно-правова база** (нормативні акти в актуальному стані, з урахуванням внесених змін та усі попередні редакції):

- Конституція, кодекси, закони та постанови Верховної Ради України;
- укази та розпорядження Президента України;
- постанови, розпорядження і декрети Кабінету Міністрів України;
- нормативні акти міністерств та відомств, зареєстровані в Міністерстві юстиції, а також вузьковідомчі документи: листи, роз'яснення, розпорядження;
- міжнародні угоди — двосторонні угоди України, міжнародні конвенції;
- чинні нормативні акти органів влади СРСР та УРСР;
- нормативні акти місцевих органів влади;
- перспективне законодавство — тексти прийнятих, але не підписаних законів, тексти резонансних законопроектів, оприлюднених для обговорення;

2) судова практика:

- рішення, висновки, ухвали Конституційного Суду України;
- постанови пленуму Верховного Суду України, ухвали судових колегій, роз'яснення, листи;
- постанови, рішення, листи Вищого Господарського Суду України;
- матеріали реальних справ у загальних судах України (трудові, житлові, сімейні, майнові, зобов'язальні, земельні, спадкові спори тощо);
- матеріали реальних справ у господарських судах України (зобов'язальні, податкові, митні, майнові, корпоративні спори, визнання недійсним актів органів влади) та аналітичні коментарі до них;

3) консультації, роз'яснення, погляди:

- дайджести опублікованих у пресі статей з поточних економічних питань;
- офіційні повідомлення та роз'яснення органів державної влади;
- ексклюзивні аналітичні статті правозастосувального характеру;

4) класифікатори, довідники, форми:

- тематичний класифікатор законодавства: тематичні добірки нормативних актів у сферах підприємництва, податкового, митного законодавства, міжнародного права, зовнішньоекономічної діяльності, бухгалтерського обліку;

- каталог публікацій нормативних актів в офіційних та відомих виданнях;
- словник термінів: визначення термінів із посиланнями на відповідні закони, підзаконні акти, судові рішення, міжнародні угоди;
- бланки звітності у форматі текстового редактора Microsoft Word, готові до заповнення та друку;
- довідник органів влади — структура, адреси, телефони, основоположні документи органів державної влади України;
- каталог порушених справ про банкрутство підприємств, підготовлений за офіційними повідомленнями господарчих судів України;
- зведені таблиці: щоденні курси валют НБУ, індекси інфляції, розміри облікової ставки, мінімальної зарплати, пенсії, податкового мінімуму, список офшорних зон і т. ін.;
- нормативно затверджені типові документи: договори, форми, бланки, правила, положення і т. ін.;
- моніторинг — щотижневий огляд нових нормативних актів.

Крім основної системи, пропонується компакт-диск **«Митний бюлетень»**, який має такий вміст:

- 1) повна нормативно-правова база;
- 2) митне законодавство — аналіз за темами «Спеціальні правові режими зовнішньоекономічної діяльності (ЗЕД)», «Система тарифного (митно-тарифного) регулювання ЗЕД», «Система нетарифного регулювання ЗЕД», «Організація митної справи», «Митний та інші види контролю», «Митні режими», «Митне оформлення», «Митні платежі», «Порядок ввозу (вивозу, пересилання) товарів фізичними особами», «Порушення митних правил і контрабанда», «Спеціальна (вільна) економічна зона» та ін.;
- 3) міжнародне митне право — міжнародні конвенції та двосторонні угоди України про співробітництво в митній галузі;
- 4) аналіз судової практики — аналіз арбітражних справ з митної діяльності;
- 5) типові документи, форми, бланки, митні довідники — структура митних органів України, курси валют НБУ, індекси інфляції, Товарна номенклатура ЗЕД, перелік банків, яким надано ліцензії на здійснення валютних операцій, перелік префіксів штрихових кодів (товарна нумерація EAN), ІНКОТЕРМС, довідники країн, перелік офшорних зон, електронні адреси торговельно-економічних місій та ін.;
- 6) словник законодавчих термінів — нормативні означення термінів з посиланнями на відповідні документи;

7) оперативна інформація в Інтернет — огляди митного законодавства та митних правил деяких країн, сайти державних органів влади України.

До сім'ї систем НАУ входить також *«Електронний інформаційний бюлетень»*, який є складовою ІС Верховної Ради України (див. розд. 6).

База даних системи НАУ має ієрархічну структуру — документи систематизовано за типами, тематикою, офіційними публікаціями, хронологією надходження. У будь-якому розділі бази працюють **універсальні пошуки** за словом чи контекстом у тексті, за контекстом у назві або за датою. Також користувачеві надається можливість задати складні комбінації контекстів із застосуванням логічних операцій ТА, ЧИ, НЕ, керувати порядком слів та їх входженням в один абзац, речення, словосполучення. Нормативні документи можна знайти і за їхніми реквізитами: видавцем, номером, датою, назвою, видом, статусом, відомостями про реєстрацію. Для реквізитів створено словники всіх можливих значень. Відразу після того, як користувач указав значення певного реквізиту, система підраховує кількість документів, які підпадають під запит, що допомагає звужувати поле пошуку.

Списки знайдених документів можна відсортувати за датою чи типом, провести серед них додатковий пошук, зберегти у власній базі. У власній базі даних (система дає змогу створити кілька баз із довільною структурою) користувач може розмістити та організувати за тематиками власні тексти і файли, посилання на документи основної бази, посилання на розділи та рубрики основної бази, закладки-коментарі до текстів, колекції пошукових запитів. На власні бази поширюється дія універсальних пошуків. Такими базами можна обмінюватися з іншими користувачами НАУ.

5.4. ОРГАНІЗАЦІЯ ПОШУКУ ПРАВОВОЇ ІНФОРМАЦІЇ В ІНТЕРНЕТ

5.4.1. Стратегії пошуку інформації в Інтернет

Сьогодні Інтернет — це найбільший світовий інформаційний ресурс, що містить практично всю інформацію, якою може зацікавитись людина. Але популярне порівняння Мережі з величезною бібліотекою неправомірне через відсутність будь-якої систематизації її ресурсів і хаотичне стрімке збільшення кількості посилань. Тому **«потенціал для вирішення задач»** Інтернет (корисність інформа-

ції, одержаної за її допомогою) є досить низьким — користувач не може розраховувати на одержання інформації, яка буде водночас задовольняти три базові вимоги — своєчасність, достовірність, повнота. Отже, використання Інтернет з професійною метою становить проблему, яка постійно ускладнюється.



Бібліотеки — цифрові і звичайні

У дискусіях щодо цифрових бібліотек, доступних через локальні або глобальні мережі, часто приймаються припущення, які при ближчому розгляді можна визначити як хибні:

▲ оцифровані матеріали з часом заміняють інші форми подання інформації. Можна сказати, що нові технології створюють і заповнюють нові ніші, але це тільки невелика частка тих інформаційних ресурсів, які людство створило протягом своєї історії;

▲ інформація в Інтернет є адекватною заміною послуг звичайних бібліотек. Насправді величезна кількість публікацій в Інтернет — це реклама і «самвидав», який не вимагає ухвали рецензента, редактора, видавця або бібліотекаря, і має досить ефемерний характер. Користувач Мережі має самостійно визначати достовірність і повноту одержаної інформації;

▲ каталоги інформаційних ресурсів малоцінні, якщо останні не доступні в режимі on-line. Але першим кроком у процесі пошуку інформації є визначення її місцезнаходження, при цьому можуть бути корисні каталоги, індекси, анотації та інші описи як електронних, так і звичайних ресурсів.

Слід зазначити, що звичними вже стали проекти, які передбачають певне поєднання можливостей звичайних бібліотек та Інтернет. Наприклад, Національна бібліотека України ім. Вернадського (<http://www.nbuv.gov.ua/>) пропонує скористатися електронним каталогом. Для кожного знайденого об'єкта (книги, дисертації та ін.) у списку, крім звичайних реквізитів, указуються індекс рубрикатора і шифр зберігання у бібліотеці, що полегшує подальшу роботу. Електронний каталог бібліотеки КНЕУ дає змогу здійснити пошук у базах даних BOOKS — «Книги бібліотеки», APEL — «Статті з періодичних видань бібліотеки», WORK — «Праці викладачів КНЕУ», AUNTD — «Законодавчі та нормативні документи». Існують і проекти переведення бібліотек у цифровий формат для надання можливості користувачам безкоштовно шукати інформацію і безкоштовно або за невелику плату користуватися нею. Найбільш масштабним українським проектом такого роду є створення Національної архівної інформаційної системи «Архівна та рукописна Україніка».

З іншого боку, електронні періодичні видання Мережі часто перетворюються на е-бібліотеки — стирається межа між списком розсилки з архівом, мережним журналом, тематичним Web-сайтом, літературним клубом і повномасштабною бібліотекою.

У цьому контексті вводиться поняття «**медіа-компетентність**», яке позначає систему навиків пошуку в середовищі Інтернет і застосування інформації з раціональним рівнем потенціалу вирішення задач. Web-серфінг — заняття захоплююче, але малопродуктивне. Тому для пошуку потрібної інформації користувач має звертатись до спеціальних сервісів.

Існують *три базові стратегії*, які можуть бути використані:

1) перегляд пошукових каталогів — найчастіше це неефективна стратегія, яка дає безсистемні результати. Пошук здійснюється кроками, через вибір загальної категорії, потім — підкатегорії і т. д. за існуючою ієрархією. Складність такого пошуку полягає в тому, що користувач має визначити, до якої категорії належить його тема, а за відсутності стандартів кожен каталог має свою систематику і специфічне наповнення;

2) перехід за гіперпосиланнями від стартової сторінки. Ефективність цієї стратегії залежить від вибору початкового сайту або Web-сторінки. Більшість мегапорталів мають рейтинги сайтів, позначені як «Тор» або «Cool». Такі рейтинги створюються за кількістю відвідувань їх користувачами. Але інформаційні потреби різних користувачів не збігаються, тому до таких рейтингів слід ставитись з обережністю. Водночас, як показує практика, більшість користувачів одного профілю мають однакові інформаційні потреби, а тому відвідують одні й ті самі тематичні сторінки, які можна розглядати як спеціалізований вхід до Інтернет. Тим, хто починає пошук правової інформації, можна, зокрема, рекомендувати сайт Верховної Ради України «Закони та підзаконні акти України в Інтернет» — <http://www.rada.gov.ua/> (див. підрозд. 5.5); «Інформаційний бізнес-портал в Інтернет — LIGA ONLINE» — <http://www.liga.kiev.ua/>; «Нормативні акти України — он-лайн» — <http://www.nau.kiev.ua/>;

3) пошук за допомогою пошукових систем. На відміну від каталогів, такий пошук не обмежується окремою категорією. Ця стратегія може бути використана і для пошуку першої сторінки.

Використовуючи пошукові системи Інтернет, потрібно враховувати такі *фактори, що впливають на результативність пошуку*:

- кожна пошукова система Мережі має свою спеціалізацію;
- пошук здійснюється не за повними текстами документів, а за їх пошуковими образами, при цьому кожна система має оригінальний механізм роботи з ключовими словами. Зокрема, якщо база даних системи невелика, то до неї записується більше термінів, в іншому разі пошуковий образ документа відбираються «найвагоміші» ключові слова;



База індексів пошукової системи — поле конкурентної боротьби

Власники (автори) Web-серверів зацікавлені в тому, щоб їх URL-адреси були відомі пошуковим системам, оскільки це прямий шлях до кінцевих користувачів. Крім звичайних прийомів при цьому застосовуються і нетрадиційні. Так, служби Lycos та AltaVista повідомили про зафіксовані спроби реєстрації вузлів з неправильними адресами і спроби видалення адрес з бази індексів, можливо, з метою нанесення шкоди конкурентам. Деякі розробники намагаються ввести в оману робітників пошукових систем за допомогою «приманок» — до Web-сторінки включаються популярні ключові слова, набрані невидимим шрифтом (таким, що збігається за кольором із фоном). Це може призвести до неправильного оцінювання релевантності сторінки.

- і запити, і їх інтерпретація реалізуються у пошукових системах по-різному. Більшість систем надають користувачеві можливість сформулювати **простий запит** у формі фрази природною мовою без загальних слів, союзів і прийменників або **складний запит**, який враховує специфіку пошукового апарата системи. Складний запит дає змогу варіювати різні параметри пошукового процесу.

Для того щоб підвищити ефективність пошуку, слід провести попередній аналіз теми інформаційного запиту і визначити:

- унікальні слова, спеціальні терміни, назви, аббревіатури або акроніми для даної теми. Пошук за такими словами найбільш ефективний. Для точного задання граматичної форми слова слід розрізняти великі і малі літери, у деяких системах з цією метою також використовується символ «!». Якщо розшукується назва, перед відповідним словом може вказуватись оператор «title:»;

- спільноти, організації, установи або окремих осіб, сайти або Web-сторінки яких можуть містити потрібну інформацію або корисні посилання. Знайдені сторінки можуть стати стартовими для подальшого пошуку;

- стійкі вирази (словосполучення, фрази), які стосуються даної теми, наприклад «правове регулювання» або «набуття чинності закону». Для такого пошуку слід використовувати лапки (дужки) або оператори відстані. Це уточнює запит і зменшує кількість документів, що видаються;

- інші слова, які можуть траплятись у *будь-якому* документі з заданої теми. Як ключові слова найчастіше використовуються іменники, рідше — прийменники і зовсім рідко — дієслова, прислівники, прийменники, сполучники.

Пошук може здійснюватись як за окремим словом, так і за їх сукупністю — слова сполучаються за допомогою логічного оператора «AND» (від англ. «та») або символу «+». За статистикою, українські користувачі вводять у запиті в середньому 2,5 слова, а закордонні — 1,5 слова. На запит з одним словом система видасть більшу кількість посилань, але при збільшенні слів результати будуть точнішими.

Бажано визначити для кожного слова із запиту можливі синоніми, еквівалентні терміни, інші варіанти написання. Синоніми можна вказати у цьому ж запиті через оператор «OR» (від англ. «або») або використати в наступному запиті, якщо перший не приніс бажаних результатів. Деякі системи дають змогу вказати сукупність еквівалентних термінів за допомогою дужок, наприклад (*french francaise*). Слід також ураховувати існування різних словоформ (наприклад, різних закінчень), якщо така можливість надається системою. Наприклад, вираз *правов** може охоплювати слова «правовий», «правове», «правова» та ін. Деякі системи роблять це автоматично.

Формуюючи запит, слід передбачати, які нерелевантні документи можуть бути видані у відповідь на запит з такими словами або фразами. Крім омонімії в одній мові, можуть траплятись слова-омоніми, що належать різним мовам. Наприклад, спільними для української та російської мов є слова «лист», «приклад», «стан» та ін. За можливістю слід вказувати мову документів, що розшуковуються.

Варто також зважати, що деякі пошукові системи ігнорують так звані «**стоп-слова**» — прийменники, частки, сполучники і т. ін., а деякі їх враховують.

Виключити з пошукового запиту певні слова можна за допомогою оператора «NOT» (від англ. «не») або символу «-». Наприклад, запит *малі підприємства -кооперативи* означає, що зі списку знайдених ресурсів будуть виключені ті, в яких трапляється слово «кооперативи».

Після завершення обробки запиту система видає список посилань на Web-сторінки та інші елементи інформаційних ресурсів Інтернет. Деякі системи пропонують виконати повторний пошук «серед знайденого», що корисно в разі великої кількості виданих елементів. Перегляд та остаточне оцінювання знайдених результатів користувач має виконувати вручну.

Якщо система не знайшла документи, що відповідають указаному запиту, рекомендується вибрати ширший термін для пошуку. Наприклад, під час пошуку деякого закону США рекомендується спочатку знайти сервери з американським законодавством. Якщо пошук проводився за словосполученням, можна поослабити умови, виключивши із запиту одне або кілька слів.

Слід також пам'ятати, що в Інтернет існують ресурси, не охоплені пошуковими системами та пошуковими каталогами — так званий «**невидимий Web**». «Невидимий Web» можна розбити на дві частини:

- вміст спеціалізованих баз даних, які не зберігаються у вигляді певних Web-сторінок, а динамічно формуються спеціально у відповідь на конкретний запит до цієї бази;
- сторінки, які виключають з поля зору пошукової системи згідно з прийнятою політикою. За відсутності конкретних технологічних причин до бази даних пошукової системи можуть включатись тільки ті сторінки, що відповідають певному критерію. Особливо це актуально для пошукових систем з величезними обсягами індексів.

У будь-якому разі пошук інформації в Інтернет — це задача, яка вимагає творчого підходу, а стратегії пошуку повинні змінюватись залежно від результатів, що видаються у відповідь на запит. Опановувати їх доцільно ще й тому, що сфера використання інструментарію пошукових систем розширюється — створюються версії популярних систем для окремих вузлів Інтернет та корпоративних інтрамереж.

5.4.2. Пошукові агенти

За останні роки технології пошуку інформації в Інтернет змінилися завдяки пошуковим агентам.

Агент — це програма, розміщена у певному середовищі і здатна до гнучкої автономної поведінки для досягнення визначеної мети. Агент не тільки сприймає імпульси від середовища, в якому він функціонує, а й може змінювати його. У користувача не має необхідності втручатись у роботу агента, контролювати його дії або внутрішній стан. Гнучкість агента виявляється у його проактивності, здатності до змін і взаємодії з користувачами та іншими агентами.

Термін «агент» використовується в обчислювальній техніці вже понад 10 років. Початковою функцією агентів був поточний контроль за діяльністю центрального процесора та периферійного обладнання. Сьогодні агенти розрізняються за функціями, що вони їх виконують, зокрема, виділяють класи мобільних та інтелектуальних («розумних») агентів.

Мобільні агенти — програми, що переміщуються по базах даних і знань (зокрема, по Web-вузлах) для пошуку інформації. Звичайний агент розміщується в інформаційній системі користувача, у той час, коли мобільний переміщується в ту систему, в якій є дані, що їх слід розшукати, і після закінчення пошуку в одній базі може перейти до іншої системи. Для прискорення процесу пошуку мобіль-

ний агент може створювати підагентів і розсилати їх для паралельної роботи. Результати пошуку передаються користувачеві через мережу. Крім пошуку інформації мобільні агенти можуть виконувати ділові процедури, наприклад, агенти покупців і продавців, зустрічаючись в Інтернет, можуть укладати комерційні угоди.

Агенти, що їх позначають як *інтелектуальні*, крім названих вище функцій, можуть вести спостереження і здійснювати вимірювання, керувати комп'ютерними мережами, передавати повідомлення, сортувати електронну пошту. Програмні агенти змінюють людино-машинний інтерфейс — на їх основі розробляються інтерактивні персонажі, з якими можна спілкуватись і радитись.

Аналітики вважають, що застосування інтелектуальних мобільних агентів може призвести до порушення захисту інформації і зниження пропускнуої спроможності каналів передавання даних. Висловлюються попередження, що роботу агентів буде неможливо контролювати через їх поширення по мережах. Ці проблеми поки неактуальні, оскільки зрілі стандарти для підготовки і впровадження досконалих агентів відсутні.

Роботи з інтелектуальних агентів є відгалуженням досліджень зі штучного інтелекту. Для їх створення застосовується апарат нейронних мереж, нечіткої логіки, інтерпретації текстів природною мовою, колаборативної фільтрації (видачі рекомендацій індивідуальному користувачеві на основі відомостей про переваги певного співтовариства, до якого він належить). Незважаючи на великі можливості названих технологій, агенти поки не можуть стати дійсно розумними. До того ж для їх реалізації потрібні потужні суперкомп'ютери, розподілені сховища даних, ефективні низькорівневі технології пошуку та операційні системи, що підтримують виконання мобільного коду.

Але незалежно від їх втілення, програмні агенти мають одне спільне завдання — підвищення продуктивності та ефективності роботи користувачів. Для цього вони виконують таку кількість дій, яку людина не в змозі зробити самостійно через їх трудомісткість або складність.

З огляду на сказане найбільш актуальним напрямом використання програмних агентів є пошук і збирання інформації. Представниками класу програмних агентів є Web-роботи, які виконують індексування для пошукових систем. **Робот** — це програма, яка автоматично простежує гіпертекстові сторінки, вибираючи документ і рекурсивно переходячи на інші документи, що він на них посилається. Для визначення порядку переходу до наступної сторінки робот може застосовувати певні евристичні. Вживання ін-

ших назв роботів — мандрівник, кроулер, павук — призводить до непорозуміння, оскільки справляє враження, що програма переміщується між сайтами як мережний комп'ютерний вірус («черв'як», див. підрозд. 3.3), тоді як робот тільки звертається до сайтів, запитуючи документи. Такі програми пропонуються і кінцевим користувачам. При цьому слід зазначити, що звичайний Web-броузер не є роботом, оскільки ним керує людина і він не видає автоматично документи за гіперпосиланнями, за виключенням рисунків.

Пошукові агенти мають такі *переваги* порівняно зі звичайним зверненням до пошукових систем:

- пошуковий агент передає користувачеві не просто результати роботи пошукової машини (машин), а й попередньо переглядає документи і вибирає з-поміж них найбільш релевантні з його погляду;
- агент може налаштовуватись на переваги користувача, враховувати обмеження на пошук;
- деякі агенти можуть працювати в off-line режимі — користувач дає завдання агенту і відключається від Мережі, а агент виконує завдання на сервері і передає результати користувачеві, як тільки він знову підключиться. Агенти можуть бути настроєні на пошук за розкладом — шукати інформацію щогодини, щодня, щотижня, щомісяця і т. д. Ця можливість корисна, наприклад, при пошуку новин, інформації, яка постійно оновлюється або постійно потрібна в роботі;
- агенти можуть навчатись — користувач оцінює роботу агента, а той може скоректувати свої критерії відбору інформації, враховуючи ці оцінки.

Таким чином, пошукові агенти можуть розглядатись як інтелектуальна надбудова над пошуковими машинами.

5.5. ЗАКОНИ ТА ПІДЗАКОННІ АКТИ УКРАЇНИ В ІНТЕРНЕТ

На Web-сервері Верховної Ради України (<http://www.rada.gov.ua/>) з 1994 року функціонує система «Закони та підзаконні акти України в Інтернет».

Сайт має такі *розділи*: Конституція України, законодавство України, законопроекти, пленарні засідання, депутатський корпус, інформаційний сервер Верховної Ради, бібліотека Верховної Ради, уповноважений Верховної Ради з прав людини, міжнародні парламентські інститути, сайти парламентів зарубіжних країн, сторінки депутатських фракцій і груп.

У розділі «**Законодавство України**» представлені в останній редакції (із внесеними змінами) закони та підзаконні акти України —

документи Верховної Ради України, Президента України, Кабінету Міністрів, міністерств і відомств, органів судової влади тощо.

Відповідні Web-сторінки мають інформаційно-довідковий характер і не можуть замінити офіційних друкованих видань («Відомості Верховної Ради України», «Голос України», «Урядовий кур'єр», «Офіційний вісник України» тощо).

База даних «Закони та підзаконні акти України в Інтернет» технологічно пов'язана із системою «Картотека» ІС Верховної Ради України і є насправді копією бази даних останньої. Оновлення інформації здійснюється двічі в робочі дні та один раз у суботу.

Користувачеві пропонуються такі *режими пошуку*:

- пошук за видавниками і роками (пошук за ієрархією) — на лівій панелі вікна наведено алфавітний список видавників, навпроти кожного з яких висвітлюється кількість доступних документів, а на правій панелі — дерево видавників, яке можна розкрити, користуючись посиланнями. Перелік документів видається незалежно від їхнього типу, для кожного з них висвітлюється назва, реєстраційний номер, дата прийняття, розмір файла, іконка — ознака наявності та стану документа в базі;

- пошук на множині міжнародних документів — на лівій панелі представлено алфавітний список видавників міжнародних документів, а на правій панелі — форма пошуку з полями: країни та організації, типи документів, дата прийняття (період «з» і «по»), номер документа, слова в назві, тексті або абзаці тексту, логічний сполучник між словами, стан документів. Таким чином, пошук міжнародних документів може бути організований як за ієрархією, так і за реквізитами (див далі);

- пошук за реквізитами (універсальний). Картка для пошуку за реквізитами має такі поля (рис. 5.3).

- 1) видавники документів — якщо значення не вибрано, пошук здійснюється серед документів усіх органів влади;

- 2) типи документів — якщо не обрано жодного типу, пошук здійснюватиметься серед усіх типів документів. Для пошуку можна вказати до 10 можливих видавників і типів документів з відповідних списків;

- 3) дата прийняття — вибирається інтервал часу (початкова та кінцева дати) у форматі «ДД.ММ.РРРР» (день.місяць.рік). Якщо вказано рік до 1990 року, задані умови ігноруються і будуть знайдені усі документи, прийняті до 1990 року, незалежно від року прийняття. Якщо не заповнено поле кінцевої дати періоду, за замовчуванням приймається поточна дата. Кнопка «по» дає змогу

скопіювати значення першої дати у друге поле для можливого коригування. Для відміни виділених елементів можна вибрати посилання «зняти виділення» або кнопку «Очистити» для очищення всієї форми;

Пошук документів

Заповніть [форму](#) та натисніть кнопку "Шукати".

Форма для пошуку	
Знайти видавника	<input type="text"/>
Видавники документів (зняти виділення)	<div>Верховна Рада Президент Кабінет Міністрів Конституційний суд</div>
Типи документів (зняти виділення)	<div>Закон Постанова Розпорядження</div>
Дата прийняття з	<input type="text"/> по <input type="text"/>
Номер документа	<input type="text"/> вхідження
Реєстр.номер Мін'юсту	<input type="text"/> вхідження
Слова в	<input type="text"/>
Логічний сполучник	<input type="radio"/> або <input type="radio"/> та <input type="radio"/> ні
Стан документів	<input type="text"/>
Перед новим пошуком необхідно очистити форму!	
<input type="button" value="Шукати"/> <input type="button" value="Очистити"/>	

Рис. 5.3. Картка пошуку за реквізитами

4) номер. Документи можуть мати один або кілька номерів (залежно від кількості видавників), а можуть бути взагалі без номера, наприклад, міжнародні документи, форми типового документа тощо. У полі «номер» вводиться власний номер — номер, присвоєний органом влади, який видав цей документ. Власні номери можуть збігатися в документах різних органів влади, тому, організуючи пошук за цим реквізитом, бажано вказувати й інші критерії, наприклад, орган влади, тип документа, дату;

5) реєстраційний номер Мін'юсту можна використовувати для пошуку, пам'ятаючи, що він існує не для всіх документів. До внесення змін у 2002 році в картці пошуку як реєстраційний номер документа вказувався системний номер — номер, який надається документові перед уведенням його до бази даних і використовується виключно для ідентифікації документів та організації посилань між ними. У більшості випадків формати номерів, що зберігаються у базі, і ті, що вказані в текстах документів, різняться.

ся несуттєво або тотожні. Нині системний номер при пошуку не використовується.

Для номера і реєстраційного номера можна вказати відповідність: «точно» — номер повинен повністю збігатися із заданим; «входження» — в номері документа повинна бути присутня задана послідовність символів;

6) слова в назві, тексті, абзаці тексту — у цьому полі може бути розміщено не більше чотирьох слів або їх частин, розділених проміжками. Назва документа в базі даних подається завжди українською мовою, хоча деякі тексти документів (наприклад, міжнародні документи, коментарі, листи тощо) можуть бути російською. Мінімальна довжина слова для назви — 2 символи, для тексту — 3 символи. Розділові знаки, спецсимволи, подвійні лапки і цифри при пошуку ігноруються. Слова з'єднуються логічним сполучником за вибором користувача (див. наступне поле). У цьому полі можна вказати також дату у форматі «число/місяць/рік» або номер документа. Для точнішого контекстного пошуку рекомендується вибирати ознаку «в абзаці тексту», що дасть змогу знаходити документи, в тексті яких указані слова трапляються поряд. При цьому варто вибирати логічний сполучник «та». Для прискорення одержання результатів рекомендується обмежувати множину документів, серед яких вестиметься пошук, через визначення інших реквізитів;

7) логічний сполучник — «або», якщо у назвах (текстах) знайдених документів повинно бути присутнім хоча б одне із вибраних слів, «та» — у назві (тексті) кожного зі знайдених документів мають бути присутніми всі слова; «ні» — якщо слово не повинне траплятись у тексті. Наприклад запит *ні «внесен» ні «змін»* дозволить дібрати закони, які не вносять змін;

8) стан документа — «усі», якщо стан не враховується, «тільки чинні», «втратили чинність», «дію призупинено».

Результатом пошуку є список знайдених документів, для кожного з яких висвітлюється назва, реєстраційний номер, дата прийняття, розмір відповідного файлу, а також позначення наявності та стану документа в базі. Для виведення на екран список розбивається на частини, перехід між ними здійснюється натискуванням на відповідне посилання, що розміщене нижче від переліку документів. Для оперативного подання інформації введені так звані «сигнальні» копії документів — незредаговані тексти або відскановані зображення документів. Після підготовки та редагування ці «сигнальні» копії замінюються зредагованими текстами.

Картку документа можна відкрити, натиснувши іконку в лівому верхньому куті вікна тексту документа. Картка дає змогу перегляну-

ти реквізити документа, його терміни та історію, пов'язані документи та відомості про опублікування документа (див. приклад на рис. 5.4).

У системі передбачено кілька пар типів зв'язків між пов'язаними документами (у кожній парі перший тип зв'язку — прямий, а другий — зворотний), зокрема, «вводить в дію, ратифікує документи» — «вводиться в дію, ратифікується документом», «відсилає до» — «має відсилання з».

Картка документа: 40-97-п

Історія Пов'язані документи Публікації Повний текст

Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи

Постанова, Концепція від 20.01.1997 № 40
Кабінет Міністрів України
Стан документа: Чинний

Терміни документа

Історія документа

- 20.01.1997 - Прийняття

Пов'язані документи

Відсилає до :

1. Конституція України від 28.06.1996 № 254к/96-ВР (254к/96-вр)
2. Про Концепцію розвитку системи Міністерства внутрішніх справ від 24.04.1996 № 456 (456-96-п)
3. Про порядок виїзду з України і в'їзду в Україну громадян України від 21.01.1994 № 3857-XII (3857-12)
4. Про органи реєстрації актів громадянського стану від 24.12.1993 № 3807-XII (3807-12)
5. Про загальний військовий обов'язок і військову службу від 25.03.1992 № 2232-XII (2232-12)
6. Про громадянство України від 08.10.1991 № 1636-XII (1636-12)

Публікації документа

- - Офіційний вісник України 1997, N 4, стор. 35

[назад] [вгору]

Рис. 5.4. Картка документа

Термінологію документів також виділено в окремий пункт у розділі «Законодавство». Після пошуку (вибору) потрібного терміна за посиланнями можна відкрити документ, де наводиться його визначення.

Особливістю системи «Закони та підзаконні акти України в Інтернет» є можливість ознайомлюватись із *законопроектами*, які зареєстровані за поточний тиждень, внесені на розгляд протягом поточного тижня, перебувають на розгляді в комітетах, а також передивляти порівняльні таблиці, організовувати пошук законопроектів за реквізитами і вивчати статистичні дані, які відбивають законодавчу роботу Верховної Ради України. Передбачається пошук законопроектів за такими реквізитами: сесія розгляду, дата реєстрації (період «з» і

«по»), номер реєстрації, тип законопроекту, вид законопроекту, тип проекту, редакція законопроекту, юридичний рубрикатор, суб'єкт законодавчої ініціативи, автор — народний депутат України, назва законопроекту або слова з назви, стан законопроекту, ознака чинного закону, головний комітет, депутатська фракція.

5.6. ГЛОБАЛЬНА МЕРЕЖА ПРАВОВОЇ ІНФОРМАЦІЇ GLIN

Для науковців, які працюють у галузі права, законотворців, юристів з міжнародної торгівлі та багатьох інших фахівців україн необхідним є знання не тільки вітчизняного законодавства, а й міжнародного, так само як законів інших країн. Задовольнити таку потребу мала на меті Міжнародна правова база даних, створена 1976 року на базі Бібліотеки Конгресу США (The Library of Congress of the United States of America, <http://lcweb.loc.gov>). Ця база виправдала себе як простий та ефективний засіб швидкого і надійного доступу до складових правового середовища різних країн і з часом видозмінилася у *Глобальну мережу правової інформації (GLIN, Global Legal Information Network, <http://www.loc.gov/law/glin/>, рис. 5.5).*

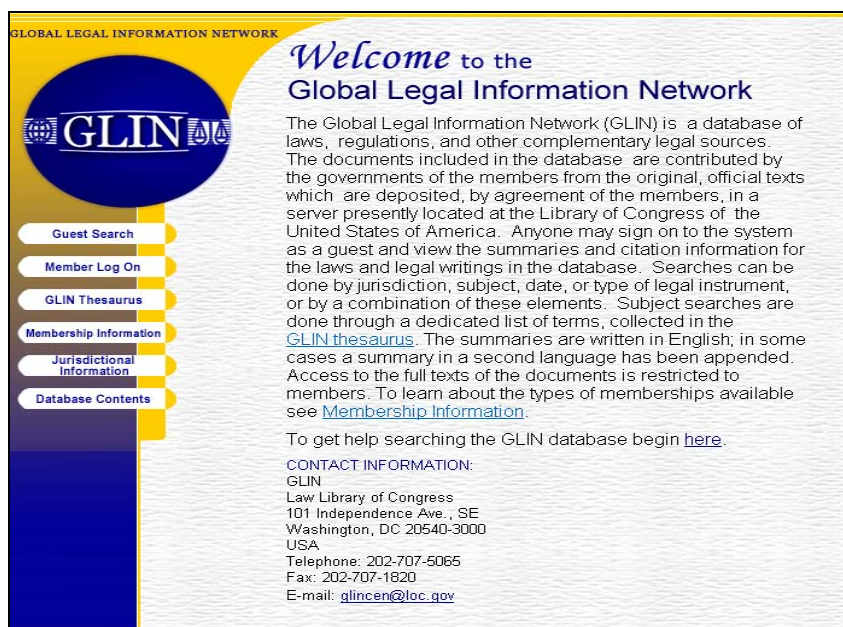


Рис. 5.5. Домашня сторінка GLIN

GLIN було засновано на таких *принципах*:

- достовірності джерел. Документи надаються урядами країн — учасниць проекту на основі офіційних текстів (з офіційного національного журналу із законодавства країни);
- простоти пошуку юридичних документів. Система може використовуватися тими, хто не має досвіду роботи з автоматизованими базами даних, і буде зрозумілою для осіб з різних культурних та освітніх середовищ;
- багатонаціональної орієнтації. GLIN відкрита для нових учасників з будь-якої країни світу.

Членом GLIN є й Україна. Секретаріат Верховної Ради України опрацьовує інформаційні бюлетені «Вісник Верховної Ради України» згідно з ідеологією та технологією робіт, прийнятими в GLIN, готує англійською мовою резюме законів України та постанов ВРУ з використанням тезауруса GLIN, надсилає їх разом з відсканованими повними текстами документів через мережу Інтернет до Бібліотеки Конгресу США, а також готує пропозиції щодо нових термінів для включення до тезауруса GLIN.

Можливості GLIN доступні і для учасників системи (CONTRIBUTOR), які підтверджують свій статус введенням ідентифікатора і пароля, і для будь-яких інших зацікавлених осіб (GUEST).

Основні елементи бази даних GLIN такі:

- повні тексти документів офіційною мовою держави походження;

- резюме або витяги з документів англійською мовою;
- тезауруси англійською та іншими офіційними мовами.

У GLIN використовуються такі *тезауруси*:

- тезаурус GLIN (Thesaurus for the Global Legal Information Network) — англословний тезаурус, який розвивається з 1950 року. Він декларується як незвичайний і, можливо, унікальний засіб пошуку правової інформації через прагматичність, орієнтацію на тривале використання, багатофасетність індексування світового законодавства;

- словник індексів законодавства (Legislative Indexing Vocabulary, LIV) — тезаурус, розроблений Службою досліджень Конгресу (Congressional Research Service) для роботи з матеріалами щодо законодавства та державної політики;

- тезаурус тематичних термінів для графічних матеріалів (Thesaurus for Graphic Materials I: Subject Terms, TGM_I), який містить тисячі термінів і численні перехресні посилання для індексування візуальних матеріалів;

- тезаурус жанрів і фізичних характеристик графічних матеріалів (Thesaurus for Graphic Materials II: Genre and Physical Characteristic Terms, TGM_II), розроблений підрозділом гравюр і фотографій Бібліотеки Конгресу (Prints and Photographs Division) з введенням інформації з інших сховищ архівних зображень.

Для створення, підтримки і роздрукування тезаурусів використовується новітня платформонезалежна інтерактивна система управління тезаурусами *Lexico* (розробник — Project Management Enterprises, Inc.). Система створена на основі мови програмування Java, підтримує клієнт-серверну архітектуру з тонким клієнтом, доступна через Web. Lexico забезпечує створення інтерактивних тезаурусів, які містять терміни, зв'язки між ними, а також обґрунтування, супроводжувальну документацію та відомості про затверджений статус кожного терміна.

Lexico забезпечує такі *основні лексикографічні функції*:

- взаємні посилання — термін вищого рівня (Top term), термін нижчого рівня (Lower term), ширший термін (Broader term), вужчий термін (Narrower term), пов'язаний термін (Related term), «використовує» (Use), «використовується» (Used for);
- автоматичне занесення всіх названих посилань при встановленні зв'язку між термінами;
- автоматична підтримка ієрархії тезауруса;
- ведення пояснювальних приміток.

Lexico не обмежує максимальну довжину елементів тезауруса, кількість рівнів ієрархії та кількість термінів, які можуть брати участь у певному зв'язку. Система автоматично впорядковує терміни за алфавітом, запобігає дублюванню елементів, установленню неправильних зв'язків або зв'язків з невизначеними термінами.

Для неавторизованих користувачів доступні тільки функції пошуку даних. Внесені зміни, якщо вони припускаються конкретним варіантом інсталяції, не будуть записані в тезаурус. Пропонується надсилати свої пропозиції електронною поштою.

Для *пошуку термінів у тезаурусі* задаються такі реквізити:

1) тип запити:

- Term — запис з терміном — пошук терміна, найближчого за написом до введених символів;
- Keyword — ключове слово з контексту — пошук слова, найближчого до введених символів за ключовим словом, включаючи терміни, що містять це слово. Рекомендується для визначення релевантних термінів, коли перше слово невідоме. Наприклад, запит «war» («війна») приведе до видачі термінів «Moral aspects of

war» («Моральні аспекти війни»), «Nuclear war» («Ядерна війна»), «War casualties» («Втрати на війні»);

2) опції пошуку терміна: «Term records» — на екран будуть виведені терміни, зв'язки і примітки; «Hierarchy» — передбачається виведення тільки ширших та/або вужчих термінів, «Hyperlinks» — зв'язки з іншими базами даних.



GLIN — реквізити резюме законів

Для зберігання резюме законів (Law Summary) у GLIN передбачені такі реквізити:

▲ PUBLICATION (публікація, обов'язкове поле) — заголовок офіційного видання, газети, реєстру, бюлетеню тощо;

▲ INSTRUMENT CLASS (клас інструменту, обов'язкове поле) — звичайно визначається призначенням: акт, закон, декрет, резолюція або ін. залежно від термінології країни;

▲ INSTRUMENT NUMBER (номер інструмента) — номер, який присвоєно конкретному інструменту органом, що він його випустив. Поле є обов'язковим для заповнення, якщо запитується;

▲ PUBLICATION DATE (дата публікації, обов'язкове поле) — дата, вказана на титульній сторінці офіційного видання у форматі DD/MM/YYYY (день/місяць/рік);

▲ ISSUANCE DATE (дата введення у дію, обов'язкове поле) — дата набрання чинності, вказана у тексті нормативного акта у форматі DD/MM/YYYY (день/місяць/рік);

▲ PUBLICATION NUMBER (номер публікації, необов'язкове поле) — номер у форматі, вказаному на титульній сторінці офіційного видання;

▲ OFFICIAL TITLE (офіційна назва, необов'язкове поле) — заголовок нормативного акта;

▲ PDF (обов'язкове поле) — посилання на файл з повним текстом. Назва файла складається з двохлітерного коду країни за стандартом ISO, дати публікації у форматі ddtтuuуу і двох цифр, які визначають номер файла, переданого у цей день;

▲ SUBJECT TERMS (тематичні терміни, обов'язкове поле) — слова і фрази з тезауруса GLIN;

▲ SUMMARY DESCRIPTION (опис резюме, обов'язкове поле) — слова і фрази, вибрані з повного тексту і граматично узгоджені для правильного відображення його змісту. Резюме включає номери постанов, статей, та/або розділів і сторінок, на яких розміщено текст;

▲ PUBLICATION SPECIFICS (характеристики публікації, необов'язкове поле) — додаток, екстраординарний випуск, перша секція тощо;

▲ STATUS (статус, необов'язкове поле) — наприклад, «Amends» (вносить поправки), «Regulates» (регулює), «Repeals» (анулює), «Amended by» (змінюється), «Regulated by» (регулюється), «Repealed» (анулюється);

- ▲ *REFERENCE* (посилання, необов'язкове поле) — наприклад, «Jurisprudence» («юриспруденція»), «Case law» («судова справа»), «Legislative Background» (пояснення), «Literature» (література), «Other Language Version» (версії іншими мовами);
- ▲ *GLIN THESAURUS* — терміни з тезауруса GLIN.

Крім операцій з нормативними актами, членам GLIN також надається можливість вводити, шукати та оновлювати **резюме правових документів** (Legal Writings), до яких відносять статті з оглядом законів, звіти, думки, коментарі. Для систематизації матеріалів такі документи повинні, де це можливо, мати зв'язок з основними документами, вже розміщеними у GLIN, шляхом вказівки унікального номера резюме закону. При цьому для підтримки цілісності матеріалів окремої країни дозволяється встановлювати зв'язок тільки з резюме законів цієї країни (навіть якщо документ стосується законодавства інших країн).



GLIN — реквізити правових документів

Для зберігання правових документів у GLIN передбачено такі реквізити:

- ▲ *PUBLICATION COUNTRY/ENTITY* (обов'язкове поле) — назва країни або установи, де було опубліковано документ;
- ▲ *PUBLICATION LANGUAGE* (обов'язкове поле) — мова публікації;
- ▲ *IID(S) OF LEGAL SUMMARY(IES) TO BE ASSOCIATED* (ідентифікатори резюме, що пов'язані з документом, необов'язкове поле) — унікальний номер, який ідентифікує певний запис і автоматично присвоєний цьому запису у процесі його створення;
- ▲ *NAME OF PUBLISHING ORGANIZATION* (назва організації-видавця, необов'язкове поле) — назва державної, академічної або приватної установи, яка видала публікацію;
- ▲ *PUBLICATION NAME* (назва публікації, необов'язкове поле) — назва журналу, бюлетеня, звіту, газети або монографії, що містить цей документ;
- ▲ *PUBLICATION SPECIFICS* (характеристики публікації, необов'язкове поле) — спеціальні характеристики видання (період публікації, якщо точна дата невідома, номер тому або випуску);
- ▲ *PUBLICATION DATE* (дата публікації, обов'язкове поле) у форматі DD/MM/YYYY («день/місяць/рік»). Якщо документ опубліковано у кварталному, сезонному або періодичному виданні (за кілька місяців), вказується дата першого дня місяця, в якому видано публікацію;
- ▲ *TITLE OF LEGAL WRITING* (заголовок документа, обов'язкове поле);
- ▲ *AUTHOR* (автор, обов'язкове поле) — ім'я та прізвище автора (авторів);

▲ *PDF* (необов'язкове поле) — посилання на повний текст документа у pdf-форматі. Назва файлу складається з двохсимвольного коду країни за стандартом ISO, символів «lw» («legal writing»), дати публікації у форматі DDMMYYYY та порядкового номера документа з даною датою публікації у базі даних;

▲ *URL* (необов'язкове поле) — адреса тексту документа у WWW у форматі URL;

▲ *SUBJECT TERMS* (тематичні терміни, обов'язкове поле) — слова і фрази з GLIN THESAURUS, присвоєні резюме згідно з ієрархічними зв'язками та відповідністю;

▲ *SUMMARY DESCRIPTION* (опис резюме, обов'язкове поле) — граматично скомпоновані слова і фрази з повного тексту, які відбивають його зміст.

Крім резюме законів та правових документів, GLIN містить відокремлений розділ «Guide to Law Online» («Гід права on-line») — анотований гіпертекстовий гід безплатних правових та урядових матеріалів усього світу, доступних в режимі on-line. Цей гід містить посилання тільки на найбільш корисні та надійні сайти, хоча включення сайту до списку не означає схвалення Правової Бібліотеки Конгресу, Дирекції бібліотечних послуг або Дирекції правових досліджень. Жодний із вказаних сайтів не визнано як такий, що повністю відповідає вимогам GLIN щодо повноти, точності та офіційно підтвердженої достовірності текстів, що вони їх надають. Перевага надається сайтам, які пропонують повні тексти законів, положень, судових рішень, а також коментарі юристів, написані для фахівців з права. До списку також включено урядові сайти, які надають загальну інформацію про себе та свої агенції.

У «Guide to Law Online» виділено підрозділи матеріалів Сполучених Штатів Америки («GUIDE: United States»), національних (GUIDE: Nations), міжнародних та міжнаціональних (GUIDE: International and Multinational) та об'єднаних за темами (GUIDE: Subjects) матеріалів.

5.7. ПОШУК ДОКУМЕНТАЦІЇ З ЄВРОПЕЙСЬКОГО ЗАКОНОДАВСТВА В ІНТЕРНЕТ

Вибір інструмента пошуку документації з Європейського законодавства залежить від поставлених цілей і має враховувати особливості конкретних сайтів і баз даних.

Головним інструментом загального бібліографічного пошуку є *Каталог бібліотек Європейської Комісії* (European Commission Libraries Catalogue, *ECLAS*, <http://www.europa.eu.int/eclas/>).



Інформаційний пошук — кілька видів

Інформаційний пошук — дії, методи та процедури для знаходження у фонді необхідної інформації.

Документальний пошук — дії, методи та процедури для знаходження у фонді необхідних документів.

Бібліографічний пошук — документальний пошук, який здійснюється з метою знаходження бібліографічних описів документів, що відповідають інформаційному запиту, без видачі самих документів.

Довідковий пошук — дії, методи та процедури для пошуку в інформаційній системі всіх видів посилань, що відповідають інформаційному запиту.

Існує три способи пошуку в базі даних ECLAS: простий пошук, експертний пошук і пошук за допомогою тезауруса. Якщо точна назва документа, що розшукується, невідома, можна скористатися пошуком за словом з назви або вибрати термін у термінологічній пошуковій системі («thesaurus search system»). Пропонуються дескриптори англійською і французькою мовами. Для пошуку матеріалів із законодавства ЄС ключовим словом є «EU/EC law» або «EU/EC policy» разом з іншими критеріями. До більшості дескрипторів, які стосуються європейських питань, на початку додається «EU/EC».

«Експертний пошук» рекомендується використовувати для пошуку інформації щодо певної статті договору або вторинного законодавчого акта. При цьому вводиться номер потрібного документа CELEX (див. далі). Ця функція не є повною, але якщо у документі існує хоча б одна стаття з визначеного питання, система виведе посилання до її тексту.

За допомогою підрозділу ECLASPro можна записати запит у формі профілю пошуку, і ECLAS щотижня надсилатиме електронною поштою нові посилання на публікації або статті в цій галузі.

Колекція ECLAS не обмежується матеріалами з Європейської тематики, при цьому вона містить документи всіма мовами. Навіть за умов відсутності фізичного доступу до цієї бібліотеки її каталог може стати в нагоді для подальшого пошуку. Каталог також містить опцію «Ресурси Інтернет» (Internet Resources) з переліком доступних в Інтернет сайтів і документів, які вважаються важливими.

Безпосередньо *тексти нормативних документів* можна знайти у базах EUR-Lex і CELEX.

EUR-Lex (<http://www.europa.eu.int/eur-lex>) — база даних з поточного Європейського законодавства одинадцятьма європейськими мовами. EUR-Lex було реалізовано у рамках політики про-

зорості ЄС — з 1 січня 2002 року все чинне законодавство Співтовариства доступне для користувачів Інтернет. EUR-Lex надає безкоштовно будь-який закон чи підзаконний акт, затверджений Європейськими установами, протягом 45 діб з дати його публікації в Офіційному журналі Європейських Співтовариств¹. Після цього даний документ можна придбати на Celex або замовити на компакт-диску².

CELEX (<http://www.europa.eu.int/celex>) є найбільшою повною платною регулярно оновлюваною базою даних з Європейського законодавства, яка містить усі угоди, що їх було коли-небудь укладено, директиви та рішення Європейського Суду одинадцятьма мовами.

І EUR-Lex, і CELEX надають користувачеві документи у форматах HTML, PDF, TIFF.

Відмінність між порталом EUR-Lex і законодавчою базою CELEX, крім платності послуг останньої, полягає у способі реалізації. Якщо завдання полягає у пошуку повного тексту документа Співтовариства, адекватним інструментом для цього є EUR-Lex. CELEX є інструментом, який було розроблено спеціально для юристів-професіоналів і має такі додаткові корисні опції: доступ до всіх актів прецедентного права, доступ до заходів з імплементації на національному рівні, огляд двома мовами, більший набір пошукових критеріїв, вибір мови експертного пошуку, опція «Звузити пошук» («Narrow down your search»), аналітична інформація (дескриптори, дати, перехресні посилання та ін.), он-лайн підтримка і панель допомоги.



Європейське законодавство — кілька джерел

Хоча більшість спеціалізованих журналів і монографій поки що не доступні в Інтернет, кількість матеріалів, що подаються в електронному вигляді академічними та офіційними установами, постійно зростає. Значна кількість міжнародних організацій публікують повні тексти робочих документів, що стосуються європейських питань, віддаючи пріоритет економічним аспектам.

¹ Період між датою прийняття акта однією або кількома установами і датою публікації в Офіційному журналі Європейських Співтовариств може варіюватися від кількох днів до кількох місяців.

² Крім CELEX та EUR-Lex, на ринку пошукових інструментів діють приватні компанії, які пропонують портали зі зведеною інформацією щодо Співтовариства, включаючи законодавство, яке зазвичай одержується з бази даних CELEX.

Прикладами є:

- ▲ сайт Ради Європи <http://www.coe.fr/>;
- ▲ база угод і конвенцій Ради Європи <http://conventions.coe.int/>;
- ▲ Бюлетень Європейського Союзу <http://europa.eu.int/abc/doc/off/bull/en/welcome.htm>;

▲ Офіційний журнал Європейських Співтовариств <http://publications.eu.int/general/en/oj-en.htm>.

Серед українських джерел, крім сайту Верховної Ради України (<http://www.rada.gov.ua/>), слід відзначити:

▲ сайт Центру порівняльного права при Міністерстві юстиції України <http://www.comparativelaw.kiev.ua/>, створеного для науково-аналітичного забезпечення стратегічного курсу інтеграції України до ЄС у правовій сфері;

▲ сайт Українсько-Європейського консультативного центру <http://www.uerplac.kiev.ua/>, який містить базу даних про міжнародні угоди України з тематичною спрямованістю на європейську інтеграцію, тематичні та аналітичні статті, а також посилання на інші європейські бази даних із законодавства;

▲ сайт Бюро інформації Ради Європи в Україні <http://www.coe.kiev.ua/>, який містить деякі угоди та конвенції, укладені Радою Європи, українською мовою.

Серед значних європейських бібліографічних інструментів пошуку слід виділити такі:

▲ Архів європейських дослідницьких робіт (European Research Papers Archive, <http://eior.or.at/erpa/>);

▲ Бібліотека Інституту Європейського Університету (European University Institute library, <http://www.iue.it/LIB/>) містить перелік академічних, офіційних і приватних установ, які публікують робочі документи, що так або інакше стосуються європейських питань;

▲ Електронний бюлетень європейської документації (Electronic Bulletin of European Documentation, <http://www.euro.ucl.ac.be/ebed/>) оновлює раз на два тижні огляд головних електронних робочих документів, опублікованих за цей період.

Якщо відомі точні дані документа (наприклад, Directive 97/15 EC), EUR-Lex передбачає пошук чинного акта за його номером. У системі виділено окремі опції пошуку директив, рішень і регламентів. Аналогічно організується пошук і через підписну базу даних CELEX. В EUR-Lex може бути організований пошук документа за датою публікації. CELEX має більші можливості — як критерій пошуку можуть бути задані дата прийняття, дата публікації в Офіційному журналі, дата набрання чинності, дата вступу у дію або дата закінчення дії акта.

Пошук за словом у тексті/назві, яке можна задати, коли точні реквізити документа невідомі, неефективний, оскільки у більшо-

сті випадків результати не точні і містять величезну кількість посилаць. Тому і EUR-Lex, і CELEX пропонують схожі опції пошуку за темою. Документи в базі індексуються відповідальними особами. Процедура пошуку полягає у послідовному виборі потрібного розділу. Результати, що їх одержують у такий спосіб, є відносно повними, але слід враховувати той факт, що іноді документ Співтовариства може належати двом різним розділам. Навіть якщо пошуковий індекс містить записи в різних розділах, може статися так, що доведеться розширити межі пошуку.

Варто зважати, що результати пошуку в EUR-Lex та CELEX надаються по-різному — у кожній загальній категорії CELEX виділено підкатегорії, EUR-Lex обмежується загальними актами. При цьому CELEX надає анотацію до кожного документа з переліком актів, якими вносяться зміни, тоді як EUR-Lex просто зазначає їх існування. У режимі експертного пошуку в CELEX можуть бути використані дескриптори багатомовного тезауруса EUROVOC.

Доступ до документів CELEX ускладнюється тим, що до кожної статті організований окремий доступ. Наприклад, для пошуку Паризького Договору 1951 року, яким засновується Європейське співтовариство вугілля та сталі, необхідно спочатку шукати у розділі «Законодавство» (Legislation), потім — у розділі «Установчі договори» (Founding Treaties), потім — за датою, яку потрібно знати. Результат пошуку видається у формі 199 документів-секцій, які охоплюють усі статті та додатки до даного договору. Цей спосіб пошуку використовується, коли не існує альтернативи.

Процедура значно спрощується, якщо відомий номер потрібної статті договору. Наприклад, стаття 86 Римського договору, ухваленого в 1957 році, має номер 11957E086, де 1 вказує на первинне законодавство/договори, 1957-й — рік підписання, E — Римський договір, 086 — номер статті. При цьому слід враховувати, що після набрання чинності Амстердамського договору відбулась перенумерація статей договорів.

Коли введено тільки перші шість знаків (у даному прикладі — 11957E), CELEX виводить на екран усі статті договору та додатки до нього. На цій стадії можна обмежити пошук, обравши опцію «contents» (зміст) для того, щоб відкрити вікно, в якому надається загальний список вибраних документів, включаючи відповідні протоколи та декларації з їхніми кодами. Пошук статті за номером і виведення тексту в режимі «all» (все) дає можливість продивитись не тільки повний текст статті, а й рішення суду, які впливають на акт.

Ще однією відмінністю між системами є те, що EUR-Lex, коли це необхідно, надає **консолідовану** версію документа. Варто зазначити, що не всі документи доступні у консолідованих версіях, оскільки їх створення — тривалий складний процес. З цієї самої причини при роботі з консолідованою версією слід звертати увагу на дату консолідації — до документа можуть бути внесені зміни вже після неї. Консолідовані версії документів у базу даних CELEX внесено протягом 2002 року.



Правові ІПС — консолідація

Консолідація — це внесення до основного законодавчого акта Співтовариства наступних змін і поправок та об'єднання їх в єдиному документі. Одержаний документ не має офіційного статусу та юридичної сили. Юридично автентичними є версії в тому вигляді, в якому вони були підписані та опубліковані в Офіційному журналі Європейських Співтовариств. Поступова консолідація документів Співтовариства проводиться Бюро публікацій ЄС (Publications Office of the EC), але це робиться тільки в документальних цілях, без прийняття відповідальності за зміст таких документів. Водночас юристи переважно працюють з консолідованими версіями, якщо такі існують, оскільки інакше фактично неможливо прочитати документ, який змінювався кілька десятків разів.

У деяких випадках юристам потрібно звернутися до оригінальної версії документа. Такі тексти в електронному вигляді доступні на сайті «Європейський Навігатор» (European Navigator, ENA, <http://www.enafree.lu>), який є проектом уряду Люксембурга, присвяченим історії Європейського Союзу.

Беручи до уваги швидкість консолідації текстів Співтовариства і поступове тлумачення законодавчих актів у Союзі та державах-членах, Законодавчий Департамент та Інститут Європейського Університету розробляють академічний сайт під назвою «Консолідація європейського публічного законодавства» (Consolidating European Public Law, <http://www.iue.it/LAW/conseulaw/>), присвячений цій проблемі.

За допомогою опції «Display the national implementing measures» («Показати заходи щодо імплементації на національному рівні»), доступної при виборі опції перегляду документа у форматі HTML «all/HTML», у CELEX можна одержати посилання на матеріали щодо введення певного акта до національних законодавств. EUR-Lex у розділі «Documents of public interest» (документи публічного інтересу) містить річні звіти з моніторингу

виконання законодавства Співтовариства («Annual report on monitoring the application of Community law»), які описують актуальний стан виконання законодавства Співтовариства державами-членами і перераховують усі справи про його порушення та судові розгляди щодо останніх.

Інша опція CELEX — «Select all documents mentioning this document» («Вибрати всі документи, які згадують цей документ») — дає можливість знайти акти прецедентного права, які стосуються одного або кількох документів вторинного законодавства.

Найефективнішим способом пошуку повних текстів угод між Європейськими Співтовариствами і третіми державами або міжнародними організаціями є експертний пошук CELEX, в якому назва третьої держави (дескриптор EUROVOC) може застосовуватися разом з іншими критеріями, які відносяться до зовнішніх відносин. EUR-Lex надає перелік таких угод за географічними зонами, тому рекомендується проводити пошук у два етапи:

- одержати посилання на угоди на сайті Бюро угод Ради Європи (Council's Agreements Office, <http://ue.eu.int/accords/>). Пошук у цій базі може виконуватись за словом з назви, за датою підписання, за сторонами, які підписували документ. Для кожної угоди виводиться назва, посилання на публікацію в Офіційному журналі Європейських Співтовариств (якщо така є), дати підписання та набирання чинності, а також перелік сторін, які підписали договір;

- шукати угоду в Довіднику чинного законодавства EUR-Lex, використовуючи посилання на публікації в Офіційному журналі Європейських Співтовариств.

Огляди щодо поточного стану відносин між ЄС (стосовно кожної держави-члена), групами держав, міжнародними організаціями та щодо поточних міжнародних справ можна знайти на сайті Генерального Директорату Європейської комісії із зовнішніх відносин (European Commission's Directorate General for External Relations, http://www.europa.eu.int/comm/external_relations/index.htm). Додаткову інформацію можна знайти на сайтах європейських делегацій у третіх державах та міжнародних організаціях (http://www.europa.eu.int/comm/external_relations/delegations/intro/web.htm), на офіційних сайтах держав, які є членами угоди.

Основним джерелом для одержання рішень і наказів Європейського Суду Справедливості і Суду Першої Інстанції та думок генерального адвоката в електронній формі є сайт названих установ **Curia** (від лат. «curia» — приміщення для засідань,

<http://curia.eu.int/>), який надає доступ до повних версій рішень усіма офіційними мовами здебільшого вже у день їх видання. Пошук можна організувати за номером справи, хронологічним періодом, назвами сторін, обставинами справи або за словом з тексту. Додатково на сайті розміщується щотижневий інформаційний бюлетень «Proceedings of the Court of Justice and the Court of First Instance of the European Communities» (Засідання Суду Справедливості та Суду Першої Інстанції Європейських Співтовариств, <http://curia.eu.int/en/act/index.htm>), який містить конспекти винесених рішень, цитати думок генеральних адвокатів і перелік тільки-но поданих справ.

Для фахівців з судових органів Європейських Співтовариств сайт Curia має розділи «Introduction to the institution» (Введення до установи) і «Texts relating to the institution» (Тексти стосовно установи), які містять Статути Судів, відомості про членів та правила процедури Суду Справедливості та Суду Першої Інстанції, інформацію щодо тактики поведінки у суді, а також іншу інформацію довідкового характеру.

Документи з прецедентного права можна одержати і в EUR-Lex та CELEX. Портал EUR-Lex надає доступ до повних текстів рішень та думок генеральних адвокатів на основі номера справи, назви сторін, слова у тексті або посилання на публікацію у Відомостях Європейського Суду (European Court Reports). Меню пошуку CELEX містить більшу кількість пошукових критеріїв, наприклад, за предметом розгляду або типом розгляду, і додаткові опції — посилання на коментарі щодо рішень, перехресні посилання, перегляд тексту двома мовами. Опція експертного пошуку CELEX надає можливість комбінувати ще більшу кількість критеріїв у формі булевого запиту з використанням сполучників «and» (і), «or» (або), «except» (за винятком) та ін. і обмежувати пошук до певного аспекту рішення (підстави позову, предмет спору, сторони, захисник, суддя-доповідач, генеральний адвокат та ін.).



Контрольні запитання і завдання

1. Які категорії інформаційно-пошукових систем виокремлюють?
2. За якими критеріями можна оцінити роботу інформаційно-пошукової системи?
3. Обґрунтуйте необхідність створення штучних інформаційно-пошукових мов.

4. Яке призначення та зміст мають тезауруси інформаційно-пошукових систем?

5. Які типи семантичних відношень передбачено в тезаурусі EUROVOC?

6. Надайте порівняльну характеристику можливостей інформаційно-пошукових систем «ЛІГА:ЗАКОН», «Нормативні акти України» та системи «Закони та підзаконні акти України в Інтернет».

7. Визначте критерії для вибору стратегії пошуку правової інформації в Інтернет.

8. Назвіть основні складові Глобальної мережі правової інформації GLIN та схарактеризуйте їх.

9. Назвіть основні інструменти пошуку інформації з Європейського законодавства в Інтернет та схарактеризуйте їх.

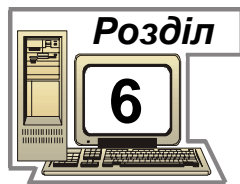


Література

1. ДСТУ 2394-94. Інформація та документація. Базові поняття. Терміни та визначення. — К.: Держстандарт України, 1994. — 53 с.

2. Матеріали сайтів <http://www.comparativelaw.kiev.ua/>, <http://europa.eu.int/>, <http://www.liga.kiev.ua>, <http://www.nau.kiev.ua/>, <http://www.rada.kiev.ua/>, <http://www.loc.gov/glin/>, <http://www.lib.berkeley.edu/>.

3. Ситник В.Ф. та ін. Основи інформаційних систем: Навч. посібник. — Вид. 2-ге, перероб. і доп. — К.: КНЕУ, 2001. — 420 с.



ІНФОРМАЦІЙНІ СИСТЕМИ ЗАКОНОДАВЧИХ ОРГАНІВ

6.1. ОСНОВНІ НАПРЯМИ РЕАЛІЗАЦІЇ ПРОЕКТІВ З ТЕЛЕДЕМОКРАТІЇ

Сьогодні в усьому світі спостерігається дедалі більше відчуження політиків від пересічних громадян і спад інтересу останніх щодо політичних проблем. Відповідно, починаючи з останньої декади XX століття у багатьох країнах було започатковано дослідження та проекти, спрямовані на пошук шляхів стимулювання демократичних процесів з використанням сучасних телекомунікаційних технологій. Пілотні проекти включають системи телеконференцій, публічні інформаційні термінали, системи телевізорів тощо. Усі такі зусилля позначаються як «теледемократія».

Теледемократія (teledemocracy) — використання телекомунікаційних технологій для більшого залучення громадян у політичні процеси на основі поліпшення передавання політичної інформації та думок між громадянами, політиками і виконавчою владою.

Демократична система має чотири складові — громадян, законодавців (політиків), виконавчу владу і судову систему. Незалежність останньої пояснює виключення її зі сфери таких досліджень, а решта складових є рівноцінними.

Очевидно, що впровадження новітніх інформаційних технологій має на меті автоматизацію не тільки діяльності окремих структур, а й інформаційної взаємодії між ними. Зв'язки громадян з органами влади забезпечують різноманітні системи електронної комерції за участю держави (див. розд. 4). Не менш важливими є інформаційні взаємозв'язки між законодавчою та виконавчою гілками влади.

Основою для виявлення та формулювання проблем, які потребують правового врегулювання, є оперативні та статистичні дані, що охоплюють усі аспекти життя суспільства і держави; засідання Верховної Ради України та інших органів вищої влади; соціологічні дослідження, рішення, звернення громадських організацій та партій; міжнародна інформація, світовий досвід; листи та звернення громадян, організацій і т. ін.

При цьому роботу законодавця (депутата) неможливо відокремити від його діяльності як політика. З урахуванням існування як формальних (офіційних) інформаційних потоків та процедур прийняття рішень, так і неформальних, автоматизоване забезпечення законотворчої діяльності має відбуватись у трьох напрямках — підтримка роботи парламенту; надання доступу до нагромаджених даних, що їх можна використати у процесі прийняття рішень; забезпечення комунікацій між політиками та їх зв'язків з органами державної влади і громадськістю.

З 1990 року у Верховній Раді України функціонує інформаційно-аналітична система, яка охоплює весь цикл забезпечення законотворчої та правозастосовної діяльності. Автоматизовані збирання, накопичення та аналіз даних з проблем, які потребують нормативно-правового регулювання; підготовка проектів нормативно-правових актів; колективне обговорення пропозицій; порівняльний аналіз, узгодження, прийняття (голосування); оперативне доведення їх до застосування на практиці; оброблення інформації і зворотний зв'язок про наслідки дії чинного законодавства та аналіз даних для прийняття рішень.

Система надає послуги не лише структурним підрозділам Верховної Ради України, а й тисячам користувачів державних і недержавних організацій, установ, закладів і підприємств, фізичним особам як в Україні, так і за її межами.

Комп'ютерна мережа, на основі якої реалізовано систему, розташована у 8 будинках Верховної Ради і об'єднує близько 400 робочих станцій. Середовищем передавання є 5 км волоконно-оптичного кабелю і понад 20 км кабелю скрученої пари. Основними *принципами побудови мережі* є висока пропускна спроможність передачі даних, ізоляція інформаційного трафіку для кожного будинку і кожного поверху в будинку, управління комп'ютерною мережею з центрального вузла, інтеграція побудови комп'ютерної мережі Верховної Ради України в регіональну мережу м. Києва та глобальну мережу України і світу, захист від несанкціонованого доступу.

Комп'ютерна мережа Верховної Ради України має вихід до Інтернет через вузли СП «Інфоком» та Українського об'єднання електрозв'язку «Укртелеком».

Доступ до інформації надається з робочих місць секретаріатів постійних комітетів, фракцій, груп та підрозділів Верховної Ради.

У структурі ІС Верховної Ради України виділено кілька функціональних і забезпечуючих підсистем (див. далі). У свою чергу, деякі з цих підсистем складаються з окремих комплексів. Напри-

клад, підсистема спеціалізованих комплексів управління законодавчим процесом містить комплекси «ПЛАН», «Реєстрація та контроль проходження законопроектів», «Контроль за проходженням документів у підрозділах», «Контроль виконання доручень і запитів народних депутатів України та інформування», інформаційно-аналітичний комплекс «Вибори». Крім того, ця підсистема містить окремі офісні завдання, що функціонують у структурних підрозділах («Кадри», «Бухгалтерія» та ін.).

Інтегрована база даних системи містить юридичну, соціально-економічну та іншу інформацію, зокрема: відомчі нормативні акти; матеріали із зарубіжного законодавства; каталоги літератури; фонди інформаційних агентств світу; стенограми засідань Верховної Ради України, інших зібрань та обговорень; пропозиції до законопроектів; результати голосувань; програми народних депутатів, партій, рухів; статистичні дані міністерств, відомств, соціологічних досліджень; звернення, скарги і пропозиції громадян, організацій тощо; відомості щодо проблем держави і суспільства.

Така інформація може надаватись користувачам на локальні ПЕОМ у вигляді протоколів поновлення, з використанням локальної мережі та мережі Інтернет, на компакт-дисках, електронною поштою у вигляді окремих файлів або протоколів. Електронна пошта, зокрема, вважається фахівцями одним із механізмів забезпечення демократичності прийняття рішень. На відміну від телефону, який закріплює існуючі інформаційні потоки, електронна пошта вирівнює участь окремих осіб в обговореннях і прийнятті рішень незалежно від їх віку, статі або соціального статусу.

Поширення матеріалів в електронному вигляді прискорює їх доставку і виключає рутинну роботу — розмноження, розкладання документів у конверти, пересилання. Дешевість такого передавання дає можливість збільшити кількість абонентів. Перевагами є також більший ступінь секретності порівняно зі звичайною поштою та асинхронність — передавання повідомлення та його одержання можуть бути розділені у часі.

6.2. ІНФОРМАЦІЙНО-ТЕХНІЧНИЙ КОМПЛЕКС «РАДА»

Інформаційно-технічний комплекс (система) «РАДА» призначений для комп'ютерного забезпечення реєстрації та голосування народних депутатів, супроводження пленарних засідань Верховної Ради України, накопичення інформації про роботу народних

депутатів, а також стенографування — комп'ютеризовану підготовку стенограм засідань Верховної Ради України в режимі реального часу. Система використовується як під час засідань, так і при проведенні аналізу роботи парламенту та фракцій народних депутатів.

Інформацією, що її видає система «РАДА», мають змогу користуватись не тільки народні депутати, а й працівники аналітичних підрозділів секретаріатів Комітетів Верховної Ради України, груп і фракцій народних депутатів, відповідних служб адміністрації Президента та Кабінету Міністрів України.

Система складається з кількох *спеціалізованих автоматизованих робочих місць*:

- АРМ «Адміністратор» є головною складовою системи. Його основними функціями є проведення голосувань і реєстрацій; запис на виступ з місця; оброблення результатів та видача їх на табло, екран головуючого та в мережу; комутація мікрофонів під час виступів народних депутатів з робочих місць; висвітлення на табло інформації про виступаючого на сесії з відліком часу його виступу та сумарного часу, виділеного на розгляд конкретного питання;

- АРМ «Секретер» призначений для формування черг на виступ з трибуни з будь-якого питання, включеного до затвердженого переліку питань порядку денного, та висвітлення оголошень на табло у сесійному залі;

- АРМ «Діагностика» безперервно приймає потік інформації з пультів народних депутатів, проводить його обробку та аналізує технічний стан пультів;

- АРМ «Головуючий» приймає аналітичну інформацію про результати голосувань, реєстрацій, списки народних депутатів, які записались на виступ з трибуни і з місця, анкетні дані народних депутатів, сумарний час виступів представників фракцій і груп;

- АРМ «Депутат» складається з інформаційно-довідкової системи про склад депутатського корпусу та програми оброблення та відображення інформації про результати поіменних реєстрацій та голосувань.

До складу системи «РАДА» також входять пульти народних депутатів, призначені для реєстрації, голосування, запису на виступ та забезпечення виступів з місця, і демонстраційні табло. На табло висвітлюються дані про виступаючого; відлік часу для виступу; результати реєстрації, голосувань та поіменних голосувань, згрупованих за фракціями та групами; відлік часу, відведеного на розгляд конкретного питання; графіки, таблиці та оголошення.

Склад і зв'язки між елементами інформаційно-технічного комплексу «РАДА» ілюструє рис. 6.1.

Вхідною інформацією системи є анкетні дані народних депутатів, перелік зареєстрованих в Україні партій, перелік фракцій та груп народних депутатів Верховної Ради, перелік постійних комітетів Верховної Ради України.

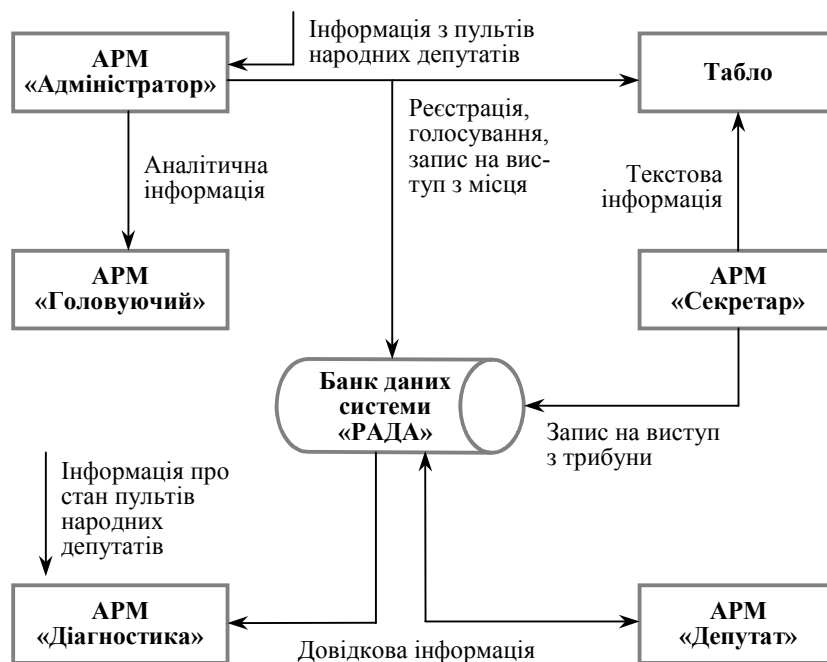


Рис. 6.1. Структура інформаційно-технічного комплексу «РАДА»

Вихідна інформація комплексу така:

- результати поіменних реєстрацій народних депутатів;
- загальні результати відкритих (не поіменних) голосувань;
- результати поіменних реєстрацій народних депутатів з групуванням за фракціями та групами;
- результати поіменних голосувань, у тому числі з групуванням за фракціями та групами і за результатами голосування;
- результати голосування фракцій та груп під час поіменного голосування;
- результати поіменних голосувань конкретного народного депутата за певний період часу;
- списки народних депутатів за їх належністю до партій, фракцій та груп, постійних Комітетів Верховної Ради України;

- списки народних депутатів, записаних на виступ з трибуни, статистика виступів народних депутатів з трибуни і з місця;
- аналітично-експертна інформація, оголошення і повідомлення, що висвітлюються на табло у сесійному залі та в холі;
- таблиць присутності народних депутатів України на пленарних засіданнях за день і за місяць;
- стенограми засідань Верховної Ради України з результатами проведених голосувань у роздрукованому вигляді та у вигляді бази даних «Стенограми», що зберігається у складі Електронного інформаційного бюлетеня;
- роздруковані тексти виступів народних депутатів України на пленарних засіданнях за конкретний період.

Інформаційні зв'язки системи «РАДА» зображено на рис. 6.2.



Рис. 6.2. Інформаційні зв'язки системи «РАДА»

Поіменна реєстрація проводиться біля столів реєстрації за особистим підписом народного депутата з пред'явленням посвідчення. Водночас реєстратор вводить номер електронної картки народного депутата, який реєструється, до системи «РАДА». Народні депутати, які запізнилися на засідання, можуть протягом даного засідання зареєструватися в електронній системі біля столів реєстрації.

Інформація про кількості зареєстрованих депутатів постійно висвітлюється на моніторі головного залу, а також може бути висвітлена на табло у сесійному залі. Може бути висвітлений і список незареєстрованих депутатів. Якщо депутат не зареєструвався, інформація про його перебування на пленарному засіданні у системі «РАДА» буде відсутня і він не зможе користуватись пультом на робочому

місці в залі. Дані реєстрації є підставою для нарахування виплат за час роботи депутата на пленарних засіданнях.

Для роботи з системою «РАДА» кожному народному депутату видається персональна картка, за допомогою якої він може підмикатися до системи на будь-якому робочому місці у залі засідань, обладнаному пультом. Протягом усього часу роботи депутата в сесійному залі картка має залишатись у гнізді пульта.

Голосування здійснюється під час появи на табло спеціальної заставки з відліком часу і звукового супроводження натисканням на пульті кнопки «Слово з трибуни» та однієї з кнопок «За», «Проти» або «Утримався». Результати голосування висвітлюються на табло.

Записатися на виступ з місця можна за допомогою кнопки пульта «Слово з місця» після оголошення головуючим і висвітлення на електронному табло напису «Проводиться запис на виступ із місця». Черговість виступу народного депутата не залежить від часу натискання кнопки, оскільки система визначає її за допомогою генератора випадкових чисел. За рішенням Верховної Ради черга на виступ може формуватись залежно від належності депутатів до фракцій. Сформовані черги передаються на монітор головуючого і можуть висвітлюватись на табло в сесійному залі. При наданні головуючим слова з місця «РАДА» висвітлює на табло відомості про депутата, який виступає, вмикається мікрофон і на пульті депутата засвітлюється лампочка. Після закінчення виступу лампочка гасне і мікрофон вимикається.

Запис на виступ із трибуни для обговорення будь-якого питання порядку денного здійснюється на основі відповідних заяв на ім'я головуючого, що подаються до Секретаріату після затвердження розкладу розгляду питань на пленарних засіданнях поточного чи наступного тижня. У порядку надходження вони заносяться до комп'ютерної бази даних, а депутатам повідомляється його номер у списку. Прийом заяв припиняється у момент оголошення головуючим початку обговорення даного питання. Слово для виступу надає головуючий на засіданні в порядку, визначеному регламентом. Перелік записаних на виступ може бути висвітлений на електронному табло перед початком обговорення.

Об'яви з питань парламентської діяльності висвітлюються на електронному табло за поданням у письмовій формі керівниками комітетів та уповноваженими представниками депутатських фракцій до Секретаріату Верховної Ради України.

6.3. ІС «ЗАКОНОПРОЕКТ»

ІС «Законопроект» обслуговує процес розроблення законодавчих актів — реєстрацію початкового варіанта; вивчення проблеми, що потребує правового регулювання; збирання пропозицій та необхідної інформації із зовнішніх джерел; формування законопроектів; кінцеве юридичне оформлення. Система дає змогу залучати до творчого процесу фахівців-виконавців і зацікавлених осіб, які бажають або зобов'язані працювати з документами, що проходять експертизу, а згодом дістають оцінку під час голосування народних депутатів.

Повнотекстові бази ієрархічної структури ІС «Законопроект» містять тексти законопроектів, порівняльні таблиці, інформаційні матеріали законотворця. Через технологію ведення «Електронного інформаційного бюлетеня» (див. далі) забезпечується доступ користувачів до еталонної бази «Закони та підзаконні акти України».

До системи входять *три інформаційно-аналітичні комплекси*.

1. Інформаційно-аналітичний комплекс планування законотворчої роботи *«ПЛАН»* призначений для оперативного формування перспективних та оперативно-календарних планів роботи Верховної Ради України та її підрозділів. Комплекс є ефективним інструментальним засобом, за допомогою якого можна працювати з банком законодавчих пропозицій та нормативно-правових актів, що підлягають розгляду на сесіях і в комітетах Верховної Ради України.

Комплекс «ПЛАН» обслуговує керівництво Верховної Ради України, народних депутатів України, підрозділи апарату Верховної Ради України, що планують законотворчу діяльність, та ін.

Використання цього комплексу забезпечує:

- вибір законопроектів для формування річного плану законодавчої діяльності Верховної Ради України;
- вибір законопроектів для формування сесійного плану законодавчої роботи Верховної Ради України;
- щомісячне планування законодавчої роботи комітетів Верховної Ради України;
- гнучкий механізм перегляду законопроектів, що дає можливість їх вибору за тематикою (відповідно до рубрикатора) та за вказаним упорядкуванням рейтингової ваги законопроектів згідно з оцінками експертів;
- проведення робіт з оновлення даних про законопроекти на загальному сервері.

Також «ПЛАН» надає можливість фахівцям з економіки та права виконувати аналітичну роботу із законопроектами, використовуючи інформацію, що міститься в базі даних.

Вхідною інформацією комплексу «ПЛАН» є інформація про законопроекти, що зберігаються на загальному сервері комп'ютерної мережі Верховної Ради України, та дані щодо кожного законопроекту: повна назва; номер та дата реєстрації; номер та дата рішення, що є підставою для внесення до плану; тип законопроекту (проект закону, пропозиція, постанова); позначення новизни (новий законопроект або зміни до існуючого); суб'єкт законодавчої ініціативи; головний комітет Верховної Ради України; відповідальний виконавець (народний депутат); комітети та підрозділи; рубрикатор; назва; орієнтовна дата виконання.

Результатом функціонування комплексу «ПЛАН» є план законодавчих робіт на рік; план законодавчої роботи комітетів Верховної Ради України на сесію; щомісячні плани роботи Верховної Ради України.

Комплекс «ПЛАН» складають кілька *програм*: «ПЛАН», «Законопроекти», «Рейтинг», «Поновлення даних». Зокрема, програма **«Рейтинг»** формує плани законодавчої діяльності на рік, сесію та чергове пленарне засідання на основі рейтингової ваги законопроектів, визначених народними депутатами.

2. Система **«Реєстрація та контроль проходження законопроектів Верховної Ради України»** призначена для автоматизації відповідних робіт з відстежуванням відповідності регламенту та порядку денному.

Система дає змогу:

- реєструвати законопроекти із здійсненням вхідного контролю за типами документів;
- вести список законопроектів, унесених до плану;
- зв'язувати зареєстровані законопроекти із законопроектами з числа запланованих;
- вести контроль за законопроектом на всіх етапах його проходження з відстежуванням за регламентними термінами виконання кожної операції;
- вести загальносистемні та локальні довідники системи;
- динамічно змінювати маршрути та технологічний регламент проходження законопроектів;
- шукати законопроекти (або їх перелік) за різноманітними критеріями та умовами пошуку;
- впорядковувати за бажаними критеріями картотеки законопроектів;

- робити довільні вибірки з виводом їх на зовнішні пристрої (текстовий файл, друкувальний пристрій);
- зберігати в архіві картотеки законопроектів з можливостями пошуку та впорядкування;
- робити дзеркальні копії інформаційної бази на зовнішні носії інформації та забезпечувати її відновлення в аварійних випадках;
- працювати з широким набором сервісних функцій (календар, записна книжка, калькулятор).

Найбільш відчутний економічний ефект від впровадження системи одержується при її використанні у локальній мережі, що дає можливість вести єдину інформаційну базу. Обсяг інформації, що її можна ввести у систему, обмежений тільки фізичними характеристиками апаратних засобів.

3. Інформаційний комплекс «**Законотворець**» призначений для підготовки законопроектів і порівняльних таблиць (формування, коригування, порівняння, аналізу) з метою їх розгляду та обговорення на пленарних засіданнях. Комплекс використовують народні депутати України, їхні помічники та апарат комітетів Верховної Ради України.

У процесі роботи інформаційний комплекс «Законотворець» виконує такі *автоматизовані функції*:

- підготовка тексту проекту закону;
- автоматична структуризація тексту;
- завантаження структурованого тексту проекту закону в базу даних;
- введення та завантаження в базу даних автоматично впорядкованого масиву зауважень та висновків комітетів до проекту закону;
- постатейний розгляд проекту закону з аналізом і врахуванням усіх пропозицій та зауважень, що надійшли до будь-якої статті;
- розгляд альтернативних варіантів одного й того самого закону та встановлення співвідношень між текстами;
- формування та друкування порівняльних таблиць до одного й того самого проекту та таблиць співвідношень до альтернативних проектів для розгляду в комітетах та робочих групах;
- формування та друкування тексту остаточної редакції.



Порівняльна таблиця до проекту Закону України
«Про електронні документи та електронний документообіг»

Реєстраційний
№ 7329

Автори: Кабінет Міністрів України (Друге читання)
Автори остаточної редакції: Комітет з питань науки і освіти
Дата розгляду в комітеті: 11.10.01

Редакція, прийнята у першому читанні	Зауваження та пропозиції до проекту	Висновки, обгр.	Редакція, запропонована н. д. України — членами Комітету
--------------------------------------	-------------------------------------	-----------------	----------------------------------------------------------

Проект

Проект

188

ЗАКОН УКРАЇНИ
Про електронні документи
та електронний
документообіг

ЗАКОН УКРАЇНИ
Про електронні документи
та електронний
документообіг

Цей Закон встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

-*А* - Н. д. Губський Б. В. (Рєстр. карт-ка № 443)

Доповнити законопроект окремою статтею про електронний цифровий підпис

-*Б* - Н. д. Філіпчук Г. Г. (Округ № 203)
Преамбулу Закону записати в наступному вигляді:
«Цей Закон встановлює основні організаційно-правові засади створення електронних документів та визначає загальний порядок електронного документообігу».

Враховано

Враховано

Цей Закон встановлює основні організаційно-правові засади створення електронних документів та визначає загальний порядок електронного документообігу.

Вхідною інформацією комплексу є проект закону, який вноситься на розгляд Верховної Ради України, і тексти альтернативних проектів.

Вихідною інформацією є порівняльні таблиці, таблиці співвідношень і текст остаточної редакції закону, ухваленого на сесії Верховної Ради України.

6.4. ЕЛЕКТРОННИЙ ІНФОРМАЦІЙНИЙ БЮЛЕТЕНЬ

Електронний інформаційний бюлетень — це ряд упорядкованих баз даних, орієнтованих на інформаційне забезпечення законотворчої діяльності і призначених для ведення, тиражування і використання електронної бібліотеки бюлетенів роботи Верховної Ради України. Він містить регламент Верховної Ради України, розклад засідань Верховної Ради України, стенограми, тексти законопроектів, нормативні акти України, законодавство країн світу, програми народних депутатів України, фахівці-розробники законопроектів, органи влади; огляд подій.

Основним джерелом даних для баз електронного бюлетеня є «Справа законопроекту» та документообіг Верховної Ради України. Основними *принципами вибору джерел даних* є відкритість, офіційність на кожному етапі життєвого циклу законотворення, обґрунтованість доведення даних до користувача з метою підвищення відкритості та демократизації суспільства, надійність джерел, можливість розширення джерел даних без суттєвих трудовитрат на переструктуризацію баз даних (адаптивність).

В «Електронному інформаційному бюлетені» вибрано ієрархічну модель баз даних. Це зумовлюється вимогами простоти і швидкості доступу до повнотекстових неструктурованих документів різного змісту.

Дерево декомпозиції ієрархічної моделі побудовано авторами на підставі аналізу реальних запитів користувачів на ту чи іншу інформацію у ході законотворчого процесу. Ієрархічна індексація відбиває частоту та кількість звернень до того чи іншого виду даних. Користувачеві також надається можливість працювати з деревом документів у власній базі — створювати, знищувати, редагувати, переміщати вітки дерева.

Система пропонує такі *варіанти організації пошуку* потрібного документа:

- пошук за деревом ведеться серед тих віток дерева, що їх позначив користувач. Можна здійснити пошук за ключовим словом, за контекстом в назві або в тексті, за датою;
- пошук за закладками ведеться серед текстів бази даних, які користувач позначив закладкою;
- пошук за картотекою ведеться в межах усієї бази даних (не всі документи, наявні в базі даних, вносяться до картотеки). Для пошуку можуть задаватись такі атрибути документа: орган видання і тип, слово з назви, реєстраційний номер, дата підписання, номер і дата реєстрації в Міністерстві юстиції (рис. 6.3). Пояснення до кожного атрибута викликаються натисненням клавіші з ім'ям атрибута.

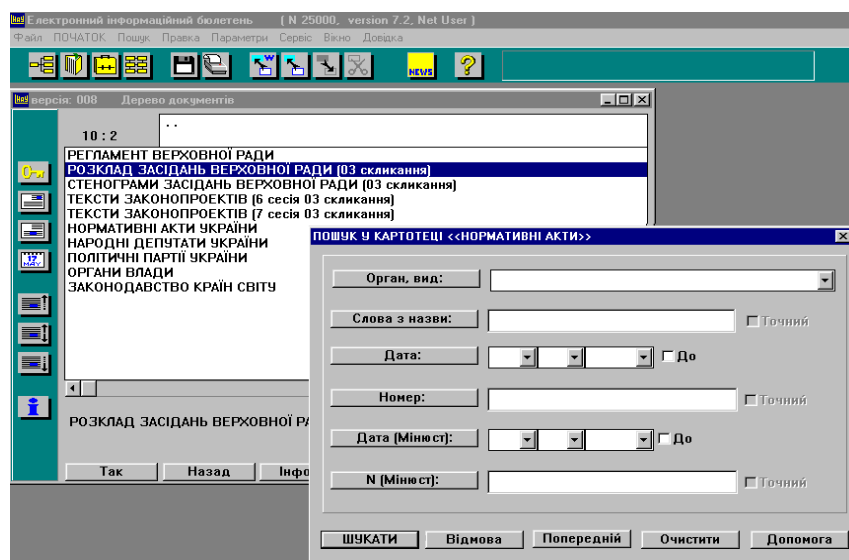


Рис. 6.3. Дерево документів «Електронного інформаційного бюлетеня» (перший рівень) і картка пошуку в картотеці

На фізичному рівні «Електронний інформаційний бюлетень» вимагає файлів dbw, розміщених в одній директорії, до яких здійснюється доступ з різних програмних модулів. Кілька фізичних файлів dbw складають один логічний об'єкт бази. Така структуризація дає змогу виділити архівну незмінну частину і частину фізичних файлів, що актуалізуються оперативно. Це зумовлюється вимогами запису бюлетеня на компакт-диски, а також ство-

рення динамічного ряду розділів системи баз даних для подальшого аналізу варіантів текстових документів і формування правил їх змінювання.

Між складовими елементами баз даних спроектовано і підтримуються логічні зв'язки, що відбивають логіку законотворення, якої дотримуються співробітники постійних комітетів Верховної Ради України, відповідальні за підготовку конкретного законопроекту.

6.5. БАЗИ ДАНИХ ПРАВОВОЇ ІНФОРМАЦІЇ ВЕРХОВНОЇ РАДИ УКРАЇНИ

Бази даних правової інформації орієнтовані на забезпечення правовою інформацією широкого кола користувачів за допомогою інформаційно-пошукових систем «Право», «Законодавство», «Картотека» і «Закони та підзаконні акти України в Інтернет», які дають змогу швидко шукати та аналізувати нормативно-правові документи.

Користувачі систем такі:

- народні депутати України та депутати місцевих рад;
- працівники структурних підрозділів Верховної Ради України, Адміністрації Президента України, Конституційного Суду України, Верховного Суду України, Вищого господарського суду України, Міністерства культури, Міністерства освіти і науки, Міністерства оборони, Міністерства праці та соціальної політики, Міністерства фінансів, Національної Академії наук, Міністерства економіки, інших міністерств і відомств, місцевих органів влади, наукових установ та навчальних закладів;
- співробітники іноземних представництв в Україні та посольств України в інших країнах;
- керівники підприємств, юристи, бухгалтери, економісти, працівники банків, юридичних фірм, інших організацій;
- абоненти мережі Інтернет, які мають відповідний доступ.

Бази даних систем містять нормативно-правові документи в остаточній редакції із внесеними змінами (у системі «Законодавство» є попередні редакції), зокрема:

- закони, постанови Верховної Ради України, постанови та укази Президії Верховної Ради України, починаючи з 1990 року;
- кодекси;
- укази та розпорядження Президента України;
- постанови та розпорядження Кабінету Міністрів України, починаючи з 1992 року;

- декрети Кабінету Міністрів України;
- документи міністерств і відомств України, зареєстровані в Міністерстві юстиції відповідно до Указу Президента України № 493/92 від 03.10.1992 р. та постанови Кабінету Міністрів України № 731 від 28.12.1992 р.;
- міжнародні угоди;
- документи міністерств і відомств України, які не підлягають реєстрації в Міністерстві юстиції (листи, роз'яснення Національного банку, Державної податкової адміністрації, рішення Конституційного Суду України, постанови Верховного Суду та Вищого господарського суду України тощо).

Бази даних систем «Законодавство» і «Право» тотожні за складом та обсягом. База даних «Закони та підзаконні акти України в Інтернет» (див. підрозд. 5.5) є копією бази даних системи «Картотека». Множина документів системи «Право» є підмножиною документів бази даних «Картотека».

Системи «Право», «Законодавство», «Картотека» забезпечують:

- пошук документів за реквізитами (назва, номер, дата прийняття, орган видання та тип документа), за ключовими словами та темами (пенсії, боротьба зі злочинністю, податки тощо);
- перегляд, сортування, друкування або виведення у файл переліку знайдених документів;
- перегляд текстів документів у багатовіконному режимі з підсвічуванням ключових слів;
- друкування цілого тексту або будь-яких його частин на принтері;
- контекстний пошук за двома словами (відстань між словами визначається користувачем);
- ведення списків (тематичних папок) користувачів;
- перегляд нормативних актів, пов'язаних з документом (що вносять зміни, вводять у дію, ратифікують, посилаються на даний документ тощо);
- переключення перегляду з одного документа на інший за посиланням у тексті (динамічний гіпертекст);
- перегляд додаткових реквізитів документа (дати набуття або втрати чинності, дати публікації у пресі), перегляд як чинних, так і нечинних документів;
- перегляд структури документа, створення закладок у текстах, власних приміток користувача до документів;
- перегляд статистики бази даних;
- актуалізація бази даних за допомогою спеціальних файлів (блоків поновлення), які передаються користувачам на дискетах

або засобами телекомунікацій (електронною поштою, через ftp-сервер мережі Інтернет тощо);

- перегляд результатів попередніх пошуків за різними критеріями, перегляд списків документів, що додавались до бази даних з окремих блоків поновлень;

- одержання довідок про стан системи (обсяг вільного дискового простору, версію системи, обсяг бази даних, номер останнього блока поновлення тощо).

Кожна з систем має певні особливості. Так, система «Законодавство» відзначається можливістю перегляду попередніх редакцій документів, що змінювались. «Картотека» характеризується потужною базою даних (понад 28 тисяч нормативно-правових документів), швидким пошуком, можливістю формування бази даних із тих органів влади, що їх замовляє користувач. Система «Право» вирізняється різноманітністю функцій, можливістю створення власних текстів та їх комбінування з текстовими фрагментами документів бази даних, високим рівнем документованості (наявна детальна контекстно залежна допомога, видано довідник користувача).

6.6. ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА «ВИБОРИ»

Важливою складовою ІС Верховної Ради України є інформаційно-аналітичний комплекс «*Зворотний зв'язок*», який забезпечує аналітичне оброблення звернень, пропозицій та скарг громадян, повідомлень преси, дає змогу відстежувати фактичні результати впровадження нормативно-правових актів щодо змін у житті суспільства та становлення нової держави. *ІС «Вибори»* у складі цього комплексу забезпечує оброблення даних про народних депутатів, їхні програми, облік та аналіз результатів виборів.

ІС «Вибори» здійснює:

- централізоване накопичення інформації, що надходить з виборчих округів, про хід виборів на всіх етапах виборчого процесу;

- облік даних про виборчі округи України з деталізацією всіх необхідних характеристик та етапів виборчого процесу щодо кожного округу;

- оброблення оперативних даних про реєстрацію претендентів і кандидатів у регіонах та виборчих округах з подальшим узагальненням;

- формування даних про кандидатів у депутати в обсязі відомостей, передбачених Законом України про вибори народних депутатів України;

- ведення облікових карток, автобіографій та програм кандидатів у народні депутати;
- збирання за допомогою електронної пошти або телеграфних повідомлень, контроль та оброблення оперативної інформації про результати виборів;
- підготовку оперативних даних про хід голосування в округах регіонів у задані інтервали часу на день виборів;
- консультативно-довідкову підтримку процесу аналізу результатів голосування;
- формування альбому-звіту з деталізованими результатами виборів по регіонах та по виборчих округах;
- формування звітів про результати кожного туру виборів — повного звіту про результати виборів щодо всіх кандидатів у народні депутати та звіту про результати виборів по округах, в яких обрано народних депутатів України;
- формування статистичних та інформаційно-аналітичних довідок.

Крім регламентних запитів, система забезпечує обслуговування запитів користувачів згідно з довільною комбінацією параметрів та їх значень, оперативно формує відповідні звіти за формою, визначеною користувачем, для перегляду на екрані або для друкування.

У комп'ютерному банку даних Центральної виборчої комісії зберігається інформація про всіх кандидатів, нагромаджено великі обсяги фактографічної та аналітичної інформації, яка є важливим інформаційним ресурсом для політологів, аналітиків та законотворців.

Інформація, нагромаджена в ІС «Вибори», становить інтерес для всіх учасників виборчого процесу, а особливо, для кандидатів у депутати. Частина даних може передаватись для автоматизованого оброблення у спеціалізованих інформаційних системах політиків, які, у свою чергу, певним чином функціонально доповнюють комплекс «Зворотний зв'язок». Так, **система інформаційно-аналітичної підтримки виборчої кампанії** використовується для розробки стратегії і тактики виборчої кампанії, їхньої послідовної реалізації та комплексного моніторингу політичних, соціальних та економічних подій у житті регіону.

При цьому вирішуються такі *функціональні задачі*:

- «Виборча кампанія» — організація благодійних акцій; участь в економічному розвитку регіону; участь у суспільно-політичному житті регіону; просвітницька діяльність; робота з молоддю, пенсіонерами, ветеранами, заслуженими людьми, твор-

чою інтелігенцією; акції з соціального захисту; підтримка суспільного порядку; взаємодія з органами, що ведуть боротьбу з корупцією та організованою злочинністю;

- «Кандидат» — створення іміджу та індивідуальності кандидата (родина, інтереси, досягнуті результати, намічені цілі, передвиборна програма, широта зв'язків і підтримки з боку електорату, ділової та політичної еліти). Також формуються: стратегія і плани-графіки виступів кандидата, його довірених осіб, уповноважених, групи підтримки;

- «Моніторинг» — відстеження стану базових суспільних відносин, насамперед соціальних, економічних, політичних і фінансових, а також умов і механізмів, що забезпечують життя регіону;

- «Стратегічне і тактичне планування» — застосування політологічних технологій для визначення життєво важливих інтересів; визначення їхньої пріоритетності; оцінка ступеня впливу основних діючих сил у регіоні; оцінка ступеня свого впливу; оцінка рівня ризику при вирішенні актуальних проблем регіону. З урахуванням результатів політологічного та економічного аналізу проводиться стратегічне і тактичне планування, здійснюється контроль. На підставі комплексного аналізу стану ситуації в регіоні, стратегічного та оперативного аналізу ефективності отриманих результатів і використання системи прогнозування генеруються нові цілі і завдання, проводиться пошук нових можливостей;

- «День виборів» — проводиться стратегічний аналіз, здійснюється прогнозування, складається тактичний огляд спільних рейтингів кандидатів по одномандатному виборчому округу (багатомандатному загальнодержавному виборчому округу) з метою вироблення рекомендацій і динамічного коригування підготовлених стратегічних і тактичних планів і дій під час проведення виборчої кампанії.

6.7. ПРОБЛЕМИ І ПЕРСПЕКТИВИ ІНТЕРНЕТ-ВИБОРІВ

Комп'ютеризоване проведення виборів (голосувань) не можна назвати новим технологічним підходом, оскільки з цією метою використовувались у різні часи і системи підрахунку голосів на основі перфокарт, і пристрої для зчитування міток, і спеціальні електронні машини підрахунку голосів з прямим записом. Деякі з названих систем застосовуються і досі. Але сьогодні впровадження нових інформаційних технологій у цій галузі пов'язується з переведенням голосувань у середовище Інтернет. Про-

ведення Інтернет-виборів розглядається як один із перспективних напрямків розвитку систем ЕК за участю держави, але водночас викликає неоднозначне ставлення фахівців і жваві дискусії щодо підходів до їх реалізації. Оцінити перспективи і проблеми проведення Інтернет-виборів можна на основі порівняння цієї технології з традиційною паперовою.

Технологія проведення виборів з використанням паперових бюлетенів широко відома. Виборці одержують бюлетені на виборчій дільниці і, зробивши позначки, опускають їх у виборчу урну. Після закриття виборчої дільниці бюлетені підраховуються і виводяться загальні підсумки. Така система вимагає проведення *спеціальних процедур*, які забезпечать легитимність виборів:

- ідентифікація виборця — можуть голосувати тільки ті, хто має на це право. Ретельно виконана процедура перевірки особи може виявитися принизливою для виборця, що може поставити під загрозу його участь у голосуванні, але недосконала ідентифікація викликає недовіру до результатів голосування;

- перевірка кількості бюлетенів — кожен виборець може голосувати тільки раз. Один з можливих способів протидії — відкритість кабінки для голосування — вступає у конфлікт з вимогою забезпечення таємності голосування. Звірка кількості заповнених бюлетенів і кількості виборців, які взяли участь у голосуванні, означає додаткове навантаження на дільничну комісію;

- забезпечення таємності голосування — бюлетень не може містити жодних позначок, які дають можливість ідентифікувати особу, що проголосувала. Також слід дотримуватись порядку збирання бюлетенів, який не дозволить відстежити послідовність їх заповнення;

- недопущення використання заздалегідь заповнених бюлетенів. Зацікавлена особа може купувати незаповнені бланки у виборців в обмін на обіцянку опустити до урни заповнений певним чином бюлетень. Ця схема особливо небезпечна, оскільки для її застосування досить мати з самого початку один незаповнений бланк бюлетеня. Можливі шляхи протидії: використання бланків, що їх важко підробити; підвищені заходи безпеки при їх друці у типографії; суворий облік бюлетенів на виборчій дільниці; перевірка бланків на відсутність позначок до видачі їх голосуючим. Вільний доступ до бланків, при якому схема не спрацьовує, неприпустимий через інші загрози, так само як і особистий обшук виборців;

- забезпечення чесної роботи дільничної комісії. Головною гарантією є відкритість процедури виборів, коли під час прове-

дення голосування і підрахунку бюлетенів жодна дія не виконується за відсутності наглядачів. Також необхідний ретельний відбір членів дільничної комісії;

- підрахунок бюлетенів. Якщо результати підрахунків викликають недовіру, передбачається механізм повторного підрахунку;

- охорона бюлетенів під час зберігання. Проблему можна охарактеризувати двома фразами: «хто простежить за сторожами?» та «на кожний замок знайдеться зламувальник»;

- охорона бюлетенів під час транспортування. Ця проблема деяким чином схожа з проблемою охорони доказів — процес починається з моменту, коли доказ було помічено, і закінчується тільки при його поданні до суду. Фактично бюлетені для голосування теж можуть стати доказами злочину. Тому кожний крок повинен фіксуватись документально: хто давав бюлетень виборцям, хто їх підраховував, хто запечатав/розпечатав виборчу урну, хто її перевозив, хто спостерігав за всіма діями. Усі записи повинні підписуватись і завірятись свідками.

Таким чином, можна визначити, що паперові системи проведення виборів не є надійними. Сьогодні все частіше звучить думка, що такі системи не в змозі повністю розв'язати всі проблеми, що виникають, а поява технологічних новинок ставить під загрозу навіть ті заходи, що їх вважають ефективними. Варто також зазначити, що історично визначення проблем відбувалось дуже повільно, а заходи протидії найчастіше починали вживати тільки після серйозних провалів, про які дізнавалась широка громадськість.

Інтернет-вибори як виборча система на основі електронних виборчих бюлетенів, що їх виборці можуть передавати офіційним особам (виборчим комісіям) через Інтернет, мають безсумнівні переваги.

По-перше, для виборця не має безумовної необхідності йти на виборчу дільницю, він може проголосувати там, де йому зручно: вдома, у крамниці, у бібліотеці, у поштовому відділенні, у готелі. Варіанти обмежуються прийнятим порядком проведення голосування, а не технологією. У першу чергу ця перевага торкається тих, хто тимчасово перебуває за межами свого виборчого округу.

По-друге, значно спрощується процес власне голосування. На екрані дисплея виводиться список позицій. Виборцю надається можливість одержати додаткову інформацію, наприклад, про партії та кандидатів переходом до їх домашніх Web-сторінок. Голосуючий вказує вибрані позиції простим дотиком руки. Результати стають відомими практично відразу після закінчення голо-

сування, оскільки всі машини для голосування мають зв'язок із сервером центральної виборчої комісії, на якому відбуваються підрахунки. Простота і доступність процедури потенційно збільшить кількість голосуючих. І головне те, що Інтернет-вибори вже розглядаються як реальність, а не віддалена перспектива.



Досвід розробки і впровадження електронних виборів — США

Компанії Compaq Computer та Cisco Systems, які створили спільну венчурну фірму VoteHere.net («ГолосуйТут.мережа»), пропонують мережні системи, в яких використовується ПЗ шифрування даних і сенсорні екрани. Кілька сотень осіб у Каліфорнії та Аризоні вже взяли участь у їх тестуванні, однак державні органи мають перевірити цілий ряд технологічних питань. Якщо буде вирішено проблеми безпеки використання таких систем, голосування вдома через Інтернет з часом замінить паперові бюлетені, механічні системи та оптичне сканування. Однак, експерти вважають, що сьогодні більш реальним є використання машин для голосування з сенсорним екраном, які підімкнені до Інтернет і обслуговуються співробітниками виборчих дільниць.

Аналогічні розробки ведуть корпорація IBM, Массачусетський технологічний інститут і Каліфорнійський технологічний університет. Свої зусилля у даному напрямку також об'єднали Unisys, Dell Computer і Microsoft. Привабливість цього сектора пояснюється тим, що законодавчі органи багатьох штатів планують виділити з бюджетів сотні мільйонів доларів на оновлення системи проведення виборів.

Водночас забезпечення безпеки і секретності передавання електронних виборчих бюлетенів потребує виконання цілої низки спеціальних процедур. Узагальнено процес можна описати наступним чином.

Етап підготовки до голосування:

- реєстрація голосуючого. У більшості випадків вимагається «живий» підпис виборця;
- одержання талона на Інтернет-голосування за аналогією з отриманням відкріпного талона. Виборцю надається тільки один талон, який визначає форму голосування (іншими словами, голосуючий має зробити вибір до формування запиту);
- авторизація — виборча комісія надсилає виборцю інформацію про порядок його аутентифікації і голосування, голосуючий позначається як такий, що одержав бюлетень для унеможливлення дублювання.

Етап голосування:

- забезпечення безпеки голосування. Якщо голосування відбувається на виборчій дільниці або за допомогою спеціального апаратного забезпечення, процедура порівняно проста. Якщо ж виборець голосує вдома або через комп'ютер, який належить третій стороні, слід забезпечити відсутність у програмному коді сторонніх команд і неможливість зовнішнього втручання у процес. Існує кілька варіантів виконання цієї процедури, включаючи перезавантаження комп'ютера у «безпечному режимі» або зі спеціального компакт-диска, який надається виборчою дільницею, або приєднання спеціального пристрою до комп'ютера та ін.;
- аутентифікація — голосуючий має засвідчити свою особу згідно із запропонованими йому правилами;
- відкриття Web-сторінки з бюлетенем на сайті Інтернет-голосування в разі нормального завершення аутентифікації;
- голосування — заповнення бюлетеня за допомогою клавіатури, миші або сенсорного дисплею, якщо такий є;
- передавання бюлетеня — до серверу виборчої дільниці бюлетень надсилається в зашифрованому вигляді, усі незашифровані записи бюлетеня на комп'ютері голосуючого знищуються;
- прийом бюлетеня сервером виборчої дільниці і підтвердження прийому (виборцю надсилається спеціальне повідомлення).

Етап обробки бюлетенів:

- перевірка та анонімізація — бюлетень, одержаний від виборця, який ще не проголосував, відділяється від ідентифікатора виборця і записується для підрахунку;
- верифікація — виборець, який проголосував, має можливість перевірити той факт, що його бюлетень не тільки було прийнято, а й записано для підрахунку, але при цьому ніхто не може перевірити результати голосування;
- підрахунок голосів;
- аудит, повторний підрахунок, вирішення спірних питань — для виконання цих операцій мають зберігатись бюлетені, відокремлені ідентифікатори виборців та інша інформація.

Багато в чому Інтернет-вибори схожі з іншими технологіями, які передбачають електронне подання бюлетенів, їх автоматичне оброблення та передавання засобами телекомунікацій. Не існує принципових розбіжностей і в інтерфейсі.

Усі такі технології потребують нормативного регулювання питань цифрового зберігання бюлетенів, подання їх на екрані дисплея та транспортування. Впровадження Інтернет-виборів додає

до цього списку проблеми регламентації використання персональних комп'ютерів та технологій WWW з метою голосування.

Водночас упровадження Інтернет-виборів неможливе без вирішення специфічних проблем, основні з яких розглянуто нижче.

Ідентифікація виборця. Ідентифікація може виконуватись різними способами, кожний з яких має свої переваги та недоліки, зокрема:

- за допомогою посилання на національну систему ідентифікації — голосуючий має вказати певну таємну інформацію (наприклад, ідентифікаційний код);
- з використанням бази біометричних даних виборців;
- за допомогою електронних цифрових підписів;
- звичайним чином (перевіркою паспорта чи посвідчення особи членом виборчої комісії, реєстрацією за допомогою паперових документів і «живого» підпису).

Ще одне рішення полягає у впровадженні системи «Надрукуй власний бюлетень» — виборець завантажує бюлетень з сервера виборчої дільниці, роздруковує його, заповнює, підписує і надсилає поштою. Працівник виборчої комісії має звірити підпис на одержаному бюлетені з тим, що зберігається у внутрішніх документах. Зрозуміло, це певна «вироджена» форма проведення Інтернет-виборів.

Забезпечення надійності та захищеності процесу підрахунку голосів — бюлетені слід правильно підраховувати, не розкриваючи вибору окремого голосуючого, при цьому неприпустимі втрати бюлетенів, їх дублювання або порушення їхньої цілісності.

Коли підрахунки виконуються за допомогою програмного забезпечення, розробленого певною фірмою, єдиною гарантією того, що оголошені результати дійсно відповідають волі виборців, є тестування, заздалегідь проведене незалежною організацією. Для того щоб цей метод спрацював, тестування має охоплювати *все!* програмне забезпечення, що використовується для подання виборчого бюлетеня голосуючому та оброблення голосів як на локальних машинах для голосування, так і на машинах центру підрахунку голосів — не тільки прикладне ПЗ, а й системні та інструментальні засоби (ОС, СКБД, компілятори, програмні оболонки тощо). Повністю виконати цю вимогу можна тільки за умов використання ПЗ з відритим кодом та додаткових заходів захисту інформації.

Іншим аспектом проблеми є трудність перевірки ідентичності ПЗ, встановленого на конкретній машині для голосування, програмі, раніше перевірених у лабораторних умовах. Навіть збіг вер-

сій не можна вважати гарантією відповідності. Виходом може стати зберігання у захищеному місці початкового та об'єктного коду кожної протестованої версії ПЗ; використання середовища програмування «прямо з коробки», яке не має незадокументованих можливостей; застосування машин для голосування, які дають змогу легко визначити справжнє встановлене на ній ПЗ. З погляду технології задовольнити ці вимоги доволі складно.



Інтернет-вибори — проблема ідентифікації програм

Якщо хтось у моїй присутності скопіює програму, запише початковий та об'єктний код на CD-ROM і дасть його мені, я не можу бути впевнена, що на диску записано саме той початковий код, який було продемонстровано. Причина полягає в тому, що я не контролюю комп'ютер, на якому виконано названі операції. Насправді цілком реально змінити звичайні команди так, щоб вони виконували зовсім інші операції.

І навіть за умов виконання всіх наведених вимог тестування має деякі обмеження:

- за допомогою тестування неможливо наблизити рівень прозорості Інтернет-виборів до рівня відкритості виборів з використанням паперових бюлетенів у присутності спостерігачів, оскільки тут зацікавлені особи мають покладатися на висновки експертів;
- тестування не може попередити атаки з боку службовців виборчих дільниць.



Підтасування результатів — електронні вибори у Чикаго

Після зачинення виборчої дільниці працівники виборчої комісії замінили машину для голосування і висунули вимогу повторного підрахунку голосів. Таким чином, саму процедуру повторного підрахунку було використано для шахрайства.

Використання «чистих» систем з точки зору користувача. Як було вже сказано, технологічно дуже важко гарантувати, що система, встановлена на комп'ютері, не має прихованих функцій. З іншого боку, завантаження сертифікованої «чистої» системи для взяття участі в Інтернет-виборах з персонального комп'ютера може бути незручним для користувача. По-перше, заміна системи може означати втрати виконаних раніше налаштувань. По-друге, сертифікація системи як «чистої» не означає, що вона не має по-

бічних ефектів з точки зору захисту приватної інформації, безперебійної роботи комп'ютера і т. ін. Загалом, необхідність зміни системи значно ускладнює просту, по суті, процедуру.

Стандартизація у галузі автоматизованих систем для проведення виборів. На сучасному ринку автоматизованих систем голосування і підрахунку голосів домінують кілька компаній, які пропонують різні технічні рішення та ПЗ. У процесі поступового впровадження технології Інтернет-виборів може скластися ситуація, коли різні виборчі округи використовуватимуть різне обладнання, а відповідні системи зберігатимуть дані в несумісних форматах. Це може звести нанівець всі переваги від використання нової технології. З іншого боку, виробники технічного і програмного забезпечення часто дуже неохоче розкривають деталі форматів даних та іншу інформацію, необхідну для перевірки надійності та захищеності роботи системи. Зрозуміло, що для додатків з Інтернет-голосувань це неприйнятний варіант. Вихід полягає у використанні відкритих стандартів, що забезпечить сумісність різних систем і надасть можливість перевірити їх захищеність не тільки уповноваженим особам, а й представникам громадськості (експертам з криптографії, наприклад). Таємницю можуть складати тільки частина ключів, які постійно змінюються.

Зберігання дублікатів даних голосування. При використанні будь-якої телекомунікаційної технології для передавання даних одна копія тимчасово зберігається на машині-відправнику, а інша — на машині-одержувачеві. Тільки після перевірки правильності передачі оригінал знищується. Під час проведення електронних виборів оригінал електронного бюлетеня залишається на машині для голосування на виборчій дільниці, і існуючі стандарти зберігання бюлетенів запечатаними тут не спрацьовують. Тому очевидно є необхідність законодавчого регулювання проблем зберігання і транспортування та ситуацій, пов'язаних з можливими відмінностями в копіях електронних бюлетенів. З погляду технології слід передбачати використання цифрових підписів або зберігання надлишкової інформації для виявлення помилок, зроблених у процесі передавання або зберігання, і фактів навмисного перекручування інформації, а також для визначення правильної копії.

Заповнення бюлетенів як операція введення даних користувачем. Перед запам'ятовуванням даних система може вимагати підтвердження правильності їх введення. Непідтверджені дані можуть розглядатися як недійсні бюлетені, але при цьому слід попереджувати ситуації, коли голосуючий вважає, що його бюле-

тень прийнятий системою. З іншого боку, виборцеві слід надати можливість внести зміни у бюлетень, який він тільки-но ввів (і тільки у цей бюлетень!) або навіть знищити його з пам'яті машини. При цьому слід установити відповідність між локальною та віддаленою копіями, якщо остання вже існує.

Забезпечення надійності роботи всієї системи. Надійною можна назвати систему Інтернет-виборів, якщо:

- вся система працює правильно навіть у разі виникнення локальних збоїв;
- нові збої призводять до поступового (а не катастрофічного) зниження продуктивності системи;
- повністю усунено ймовірність глобальних збоїв системи;
- голосуючі одержують безсумнівні підтвердження того, що їх голосів не торкнулись збої будь-якого роду;
- усунено можливість втрати бюлетеня, одержаного від виборця, через технічні проблеми після підтвердження його прийому;
- усі процедури з проведення Інтернет-виборів захищені від людських помилок або навмисних дій, які можуть вплинути на результати голосування.



Контрольні запитання і завдання

1. Що мають за мету проекти з теледемократії і які технології для цього використовуються?
2. Схарактеризуйте ІС Верховної Ради України.
3. Яку структуру має інформаційно-технічний комплекс «РАДА»?
4. Що є вихідною інформацією інформаційно-технічного комплексу «РАДА»?
5. Які інформаційні зв'язки має система «РАДА»?
6. Яке призначення має ІС «Законопроект»?
7. Назвіть і опишіть призначення, вхідну та вихідну інформацію інформаційно-аналітичних комплексів, що входять до ІС «Законопроект».
8. Схарактеризуйте «Електронний інформаційний бюлетень».
9. На яких користувачів зорієнтовано інформаційно-пошукові системи, що входять до ІС Верховної Ради України?
10. Які функціональні можливості має ІС «Вибори»?
11. Обґрунтуйте думки фахівців щодо організації Інтернет-виборів:
 - організувати традиційну систему електронної комерції легше, ніж систему Інтернет-виборів;

- Інтернет-вибори варто впроваджувати поступово;
 - голосування через Інтернет спочатку слід реалізувати на регулярних виборчих дільницях;
 - під час проведення Інтернет-виборів до складу наглядачів необхідно включати обізнаних технічних експертів.
12. Які переваги і недоліки мають підходи до ідентифікації учасника Інтернет-голосування?



Література

1. Горьовий Л. Є. та ін. Комп'ютеризована система інформаційно-аналітичного забезпечення законотворчої та правозастосовної діяльності. — К., Парламентське вид-во, 1998. — 149 с.
2. Косолапов В. Л. Автоматизированная система обработки информации и экспертных оценок при анализе общественно-политических процессов // УСиМ. — 1998. — № 1. — С. 25—32.
3. Косолапов В. Л. Информационно-аналитическая технология поддержки избирательной кампании. — <http://www.cec.kiev.ua/new/r8/kos.htm>.
4. Матеріали сайтів <http://www.cs.uiowa.edu/~jones/voting/>, <http://www.electioncenter.org/>, <http://www.misq.org/discovery/articles96/>.



Розділ

7

ІНФОРМАЦІЙНІ СИСТЕМИ ОРГАНІВ ЮСТИЦІЇ УКРАЇНИ

7.1. КОНЦЕПЦІЯ СТВОРЕННЯ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІВ ЮСТИЦІЇ УКРАЇНИ

Ієрархічний територіальний принцип побудови організаційної структури і спеціалізація органів юстиції визначають вимоги до функціональної структури інформаційної системи. У ній можна виокремити три рівні — центральний, обласний, міський (районний для сільської місцевості). За логічною структурою відповідно до спеціалізації органів юстиції можна виокремити такі основні функціональні підсистеми: нотаріату, відділів реєстрації актів громадянського стану (РАГС), органів реєстрації громадських організацій, інформаційно-правового забезпечення правореалізаційної діяльності, діловодства. Інформаційні системи нотаріату мають забезпечувати підготовку нотаріальних документів, ведення реєстру нотаріальних дій, електронного архіву нотаріальних документів (обласний, центральний рівні), державних реєстрів. В ІС РАГС мають вирішуватись завдання ведення реєстрів фактів народження, смерті, змін прізвищ тощо. У підсистемі органів реєстрації громадських організацій мають вестися реєстри фактів реєстрації та відмов у цьому.

Підсистема інформаційно-правового забезпечення правореалізаційної діяльності повинна забезпечувати кодифікацію і ведення банку даних законодавчих та інших нормативно-правових актів урядових органів, а також органів місцевого самоврядування (залежно від рівнів інформаційної системи), ведення банку даних методичних рекомендацій із судової та нотаріальної практики, пошук необхідної нормативної інформації за різних умов.

Автоматизованою підтримкою має бути забезпечена також правотворча, легалізаційна і консультативна діяльність органів юстиції. В ІС на всіх рівнях і в усіх підрозділах органів юстиції має бути присутня підсистема діловодства, до завдань якої вхо-

дять облік вхідної та вихідної кореспонденції, підготовка і контроль за виконанням документів. Для автоматизації бухгалтерського обліку та інших подібних внутрішніх задач можуть бути використані сучасні універсальні (такі, що не мають галузевої спеціалізації) прикладні програмні продукти. Інформаційна система органів юстиції також має забезпечувати інформаційні взаємозв'язки з ІС органів законодавчої і виконавчої влади, зокрема з ІС інших правоохоронних органів.



Інформаційні системи Міністерства юстиції — досвід США

На забезпечення виконання Акта про свободу інформації від 1966 року (The Freedom of Information Act, FOIA), згідно з яким будь-яка особа має право на доступ до інформаційних записів федеральних агентств, сайт Міністерства юстиції США (Department of Justice, <http://www.usdoj.gov/>) містить рекомендації щодо процедури подання такого запиту. Зокрема, на сайті описано всі інформаційні системи Міністерства (понад 150), для кожної з яких наведено назву; акронім, якщо такий є; повні реквізити розробника, включаючи приймальні години; стислий опис і мету функціонування системи; обмеження на доступ; джерело інформації; реквізити підрозділу (установи), відповідального за надання інформації, включаючи приймальні години; процедуру подання запиту; підрозділ (установу), який може надати додаткову інформацію.

З метою розробки та впровадження комп'ютерних технологій в органах юстиції, створення комп'ютерної мережі Міністерства юстиції та організації міжвідомчої інформаційної взаємодії у 1997 році було засноване державне підприємство «Інформаційний центр» Міністерства юстиції України (Держінформ'юст), яке працює виключно на госпрозрахунковій основі. Його організаційна структура містить головне підприємство і 25 регіональних філій в обласних центрах України та місті Севастополі. Серед основних напрямків діяльності цього підприємства — інформатизація нотаріату України, судової діяльності та органів реєстрації актів громадянського стану. Держінформ'юст є адміністратором реєстрів Міністерства юстиції (див. далі) — супроводжує програмно-інформаційне забезпечення реєстрів, відповідає за їхнє функціонування, збереження даних і захист їх від руйнування, надає і контролює доступ до реєстрів реєстраторів і користувачів. Реєстратори укладають відповідні угоди з адміністратором і мають повний прямий доступ до реєстру через комп'ютерну мережу.

7.2. ЄДИНІ ТА ДЕРЖАВНІ РЕЄСТРИ МІНІСТЕРСТВА ЮСТИЦІЇ

Визначальним аспектом нотаріальної діяльності є інформаційний, тому впровадження комп'ютерних технологій у нотаріальний процес стало пріоритетним серед сукупності різних технологічних та організаційних рішень у Міністерстві юстиції. Першим проектом у цьому контексті стало впровадження в 1994 році Управлінням юстиції в м. Києві разом з Агентством нерухомості «Янус» на базі Першої київської державної нотаріальної контори комп'ютерного реєстру заборон на відчуження об'єктів нерухомого майна по місту Києву. На основі досвіду його використання та вивчення міжнародного досвіду в 1997 році реалізовано концепцію створення Єдиного реєстру заборон на відчуження об'єктів нерухомого майна.

В основу цієї концепції покладено такі *принципові рішення*:

- державна власність на банки даних, в яких здійснюється нагромадження та оброблення нотаріальної інформації;
- централізоване зберігання та оброблення інформації;
- оброблення запитів користувачів у реальному часі з реєстрацією запитів в електронному журналі;
- застосування програмних та технічних засобів, придатних для створення промислових систем (ОС UNIX, СКБД Oracle).

За цією концепцією організовані й інші реєстри, кількість яких постійно збільшується.

7.2.1. Єдиний державний реєстр нормативно-правових актів

Єдиний державний реєстр нормативно-правових актів — це автоматизована система збирання, накопичення та опрацювання актів законодавства, яка складається з еталонного, страхового, робочого, інформаційного фондів та окремого розділу.



Єдиний державний реєстр нормативно-правових актів — складові

Еталонний фонд реєстру — комп'ютерна інформаційна система, призначена для зберігання та обліку еталонних текстів нормативно-правових актів у контрольному стані. Еталонний фонд формується і зберігається в Міністерстві юстиції. Цілісність еталонного тексту реєстру у формі комп'ютерного файла забезпечується за допомогою спеціальних ознак.

Робочий фонд реєстру — комп'ютерна інформаційна система, яка підтримує технологію ведення реєстру і використовується для підготовки та опрацювання текстів нормативно-правових актів при внесенні їх до еталонного фонду реєстру.

Страховий фонд реєстру — архівні копії еталонного фонду реєстру, які зберігаються в Мін'юсті на електронних носіях і призначені для відновлення в автентичній формі еталонного фонду реєстру в разі його повної або часткової втрати.

Інформаційний фонд реєстру — спеціально створена для надання широкому колу користувачів інформації з реєстру комп'ютерна інформаційна система у формі окремої бази даних, в якій зберігаються копії еталонних текстів нормативно-правових актів.

Окремий розділ реєстру — комп'ютерна інформаційна система, що використовується для підготовки та накопичення текстів нормативно-правових актів з відповідним грифом секретності. Ведення цього розділу здійснюється відповідно до вимог законодавства.

Реєстр створено за Постановою Кабінету Міністрів України від 11.12.1996 р. № 1504 «Про запровадження Єдиного державного реєстру нормативних актів та здійснення правової інформатизації України».

Мета створення реєстру — забезпечення додержання єдиних принципів ідентифікації нормативно-правових актів та ведення їх державного обліку в межах інформаційного простору України; створення фонду та підтримання в контрольному стані нормативно-правових актів, надання інформації про них; забезпечення в межах, визначених законодавством, доступності, гласності та відкритості правової інформації для користувачів.

Мін'юст — держатель реєстру — розробляє організаційні та методологічні принципи ведення реєстру, приймає рішення про включення нормативно-правових актів до реєстру, здійснює їх опрацювання, ідентифікацію, класифікацію, відповідає за автентичність та контрольний стан еталонних текстів, забезпечує внесення нормативно-правових актів до еталонного фонду і його збереження та здійснює контроль за наданням інформації з реєстру. Держінформ'юст відповідає за технічну підготовку текстів нормативно-правових актів для внесення їх до відповідного фонду реєстру зі збереженням спеціальних ознак для забезпечення їх цілісності; формування і підтримання інформаційного фонду; відповідність інформації, що надається юридичним і фізичним особам з інформаційного фонду реєстру, еталонним текстам реєстру. Користувачами реєстру можуть бути будь-які юридичні та фізичні особи, які мають доступ до інформаційного фонду реєстру.

До реєстру включаються:

- нормативно-правові акти, видані починаючи з дня прийняття Акта проголошення незалежності України, — чинні, опубліковані та неопубліковані, у тому числі з обмежувальними грифами, закони України, постанови Верховної Ради України, укази і розпорядження Президента України, декрети, постанови і розпорядження Кабінету Міністрів України, рішення і висновки Конституційного Суду України, зареєстровані в Мін'юсті нормативно-правові акти міністерств, інших центральних органів виконавчої влади, органів господарського управління та контролю, Національного банку, а також міжнародні договори України;
- нормативно-правові акти, видані до прийняття Акта проголошення незалежності України, що не втратили чинності та не суперечать законодавству України;
- тимчасові нормативно-правові акти з терміном дії рік і більше та з терміном дії менше року в разі наступного його продовження.

Не підлягають включенню до реєстру акти, які не містять правових норм, зокрема: про призначення на посаду та звільнення з посади; про скликання нарад, конференцій, семінарів тощо; про розгляд проектів нормативно-правових актів; з питань організації виконання раніше прийнятих нормативно-правових актів; про спорудження пам'ятників, бюстів, монументів конкретним особам і на честь певних подій, нагородження грамотами, відзнаками тощо; про затвердження стандартів, технічних умов, будівельних норм і правил, іншої нормативно-технічної документації, тарифно-кваліфікаційних довідників, форм звітності.

Для включення до реєстру повні офіційні тексти рішень і висновків Конституційного Суду України, нормативно-правових актів з усіма додатками, прийнятих Верховною Радою України, Президентом України, Кабінетом Міністрів України, подаються до Мін'юсту протягом трьох робочих днів з дня їх прийняття (законів України — протягом трьох робочих днів з дня підписання Президентом України). Тексти міжнародних договорів України із зазначенням дати підписання, дати ратифікації (затвердження), дати набрання чинності та терміну дії договору подаються Міністерством зовнішніх справ (МЗС) протягом п'яти робочих днів з дня набрання ними чинності. МЗС надає також інформацію про денонсацію, внесення змін до міжнародних договорів України.

Нормативно-правові акти, які підлягають державній реєстрації відповідно до Указу Президента України від 3.10.1992 р. № 493 «Про державну реєстрацію нормативно-правових актів мініс-

терств та інших органів виконавчої влади» та постанови Кабінету Міністрів України від 28.12.1992 р. № 731 «Про затвердження Положення про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади», включаються до реєстру після їх державної реєстрації в Мін'юсті.

Для включення до реєстру нормативно-правові акти подаються Мін'юсту на електронних та паперових носіях. Копія нормативно-правового акта має бути підписана відповідальною особою та засвідчена печаткою органу, що його видав, копія міжнародного договору України — МЗС.

Рішення про включення нормативно-правового акта до реєстру ухвалюється протягом п'яти робочих днів з дня його подання, після чого органу, який видав цей акт, надсилається відповідне повідомлення.

До реєстру вносяться такі дані *про нормативно-правовий акт*: дата, номер, назва, текст, реєстраційний код, дата присвоєння реєстраційного коду, дата реєстрації в Мін'юсті, реєстраційний номер, класифікаційний індекс.

Реєстраційний код акта — це система цифрових знаків, що складається з двох частин: порядкового номера, який присвоюється нормативно-правовому акту при прийнятті рішення про включення його до реєстру, і року прийняття такого рішення.

Нормативно-правові акти, включені до реєстру, підтримуються Мін'юстом в контрольному стані.

Юридичні та фізичні особи за встановлену плату можуть одержати копії еталонних текстів нормативно-правових актів з інформаційного фонду реєстру на електронних чи паперових носіях шляхом звернення до адміністратора реєстру або безпосереднього санкціонованого доступу до інформаційного фонду реєстру. Верховна Рада України, Кабінет Міністрів України, Адміністрація Президента України, Конституційний Суд України, Верховний Суд України, Вищий господарський суд України, Генеральна прокуратура України, центральні органи виконавчої влади одержують інформацію з реєстру безоплатно.

Для забезпечення контролю за доступом до інформаційного фонду реєстру кожному користувачеві видається унікальний програмно-технічний ключ-ідентифікатор.

У разі внесення змін, доповнень або визнання таким, що втратив чинність, акта законодавства, відповідно до якого прийнято нормативно-правовий акт, орган, що видав цей нормативно-правовий акт, зобов'язаний у місячний термін внести до нього відповідні зміни, доповнення або визнати його таким, що втратив

чинність, що підлягає державній реєстрації в описаному вище порядку.

Нормативно-правовий акт, рішення про державну реєстрацію якого скасовано, виключається з державного реєстру через 10 днів після ухвалення рішення про його скасування, а в разі оскарження цього рішення — з дня отримання реєструючим органом висновку за результатами розгляду скарги. Нормативно-правовий акт, виключений з державного реєстру, підлягає негайному скасуванню органом, що його видав.

7.2.2. Єдиний реєстр заборон відчуження об'єктів нерухомого майна

Єдиний реєстр заборон відчуження об'єктів нерухомого майна — це комп'ютерна база даних, яка містить відомості про накладені заборони та арешти; зняття заборон та арештів; видані довідки про відсутність або наявність заборон та арештів.

Реєстр запроваджений у травні 1997 року.

Мета створення реєстру — захист майнових прав та інтересів громадян і організацій шляхом накопичення та використання даних про заборону відчуження й арешти нерухомого майна юридичних та фізичних осіб. Реєстром користуються нотаріуси України та правоохоронні органи. На цей час реєстр охоплює понад 80 обласних та великих промислових міст, де здійснюється до 70 % операцій з нерухомим майном.

Реєстратори — державні нотаріальні контори, державні нотаріальні архіви, приватні нотаріуси — приймають повідомлення про накладені (зняті) заборони та арешти від інших установ та осіб, які мають право накладати (зняти) заборони або арешти, вносять відповідні записи до реєстру й отримують довідки про відсутність чи наявність заборони або арешту щодо вчинюваних ними нотаріальних дій, а також видають такі довідки за письмовим запитом. Реєстратори несуть у повному обсязі відповідальність за помилки, яких вони припустилися під час реєстрації накладення або зняття заборон та арештів, надання довідок, а також за неправомірну відмову у внесенні записів до реєстру та в наданні довідок.

Користувачі реєстру — державні нотаріальні контори та приватні нотаріуси, які уклали відповідні угоди з адміністратором, мають доступ до реєстру через комп'ютерну мережу, отримують довідки про відсутність або наявність заборони та арештів у зв'язку із вчиненням ними нотаріальних дій. Користувачі несуть

у повному обсязі відповідальність за помилки, допущені ними при виготовленні довідок.

Для роботи реєстраторові (користувачеві) надається ідентифікатор та пароль, при цьому визначаються виконавці, які будуть працювати з програмою (оператори). Факт встановлення програми та адреса розташування комп'ютерного робочого місця реєструються Держінформ'юстом.

Підстави для внесення у реєстр відомостей про накладені заборони відчуження та арешти об'єктів нерухомого майна такі:

- накладення заборони відчуження на об'єкт нерухомого майна державним або приватним нотаріусом, які є реєстраторами;
- повідомлення про накладення заборони відчуження на об'єкт нерухомого майна державною нотаріальною конторою або приватним нотаріусом, які не є реєстраторами;
- повідомлення посадової особи виконавчого комітету сільської, селищної, міської ради про накладення заборони відчуження на об'єкт нерухомого майна;
- повідомлення судових і слідчих органів про накладення арешту на об'єкт нерухомого майна;
- повідомлення органів державної виконавчої служби про накладення арешту на об'єкти нерухомого майна.

Заборону на відчуження об'єктів нерухомого майна знімають нотаріуси, які є реєстраторами. Підставами для цього можуть бути також відповідні повідомлення від державних нотаріальних контор або приватних нотаріусів, які не є реєстраторами; посадових осіб виконавчого комітету сільської, селищної або міської ради; судових і слідчих органів. Органи та особи, які надали інформацію про накладення (зняття) заборон або арештів, що вносяться до реєстру, несуть відповідальність за її вірогідність.

Повідомлення про накладення (зняття) заборони відчуження або арешту об'єктів нерухомого майна надсилаються реєстратору в день виконання відповідної дії. У ньому зазначаються такі дані: відомості про нотаріуса, орган або посадову особу, які виконали дію; дата та час виконання дії; відомості про документ, на підставі якого виконано дію (найменування, номер, дата, видавець); відомості про об'єкт, на який було накладено заборону відчуження або арешт (назва, адреса розташування, розмір частки, площа тощо); відомості про власника майна, щодо якого накладено заборону відчуження або арешт (для фізичних осіб — прізвище, ім'я, по батькові; місце проживання; серія, номер та дата видачі паспорта; для юридичних осіб — найменування, юридична адреса).

Відомості про накладені заборони та арешти вносяться до реєстру в день їх надходження.

Довідки про відсутність або наявність заборони відчуження та арештів об'єктів нерухомого майна мають право одержувати:

- державні нотаріальні контори та приватні нотаріуси;
- за письмовим запитом — суди, прокуратура, органи дізнання і слідства — у зв'язку з кримінальними, цивільними або господарськими справами, що перебувають у їх провадженні, а також органи державної виконавчої служби — у зв'язку з відкриттям виконавчого провадження;
- за письмовим запитом БТІ — у зв'язку зі здійсненням ними реєстрації прав власності на нерухоме майно — довідки про відсутність арештів об'єктів нерухомого майна.

7.2.3. Єдиний реєстр захисних знаків та спеціальних бланків нотаріальних документів

Єдиний реєстр захисних знаків та спеціальних бланків нотаріальних документів — це комп'ютерна база даних, призначена для обліку надходження і витрачання спеціальних бланків і знаків, перевірки їх справжності та статистичного аналізу. Єдиний реєстр включає реєстр нотаріусів (державних і приватних, див. п. 7.2.4) і реєстр спеціальних бланків та знаків нотаріальних документів.

Реєстр запроваджений у серпні 1997 року.

Мета створення — надання нотаріусам України та правоохоронним органам можливості перевірити справжність нотаріальних документів, виконаних на спеціальних бланках нотаріальних документів, що сприяє уникненню укладання угод, які суперечать законним інтересам фізичних та юридичних осіб. Щоденно у реєстр вносяться відомості про витрачання близько 21 тис. бланків.

Ведення реєстру покладено на Держінформ'юст, який також відповідає за організацію виготовлення захисних знаків, їх постачання державним нотаріальним конторам і приватним нотаріусам; ведення обліку постачання і витрачання захисних знаків та спеціальних бланків нотаріальних документів. Аналогічні функції щодо спеціальних бланків нотаріальних документів виконує підприємство «Інформаційно-видавничий центр українського нотаріату» (ІВЦУН). Бланки та знаки виготовляються відповідно до зразка й опису, затверджених Міністерством юстиції України. Міністерство юстиції забезпечує

організацію постачання, зберігання, обліку постачання й звітності витрачання бланків та знаків.

Відомості для внесення до реєстру надходять до Держінформ'юсту з управління юстиції, від державних нотаріальних контор, приватних нотаріусів та ІВЦУН. Первинні документи обліку такі:

- у Міністерстві юстиції України — журнал реєстрації виданих свідоцтв про право на заняття нотаріальною діяльністю;
- в управлінні юстиції — журнал реєстрації приватної нотаріальної діяльності; повідомлення відділу кадрів управління юстиції про призначення, переведення та звільнення державних нотаріусів; видаткова накладна на відправлення бланків (знаків) ІВЦУН (Держінформ'юстом); звіт про витрачання бланків; копії доповідних записок про викрадені бланки та знаки; акти про прийняття-передання або знищення зіпсованих, анульованих і дефектних бланків та знаків.

Управління юстиції до 10 числа кожного місяця в порядку, встановленому Міністерством юстиції України, надсилають Держінформ'юсту для ведення реєстру нотаріусів повідомлення про зміни в складі приватних нотаріусів і державних нотаріальних контор.

Державні нотаріальні контори та приватні нотаріуси щомісячно до 10 числа наступного за звітним місяця надсилають Держінформ'юсту звіти про витрачання бланків та знаків, у яких зазначаються серія, номери бланків і знаків, коди та дата їх витрачання.

ІВЦУН щоденно надсилає до Держінформ'юсту відомості про постачання бланків державним нотаріальним конторам і приватним нотаріусам.

Копії доповідних записок про викрадені бланки та знаки державні нотаріальні контори й приватні нотаріуси надсилають до Держінформ'юсту негайно в разі виявлення факту крадіжки.

Дані, що містяться в реєстрі, доступні для перевірки всім користувачам інформаційної мережі Міністерства юстиції України. Перевірка може здійснюватись за допомогою телефонного зв'язку з черговим адміністратором реєстру.

ІВЦУН, державні нотаріальні контори та приватні нотаріуси відповідають за своєчасність і вірогідність відомостей, наданих Держінформ'юсту для внесення до реєстру.

Держінформ'юст відповідає за своєчасність унесення та відповідність даних у реєстрі даним звітів державних нотаріальних контор і приватних нотаріусів та відомостям, наданим ІВЦУН.

7.2.4. Єдиний реєстр нотаріусів України

Єдиний реєстр нотаріусів України — це комп'ютерна база даних, у якій містяться відомості про нотаріальні округи, державні нотаріальні контори, державних та приватних нотаріусів України.

Реєстр введений у дію в серпні 1997 року.

Мета створення реєстру — забезпечення упорядкування обліку державних та приватних нотаріусів України.

Ведення реєстру здійснює Держінформ'юст. Він несе відповідальність за зміст даних реєстру. Дані, що містяться в реєстрі (за винятком особових даних), доступні для перевірки всім користувачам інформаційної мережі Міністерства юстиції України.

Інформація вноситься до реєстру на підставі повідомлень, що їх щомісяця надсилають Держінформ'юсту його філії. За своєчасності надання, повноту та вірогідності відомостей, що надаються філією Держінформ'юсту, відповідає директор філії.

Повідомлення про внесення відомостей до реєстру повинно містити назву регіону, дату складання повідомлення, змістову частину повідомлення, посаду і прізвище особи, яка склала повідомлення.

Змістова частина повідомлення складається з реквізитів таких форм:

1. «Прийом на роботу державного нотаріуса» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю та дата його видачі (якщо цих відомостей немає — причина їх відсутності); дата прийому на роботу; місце роботи (назва нотаріальної контори); посада; дата народження; домашня адреса та телефон (за згодою нотаріуса);

2. «Звільнення державного нотаріуса» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю; місце роботи (назва нотаріальної контори); посада; дата звільнення;

3. «Переведення державного нотаріуса на іншу посаду в межах області (міста)» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю та дата його видачі (якщо ці відомості відсутні — причина їх відсутності); дата переведення; нове місце роботи (назва нотаріальної контори); посада;

4. «Переведення державного нотаріуса на нову посаду в межах нотаріальної контори» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю та дата його видачі (якщо ці відомості відсутні — причина їх відсутності); дата переведення; місце роботи (назва нотаріальної контори); посада (нова);

5. «Реєстрація приватної нотаріальної діяльності» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю та дата його видачі; номер реєстраційного посвідчення про реєстрацію приватної нотаріальної діяльності та дата його реєстрації; нотаріальний округ; поштовий індекс та адреса розташування робочого місця; робочий телефон; дата народження; домашня адреса і телефон (за згодою нотаріуса);

6. «Тимчасове припинення (призупинення) приватної нотаріальної діяльності» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю; дата, термін і підстава тимчасового припинення (призупинення) приватної нотаріальної діяльності;

7. «Поновлення приватної нотаріальної діяльності» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю; номер реєстраційного посвідчення; дата поновлення приватної нотаріальної діяльності;

8. «Зміна адреси розташування робочого місця приватного нотаріуса (робочого телефону) в межах одного нотаріального округу» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю; поштовий індекс та адреса розташування робочого місця (нового); робочий телефон (новий);

9. «Зміна нотаріального округу приватного нотаріуса» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю; нотаріальний округ (новий); поштовий індекс та адреса розташування робочого місця; робочий телефон;

10. «Припинення приватної нотаріальної діяльності» — прізвище, ім'я, по батькові; номер свідоцтва про право на заняття нотаріальною діяльністю; дата і підстава припинення приватної нотаріальної діяльності (наказ начальника управління, наказ Міністра юстиції);

11. «Зміна прізвища нотаріуса» — колишнє прізвище, ім'я та по батькові; нове прізвище; номер свідоцтва про право на заняття нотаріальною діяльністю.

7.2.5. Єдиний реєстр доручень

Єдиний реєстр доручень, посвідчених у нотаріальному порядку — це комп'ютерна база даних, в якій здійснюється обов'язкова реєстрація посвідчених нотаріусами доручень на право користування та/або розпорядження майном, у тому числі транспортними засобами, а також реєстрація припинення їх дії.

Реєстр започаткований у травні 1998 року.

Метою створення реєстру є профілактика злочинів проти власності завдяки нагромадженню та використанню нотаріусами, органами ДАІ та іншими правоохоронними органами відомостей про посвідчені доручення. Щоденно у реєстрі реєструється понад 7000 доручень.

Реєстратори вносять записи про посвідчені доручення, про припинення дії доручень та перевіряють дійсність доручень через запити до реєстру.

Користувачі реєстру — державні нотаріальні контори, приватні нотаріуси та інші установи й організації, які уклали відповідні угоди з адміністратором, мають доступ до реєстру через комп'ютерну мережу, перевіряють дійсність доручень шляхом запитів до нього.

Установи та організації, яким може бути надано право користування реєстром (за умови, що перевірка дійсності доручень потрібна їм у зв'язку з виконанням покладених на них обов'язків і не порушує таємниці нотаріальних дій), визначаються Міністерством юстиції України.

Внесення запису до реєстру здійснюється реєстратором в день посвідчення доручення або отримання заяви про реєстрацію доручень від інших нотаріусів чи адміністратором в день отримання такої заяви. Заяви про реєстрацію доручень подаються державними та приватними нотаріусами не пізніше наступного дня після посвідчення доручень. Реєстраційний запис має містити: номер та серію спеціального бланка нотаріальних документів, на якому викладено текст доручення; дату посвідчення доручення; строк дії доручення; номер запису в реєстрі нотаріальних дій; посаду, прізвище, ім'я, по батькові нотаріуса, який посвідчив доручення.

До реєстру вносяться відомості про припинення дії доручення в разі одержання нотаріусами заяви від особи, яка видала доручення, про його скасування або заяви від особи, якій видано доручення, про відмову від нього, а також у разі одержання повідомлень про припинення діяльності юридичної особи, від імені якої видано доручення, або про смерть громадянина, який видав доручення, про визнання його недієздатним, обмежено дієздатним або безвісти пропалим. Відомості вносяться в день їх одержання.

Реєстраційний запис про припинення дії доручення має містити: підставу і дату припинення доручення; прізвище, ім'я, по батькові нотаріуса, якому надійшло повідомлення про припинення дії

доручення; серію та номер спеціального бланка нотаріальних документів, на якому викладено текст цього доручення; дату його посвідчення; номер відповідного запису в реєстрі нотаріальних дій; посаду, прізвище, ім'я, по батькові нотаріуса, який посвідчив доручення.

На прохання особи, яка бажає припинити дію доручення, що було посвідчено відповідно до чинного законодавства до введення в дію Єдиного реєстру доручень або не було зареєстровано в цьому реєстрі з інших причин, нотаріус одночасно вносить до реєстру доручень реєстраційний запис та відомості про припинення дії такого доручення.

Нотаріуси при посвідченні угод за участю осіб, які діють на підставі доручень, користуються даними реєстру (за відсутності комп'ютерного доступу — за запитом до адміністратора або реєстратора, який містить серію та номер спеціального бланка нотаріальних документів, на якому викладено текст доручення), перевіряючи за їх допомогою дійсність цих доручень, строк їхньої дії тощо.

7.2.6. Державний реєстр застав рухомого майна

Державний реєстр застав рухомого майна — єдина комп'ютерна база даних, яка забезпечує зберігання інформації про застави рухомого майна, її видання та захист від несанкціонованого доступу.

Реєстр уведений в дію 1.03.1999 р. і функціонує відповідно до статей 15, 151 Закону України «Про заставу» та постанови Кабінету Міністрів України від 30.07.1998 р. № 1185.

Мета створення реєстру — забезпечення переважного права заставодержателя у задоволенні вимог із заставленого майна перед заставодержателями незареєстрованих або зареєстрованих пізніше застав; надання в інтересах юридичних та фізичних осіб інформації про заставлене рухоме майно або про відсутність застав рухомого майна.

Міністерство юстиції — держатель реєстру — надає завірені витяги з нього, які свідчать про внесення запису або про його відсутність.

Реєстраторами є Держінформ'юст, державні нотаріальні контори, приватні нотаріуси, комерційні банки, які згідно з відповідними договорами з Держінформ'юстом приймають заяви про внесення записів до реєстру, внесення змін до записів, виключення записів з реєстру, приймають запити, надають витяги з реєстру та ін.

Суб'єкти реєстрації застав рухомого майна — заставодавець, заставодержатель або особи, які діють від їх імені за дорученням, орган державної податкової служби, реєстратори, держатель реєстру.

Будь-яка фізична чи юридична особа може користуватися інформацією у реєстрі шляхом підключення до нього через комп'ютерну мережу. Підключення здійснюється адміністратором реєстру на підставі відповідного договору.

Реєстрація застави рухомого майна в реєстрі здійснюється реєстратором за вибором заявника, яким може бути заставодержатель або заставодавець. Заява реєструється у Книзі обліку заяв, де зазначаються: вхідний номер і дата надходження заяви; відомості про заявника¹; дата реєстрації застави або відмови в реєстрації; реєстраційний код застави рухомого майна в реєстрі. У заяві зазначаються: відомості про заставодавця та заставодержателя¹ і загальний опис предмета застави².

Під час подання заяви заявник пред'являє паспорт або інший документ, що засвідчує його особу, а в разі, коли він діє від імені заставодавця або заставодержателя, — відповідне доручення. До заяви додається документ про внесення плати за здійснення запису до реєстру.

Реєстратор видає заявникові довідку про прийняття заяви, в якій зазначаються відомості про реєстратора і заявника та дата прийняття заяви, або відмову у внесенні запису в письмовій формі з зазначенням причин відмови. Будь-яка особа на підставі такої довідки має право безоплатно отримати від реєстратора витяг, який свідчить про реєстрацію застави рухомого майна. У витягу зазначаються: дата реєстрації застави рухомого майна; відомості про заставодержателя та заставодавця; загальний опис предмета застави.

Запис до реєстру вноситься реєстратором протягом двох днів з дати прийняття заяви. Запис містить: відомості про заставодавця та заставодержателя; відомості про предмет застави; вхідний но-

¹ Для юридичних осіб — резидентів — найменування, юридична адреса та ідентифікаційний код в Єдиному державному реєстрі підприємств та організацій України (ЄДРПОУ). Для юридичних осіб — нерезидентів — найменування, юридична адреса та країна, де зареєстровано особу. Для фізичних осіб — громадян України — прізвище, ім'я, по батькові, адреса постійного місця проживання та ідентифікаційний номер у Державному реєстрі фізичних осіб. Для іноземців — прізвище, ім'я, по батькові (в разі наявності такого), країна та адреса постійного місця проживання за межами України.

² Якщо предметом застави є рухоме майно, яке підлягає державній реєстрації відповідно до законодавства (транспортні засоби: автомобілі, причепи, катери, судна, літаки тощо), до загального опису включаються відомості щодо серійного номеру транспортного засобу, назви моделі та року виробництва.

мер заяви, за якою вноситься запис; дата прийняття заяви; дата внесення відомостей до реєстру; реєстраційний код запису; відомості про реєстратора; прізвище посадової особи, яка внесла запис до реєстру. Дата внесення відомостей до реєстру, відомості про реєстратора та реєстраційний код запису в реєстрі визначаються і вносяться автоматично. Реєстраційний код запису, визначений системою, заноситься реєстратором у Книгу обліку заяв.

Датою реєстрації застави рухомого майна в реєстрі вважається дата внесення до нього відповідного запису. Протягом двох робочих днів з дати реєстрації застави рухомого майна реєстратор поштою направляє заставодержателеві та заставодавцеві витяги, які свідчать про внесення відповідного запису до реєстру і реєструються в Книзі обліку витягів. Заставодержателеві надсилається також бланк заяви про внесення змін до запису для заповнення в разі виявлення помилок у витягу.

Внесення змін до реєстру здійснюється в порядку, аналогічному до внесення записів.

Записи про реєстрацію застави рухомого майна у реєстрі зберігаються з дати внесення до дати виключення запису, але не більше п'яти років. Заставодержатель може продовжити термін дії реєстрації застави рухомого майна в будь-який час протягом останнього року дії такої реєстрації на наступні п'ять років шляхом подачі відповідної заяви.

Виключення запису про реєстрацію застави рухомого майна в реєстрі виконується в разі закінчення 5-річного терміну; надходження заяви заставодержателя про виключення запису з реєстру; рішення суду. При цьому в реєстрі вказуються підстава і дата виключення запису, відомості про реєстратора. Після виключення запису з реєстру протягом двох днів заставодавцеві та заставодержателеві надсилаються відповідні витяги.

Витяг з реєстру про наявність або відсутність у ньому запису про заставлене рухоме майно, фізичні та юридичні особи можуть одержати шляхом подання запиту держателеві реєстру або реєстратору. Запит за підписом заявника має містити один із варіантів:

- реєстраційний код запису в реєстрі;
- найменування або код в ЄДРПОУ для юридичної особи, що є заставодавцем;
- прізвище, ім'я, по батькові або ідентифікаційний номер у Державному реєстрі фізичних осіб для фізичної особи, що є заставодавцем;
- серійний номер транспортного засобу, назва моделі, якщо предметом застави є транспортний засіб.

У запиті зазначається вид витягу (завірений чи незавірений), який бажає отримати заявник, і адреса, якщо заявник бажає отримати витяг поштою. До запиту додається документ про внесення плати за одержання витягу. Факт надання витягів реєструється в базі даних реєстру.

Існують певні особливості реєстрації *податкової застави рухомого майна*. Підставою для реєстрації такої застави є заява відповідного органу державної податкової служби, яка за підписом відповідної посадової особи подається адміністратору реєстру. У заяві зазначаються відомості про платника податків (див. примітку вище); дата виникнення податкової застави; відомості про орган державної податкової служби, за заявою якого здійснюється реєстрація. Реєстрація податкової застави здійснюється безоплатно.

До реєстру вносяться: відомості про орган державної податкової служби — найменування, юридична адреса та код в ЄДРПОУ; вхідний номер заяви, за якою здійснюється реєстрація, та дата її надходження; відомості про платника податків (для юридичної особи — найменування, юридична адреса та код в ЄДРПОУ; для фізичної особи — суб'єкта підприємницької діяльності — прізвище, ім'я, по батькові, адреса постійного місця проживання та ідентифікаційний номер у Державному реєстрі фізичних осіб); дата виникнення податкової застави; дата внесення відомостей до реєстру; реєстраційний код запису; відомості про адміністратора; прізвище посадової особи, яка внесла запис.

Протягом двох робочих днів з дати реєстрації податкової застави адміністратор поштою направляє відповідному органу державної податкової служби та платнику податків витяги, що свідчать про внесення відповідного запису до реєстру. У витягу зазначаються: реєстраційний код запису; дата реєстрації податкової застави; дата виникнення податкової застави; відомості про платника податків; відомості про орган державної податкової служби, за заявою якого внесено запис до реєстру. Відповідному органу державної податкової служби надсилається також примірник заяви про внесення змін до запису для заповнення в разі виявлення помилок у витягу.

Записи про реєстрацію податкової застави рухомого майна у реєстрі зберігаються з дати внесення до дати виключення запису, але не більше п'яти років. Запис про податкову заставу підлягає виключенню з реєстру на підставі повідомлення відповідного органу державної податкової служби про припинення податкової застави.

7.2.7. Єдиний державний реєстр об'єднань громадян та благодійних організацій

Єдиний державний реєстр об'єднань громадян та благодійних організацій — це комп'ютерна база даних, створена за допомогою автоматизованої комп'ютерної системи, яка складається із сукупності електронних копій державних реєстрів об'єднань громадян та благодійних організацій, книг обліку філій, представництв всеукраїнських, міжнародних благодійних організацій, об'єднаних на основі єдиних правил, стандартів та процедур обміну інформацією.

Єдиний державний реєстр об'єднань громадян та благодійних організацій введений у дію 10.03.1999 р. на виконання Законів України «**Про об'єднання громадян**» та «**Про благодійництво та благодійні організації**», а також Положення про порядок легалізації об'єднань громадян і Положення про порядок державної реєстрації благодійних організацій, затверджених постановами Кабінету Міністрів України, відповідно, № 40 від 26.02.1993 р. і № 382 від 30.03.1998 р.

Мета створення реєстру — забезпечення переважного права на використання назви об'єднання громадян, яке зареєстровано в реєстрі, перед іншими об'єднаннями, що легалізуються пізніше.

Реєстраторами є Міністерство юстиції України, Головне управління юстиції Міністерства юстиції України в Автономній Республіці Крим, управління юстиції в областях, а також управління юстиції в містах Києві та Севастополі.

У день державної реєстрації до реєстру вносять такі реквізити: реєстраційний номер і дата реєстрації; назва; статус; дата надходження документів на реєстрацію; мета діяльності; юридична адреса; відомості про засновників; відомості про органи управління; номер та дата видачі свідоцтва про державну реєстрацію, його дубліката чи дубліката статуту; відомості про зміни, внесені до статутних документів; відомості про припинення діяльності (ліквідацію, реорганізацію); реєстраційний орган, який здійснив державну реєстрацію організації.

Про зареєстровані філії та представництва всеукраїнських, міжнародних благодійних організацій до реєстру вносять такі реквізити: назва філії, представництва всеукраїнської або міжнародної благодійної організації; дата надходження документів на реєстрацію; юридична адреса; номер та дата видачі свідоцтва про державну реєстрацію всеукраїнської або міжнародної благодійної

організації; відомості про припинення діяльності (реорганізацію або ліквідацію); номер та дата листа-повідомлення про реєстрацію; реєстраційний орган, який здійснив реєстрацію.

Внесення до реєстру відомостей здійснюється безкоштовно.

7.2.8. Єдиний реєстр заповітів та спадкових справ

Єдиний реєстр заповітів та спадкових справ — це комп'ютерна база даних, що містить відомості про заповіти та спадкові справи.

Реєстр введений у дію 1 грудня 2000 року.

Мета створення реєстру — захист майнових прав та інтересів громадян і юридичних осіб, створення єдиної системи обліку заповітів та спадкових справ, зменшення навантаження на суди за рахунок розв'язання питань спадкування у безспірному порядку.

Реєстратори — державні нотаріальні контори, державні нотаріальні архіви, приватні нотаріуси — здійснюють реєстрацію посвідчення, зміни, скасування заповітів, зміни місця зберігання заповітів, заведення спадкових справ, видачу свідоцтв про право на спадщину, списання спадкових справ до архіву та зміни місця зберігання спадкових справ, а також приймають на реєстрацію відповідні заяви від інших державних нотаріальних контор, державних нотаріальних архівів, приватних нотаріусів, які не є реєстраторами, та заповідачів¹, виконують перевірки за даними реєстру і видають довідки про наявність або відсутність заповітів та спадкових справ.

Відповідальність за вірогідність відомостей, що вносяться до реєстру, несуть особи, які надали цю інформацію.

Заповіти, складені та посвідчені, змінені або скасовані в установленому законодавством порядку, та заведені спадкові справи підлягають обов'язковій реєстрації в реєстрі. Реєстрація здійснюється шляхом унесення запису до реєстру протягом 5 робочих днів із часу посвідчення реєстратором заповіту або не пізніше наступного робочого дня з часу отримання від інших нотаріусів або заповідачів¹ відповідної заяви і не пізніше наступного робочого дня з моменту заведення спадкової справи або надходження відповідної заяви. Відомості про видачу свідоцтва про право на спадщину вносяться до реєстру не пізніше 5 робочих днів після видачі такого свідоцтва або не пізніше наступного робочого дня після

¹ Див. статтю 40 Закону України «Про нотаріат».

одержання від інших нотаріусів відповідної заяви. В аналогічному порядку до реєстру вносяться реєстраційні записи про списання до архіву.

Нотаріуси, які не мають систем комп'ютерного доступу до реєстру, подають заяви встановленого зразка про реєстрацію протягом 5 робочих днів з часу посвідчення заповіту або отримання заповіту від осіб, що перераховані у ст. 40 Закону України «Про нотаріат», і не пізніше наступного робочого дня після заведення спадкової справи.

Реєстраційний запис про посвідчення заповіту має містити такі відомості: прізвище, ім'я, по батькові заповідача; дата, місце народження заповідача; серія, номер спеціального бланка нотаріального документа, на якому викладено текст заповіту; дата, час і місце посвідчення заповіту; номер запису в реєстрі для реєстрації нотаріальних дій, за яким посвідчено заповіт; місце зберігання заповіту; відомості про особу, яка посвідчила заповіт; відомості про реєстратора.

Реєстраційний запис про посвідчення заповіту, що скасовує або змінює попередній заповіт, здійснюється за заявою заповідача аналогічним чином не пізніше наступного робочого дня після вчинення нотаріальних дій або не пізніше наступного робочого дня після одержання від інших нотаріусів відповідної заяви. Він має містити такі відомості: серія та номер спеціального бланка нотаріального документа, на якому викладено текст заяви; номер запису в реєстрі для реєстрації нотаріальних дій, за яким засвідчується справжність підпису на заяві, якою змінюється або скасовується заповіт; дата зміни або скасування заповіту; відомості про заповідача (прізвище, ім'я та по батькові; дата народження; місце народження); відомості про заповіт, який змінюється або скасовується (серія та номер спеціального бланка нотаріального документа; дата посвідчення заповіту; номер запису в реєстрі для реєстрації нотаріальних дій; місце посвідчення заповіту); відомості про нотаріуса, який засвідчив справжність підпису на заяві; відомості про реєстратора.

Реєстраційний запис про заведення спадкової справи містить такі відомості: номер спадкової справи; дата заведення спадкової справи; місце заведення спадкової справи; прізвище, ім'я, по батькові спадкодавця; дата народження; дата смерті; відомості про нотаріуса, в провадженні якого знаходиться спадкова справа; місце зберігання спадкової справи; відомості про реєстратора.

Реєстраційний запис про видачу свідоцтва про право на спадщину має містити такі відомості: серія та номер спеціального

бланка нотаріального документа, на якому викладено текст свідоцтва про право на спадщину; дата видачі свідоцтва; номер запису в реєстрі для реєстрації нотаріальних дій; відомості про нотаріуса, який видав свідоцтво; відомості про реєстратора.

При надходженні заповіту або спадкової справи на зберігання до державної нотаріальної контори чи державного нотаріального архіву нотаріус безпосередньо вносить реєстраційний запис про зміну місця зберігання заповіту до реєстру або надсилає про це заяву реєстраторові.

Під час заведення спадкової справи нотаріус самостійно або шляхом подання письмового запиту реєстраторові зобов'язаний перевірити за даними реєстру наявність заведеної спадкової справи, а по закінченні 5 робочих днів після заведення спадкової справи — наявність або відсутність заповіту, складеного спадкодавцем. За результатами перевірки робиться відповідна службова позначка на заяві чи іншому документі, на підставі якого відкрита спадкова справа, і/або виготовляється витяг.

Для підтвердження факту внесення інформації до реєстру реєстратор виготовляє відповідну довідку або робить службову позначку (із зазначенням номера та дати видачі довідки) на копії заповіту, заяві про прийняття спадщини або іншому документі, що залишається у справах нотаріуса. Довідка приєднується до примірника документа, що залишається у справах нотаріуса і надається (надсилається поштою) особі, яка надала відомості на реєстрацію, протягом двох робочих днів з дати реєстрації. У разі виявлення помилок у довідці особа, яка надала відомості на реєстрацію, звертається до реєстратора із заявою про внесення змін до відповідного реєстраційного запису.

Реєстратор видає витяги про наявність або відсутність заповітів на письмовий запит нотаріусів; особи, яка є спадкоємцем за законом при пред'явленні документа, що свідчить про родинні зв'язки з спадкодавцем, та свідоцтва про смерть останнього; суду, прокуратури, органів дізнання і слідства — у зв'язку з кримінальними, цивільними або господарськими справами, що перебувають у їх провадженні при пред'явленні свідоцтва про смерть спадкодавця. У витягу про наявність заповіту зазначаються: прізвище, ім'я, по батькові заповідача; дата, місце народження заповідача; відомості про посвідчення, зміну, скасування заповіту (дата посвідчення, зміни або скасування заповіту; номер запису в реєстрі для реєстрації нотаріальних дій; серія та номер спеціального бланка нотаріального документа, на якому викладено текст заповіту або заяви про зміну чи скасування заповіту; прізвище,

ім'я та по батькові нотаріуса, який вчинив нотаріальні дії щодо посвідчення, зміни або скасування заповіту); відомості про місце зберігання заповіту; відомості про реєстратора.

Витяги про наявність або відсутність спадкової справи видаються реєстратором на письмовий запит нотаріусів. У витязі про наявність спадкової справи зазначаються: прізвище, ім'я, по батькові спадкодавця; дата смерті; місце та дата заведення спадкової справи; відомості про нотаріуса, в провадженні якого знаходиться спадкова справа; відомості про реєстратора.

Заяви до реєстру, витяги про наявність або відсутність заповіту, складеного спадкодавцем, та витяги про наявність або відсутність спадкової справи виготовляються з використанням захисних знаків нотаріальних документів. Довідки про внесення реєстраційного запису до реєстру виготовляються з використанням спеціальних бланків документів.

7.2.9. Державний реєстр атестованих судових експертів державних і підприємницьких структур та громадян

Державний реєстр атестованих судових експертів державних і підприємницьких структур та громадян є офіційною автоматизованою системою обліку фахівців, яким органи дізнання, попереднього слідства і суди зобов'язані переважно доручати проведення судової експертизи.

Реєстр ведений у дію 4.02.2002 р. відповідно до статті 9 Закону України «**Про судову експертизу**».

Метою створення реєстру є здійснення обліку атестованих судових експертів та створення інформаційного фонду про осіб, які одержали в установленому порядку дозвіл на проведення конкретного виду судової експертизи за відповідною експертною спеціальністю, а також забезпечення в установленому порядку органів дізнання, попереднього слідства й судів, інших зацікавлених юридичних та фізичних осіб необхідною інформацією з фонду реєстру.

Обов'язки з ведення реєстру, розроблення організаційних заходів та впровадження методологічних принципів, створення та підтримки у контрольному стані автоматизованої бази даних реєстру та надання інформації з використанням фонду реєстру покладено на управління інформаційного забезпечення Міністерства юстиції.

Фонд реєстру складається з державного фонду офіційних відомостей про фахівців, які одержали дозвіл на проведення судо-

вих експертиз, з державного страхового фонду і робочого фонду таких відомостей та з довідково-пошукового апарату.

До реєстру вносять такі реквізити: реєстраційний номер; прізвище, ім'я, по батькові судового експерта; дата включення до реєстру; вид експертизи, експертна спеціальність; адреса, телефон, факс судового експерта державної, підприємницької структури або судового експерта — громадянина; найменування експертно-кваліфікаційної комісії, дата і номер її рішення; номер і термін дії свідоцтва; кваліфікаційний клас судового експерта.

Підставою для включення до реєстру атестованих судових експертів державних структур та їх позаштатних співробітників є подання керівників цих структур, а для атестованих судових експертів підприємницьких структур і громадян, які проводять експертизи за разовими договорами, — їх особиста заява, що подається до Міністерства юстиції. До заяви або подання додаються копія виданого експертно-кваліфікаційною комісією державної структури свідоцтва про кваліфікацію судового експерта з дозволом на проведення конкретного виду судової експертизи за відповідною експертною спеціальністю; документ про присвоєння кваліфікаційного класу (для судових експертів державних структур); копія ліцензії на судово-експертну підприємницьку діяльність (для судових експертів підприємницьких структур). Документи, що надходять від установ і окремих експертів, становлять фонд реєстру.

Міністерство юстиції протягом десяти робочих днів з дня надходження перевіряє правильність оформлення поданих документів та приймає рішення щодо внесення даних до реєстру.

Кожному судовому експерту в реєстрі надається **особистий реєстраційний номер**, який складається з таких елементів:

- літерне позначення: «Д» — для судових експертів державних структур, «П» — для судових експертів підприємницьких структур, «Г» — для судових експертів — громадян;
- порядковий номер державної реєстрації;
- рік реєстрації.

Зміни та доповнення до реєстру вносяться за поданням керівників державних структур або особистою заявою судових експертів підприємницьких структур і громадян, до яких додаються копії документів про надання права проведення іншого виду судової експертизи або з іншої експертної спеціальності; присвоєння чергового кваліфікаційного класу або його пониження; продовження терміну дії свідоцтва про присвоєння кваліфікації судового експерта; звільнення з державної установи чи

підприємницької структури, яка провадить судову експертизу; продовження терміну дії ліцензії, виданої підприємцеві.

Підставою для виключення з реєстру є рішення експертно-кваліфікаційної комісії державної структури про позбавлення кваліфікації судового експерта та кваліфікаційного класу; скасування свідоцтва про присвоєння кваліфікації судового експерта внаслідок визнання судового експерта недієздатним або його за-судження. Підлягає також виключенню із реєстру судовий експерт у разі позбавлення підприємця ліцензії на судово-експертну діяльність, виїзду на постійне місце проживання за межі України, а також за власним бажанням.

7.2.10. Реєстр прав власності на нерухоме майно

Реєстр прав власності на нерухоме майно є інформаційною системою, яка містить відомості про зареєстровані права власності, суб'єктів прав, об'єкти нерухомого майна, правовстановлювальні документи, на підставі яких здійснено реєстрацію прав власності.

Реєстр прав власності на нерухоме майно включає в себе реєстр заяв і запитів та реєстраційні справи, які не можуть бути вилучені.

Реєстр запроваджений з 1.10.2002 р. на виконання постанов Кабінету Міністрів України від 18.02.1998 р. № 192 «Про заходи щодо створення системи реєстрації прав на нерухоме та рухоме майно» та від 16.05.2002 р. № 661 «Про заходи щодо створення системи реєстрації прав власності на нерухоме майно» до прийняття та набрання чинності законом України про державну реєстрацію прав на об'єкти нерухомого майна.

Мета створення реєстру — забезпечити визнання та захист прав власності на нерухоме майно фізичних та юридичних осіб в Україні, створення умов для функціонування ринку нерухомого майна, активізації інвестиційної діяльності.

Реєстрація прав власності на нерухоме майно — це внесення запису до реєстру прав власності на нерухоме майно у зв'язку з виникненням, існуванням або припиненням права власності на нерухоме майно, що здійснюється БТІ за місцезнаходженням об'єктів нерухомого майна на підставі правовстановлювальних документів, за рахунок коштів особи, що звернулася до БТІ.

Обов'язковій реєстрації підлягає право власності на нерухоме майно фізичних та юридичних осіб, у тому числі іноземців та

осіб без громадянства, іноземних юридичних осіб, міжнародних організацій, іноземних держав, а також територіальних громад в особі органів місцевого самоврядування. Реєстрації підлягають права власності тільки на об'єкти нерухомого майна, будівництво яких закінчено та які прийнято в експлуатацію в установленому порядку за наявності матеріалів технічної інвентаризації, підготовлених відповідним БТІ. Не підлягають реєстрації тимчасові споруди, а також споруди, не пов'язані фундаментом із землею.

Технологічні та технічні засоби ведення реєстру забезпечують довічне зберігання та достовірність інформації, її захист від несанкціонованого доступу та внесення недокументованих записів, можливість оновлення, архівування та відновлення даних, їх оперативного пошуку та документального відтворення процедури реєстрації, контроль реєстраційних записів і запитів до реєстру, оперативне надання витягів із реєстру.



Реєстр прав власності на нерухоме майно — суперечності між електронними і паперовими носіями

У разі виявлення невідповідності запису реєстру на електронних носіях запису на паперових носіях пріоритет має запис на паперових носіях.

Реєстрація прав власності здійснюється в такому порядку:

- приймання під розписку і перевірка документів, поданих для реєстрації прав власності на нерухоме майно, реєстрація заяви в реєстрі заяв та запитів;
- установлення відсутності підстав для відмови в реєстрації прав;
- прийняття рішення про реєстрацію прав власності або про відмову в реєстрації прав (не пізніше ніж через 20 робочих днів з дня отримання заяви БТІ без урахування терміну проведення інвентаризаційних робіт);
- внесення записів до реєстру;
- виконання написів на правовстановлювальних документах;
- видача витягів із реєстру про реєстрацію прав (з реєстрацією відповідних запитів у реєстрі заяв та запитів) і повернення правовстановлювальних документів (з позначкою у реєстрі заяв та запитів).

При реєстрації прав власності на нерухоме майно, які виникли відповідно до договорів про відчуження нерухомого майна між юридичними особами, в разі, якщо такі договори не були нотаріально посвідчені, юридичні особи подають також довідку про

відсутність або наявність арештів з Єдиного реєстру заборон відчуження об'єктів нерухомого майна, яка видається на підставі відповідного запиту БТІ.

Під час подання заяви про реєстрацію прав власності фізична особа повинна пред'явити документ, що посвідчує її особу, а в разі подання заяви представником фізичної чи юридичної особи — документ, що підтверджує повноваження діяти від імені цих осіб.

Заява про реєстрацію прав власності на нерухоме майно може бути відкликана заявником (заявниками) у будь-який момент до прийняття реєстратором рішення щодо цієї заяви шляхом подання письмового клопотання встановленої форми, яке реєструється у реєстрі заяв та запитів.

При реєстрації заяв вказують: порядковий номер заяви; дату її надходження; порядковий номер нерухомого майна, якщо право власності на нього вже зареєстроване; відомості про заявника¹; перелік документів, які додаються до заяви; запис про прийняте рішення, надання витягу (заноситься після прийняття рішення), дату його прийняття, прізвище реєстратора.

Рішення реєстратора про реєстрацію чи про відмову в реєстрації прав власності на нерухоме майно має містити: дату й місце прийняття рішення; стислий опис майна, щодо якого приймається рішення; підстави винесення рішення, а в разі прийняття рішення про відмову — правове обґрунтування; порядковий номер об'єкта нерухомого майна.

У реєстрації прав на нерухоме майно може бути відмовлено, якщо:

- заявлене право не є таким, що підлягає реєстрації;
- об'єкт нерухомого майна розташований на території, реєстрацію прав власності на якій здійснює інше БТІ;
- із заявою про реєстрацію прав власності на нерухоме майно звернулася особа, яка не може бути заявником;
- подані документи не відповідають вимогам або не дають змоги встановити відповідність заявлених прав і поданих документів вимогам законодавства;

¹ Для фізичних осіб — громадян України — прізвище, ім'я та по батькові, ідентифікаційний номер у Державному реєстрі фізичних осіб — платників податків та інших обов'язкових платежів. Для іноземних громадян — прізвище, ім'я та по батькові (за наявності останнього), адреса постійного місця проживання за межами України. Для юридичних осіб — резидентів — найменування, адреса постійного місцезнаходження, код в ЄДРПОУ. Для юридичних осіб — нерезидентів — найменування, адреса постійного місцезнаходження, країна, де зареєстровано юридичну особу, та відомості про особу, яка представляє інтереси заявника.

- заявлене право вже зареєстровано;
- не проведено інвентаризаційних робіт або якщо вони проведені не тим БТІ, яке здійснює реєстрацію прав власності на нерухоме майно;
- у разі отримання інформації про накладення арешту на відчуження об'єктів нерухомого майна з Єдиного реєстру заборон відчуження об'єктів нерухомого майна.

Реєстрація прав проводиться після технічної інвентаризації об'єкта.

У реєстрі прав на кожне нерухоме майно, право власності на яке заявлено вперше, за рішенням реєстратора про реєстрацію права власності відкриваються відповідні розділи. Кожен розділ має дві частини, які включають записи про нерухоме майно та про право власності на нього.

Записи про нерухоме майно містять: порядковий номер запису; порядковий номер об'єкта нерухомого майна та відомості про його місцезнаходження; призначення нерухомого майна; опис нерухомого майна, отриманий у порядку технічної інвентаризації; зміни в описі нерухомого майна (у разі добудови, знесення, нового будівництва тощо), отримані в порядку технічної інвентаризації; вартість нерухомого майна за станом на дату проведення інвентаризаційних робіт; дату внесення записів та дату внесення змін до записів; прізвище реєстратора та дату прийняття рішень.

Записи про право власності на нерухоме майно містять: порядковий номер запису; відомості про власників (співвласників)¹; вид спільної власності та розмір часток, якщо майно належить на праві спільної часткової власності; підстави виникнення права власності; дату внесення записів та дату внесення змін до записів; прізвище реєстратора та дату прийняття рішень.

Реєстраційна справа відкривається на нерухоме майно, право власності на яке підлягає реєстрації, і містить такі документи: заяви про реєстрацію відповідних прав; копію розділу реєстру; рішення реєстратора; копії правовстановлювальних документів, що підтверджують права на нерухоме майно, завірені реєстратором; докумен-

¹ Для фізичних осіб — громадян України — прізвище, ім'я та по батькові, дата і місце народження, адреса постійного місця проживання, ідентифікаційний номер у Державному реєстрі фізичних осіб — платників податків та інших обов'язкових платежів, дані документа, що посвідчує особу. Для іноземних громадян — прізвище, ім'я та по батькові (за наявності останнього), адреса постійного місця проживання за межами України, дані документа, що посвідчує особу. Для юридичних осіб — резидентів — назва, адреса постійного місцезнаходження, код в ЄДРПОУ. Для юридичних осіб — нерезидентів — найменування, адреса постійного місцезнаходження і країна, де зареєстровано юридичну особу.

ти, що свідчать про внесення плати за реєстрацію; інформацію про видані витяги з реєстру; дані технічної інвентаризації; інші документи, що є підставою для прийняття рішення реєстратором.

Документи в реєстраційній справі розміщуються в порядку їх надходження, мають послідовну нумерацію і не можуть бути вилучені.

Розділ реєстру і реєстраційна справа закриваються на підставі рішення реєстратора в разі знищення, поділу або об'єднання нерухомого майна. Закриті реєстраційні справи зберігаються в архіві БТІ в установленому чинним законодавством України порядку.

Витяг з реєстру надається (або приймається рішення про відмову в наданні такого витягу) після отримання відповідної заяви встановленої форми чи офіційного запиту протягом десяти днів з дня реєстрації заяви (запиту).

Під час реєстрації запитів на надання витягів із реєстру фіксуються: порядковий номер запиту; дата надходження запиту; дані про особу, яка звернулася із запитом; дані про документи, які посвідчують особу; порядковий номер та адреса нерухомого майна, щодо якого здійснено запит; мета (інтерес), з якою здійснюється запит; запис про надання витягу або про відмову в наданні витягу (заноситься після прийняття рішення), дата його прийняття, прізвище реєстратора.

Право на отримання витягів із реєстру про зареєстровані права мають: власник (власники), його спадкоємці та правонаступники юридичних осіб, уповноважені ним особи; суд, органи внутрішніх справ, органи прокуратури, органи державної податкової служби, органи Служби безпеки України, державні виконавці, нотаріуси та інші органи державної влади (посадові особи), якщо запит зроблено у зв'язку зі здійсненням ними повноважень, визначених чинним законодавством України.

7.3. БАГАТОРІВНЕВА ІЄРАРХІЧНА ІС «РАГС»

Багаторівнева ієрархічна ІС «РАГС» складається з інформаційних підсистем відділів реєстрації актів громадянського стану районних, районних у містах, міських (міст обласного значення) управлінь юстиції, виконавчих органів сільських, селищних, міських (крім міст обласного значення) рад, які проводять реєстрацію народження, смерті, одруження та встановлення батьківства, а також консульських установ і дипломатичних представництв України, які виконують зазначені функції.

Багаторівнева ієрархічна ІС «РАГС» містить:

1) автоматизовану систему реєстрації актових записів, що складається з підсистем «Народження», «Укладання шлюбу», «Розлучення», «Смерть», «Встановлення батьківства», «Усиновлення (удочеріння)», «Зміна прізвища, імені, по батькові», «Відновлення актового запису», «Статистика»;

2) автоматизовану систему «Архів», що складається з підсистем «Народження», «Укладання шлюбу», «Розлучення», «Смерть», «Встановлення батьківства», «Усиновлення (удочеріння)», «Зміна прізвища, імені, по батькові», розроблених з урахуванням усіх змін форм актових записів і законодавства РАГС за період з 1918 року і донині; підсистем «Електронна картотека актових записів» та «Електронна картотека метричних церковних книг», підсистеми «Листи», розробленої з урахуванням специфіки кореспонденції, якою обмінюються органи РАГС з іншими організаціями і між собою;

3) автоматизовану систему «Внутрішня взаємодія», яка забезпечує централізацію даних із районних відділів РАГС, селищних або сільських рад, консульських установ і дипломатичних представництв України у міський або обласний архів як по каналах зв'язку, так і за допомогою магнітних носіїв інформації (дискет);

4) автоматизовану систему «Зовнішня взаємодія», яка забезпечує інформаційну взаємодію з органами галузевого і територіального управління за даними відділів РАГС, а також обмін інформацією і документами з архівами інших регіонів країни по каналах зв'язку з використанням методів криптологічного контролю і захисту від несанкціонованого доступу;

5) інформаційно-довідкову систему «Закон», яка забезпечує правову консультацію з питань реєстрації актів громадянського стану.

Використання системи забезпечує виконання таких функцій:

- ведення актових записів з логічним та юридичним контролем даних, що вводяться;
- автоматизоване формування, перегляд, редагування і друкування актових записів, свідоцтв, довідок, сповіщень, карток, відомостей, статистичної звітності;
- автоматизований пошук актових записів за будь-якими реквізитами, що мають юридичні наслідки;
- формування і ведення архівів по всіх архівних фондах (метричних церковних книгах будь-яких релігійних конфесій, актових записах за період з 1918 року й донині, консульських установ і дипломатичних представництв);

- формування і ведення електронних картотек по всіх архівних фондах;
- формування і ведення довідників і словників архівів відділів РАГС, селищних і сільських рад, церков, консульських установ, формулювань, що вносяться в графу «особливі позначки» актового запису відповідно до вимог законодавства РАГС з 1918 року й донині та ін.;
- формування і видача описів архівних фондів по всіх архівах та одиницях зберігання;
- облік зберігання і витрачання гербових бланків свідоцтв;
- оперативний контроль керівників за діяльністю персоналу відділу РАГС і архіву;
- одержання юридичних консультацій з питань реєстрації актів громадянського стану в автоматизованому режимі;
- видача необхідної інформації по матеріалах відділів РАГС органам галузевого і територіального управління, а також у військкомати, органи соціального забезпечення і соціального захисту, органи внутрішніх справ і т. ін.;
- автоматизоване збирання і централізація даних в міському або обласному архіві;
- обмін інформацією і документами з іншими регіонами країни;
- актуалізація бази даних «Регістр населення».



Контрольні запитання і завдання

1. *Схарактеризуйте основні функціональні підсистеми ІС органів юстиції.*
2. *Які Єдині реєстри Ви знаєте і які принципові рішення покладено в основу концепції їх створення?*
3. *Яке призначення і зміст має Єдиний реєстр заборон відчуження об'єктів нерухомого майна?*
4. *Як функціонує Єдиний реєстр доручень?*
5. *З якою метою створено Єдиний реєстр спеціальних бланків та захисних знаків нотаріальних документів?*
6. *Яку змістовну частину може мати повідомлення про внесення відомостей до Єдиного реєстру нотаріусів?*
7. *Назвіть суб'єктів реєстрації застав рухомого майна і зміст Державного реєстру застав рухомого майна.*
8. *Опишіть порядок функціонування Єдиного реєстру доручень.*
9. *Визначте складові Єдиного державного реєстру об'єднань громадян та благодійних організацій.*

10. З якою метою створено Державний реєстр атестованих судових експертів державних і підприємницьких структур та громадян?

11. Опишіть порядок реєстрації прав власності на нерухоме майно.

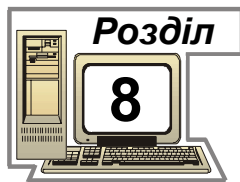
12. Яке місце посідають Єдині реєстри у нотаріальному процесі?

13. Визначте складові багаторівневої ієрархічної ІС «РАГС».



Література

1. Матеріали сайтів <http://www.informjust.kiev.ua/>, <http://www.minjust.gov.ua/>, <http://www.compulog.ru/komit/infores>, <http://www.rada.gov.ua/>.



Розділ

8

ІНФОРМАЦІЙНІ СИСТЕМИ ОРГАНІВ СУДОВОЇ ВЛАДИ, ПРОКУРАТУРИ, СУДОВОЇ ЕКСПЕРТИЗИ

8.1. ІНФОРМАЦІЙНІ СИСТЕМИ СУДОВИХ ОРГАНІВ

8.1.1. Проблеми і перспективи інформатизації судів

Комп'ютеризація судів сьогодні є стратегічним напрямом підвищення оперативності судочинства. У зв'язку зі змінами соціально-економічної ситуації в країні, зростанням злочинності, збільшенням і якісною зміною змісту цивільних справ, розширенням можливостей оскарження у суді неправомірних дій посадових осіб навантаження на органи судової влади зростає з кожним роком. За відсутності в більшості судів першої інстанції сучасних комп'ютерних технологій судова практика характеризується серйозними порушеннями процесуальних термінів розгляду справ і заяв. Майже половина позовів про поновлення на роботі, щодо житлових спорів, про позбавлення батьківських прав тощо не розглядаються судами вчасно. Повільність судів при розгляді кримінальних справ призводить до збільшення термінів утримання обвинувачуваних під арештом. Водночас вступ України до Європейського Союзу неможливий без впровадження міжнародних стандартів обміну правовою інформацією (включаючи судову) в електронному вигляді через Інтернет.

Аналіз робіт з інформатизації судів показує, що ці роботи виконуються непослідовно, в умовах відсутності єдиного державного проекту і належного фінансування. Недостатня забезпеченість обчислювальною технікою, велика частка застарілих комп'ютерів ускладнюють впровадження новітніх інформаційних технологій. Зокрема, використання відокремлених АРМ унеможливорює перехід до електронного документообігу. Недостатня увага приділяється розробці організаційно-правового та методичного забезпечення, формуванню єдиної системи класифікації і кодування та уніфікованої системи документообігу. Зміст баз даних правової інформації, що використовуються в судах, не враховує достатньою мірою специфіку потреб суддів та апаратів судів. У зв'язку з цим необхідно вирішити проблему адаптації інформаційного забезпечення та оперативного надходження правової інформації, а також узагальнення і

систематизації матеріалів судової практики. Вимагає вирішення проблема телекомунікаційного забезпечення інформаційної взаємодії судів з правоохоронними органами та органами державної влади України. Відповідні рішення також мають забезпечувати контакти у рамках міжнародного суддівського співтовариства — оперативну взаємодію між центральними національними органами забезпечення діяльності судів (у першу чергу, в рамках СНД), а також з провідними міжнародно-правовими і судовими організаціями — Міжнародним Судом, Радою Європи, регіональними та всесвітніми суддівськими асоціаціями.



Зміни судової системи — проекти Інтернет-судів

Судова система, яка залишалась майже незмінною більше століття, може змінитися завдяки новітнім інформаційним технологіям. Збільшується кількість пілотних проектів заміни судів деяким єдиним сервісом, за допомогою якого можна подавати позови через Інтернет. Електронна система судочинства може суттєво знизити витрати на утримання судів і зменшити кількість людей, які працюють у цих структурах. Найбільш відомим подібним проектом є «Віртуальний суддя» (Virtual Magistrate) з мережного права, який надає можливість за 10 дол. кожному відвідувачеві сайту подати офіційну скаргу і протягом кількох днів одержати електронною поштою рішення кваліфікованого третейського судді. На жаль, така система поки здатна працювати тільки при вирішенні нескладних справ, коли документів небагато, не потрібно допитувати свідків і брати показання під присягою. Іншим масштабним проектом є інтерактивна система розв'язання суперечок між власниками торгових марок та імен доменів Всесвітньої організації з інтелектуальної власності WIPO.

Основні завдання інформатизації органів судової влади такі:

- 1) забезпечення збирання інформації з питань судового розгляду від першоджерел в електронній формі;
- 2) підготовка, узгодження, виготовлення і передавання в електронній формі підтримуючих і реєструючих документів судочинства за єдиними правилами в усіх інстанціях;
- 3) організація внутрішнього і зовнішнього електронного документообігу;
- 4) систематизація архівного збереження електронних документів за єдиними правилами їх збереження, пошуку і використання у системі органів судової влади;
- 5) інформаційна підтримка прийняття рішень голів судів і керівництва державної судової адміністрації;

- 6) збирання та оброблення судової статистики;
- 7) передавання та оброблення електронних даних з організаційного, фінансового, матеріально-технічного, кадрового та інших видів забезпечення діяльності судів;
- 8) контроль виконання директивних документів у системі державної судової адміністрації.

Виконання зазначених завдань матиме такі позитивні *наслідки*:

- підвищення оперативності збирання та оформлення судових документів під час підготовки і слухання справ;
- скорочення термінів розгляду карних і цивільних справ;
- формування єдиної інформаційної технології судового діловодства та електронного документообігу, а також оброблення судової статистики зі скороченням часу на листування та передавання інформації;
- забезпечення швидкого доступу суддів і співробітників апаратів судів до великого обсягу актуальної і точної інформації з чинного законодавства і правозастосовної практики;
- підвищення повноти і вірогідності інформації, скорочення термінів її подання до центрального апарату державної судової адміністрації із судів і територіальних управлінь;
- підвищення оперативності збирання та оброблення судової статистики із забезпеченням об'єктивного аналізу правозастосовної практики, структури правопорушень і напрямків криміналізації суспільства;
- підвищення ефективності кадрового, організаційного, матеріально-технічного і ресурсного забезпечення діяльності судів зі створенням інструмента інформаційно-аналітичної підтримки прийняття рішень у всіх сферах забезпечення судової діяльності;
- підвищення якості судових документів;
- підвищення оперативності реагування на звертання суддів і громадян до державної судової адміністрації;
- підвищення оперативності інформаційної взаємодії судів з Верховним Судом України, державною судовою адміністрацією, слідчими органами, прокуратурою, Міністерством юстиції, органами державної влади.



Інформаційні зв'язки судів — відеоконференц-зв'язок у залі судового засідання

Інформаційні зв'язки судів не обмежуються використанням розподілених баз даних та передаванням електронних документів. Ілюстрацією до цього твердження є система відеоконференц-зв'язку для дистанційної участі засуджених у касаційних судових

засіданнях. Розробка ініційована Верховним Судом Російської Федерації і зумовлена тим, що згідно з рішенням Конституційного Суду суди мають забезпечити участь у касаційних засіданнях усіх засуджених, які подали відповідне клопотання. При цьому виникає ряд проблем, пов'язаних з організацією конвоювання засуджених зі слідчих ізоляторів, охороною у суді та оплатою витрат на доставку засуджених до місця розгляду справи. Ця проблема вирішується на основі використання комп'ютерів і засобів телекомунікацій, що відповідає міжнародній практиці і не суперечить закону. Схему організації відеоконференц-зв'язку наведено на рис. 8.1.

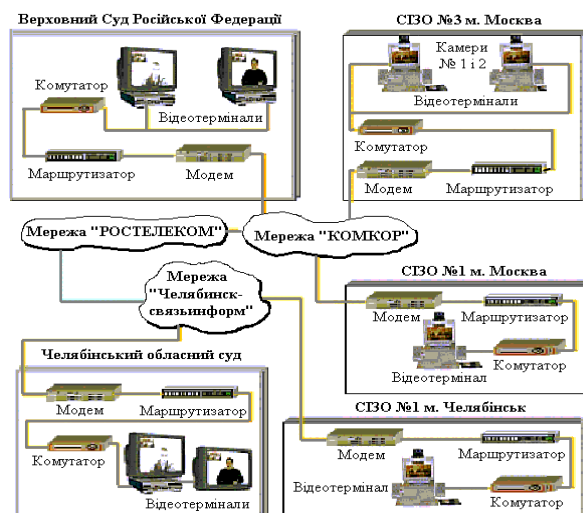


Рис. 8.1. Схема відеоконференц-зв'язку
«Верховний Суд Російської Федерації — обласний суд — СІЗО»

8.1.2. Інформаційні технології в діяльності Верховного Суду України

Базою впровадження інформаційних технологій у Верховному Суді України є локальна комп'ютерна мережа, яка на даний момент поєднує на основі оптоволоконних каналів два адміністративні будинки суду і забезпечує групову роботу та спільне використання мережних ресурсів і баз даних майже двома сотнями користувачів — суддями й працівниками апарату. Кожне робоче місце оснащено засобами роботи з електронною поштою і має доступ до глобальної мережі Інтернет. Створено можливості використання цих ресурсів іншими судами України.

Зважаючи на значні методичні труднощі та великий обсяг робіт, упровадження нових інформаційних технологій відбувається крок за кроком введенням у дію та поступовим розвитком окремих інформаційних систем, які в перспективі складатимуть єдину інформаційну систему Верховного Суду України. Серед них можна назвати наступні.

1. *Автоматизована система судового діловодства «КАРС»*, розроблена і введена в експлуатацію у 1998 році у Верховному Суді України спільно з науково-виробничою фірмою «КІМ». Система охоплює весь цикл діловодства за скаргами і зверненнями від їх надходження до накопичення в архіві Верховного Суду України та передачі матеріалів до Державного комітету архівів України.

Система «КАРС» автоматизує процес реєстрації скарг, який полягає у виконанні роботи з ідентифікації скарги («розмітка») та у формуванні відповідного провадження («заведення»). До бази даних вводяться відомості про номер провадження, дату заведення, суд, рішення якого оскаржується, головуємого засідання в першій інстанції, сторони або засудженого (прізвище, ім'я та по батькові, назва юридичної особи), статті, міру покарання, для неповнолітніх — дату народження.

У процесі розгляду скарги (для першої інстанції — справи) в базу даних вводиться така інформація: категорія скарги (касаційна скарга, касаційне подання, окрема скарга, окреме подання, окрема скарга (подання) на постанову про застосування заходів адміністративного стягнення); дата, на яку призначено розгляд скарги у Верховному Суді України; дата передачі справи судді; прізвище судді, якому передано справу на розгляд. Вноситься вся інформація про перенесення дати розгляду справи та направлення на дооформлення.

Після завершення процесу розгляду скарги (справи) і винесення відповідного рішення фіксуються результати її розгляду (знято з розгляду, відкликано, направлено до обласного суду тощо). До бази даних заноситься повний текст рішення чи ухвали.

Система «КАРС» оснащена засобами пошуку. За будь-якими даними, що попередньо були внесені в базу, можна здійснити пошук потрібного провадження або дати відповідь, що подібна скарга у Верховному Суді не розглядалась.

У результаті впровадження цього програмного комплексу поліпшились умови праці секретарів (у роботі стали непотрібними великі та маленькі картки, шафи для їх зберігання), підвищилась якість роботи секретаріату, зникла проблема дублювання карток.

Для автоматизації роботи архіву та процесів взаємодії канцелярій із ним розроблено підсистему «**Архів**». Система забезпечує як щорічну передачу проваджень на зберігання в архів із канцелярій, так і щоденну взаємодію. У першому випадку описи проваджень, які передаються до архіву, автоматично створюються засобами системи, що значно полегшує і прискорює роботу фахівців канцелярій, оскільки тепер не треба виконувати досить громіздку машинописну роботу зі створення цих описів. Система також веде облік тих проваджень, які на момент передачі в архів знаходяться у процесі розгляду. Усе це сприяє більш чіткому і правильному виконанню зазначених робіт.

Щоденна робота канцелярій з архівом пов'язана з веденням шести журналів, у яких фіксуються дані запитів до архіву і результати пошуку проваджень у ньому. У підсистемі «Архів» використовуються права доступу до даних з того чи іншого робочого місця. Таке розмежування прав забезпечує відповідальність кожного працівника за внесення, зміну і використання даних про переміщення провадження від одного робочого місця до іншого.

Впровадження системи «Архів» значно зменшило сумарну кількість операцій, які виконуються працівниками, і чисельність звернень до архіву, оскільки відразу при розмітці в канцелярії можна одержати відповідь, де знаходиться дане провадження. Усе це разом сприяє скороченню часу, що минає з моменту надходження скарги до її розгляду.

Система «КАРС» оснащена засобами, призначеними для підтримки роботи відділу прийому громадян — робоче місце «**Прийом громадян**». Впровадження цієї підсистеми значно полегшує і прискорює роботу працівників відділу, оскільки система дає змогу здійснювати пошук інформації про скаргу чи заяву громадян у Верховний Суд України без звернення до канцелярій та одержувати інформацію про будь-яке провадження незалежно від того, де воно міститься — у канцелярії чи в архіві, а також про існування даного провадження, місце його знаходження, стадії розгляду, переглядати перелік і текст документів, що є в даному провадженні.

У рамках системи «КАРС» вирішено **задачу автоматизованого збирання статистичних даних** для формування затвердженої Міністерством юстиції України статистичної звітності, досліджено процес нагромадження статистичних даних у судових колегіях, на підставі процесуальних норм та інструктивних матеріалів розроблено чіткі правила занесення інформації до бази да-

них. Слід зазначити, що впровадження автоматизованої системи статистичної звітності істотно скоротило час формування відповідних таблиць. Наприкінці півріччя на виконання цих робіт витрачається лише п'ять хвилин роботи комп'ютера. Такий результат особливо відчутний під час формування звітності за розглядом кримінальних скарг (при паперовій технології на виконання цієї роботи відводилося два тижні).

Подальша робота з розширення функціональних можливостей системи «КАРС» полягає у формуванні автоматизованих засобів ведення журналів обліку, засобів формування внутрішніх статистичних форм та довідок, автоматизації процесу розподілу скарг для розгляду.

2. Система планово-економічного відділу «*Радамант*», розроблена спільно з НДЦ «Крокус» кафедри спеціалізованих комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут». Система «Радамант» призначена для підтримки процедур складання плану бюджету та аналізу його виконання, автоматизації статистичної звітності, створення баз даних для збереження архівної інформації про фінансові операції.

У системі створено такі АРМ:

- економістів кожного структурного підрозділу Верховного Суду. АРМ призначені для первинного введення та коригування проекту видатків відповідного відділу, розподілу їх у часі, аналізу фактичного використання видатків, порівняння плану видатків із фактичним використанням коштів. АРМ економіста планово-економічного управління доповнюється функціями зі збирання даних від інших структурних підрозділів;

- працівників планово-бюджетного управління для формування плану видатків, що полягає в нагромадженні інформації, внесеної відділами та управліннями, коригуванні одержаної інформації та аналізі формування проекту видатків;

- планово-бюджетного управління для формування розпису видатків — нагромадження інформації, внесеної відділами та управліннями, коригування одержаної інформації щодо розподілу видатків у часі, ведення журналу змін у затвердженому розподілі видатків у часі, аналізу формування цього розподілу (аналіз видатків полягає у створенні засобів введення та накопичення платіжних доручень, а також аналізу фактичного використання коштів);

- керівника планово-бюджетного управління для здійснення автоматизованого формування проекту видатків, порівняння цього проекту з фактичним використанням коштів;

- адміністратора системи для забезпечення додержання прав доступу користувачів до тієї чи іншої інформації, розподілу та перерозподілу функцій між користувачами системи.

База даних системи «Радамант» містить багато довідників, класифікаторів (товарів, послуг, штатних одиниць), що робить систему дуже зручною і гнучкою в користуванні.

3. Система **«КАДРИ Верховного Суду України»**, розроблена ТОВ «МККУ-Мережі» для ведення кадрового обліку в управлінні кадрів. Ця система складається з таких підсистем:

- підсистема ведення особових карток дає змогу оперативно, не звертаючись до паперового варіанта, переглянути будь-яку інформацію з особової справи (посада, оклад, надбавка, ранг, клас, відомості про рішення кваліфікаційної комісії, стаж, відпустки, лікарняні та ін.). Вона функціонує з урахуванням специфіки ведення особових справ у Верховному Суді України, тобто відокремлює ведення кадрового обліку суддів і працівників апарату. Разом з тим система підтримує експорт-імпорт даних із системи «Картка» Головного управління державної служби України, що спрощує кадровий облік державних службовців у разі зміни місця роботи;

- підсистема «Штатний розпис» дає змогу вести штатний розклад установи (чинний на сьогоднішній день), а також його архів. У цій підсистемі реалізовано функції зарахування особи до штату суду, звільнення та просування по службі в межах установи з подальшим автоматичним оновленням особових карток. На основі даних підсистеми можливе автоматичне одержання таких форм звітності: форма 1-КЮ (державна статистична звітність про склад суддів і апарату Верховного Суду України); форма 9-ДС (державна статистична звітність про склад державних службовців Верховного Суду України); штатна книга; звіти про стан штатного розкладу. Впровадження зазначеної системи здійснюється з урахуванням можливого майбутнього кадрового обліку всього суддівського корпусу України.

4. Довідкові системи, які забезпечують відбір та перегляд раніше підготовленої інформації — **«Законодавство»**, **«Закон»**, **«Суди України»**.

5. Система **«Судові рішення»**. Завдяки застосуванню цієї системи має бути забезпечено нагромадження інформації щодо судової практики і створено умови для її подальшої аналітичної обробки, зокрема для багатокритеріального аналізу та узагальнення. Для вирішення цього завдання створено базу даних судової практики, де кожне судове рішення класифіковано за

розробленими класифікаторами, пов'язано з проходженням відповідної справи та доповнено матеріалами узагальнення судової практики. Така база даних містить рішення Верховного Суду України з 1998 року. За допомогою спеціально розроблених засобів упроваджується механізм передавання даних з оперативної системи «КАРС». Реалізація OLAP-системи на основі цієї бази даних вимагає створення єдиних форматів процесуальних документів — чим більш формалізованим буде документ, тим більше можливостей буде для його автоматизованого оброблення. З урахуванням найперспективніших стандартів представлення документів і відповідних засобів їх оброблення та відображення вже розпочато роботи зі створення схем документів судової практики у форматі XML.

8.1.3. Типові автоматизовані робочі місця судів загальної юрисдикції

Інформатизація органів судової влади вимагає створення типових інформаційних систем, основу структури яких складають автоматизовані робочі місця працівників судів, об'єднані у локальні обчислювальні мережі. Перелік таких АРМ наведено нижче.

Типові АРМ Верховного суду України, Верховного суду Автономної Республіки Крим, обласних і прирівняних до них судів: голови суду, заступника голови суду з кримінальних справ, заступника голови суду з цивільних справ, судового розпорядника, начальника приймальні суду, канцелярії судової колегії 1-ї інстанції з кримінальних справ, завідувача канцелярією суду 1-ї інстанції, секретаря суду, канцелярії судової колегії 1-ї інстанції з цивільних справ, секретаря судової колегії 2-ї інстанції, завідувача канцелярією, відповідального секретаря 2-ї інстанції, канцелярії 2-ї інстанції з цивільних справ, провідного фахівця із судової статистики суду, завідувача канцелярією — відповідального секретаря Президії суду, секретаря судової колегії — секретаря керівництва, канцелярії судової колегії 2-ї інстанції з кримінальних справ, канцелярії Президії суду, судді, секретаря судового засідання в карному процесі, старшого консультанта групи нагляду суду, консультанта групи нагляду суду, консультанта групи виконання рішень суду, секретаря судового засідання в цивільному процесі, секретаря експедиції, архіву суду з обліку та збереження кримінальних справ, архіву суду з обліку та збереження цивільних справ, консультанта суду з кодифікації законодавства (кодифікатора), консультанта суду з інформатизації.

Типові АРМ районних (міських), окружних (міжрайонних), між-обласних та прирівняних до них судів: голови суду, заступника голови суду, секретаря голови суду, судового розпорядника, завідувача канцелярією суду, канцелярії з цивільних справ, канцелярії з кримінальних справ, консультанта суду, судді, секретаря судового засідання з цивільних справ, секретаря судового засідання з кримінальних справ, експедиції, архіву зі збереження цивільних справ, архіву зі збереження кримінальних справ, архіву зі збереження адміністративних матеріалів, інформаційно-правового забезпечення діяльності суду.

Для автоматизованого формування складу судів присяжних і народних засідателів створюються типові АРМ «Присяжні» та «Народні засідателі».

Крім перелічених, у кожному суді створюються АРМ для вирішення загальнофункціональних задач, таких як «Фінанси», «Облік робочого часу і нарахування заробітної плати» та ін.

8.1.4. Автоматизація судового діловодства і судочинства

Робота суддів і суду в цілому — відправлення правосуддя, що виражається в підготовці і винесенні вироків, рішень, визначень, випуску процесуальних документів у точно визначений термін і за встановленою формою. Значну частину свого часу суддя неминуче витрачає не лише на свою головну діяльність — підготовку й ухвалення юридичного рішення, а й на рутинну багаторазово повторювану роботу — написання або друкування однакових процесуально необхідних словесних оборотів, що повторюються в кожному однотипному документі. З появою персональної комп'ютерної техніки для цих задач почали використовувати текстові редактори (зокрема, «MS Word»). При цьому документ, ретельно підготовлений і взятий як зразок, надалі доповнюється необхідними для певної справи конкретними даними — замінюються прізвища, посилання на процесуальні статті тощо. Це значно скорочує час, необхідний для підготовки документа, водночас значно поліпшуючи його якість як з юридичного, так і з формального погляду. Останнє важливо, оскільки сприяє підвищенню авторитету судового документа в очах громадянина.

Однак створення повноцінних спеціалізованих шаблонів для більшого підвищення ефективності роботи, вимагає майже про-

фесійних навичок з програмування і недоступне для обтяженого роботою судді. З іншого боку, голова суду та його апарат (помічники, канцелярія, експедиція, архів, секретаріат суду) зобов'язані забезпечити чітке проходження справ через усі підрозділи суду, передачу справ суддям і від суддів у канцелярію та інші операції, докладно регламентовані інструкцією з діловодства в суді. Цей процес дуже чутливий до неминучих помилок — неправильно заповнена картка обліку, несвоєчасно зроблена в ній оцінка, неправильно зазначені реквізити в справі призводять до тяжких наслідків.

Усе сказане зумовлює необхідність інтеграції технологій діловодства в єдиний процес, що не тільки підвищить рівень організації праці робітників судів, а й прискорить розгляд справ у суді на будь-якій стадії процесу, збільшить період часу для аналізу справ, надасть можливість більш повного та оперативного оброблення статистичних даних, забезпечить ефективний пошук інформації, її надійність і конфіденційність, а також створить передумови для удосконалення контролю керівництва за діяльністю підлеглих підрозділів і суддів та своєчасного поширення судової практики, пов'язаної у першу чергу з постійними змінами норм процесуального і матеріального права.

Інтегрована технологія діловодства реалізується на основі комплексів АРМ співробітників канцелярій, суддів, секретарів судового засідання та інших посадових осіб, організованих за єдиним принципом. Кожне робоче місце забезпечує введення всієї необхідної інформації та її оброблення з метою реалізації функцій співробітників судів різних рівнів згідно з процесуальними нормами та інструктивними матеріалами.

Введення інформації здійснюється за допомогою вбудованого редактора — заповнення шаблонів процесуальних документів забезпечується вибором усієї необхідної інформації з можливістю подальшого редагування одержаного тексту документа (рис. 8.2). Наявні також інструменти зміни шаблонів та їх поповнення.

Кожне АРМ також оснащено:

- засобами автоматичного формування документів будь-якої форми, створюваних у процесі руху справи, на основі раніше введеної інформації (рис. 8.3);
- засобами контролю процесуального і логічного характеру;
- різного роду довідниками, які містять законодавчу і нормативну інформацію.

АРМ секретарів канцелярій містять функції одержання статистичної звітності за будь-який період за визначеними формами з

можливістю їхньої подальшої модифікації без залучення програмістів, видачі довідок і запитів за довільною формою для всіх користувачів, що мають доступ до цієї інформації.

Рис. 8.2. Шаблон «Відомості про звинувачених (підсудних)»

Название поля	Значение
Текущая дата	31/10/2000
Номер дела	2-2/1998
Дата поступления	09/01/1997
Количество томов (поступило)	149
Откуда поступило	обл. прокуратура
Входящий номер	280/97
Уго поступило	Дело с обвинительным заключением
Порядок поступления	Впервые
Кем расследовано	Органы прокуратуры
Категория дела	Присвоение или растрата
Строка статистика	13
Судья гр. иска (г.р.)	
Место соверш. преступления	г. Челябинск
Основная статья (поступление)	147-1 ч.3
Принято к изучению (судья)	09/01/1997
Секретарь судебн. заседания	Горбулан Сергей Борис
ФИО судьи	
Дата конца изучения	07/02/1997
Результат подготовки	Рассмотрение назначено
Дата назначения к слушанию	07/02/1997
Дата вынесения решения	30/03/1998
Приговор, опред. постанов	обвинительный приговор
Кем принято	С нар. заседат.
Основная статья (вынесение)	РФ 160 ч.3 п.а

Рис. 8.3. Формування документа зі справи за полями бази даних

Усі АРМ працюють з єдиною базою даних, що дає змогу:

- забезпечити введення в базу даних інформації там, де вона виникає;
- реалізувати принцип колективної роботи в мережі, що виключає повторне введення даних;
- зберегти службові функції співробітників, закріплені за ними посадовою інструкцією з діловодства.

АРМ керівників суду мають доступ до інформації з усіх підрозділів суду в режимі перегляду і контролю за діяльністю його співробітників і діловодства в цілому. Голова суду або канцелярія за його дорученням у будь-який момент можуть одержати відомості про справи, призначені до слухання на певний період, про призупинені або відкладені справи, про справи, що їх не здали у канцелярію, про результати розгляду справ.

АРМ адміністратора координує роботу всіх підрозділів, має функції резервного копіювання, відновлення даних, відповідає за розмежування доступу, контроль за «зовнішніми» користувачами системи, створення додаткових запитів до БД за вимогою керівництва суду, має функції супроводження єдиних каталогів БД.

«Віддалені» користувачі з метою підвищення секретності і захищеності інформації мають доступ тільки до сервера додатків у режимі перегляду, без права доступу до основної бази даних.

8.1.5. Автоматизоване робоче місце судового виконавця

Автоматизована технологія виконавчого судового виробництва являє собою трирівневу систему, основним елементом якої є АРМ судового виконавця. Такий АРМ, підімкнений до ЛОМ свого підрозділу або працюючий автономно, є типовим і призначений для занесення інформації із судового виробництва, формування всіх необхідних документів з виконавчого виробництва, видачі довідок і підготовки статистичної звітності.

В ІС виконуються такі *функції*:

- первинний облік виконавчих документів, прийнятих від стягувача, прокурора, осіб, які мають право звертатись до суду із заявами на захист прав та інтересів, що охороняються законом, органів Антимонопольного комітету України і т. ін. (реєстрація);
- оформлення і ведення виконавчого виробництва;

- оформлення документів виконавчого виробництва з питань конфіскації, обліку, оцінки, збереження та реалізації арештованого майна боржника;
- ведення фінансових документів у рамках виконавчого виробництва;
- закінчення виробництва та оформлення відповідних документів;
- ведення книг обліку виконавчого виробництва;
- пошук і вибір записів з бази даних;
- ведення обліково-статистичних документів.

Виконавчі документи, що надійшли у підрозділ судових приставів, реєструються діловодом або особою, що відповідає за реєстрацію в книзі обліку виконавчих документів, у порядку їхнього надходження з присвоєнням номера (цей номер згодом присвоюється виконавчому виробництву). Реєстрація нового виконавчого документа може відбуватись у двох режимах залежно від зроблених налаштувань:

- користувач (старший судовий пристав) сам визначає пристава-виконавця з конкретного виконавчого виробництва;
- до початку реєстрації виконавчого документа система пропонує перелік адрес (ділянок); після вибору користувачем адреси, зазначеної у виконавчому документі (місця виконання) автоматично визначається номер виконавчого виробництва і виконавець, усі дані заносяться у картку.

Судовий пристав-виконавець при одержанні виконавчих документів перевіряє їх дійсність і наявність усіх необхідних реквізитів, а також терміни пред'явлення їх до виконання. За результатами перевірки судовий пристав-виконавець виносить постанову про порушення виконавчого виробництва, або про повернення виконавчого документа. Якщо порушення були допущені в оформленні виконавчого листа, то призначається термін для їх усунення. Картка обліку заводиться на одного боржника і може містити інформацію щодо кількох стягувачів.

У разі порушення виконавчого виробництва система дає змогу зв'язати різні виробництва, іншими словами — «зв'язати» між собою кілька карток для зручності роботи. Документи формуються на основі закладених шаблонів і введених даних з усіма реквізитами типових форм. У необхідних випадках у документи вводяться додаткові реквізити, обумовлені характером дій із проведення виконавчого виробництва.

Якщо строк добровільного виконання судових рішень минув, судовий виконавець стягує суму виконавського збору (система

автоматично розраховує цю суму) і готує необхідні на цьому етапі документи.

У процесі оформлення документів з питань арешту майна боржника реєструється все арештоване майно зі справи. Основою може бути як попередній опис, так і акти арешту. Вказуються реквізити актів арешту майна, детальний опис майна з наступною реалізацією. Оцінка всього майна проводиться автоматично за всіма одиницями описаного майна.

Судовий виконавець може відкласти, призупинити або відстрочити виконавчі дії у випадках, передбачених законодавством. У всіх цих випадках вноситься відповідна постанова або оформлюється інший необхідний документ, копії якого передаються боржнику, стягувачеві та органу, що видав виконавчий документ. Система автоматично розраховує термін перебування справи у виробництві з урахуванням призупинень і відстрочок виконавчих дій.

За умов, передбачених законодавством, судовий виконавець формує постанову про закінчення виконавчого виробництва, копії якої передаються боржнику, стягувачеві та органу, що видав виконавчий документ. В ІС закінчення виконавчого виробництва фіксується введенням даних про результати і дати закінчення, прізвища виконавця, фактично стягнених сум з можливістю формування документів, що відносяться до стадії закінчення. Якщо справа перебувала на контролі, ведеться хронологія результатів перевірки контролюючою організацією. Також реєструються витрати на здійснення виконавчих дій, накладені штрафні та інші санкції за невиконання виконавчого документа.

Видача грошових сум стягувачам може проводитись шляхом виписки іменного чека на ім'я стягувача — фізичної особи або особи, яка має доручення, або платіжного доручення на перерахування стягнених сум організації-стягувачеві. Система реєструє всі сформовані платіжні документи.

Для контролю і перевірки руху коштів, що надходять у тимчасове розпорядження підрозділу судових виконавців відповідальною особою ведеться книга обліку депозитних сум. Дані до цієї книги вводяться на підставі виписки з банку, де відкрито відповідний рахунок.

Для узагальнення практики виконавчого виробництва і формування статистичної звітності передбачаються можливості пошуку даних за різними реквізитами, наприклад, за прізвищем (назвою) боржника; ведення облікових карток («Обліково-статистична картка за поточним виконавчим виробництвом», «Коротка довідка щодо поточного виконавчого виробництва») і

журналів («Книга обліку виконавчих виробництв», «Алфавітний покажчик боржників», «Алфавітний покажчик стягувачів» «Зональна книга обліку виконавчих виробництв», «Книга обліку арештованого майна» та ін.); формування звітних форм.

8.1.6. Функціональні підсистеми ІС державної судової адміністрації

ІС державної судової адміністрації призначена для забезпечення реалізації функцій Державної судової адміністрації України та територіальних управлінь державної судової адміністрації — організаційного забезпечення діяльності судів загальної юрисдикції, а також інших органів та установ судової системи відповідно до Закону України «**Про судоустрій України**»¹. Організаційне забезпечення діяльності судів відповідно до цього Закону становлять заходи фінансового, матеріально-технічного, кадрового, інформаційного та організаційно-технічного характеру, спрямовані на створення умов для повного і незалежного здійснення правосуддя.

ІС державної судової адміністрації відповідно до організаційної структури і повноважень відповідних органів має містити такі *типові функціональні підсистеми*:

1) «Керування» — підсистема підтримки прийняття рішень і контролю їхнього виконання в системі державної судової адміністрації;

2) «Адміністрування» — підсистема організаційного забезпечення діяльності судів і територіально-об'єктного контролю. У підсистемі організується узагальнення даних територіально-об'єктного контролю з усіх видів забезпечення діяльності судів;

3) «Фінанси» — підсистема фінансового забезпечення діяльності судів і органів державної судової адміністрації. Підсистема включає засоби програмного та інформаційного забезпечення бухгалтерського обліку і звітності, обробки оборотних балансів і формування зведеної звітності судів загальної юрисдикції та органів державної судової адміністрації; комплекс програм і баз даних для задач економічного аналізу і прогнозування різних ситуацій; комплекс засобів, які забезпечують вирішення задач фінансування судів і органів державної судової адміністрації, обліку виділених фінансових коштів, розрахунку заробітної плати, формування бюджету і контролю його виконання;

¹ Організаційне забезпечення діяльності Верховного Суду України, Конституційного Суду України та вищих спеціалізованих судів здійснюється апаратами цих судів.

4) «Ресурси» — підсистема автоматизованого вирішення задач матеріально-технічного (ресурсного) забезпечення діяльності судів. У підсистемі організується автоматизований облік інформації про норми забезпечення, потреби, наявність і рух різних ресурсів у судах і органах державної судової адміністрації;

5) «Право» — підсистема інформаційно-правового забезпечення діяльності судів і органів державної судової адміністрації з організацією доступу до систем правової інформації а також веденням баз даних із судової практики;

6) «Статистика» — підсистема судової статистики;

7) «Діловодство» — підсистема автоматизованого діловодства і документообігу судів і органів державної судової адміністрації;

8) «Кадри» — підсистема автоматизованого вирішення задач керування кадрами. У підсистемі реалізуються задачі кадрового забезпечення діяльності судів і органів державної судової адміністрації, задачі соціального забезпечення суддів, у тому числі суддів у відставці, членів їхніх родин і державних службовців. Створюються та оновлюються бази даних «Штатний розклад», «Кадри», «Соціальне страхування»;

9) «Будівництво» — підсистема автоматизованого вирішення задач капітального будівництва, експлуатації будинків і споруджень судів та органів державної судової адміністрації;

10) «Навчання» — підсистема дистанційного навчання працівників судів і органів державної судової адміністрації;

11) «Контроль» — підсистема автоматизованого вирішення контролю-ревізійних задач;

12) «Звернення» — підсистема обліку звернень громадян, обробки повідомлень і контролю виконання доручень;

13) «Взаємодія» — підсистема взаємодії з органами державної влади і доступу до єдиної інформаційної бази;

14) «Співробітництво» — підсистема інформаційного забезпечення міжнародного співробітництва;

15) «Техдопомога» — підсистема технологічного і методичного забезпечення роботи судів і органів державної судової адміністрації.

ІС державної судової адміністрації має бути реалізована відповідно до принципів відкритих систем на базі інтранет-технологій. Перелічені функціональні підсистеми мають передбачати поєднання за вертикаллю інформаційної взаємодії — від первинного джерела інформації до центрального апарату.

8.2. КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ

8.2.1. Концепція створення КІС органів прокуратури України

Постійно зростаючий інформаційний потік вимагає істотного підвищення оперативності та ефективності роботи органів прокуратури, що сьогодні практично неможливо без впровадження новітніх комп'ютерних технологій. Автоматизація одержання, опрацювання, надання і використання всього обсягу інформації, що має відношення до питань охорони суспільного порядку і боротьби зі злочинністю, а також інших відомостей, необхідних для правоохоронних органів і відповідних міністерств і відомств, є одним із головних завдань органів прокуратури згідно з Державною програмою боротьби зі злочинністю.

Сьогодні в органах прокуратури переважає ручна праця з оброблення інформації. У сполученні з достатньо формалізованим карним процесом і методами керування це породжує величезний документообіг. У свою чергу, це відриває і без того обмежені ресурси від безпосередньо правоохоронних функцій на суто офісну діяльність. При цьому службові документи важко доступні і не можуть бути ефективно використані для прийняття рішень.

Технічне забезпечення здебільшого складають застарілі комп'ютери. Більш того, відсутня система їх технічного обслуговування.

Особливу проблему становить координація та обмін інформацією між різними відомствами. Кожне відомство має свою власну систему обліку і звітності. Це породжує дублювання і плутанину. В Україні не існує незалежної, позавідомчої структури, яка б могла своєчасно надати надійні статистичні дані про злочинність та законність і допомогти у проведенні наукового аналізу ефективності правоохоронної роботи. Як наслідок, втрачається цінний організаційний досвід, знижується продуктивність праці.

У контексті задач і проблем інформаційно-правового і комп'ютерного забезпечення діяльності органів прокуратури України комп'ютерною службою Генеральної прокуратури розроблена і поступово впроваджується **«Концепція створення корпоративної інформаційної системи органів прокуратури України»**. Концепція реалізується у рамках національної програми інформатизації, при цьому враховується можливість інтеграції корпоративної інформаційно-обчислювальної мережі органів прокура-

тури України в загальну ІС правоохоронних органів України, а також інтеграцію в загальнодержавну інформаційно-обчислювальну мережу України.

Головна мета Концепції — створення на всій території України високоефективного автоматизованого інформаційно-обчислювального середовища, спроможного найбільш повно й оперативно задовольняти інформаційні потреби органів прокуратури всіх рівнів управління під час здійснення ними своїх функцій. Технічні і програмні засоби, впровадження яких передбачено, мають забезпечити виконання таких *задач*:

- міжвідомчі зв'язки — забезпечення двосторонніх електронно-інформаційних зв'язків між органами прокуратури України всіх рівнів з різними організаціями і службами України та приватними особами, які перебувають як на території України, так і за кордоном;
- статистика — забезпечення керівництва органів прокуратури, державних органів влади та управління на рівні району, міста, області й України статистичною інформацією про стан законності, правопорядку, злочинності та про результати діяльності органів прокуратури;
- документообіг — формування, збереження, пошук, аналіз і видача законодавчих і нормативних актів при здійсненні прокурорами нагляду за виконанням законів і проведенні профілактичних заходів щодо попередження порушень закону;
- впровадження безпаперової технології групової роботи — систем автоматизації ділових процедур (електронного документообігу);
- робота з кадрами — комплексне вирішення питань управління кадрами, підвищення оперативності виконання функціональних обов'язків співробітниками кадрових служб, зниження трудомісткості і строків підготовки та обґрунтованості аналітичних матеріалів, підвищення достовірності облікових даних.

При створенні КІС прокуратури України враховується *трирівнева структура* системи органів прокуратури України: перший рівень — Генеральна прокуратура України; другий рівень — прокуратури областей і прокуратури, прирівняні до них; третій рівень — прокуратури районів і міст, а також прокуратури, прирівняні до прокуратур районів. Органи прокуратури складають єдину централізовану систему з підпорядкуванням органів нижчого рівня вищому і Генеральному прокуророві.

Генеральна прокуратура України повинна мати *інформаційні зв'язки* з такими органами:

- вищими органами державної влади і управління — Верховною Радою України, Президентом України, урядом;
- судовими і правоохоронними органами — Конституційним Судом України, Верховний Суд України, Вищим господарським судом України, Міністерством юстиції України, Міністерством внутрішніх справ України;
- іншими міністерствами і відомствами.

Прокуратури другого та третього рівнів повинні мати аналогічні інформаційні зв'язки з представницькими і виконавчими органами відповідних рівнів, а також з прокуратурами вищого і нижчого рівнів підпорядкування (рис. 8.4).

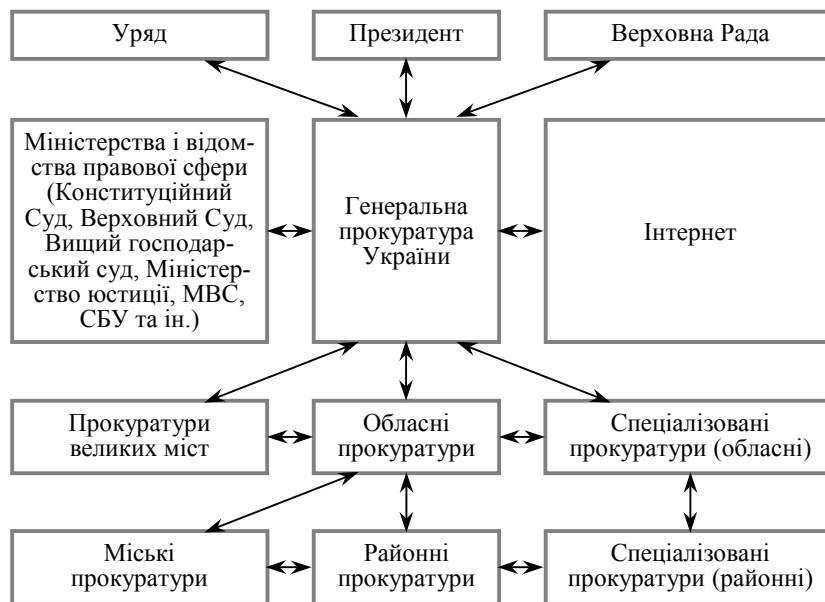


Рис. 8.4. Схема інформаційних взаємозв'язків органів прокуратури України

Створення корпоративної ІС відбувається поетапно, при цьому частина робіт з окремих етапів проводиться паралельно. Виділено такі *етапи проведення робіт*:

1) створення ЛОМ Генеральної прокуратури України — встановлення структурованих кабельних систем у двох адміністративних будинках і з'єднання їх між собою; закупівля і встановлення активного мережного обладнання, робочих станцій і серверів;

проведення виділеної широкополосної лінії зв'язку до найближчого значного вузла Інтернет; закупівля і встановлення необхідного програмного забезпечення; навчання фахівців служби комп'ютеризації і користувачів;

2) створення ЛОМ у прокуратурах обласного рівня; з'єднання їх з ЛОМ Генеральної прокуратури по комутованих каналах АТС Мінзв'язку України, системі безпосереднього модемного зв'язку «АСТРА»; встановлення зв'язку по виділених або комутованих лініях з прокуратурами районного рівня (комутовані канали АТС Мінзв'язку України, система некомерційного модемного зв'язку FIDONET); інтеграція баз даних із базами даних Генеральної прокуратури;

3) створення автоматизованих робочих місць на базі персональних комп'ютерів у прокуратурах районного рівня і з'єднання їх з ЛОМ прокуратур обласного рівня.

Основні стандартизовані компоненти системи:

- протокол взаємодії віддалених мереж — TCP/IP;
- внутрішньомережний протокол — IPX/SPX;
- мережна операційна система — NetWare 4.11 (IntranetWare);
- операційна система додатків — UNIX;
- базова система електронної пошти і документообігу — Lotus

Notes;

- обладнання міжмережної взаємодії — Motorola;
- система керування базами даних — Oracle.

Особлива увага під час створення системи приділяється захисту інформації. Інформаційна безпека розглядається як чинник, від якого залежить надійність системи безпеки органів прокуратури України в цілому. Тому комплексна система захисту інформації від несанкціонованого доступу має:

- оперативно реагувати на зміни чинників, які визначають методи і засоби захисту інформації;
- базуватися на кращих алгоритмах закриття інформації, які гарантують надійний криптографічний захист;
- мати найважливіші елементи ідентифікації користувачів і контролю істинності інформації, що передається і зберігається;
- здійснювати захист від несанкціонованого доступу до інформації в базах даних, файлах, на носіях інформації, а також під час її передавання по лініях зв'язку в локальних і глобальних мережах;
- забезпечувати режим спеціально захищеної електронної пошти для обміну секретною інформацією з високою швидкістю і достовірністю передачі інформації адресату;

- мати зручну і надійну ключову систему, яка гарантує безпеку під час підготовки і розподілу ключів між користувачами;
- забезпечувати різні рівні доступу користувачів до інформації, що захищається.

Завершення проекту забезпечить значне покращення інформаційно-аналітичних служб на всіх рівнях правоохоронної системи, зменшення дублювання численних форм державної і відомчої звітності, ефективну координацію та обмін інформацією між різними відомствами. Водночас, для одержання повного ефекту необхідні розробка, узгодження та уточнення стандартів обміну інформацією між правоохоронними відомствами, сумісних зі стандартами, рекомендованими ООН та Радою Європи.

8.2.2. Автоматизовані системи та задачі органів прокуратури

Інформаційна система органів прокуратури у цілому має забезпечувати виконання таких *завдань*:

- розслідування постійно зростаючої кількості кримінальних справ (аналіз великої кількості аналогічних злочинів, груп осіб і т. ін.);
- підвищення інтенсивності нагляду за законністю в органах внутрішніх справ та інших органах, які ведуть боротьбу зі злочинністю та іншими правопорушеннями і розслідують діяння, що містять ознаки злочину;
- нагляд за судовими постановами з кримінальних, цивільних і господарських справ;
- проведення систематичних перевірок великого обсягу нормативного матеріалу, що видається органами влади і управління.

Виходячи з цього, можна визначити такі *задачі автоматизації*:

- ведення слідства, облікових даних на звинувачуваних, підозрюваних, свідків, даних про проведення експертиз, відомостей про передачу матеріалів до суду і результати розгляду справ у суді;
- ведення матеріалів про інциденти, кримінальні справи;
- контроль за термінами слідства і термінами утримання під вартою;
- ведення бази даних кореспонденції, що надходить;
- контроль виконання скарг, заяв і окремих доручень;
- ведення бази даних вихідної кореспонденції;
- реєстрація і систематизація даних про осіб, які звертаються в прокуратуру, а також про осіб, які є предметом її розгляду.

Схему формування бази даних ІС прокуратури наведено на рис. 8.5.



Рис. 8.5. Схема формування бази даних ІС прокуратури

Зокрема, база даних з карного правосуддя має містити:

- деталі всіх зареєстрованих злочинів, дані про осіб, яких звинувачено у злочинах, і наступні рішення про судові переслідування, вжиття або невжиття заходів;
- деталі справ, що знаходяться в судах, із взаємними посиланнями на злочини та осіб, що проходять по справах;
- деталі справ, одержаних прокурорами, з інформацією про зміни в деталях обвинувачення і рішеннями про те, чи слід починати розслідування та про час, необхідний для підготовки справи до слухання у суді;
- рішення, прийняті судами з кожної справи (для кожного злочину та звинувачуваного) зі встановленими взаємозв'язками;
- дані про ув'язнених (щойно заарештованих і кількість осіб, що утримуються) і звільнення до/після суду;
- дані про терміни покарання для засуджених і фактичний час, проведений ними під вартою;
- рішення судів про умовне звільнення;

- реакцію установ, відповідальних за умовний осуд і суспільні роботи (зроблені рекомендації, взяті до уваги чинники і т. ін.);
- дані про осіб, які відбувають термін покарання;
- дані про притягнення до суспільних робіт, про порушення, що мали місце і т. ін., а також інформацію про кількість поточних справ;
- дані про виплати, накладення судами штрафів і відшкодувань;
- дані про апеляції щодо перегляду судових рішень і вжитих у зв'язку з цим заходів.

Архів кримінальних справ має містити:

- ▲ відомості про зареєстрованих небезпечних злочинців та їх засудження;
- ▲ деталі злочинів і вироків;
- ▲ деталі місць вчинення злочинів, про служби, що виконали арешти, і суд, який виніс вирок;
- ▲ деталі інших злочинів, які було взято до уваги;
- ▲ в деяких випадках, деталі поводження злочинців.

У такій системі може бути і ряд *ресстрів*, які не мають безпосереднього відношення до кримінальної справи:

- викрадених транспортних засобів;
- осіб, які зникли безвісті;
- нерозкритих злочинів;
- викраденої власності (крім транспортних засобів);
- наркоманів;
- незапитаної власності;
- розшукуваних злочинців.

На різних рівнях прокуратури щойно наведені задачі вирішуються за допомогою сукупності інформаційних систем, типовий перелік яких можна сформулювати наступним чином.

ІС міських (районних) прокуратур:

1) нагляду за виконанням законів під час проведення попереднього слідства і дізнання:

- нагляду за розглядом заяв і повідомлень про заподіяні злочини;
- нагляду за обґрунтованістю відмов у порушенні карної справи;
- нагляду за виконанням законів при проведенні попереднього слідства і дізнання;
- оброблення даних про роботу прокурора з нагляду за слідством і дізнанням;

2) оброблення даних про демографію, економіку, культуру та побут («Соціальна статистика»);

3) нагляду за законністю судових постанов за карними справами («Судовий нагляд»);

4) нагляду за виконанням законів стосовно неповнолітніх («Неповнолітні»);

5) оброблення даних про скарги («Скарга»);

6) оброблення інформації, що проходить через канцелярію прокуратури («Канцелярія»).

В *обласних прокуратурах* створюються такі ІС:

1) нагляду за виконанням законів під час проведення слідства і дізнання:

- оброблення інформації по карних справах з продовженими строками слідства або утримання під вартою («Строки»);

- оброблення інформації по карних справах щодо злочинів, заподіяних злочинними угрупованнями («Організована злочинність»);

- оброблення інформації про демографію, економіку, культуру та побут («Соціальна статистика»);

2) нагляду за законністю судових постанов з карних справ;

3) організаційного забезпечення, статистики та контролю:

- оброблення даних про виконання плану та позапланових завдань («План»);

- оброблення даних про виконання рішень колегії та оперативних нарад («Рішення»);

- оброблення даних про документи, виконання яких узятو на контроль («Документ»);

- оброблення даних про листи, скарги та заяви громадян, які взято на контроль («Скарга»);

- оброблення даних про публікації у пресі («Публікація»);

- оброблення даних про контрольні перевірки («Перевірка»);

4) оброблення даних про кадровий склад органів прокуратури:

- персонального обліку кадрів («Кадри»);

- контролю за своєчасним атестуванням співробітників прокуратури і реалізації результатів їх проведення («Атестація»);

- контролю за своєчасним присвоєнням класних чинів («Класність»);

- оброблення статистичної інформації про рух кадрів в органах прокуратури;

б) оброблення статистичної інформації органів прокуратури.

ІС забезпечення розслідування злочинів:

1) інформаційного забезпечення розслідування карних справ про масові безпорядки на міжнаціональній основі;

- 2) інформаційного забезпечення розслідування порушень правил безпеки руху на залізничному транспорті;
- 3) інформаційного забезпечення розслідування порушень правил безпеки руху на морському транспорті;
- 4) інформаційного забезпечення розслідування навмисних злочинів, заподіяних:
 - на сексуальному підґрунті;
 - з розбійними нападами на житло;
 - з метою заволодіння автотранспортом;
 - розслідування навмисних вбивств, які мають схожі криміналістичні характеристики.



Автоматизація прокуратури — закордонний досвід¹

Однією з найбільш відомих комп'ютерних систем, що використовуються для автоматизації роботи прокуратури є PROMIS (Prosecutor's Management Information System, Управлінська ІС прокуратури), розроблена на початку 1970-х років за грантом Адміністрації допомоги правоохоронним органам Міністерства юстиції США (U.S. Department of Justice Law Enforcement Assistance Administration, LEAA). Авторство і права на удосконалену версію системи належать корпорації Inslaw (<http://www.inslawinc.com/>).

Головним призначенням PROMIS є нагромадження всієї інформації, з якою працює прокурор. Зокрема, по кожному підсудному, якому присвоєно унікальний ідентифікатор, зберігаються відомості про фізичні ознаки, прізвиська, попередні арешти та/або засудження, відомих співників, адреси, застереження і т. ін. Система також надає доступ до інформації щодо свідків, жертв, прокурорів, адвокатів, суддів, експертів, доказів і показань свідків, вироків та апеляцій. Функціями PROMIS є відстеження стану справи, виконаних і запланованих дій; оцінювання справ, що розглядаються, і впорядкування їх за тяжкістю злочинів та обставинами їх заподіяння (наприклад, насильницький злочин або рецидивізм); генерування календарних планів судових засідань для розподілу навантаження й організації підготовки до слухання справ; складання графіків появи свідків у суді тощо. Нагромаджена системою статистика є основою для визначення та оцінювання політики і пріоритетів щодо вирішення проблем боротьби зі злочинними угрупованнями, наркоманією, підлітковою злочинністю та ін.

Застосування PROMIS (в окрузі Вашингтон — з 1971 року) показало, що до її впровадження не виконувалось повне об'єднання

¹ За матеріалами сайтів <http://www.inslawinc.com/>, <http://www.eff.org/>, <http://www.copyright.com/>.

ня дій прокуратури. Усвідомлення цієї проблеми призвело до збільшення кількості середнього юридичного персоналу — підвищення структурованості і систематизованості роботи да-
ло можливість передати більше завдань працівникам, які не мають диплома юриста. Додатково до цього PROMIS використовується під час визначення напрямів підвищення кваліфікації працівників.

Водночас застосування PROMIS супроводжується численними гучними скандалами. За твердженням Білла Хеміптона, засновника і співвласника Inslaw Inc., Міністерство юстиції, одержавши систему, припинило виплати по укладеному десятимільйонному контракту. Розпочатий судовий розгляд є прикладом нескінченної тяжби. Справа має особливий аспект, оскільки PROMIS з певними доробками було продано у Канаду, Австралію, Бразилію, Великобританію, Ірак та деякі інші країни. Нещодавно у засобах масової інформації було розповсюджено повідомлення про те, що модифікована система містила «чорний хід», який давав можливість спецслужбам США та Ізраїлю проникати у секретні бази даних країн-покупців. Цей факт повною мірою можна оцінити тільки з огляду на те, якою зброєю стала PROMIS.

Призначена для використання і на мейнфреймах, і в мережному середовищі, PROMIS з самого початку була спроможна до одночасного читання та інтегрування будь-якої кількості різних комп'ютерних програм і баз даних, незважаючи на мови програмування, операційні системи, апаратні платформи. У 1980-х роках систему було доповнено елементами штучного інтелекту. Сьогодні вона спроможна контролювати розвідувальні операції, агентів і цілі. Її можливості, зокрема, використовуються для відстеження терористів на основі фінансової інформації — операцій з кредитними картками, спекуляцій з цінними паперами, купівель авіаквитків, оренди автомобілів та ін.

Завдяки локальним комп'ютерним мережам в органах прокуратури України вже стало можливим використання:

- мережного варіанта комп'ютерної правової бібліотеки «ЗАКОН» інформаційно-аналітичного центру «Ліга»;
- мережного варіанта комп'ютерної інформаційно-пошукової правової бази «ЗАКОНОДАВСТВО» Секретаріату Верховної Ради України;
- мережного варіанта оброблення статистичної звітності;
- мережного варіанта оброблення карток по скаргах;
- мережного варіанта пакета прикладних бухгалтерських програм «1С-Бухгалтерія»;
- мережного варіанта документообігу міжнародно-правового управління (у Генеральній прокуратурі України).

Впровадження в експлуатацію систем електронного модемного зв'язку надало можливість вирішити такі прикладні задачі:

- щотижневе оновлення даних комп'ютерної інформаційно-пошукової правової бази «ЗАКОНОДАВСТВО» у прокуратурах обласного рівня;
- збирання даних місячної статистичної звітності в органах прокуратури;
- обмін інформаційними посилками з прокуратурами обласного рівня;
- обмін інформаційними посилками з центральними органами влади України.

8.2.3. Документообіг Генеральної прокуратури України

Поліпшення діловодства і документообігу для органів прокуратури України, як і для інших правоохоронних органів, є надзвичайно важливим завданням. Сьогодні в органах прокуратури всіх рівнів пересилається більше 290 тис. службових і процесуальних документів щорічно. Це означає у середньому 650 документів на 1 працівника, а за деякими службами — до 1000 документів на особу. Потреба в папері становить 30 т на рік — його нестача часто призводить до затримок у листуванні.

У середньому на одного співробітника припадає 3 міжміських дзвінка на день. Понад 5 тис. карних і цивільних справ пересилається щорічно для перевірки і дачі вказівок вищими органами прокуратури. Крім того, звичайною є практика виклику місцевих оперативних працівників у відрядження для доповідей і звітів.

Усе сказане зумовлює потребу в системі автоматизації документообігу, електронній пошті, сучасних засобах телеконференцій, можливо, з передачею «відео-голос-дані» для скорочення і прискорення документообігу, а отже, продуктивнішого використання робочого часу.

Розглянемо схему документообігу на прикладі Генеральної прокуратури України (рис. 8.6). Уся кореспонденція, що надходить, поступає у секретаріат (відділ, прирівняний до управління), де документи проходять первинне сортування. Якщо в супроводжувальному листі вказано, в якій підрозділ та з якого питання надісланий документ, його передають у відповідний підрозділ.



Рис. 8.6. Схема документообігу в Генеральній прокуратурі України

Листи, які надходять особисто на ім'я Генерального прокурора, його заступників і помічників, передаються у відповідні приймальні. Якщо зі змісту документа не зрозуміло, в яке управління він надійшов, його направляють Генеральному прокуророві або його заступникам для накладання резолюції та розпису виконавців. У разі потреби вказується строк виконання і документ автоматично ставиться на контроль. Усі дані щодо сортування документів, їх руху, виконання, контролю та ін. відображаються у картотеці секретаріату.

Після цього документи надходять до канцелярії управління та у відділи, прирівняні до управління. Там вони передаються начальникам на резолюцію та розпис виконавців, проходять реєстрацію і ставляться на контроль, якщо були вказані кінцеві строки розгляду документа. Якщо до складу управління входять відділи, то документи проходять тільки етап накладення резолюцій начальником відділу і розпис підлеглим прокурорам на виконання.

Після надходження документа до кінцевого виконавця (прокурора або слідчого) він розглядається, на нього даються відповіді та зауваження. Після підготовки відповіді на надісланий документ, її підписує безпосередньо сам виконавець, начальник відділу, начальник управління, один із заступників Генерального прокурора або особисто Генеральний прокурор. Підписаний документ з додатками (якщо надісланий документ підлягає поверненню) передається у канцелярію управління. У канцелярії управління реєструється відповідь і вносяться необхідні дані про виконання документа. Після реєстрації у канцелярії управління документ передається у секретаріат в експедицію для відправлення адресату. Якщо документ знаходився на контролі, його реєструють та вносять необхідні дані у картотеку.

За аналогічною схемою зверху вниз передаються накази, розпорядження та вказівки на виконання.

Як середовище створення системи автоматизації документообігу було вибрано систему **Lotus Notes** — мережну платформу типу клієнт—сервер для розробки і розміщення прикладних програм, яка забезпечує спільну роботу людей (які перебувають в одному приміщенні або розділені територіально) над спільними завданнями в єдиному технологічному циклі. Lotus Notes відноситься до класу програм, орієнтованих на спільне виконання завдань робочими групами (groupware, див. розд. 4).

Робочий простір Lotus Notes ідентичний робочому столу ОС Windows і складається з фіксованих екранних вікон, у яких розміщені піктограми, що подають бази документів системи.

Документ є базовим поняттям системи Lotus Notes. База документів поєднує в собі властивості бази даних і додатку. Вона містить різноформатні документи, бланки документів, макроси і засоби перегляду вмісту бази та її елементів. База документів, як правило, перебуває у колективному використанні і розміщується на одному чи кількох серверах, але може бути і локальною, наприклад для розміщення незавершеної роботи або копії колективної бази даних при віддаленій роботі.

Документ для бази даних не потрібно конструювати спеціальним чином, він відповідає паперовому документу. Його структура визначається бланком і може містити числові, текстові і «розширені» поля. Останні складають основу документів і забезпечують їх різноманіття. Вони можуть містити текст, таблиці, графіку, звук, відео, а також об'єкти, які було впроваджено засо-

бами OLE (Windows), у тому числі і мультимедіа-продукти. Єдиний тип зв'язку, який підтримує Lotus Notes, — зв'язок супідрядності «основний документ — документ у відповідь».

Крім документної структури даних і мережної організації Lotus Notes має такі особливості:

- єдиний користувацький інтерфейс для звертання до інших користувачів, усіх мережних ресурсів та інформації;
- відкритість — підтримка багатьох операційних систем, додатків, зовнішніх джерел даних, систем передачі повідомлень тощо;
- масштабовуваність — підтримка організацій будь-якого розміру від робочої групи з двох осіб до корпоративної мережі з десятками тисяч користувачів;
- забезпечення повного життєвого циклу кожного документа в організації — відстеження його руху, візування, узгодження, прийняття, здача до архіву, зберігання;
- функції повнотекстового пошуку документів за словами, фразами, числами і датами;
- контекстний пошук за заданими документами і полями;
- підтримка версій документів (зберігання та оброблення кількох редакцій одного документа);
- вбудована поштова система із засобами повідомлення, автоматичної маршрутизації і циркулярної розсилки документів;
- механізм реплікації (тиражування) — забезпечення доступу до нової інформації всіх співробітників, у тому числі територіально віддалених, процедура виконується автоматично на рівні серверів;
- повна система захисту інформації на всіх рівнях (обмеження доступу, шифрування, електронний підпис);
- розвинена система швидкої розробки додатків, включаючи засоби проектування бланків, настройки засобів перегляду баз і документів, використання макросів і функцій. Сама розробка може бути еволюційною: спочатку форми документів, які передбачають ручне заповнення, потім — програмні сервісні функції, наприклад, автоматичний агент, який перевіряє час, відведений на роботу з документами або описаний механізм заповнення за шаблонами, і нарешті, повністю автоматичні учасники бізнес-процесу з досить складною поведінкою;
- засоби підтримки відкритості системи у вигляді версій для різних платформ, підтримки різних комунікаційних протоколів і зовнішніх баз даних. Можливою є інтеграція створеної системи з іншими продуктами, наприклад з СКБД.

The image displays three overlapping screenshots of the 'Megdunar' system interface, showing different stages of document processing.

Top Screenshot (Form1): This window is titled 'Реєстрація документа' (Document Registration). It contains fields for 'Індекс відділу' (14/1), 'Індекс виконавця', 'Дата надходження' (01/13/19), 'Вхідн. №', and 'Вихідн. №'. Below these are sections for 'Кореспондент' (Ukraine, International organization, Direction of document forwarding) and 'Дані про розгляд чи виконання' (Accepted for execution, Executed, etc.).

Bottom Left Screenshot (Form1): This window shows a list of document types under 'Реєстрація документа'. The list includes:

- 1. Організація роботи
- 2. Звернення про правову допомогу (with sub-options for procedural acts, extradition, and criminal proceedings)
- 3. Скарги та запити
- 4. Відраження
- 5. Договірна робота (with sub-options for bilateral and multilateral)
- 6. Співробітництво (with sub-options for programs, meetings, seminars, training, and cooperation)
- 7. Виступи в засобах масової інформації
- 8. Виступи з доповідями та лекціями
- 9. Отримання і передача кримінальних справ
- 10. Переклади (with sub-options for translation and interpretation)

 Buttons at the bottom include 'Додати', 'Зберегти', and 'Вихід'.

Bottom Right Screenshot (Form1): This window is titled 'КОНТРОЛЬ ЗА ВИКОНАННЯМ ДОРУЧЕННЯ (ДОКУМЕНТА)' (Control of execution of the assignment (document)). It contains several tables:

- КОНТРОЛЬ ЗА ВИКОНАННЯМ ДОРУЧЕННЯ (ДОКУМЕНТА):** A table with columns 'Дата' and 'Ким встановлено контроль'.
- ВИХІДНІ ВІД ПОЧАТКОВОГО ДОРУЧЕННЯ (ДОКУМЕНТА):** A table with columns 'Дата', 'Куда', 'Зміст', and 'Ім'я файла'.
- ВИХІДНІ ДО ДОРУЧЕННЯ (ДОКУМЕНТА):** A table with columns 'Дата', 'Номер', 'Звідки', 'Зміст'.
- РУХ НАГЛЯДОВОГО ПРОВАНДЖЕННЯ:** A table with columns 'Дата', 'Кому', 'Коментар'.

 Buttons at the bottom include 'Додати', 'Зберегти', and 'Вихід'.

Рис. 8.7. Форми введення документів у системі «Megdunar»

Як базову прикладну систему спільної роботи з документами в органах прокуратури вибрано систему автоматизованого документообігу «ЭСКАДО», призначену для підготовки, зберігання, класифікації та пошуку довільних документів. «ЭСКАДО» забезпечує: захист від несанкціонованого доступу; підтримку кількох електронних підписів; прийом і зберігання документів у довільному форматі (факси, телетайпи, пошта і т. ін.); підготовку і відправлення документів у довільному форматі; спільне використання документів; об'єднання документів у групи за певними ознаками (договори, угоди, контракти); планування роботи співробітників; відстеження взаємодії з іншими організаціями.

У Міжнародно-правовому управлінні Генеральної прокуратури України використовується автоматизована система забезпечення оперативного контролю за станом роботи у сфері надання правової допомоги та міжнародного співробітництва («Megdunar»). Система призначена для обліку виконаної роботи працівників управління шляхом уведення документів за визначеними критеріями (рис. 8.7), їх оброблення і формування звітів і довідок, а також для здійснення контролю за термінами виконання окремих завдань.

8.3. КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ В СУДОВІЙ ЕКСПЕРТИЗИ

8.3.1. Основні напрями комп'ютеризації судової експертизи

Поняття «судова експертиза» позначає широке коло різноманітних досліджень, що їх проводять у тих випадках, коли при дізнанні, попередньому слідстві або судовому розгляді необхідні спеціальні знання з науки, техніки, мистецтва або ремесла, щоб виявити і пізнати приховану сутність явищ і речей і дати їх наукове тлумачення.

Юридичні факти встановлюються сукупністю доказів. Висновок судового експерта входить у зазначену сукупність. У такому висновку відображається зв'язок між запитаннями, поставленими перед експертом, джерелами інформації, інформаційним полем, завданнями дослідження, предметом дослідження, методами дослідження і доказом юридичних фактів. Отже, можна говорити про певний вид інформаційної діяльності.

Тривалий час зберігався суттєвий розрив між теорією і практикою використання інформаційних технологій у судовій експер-

тизі. Існували значні проблеми науково-методичного та інформаційного забезпечення експертної діяльності. Зміни ситуації обумовлені *сучасними умовами*:

- сьогодні об'єктами експертного дослідження можуть бути тисячі різновидів матеріалів, речовин і виробів, кожен з яких характеризується багатьма властивостями й ознаками;

- оперативне одержання інформації про конкретний об'єкт дослідження та її аналіз стали можливими лише за умов використання різних сучасних автоматизованих систем і комплексів, на базі яких нині розроблено безліч методик вирішення широкого кола експертних задач;

- використання новітніх технічних засобів і технологій дає змогу визначити шляхи розвитку нових методів, спрямованих на об'єктивізацію досліджень і підвищення наукової обґрунтованості висновків експертів;

- важливою сферою автоматизації стала організаційно-управлінська діяльність у галузі судової експертизи.

Сьогодні виділяють кілька напрямів комп'ютеризації судово-експертної діяльності. Їх можна класифікувати за такими *ознаками*:

1) за характером математичного апарату, на якому базуються комп'ютерні технології і конкретні методики судово-експертних досліджень — методики, основані на даних метрології, теорії ймовірностей і математичної статистики, проективної геометрії і т. ін.;

2) за характером експертних задач, що вирішуються. У цьому разі можна говорити про застосування математичного апарату (будь-якого) та обчислювальної техніки для вирішення:

- діагностичних задач (наприклад, установлення факту виконання тексту навмисно зміненим почерком, скорописним способом, установлення факту контактної взаємодії двох об'єктів);

- класифікаційних задач (наприклад, установлення статі або темпераменту за почерком, віднесення невідомої речовини до групи наркотичних);

- ідентифікаційних задач (стосовно людини, знаряддя, матеріалу, речовини і т. ін.);

3) за характером задач, не пов'язаних з виробництвом конкретного експертного дослідження, але спрямованих на оптимізацію і підвищення ефективності рішення експертних задач певного виду або експертної діяльності в цілому:

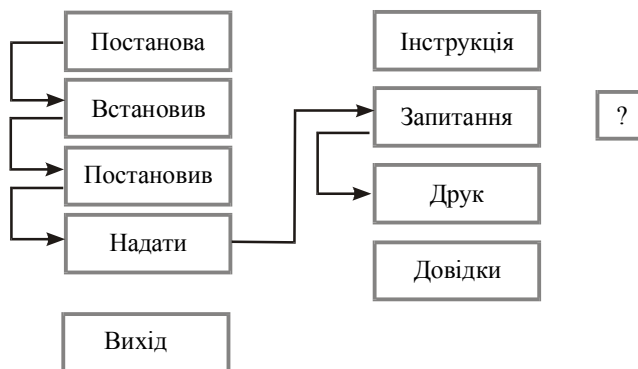
- автоматизація вимірювань і первинного оброблення даних;
- створення та експлуатація автоматизованих банків даних про властивості різноманітних об'єктів;

- розв'язування складних обчислювальних задач, що виникають як у науково-дослідній роботі, так і в експертному виробництві;
- створення та експлуатація програм для логічного аналізу даних;
- використання автоматизації для вирішення задач управління, обліку кадрів, збирання статистичних даних з судової експертизи і т. ін.



Судові експертизи — приклад експертної системи

Працівниками прокуратури Полтавської області створено програму «Судові експертизи». Проаналізувавши судово-слідчу практику і відповідні наукові розробки, автори систематизували в приблизний перелік запитання, які можуть бути поставлені перед експертом під час проведення судових експертиз. У програмі розроблено варіанти призначення більше сотні різноманітних експертиз. Це не вичерпний перелік досліджень, які можуть проводитись в експертних закладах України. Для інших експертиз поки недостатньо відпрацьована методика проведення або вони передбачають унікальні дослідження. Схему роботи програми показано на рис.



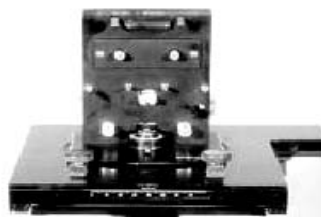
Користувач може залишати формулювання конкретних запитань в редакції авторів або створювати і записувати до бази даних власні запитання.

У судовій експертизі застосовуються найрізноманітніші пристрої. Наприклад, для дослідження рельєфних клейм і маркірувань, нанесених на поверхні виробів з магнітного металу в Київському НДЦ судових експертиз (<http://www.expert.com.ua/>) використовується портативний магнітооптичний візуалізатор

«Подорожник» (рис. 8.8, *а*), а для дослідження фонограм (відеофонограм) з метою виявлення способу їх виготовлення (ознак монтажу), визначення їх оригінальності та ідентифікації записуючої апаратури — «Магнітоскоп» (див. рис. 8.8, *б*).



а



б

Рис. 8.8. Технічні засоби експертизи:
а — «Подорожник», *б* — «Магнітоскоп»

Існують і суто програмні розробки, наприклад, транскрайбер RAT — програмний продукт, призначений для розшифрування фонограм за допомогою комп'ютера, програмний пакет VIS для автоматичної текстонезалежної ідентифікації за голосом на основі довгочасового усереднення параметрів мовлення. Але найбільший ефект дають комплекси, в які входять спеціальні пристрої і комп'ютер.

Одним із прикладів таких комплексів є вимірювально-обчислювальний комплекс дослідження фонограм, до складу якого входить студійний цифровий магнітофон, спектроаналізатор типу сонограф (наприклад, DSP SONA-GRAPH моделі 4300 або його апаратно-програмний аналог) і персональна ЕОМ з периферійними пристроями. Наявність ЕОМ дає змогу не тільки автоматизувати процес порівняння фонограм, а й побудувати спеціальні алгоритми оброблення інформації, входом в які є показники сонографа, представлені у цифровому виді, а виходом — акустичні ознаки, що характеризують особу, яка говорить. Для експертизи відеозаписів необхідні мультисистемний (PAL, SECAM, NTSC) відеоманітофон з можливістю роботи у режимах запису SP і LP; два відеоманітофона формату запису S-VHS з можливістю покадрового режиму роботи і з наявністю лічильника фреймів, шкали регулювання трекінгу та аудіосигналу; два монітори з можливістю комутації по двох лініях; мікшерний пульт; відеопринтер; осциллограф з можливістю виділення телевізійного рядка; комп'ютер з можливістю введення та оброблення відеокадрів; відеокамера.

Ще одним важливим напрямом використання подібних комплексів є організація *спеціалізованих інформаційно-пошукових систем*. Прикладом є автоматизована дактилоскопічна інформаційно-пошукова система DEX, перша версія якої («Дактоексперт») встановлена в Печерському РУ ГУ МВС України м. Києва та в м. Обухові.

На сьогодні в Україні проблему виявлення, вилучення та дослідження слідів дактилоскопічного походження загалом вирішено. Накопичено великі масиви слідів і дактилокарт осіб, які підлягають обліку. Їх обробка методом ручного візуального порівняння практично неможлива через необхідність значних затрат людських і матеріальних ресурсів. Система DEX призначена:

- для встановлення особистості за відбитками пальців рук;
- для розкриття злочинів — сліди дозволяють установити підозрюваного, а також об'єднати нерозкриті злочини, якщо встановлено, що вони вчинені однією особою;
- для виявлення дублікатів дактилокарт — виявлення осіб, зареєстрованих під різними прізвищами та виявлення надлишкових карток реєстрації осіб.

DEX реалізується як сукупність апаратних підсистем, що взаємодіють одна з одною на лініях різної пропускної спроможності. Кожна підсистема будується на базі окремих спецпроцесорів відповідної потужності, які забезпечують незалежну паралельну роботу над загальними полями пам'яті. Автономні повнофункціональні модулі DEX утворюють DEX-кластери, з яких формується глобальна обчислювальна та інформаційна мережа DEXNET, в якій здійснюється:

- введення, коригування, вилучення, архівація, пересилка дактилоскопічної інформації;
- формування, коригування, вилучення, запуск, пересилка пакетів завдань;
- автоматичне кодування зображення відбитка чи сліду пальця руки;
- автоматичне порівняння пари кодів відбитка чи сліду пальців рук.
- перегляд, варіація, коригування, вилучення, роздрукування, пересилка пакетів результатів;
- підготовка, коригування, вилучення, роздрукування, пересилка пакетів електронних експертиз та іншої дактилоскопічної і системної інформації.

Пошук дактилоскопічної інформації відбувається за *схемами*:

- «карта—карта» — встановлення особи з певною дактилокартою;

- «слід—карта» — для розкриття злочинів;
- «карта—слід» — встановлення злочинів, вчинених певною особою;
- «слід—слід» — встановлення можливості об'єднання вчинених нерозкритих злочинів.

Усі види пошуку можливі як у керованому оперативному, так і в цілковито автоматичному режимі. У першому випадку експерт сам ініціює процес обробки і перегляд результатів, у другому система визначає необхідність порівняння, проводить пошук і зберігає результати для наступного негайного пред'явлення за запитом експерта.

Процес інформаційного пошуку в системі DEX та інших має свою *специфіку*. По-перше, якщо експерт має можливість аналізувати і використовувати всю гамму ознак і властивостей об'єкта, виділених в інформаційному полі, то ІПС оперує тільки тими ознаками, що їх було введено у систему. Наприклад, в основу алгоритму порівняння «слід—відбиток», що використовується у значній кількості закордонних дактилоскопічних ІПС (японській «NEC», американській «Принтрак», німецькій «Дермалог», російських «Сонда» і «Папілон») покладено менуціальний принцип порівняння (за індивідуальними особливостями), взятий фірмами-розробниками з традиційної дактилоскопії. Застосування цього принципу в автоматичній дактилоскопії надто обмежене через високий ступінь геометричних та інших викривлень дактилоскопічної інформації, що з'являються при слідоутворенні, а також через значний вплив суб'єктивізму людини при візуальному визначенні індивідуальних особливостей. Як показує практика, неможливо двічі отримати однакові відбитки певного пальця. Розробники ж алгоритму порівняння системи DEX за основу алгоритму взяли найбільш незмінну ознаку дактилоскопічного відбитку (сліду) — інтегральну кривизну потоків папілярних ліній. Мєнуціальний принцип, доданий в алгоритм, дає змогу розкривати злочини за «важкими» слідами.

По-друге, потребують адекватного сприйняття результати експертизи, одержані за допомогою комп'ютерної техніки на основі кількісних методів. Так, однією з особливостей судової відеофонографічної експертизи є застосування програм, які використовують різні ймовірно-статистичні методи оцінки збігів і відмінностей ідентифікаційних ознак (наприклад, ознак голосу і мови). Можливості таких методів у даний час далеко не безмежні, тому експерт не завжди може зробити категоричний висновок і іноді змушений удаватися до ймовірної форми висновків.

Водночас практична корисність ймовірних висновків не викликає сумніву — вони можуть служити для побудови версій, визначення напрямку розслідування, виявлення інших доказів і тим самим сприяти розкриттю злочину.

Ще одна важлива особливість пов'язана зі специфікою автоматизованого оброблення інформації. Більшість методів і результатів застосування ЕОМ під час дослідження, наприклад голосу, не забезпечує ілюстративності у звичайному розумінні. Експерт одержує інформацію про досліджуваний об'єкт після того, як за допомогою ЕОМ програмно виділить і порівняє ознаки голосу. Тому, оцінюючи такі висновки, слідчий і суд повинні перевірити дані, що їх було введено до ЕОМ (такі дані експерт повинен повно і доступно описати у висновку).

8.3.2. Судові комп'ютерно-технічні експертизи

Прогрес у сфері інформаційних технологій, впровадження нових засобів обчислювальної техніки і телекомунікаційних систем, широке використання ІС в економіці, зокрема у фінансовій і банківській діяльності, мають за наслідок не тільки зростання комп'ютерної злочинності, а й застосування новітніх технологій при вчиненні інших видів злочинів. Сьогодні є всі підстави прогнозувати подальше зростання рівня правопорушень у сфері комп'ютерної інформації, оскільки інформація нині є найдорожчим товаром, який дає високі прибутки, а отже, стає предметом злочинних зазіхань. Водночас правоохоронні органи поступово нагромаджують досвід боротьби з цими злочинами і розробляють способи їх виявлення і доведення, в тому числі з застосуванням сучасних інформаційних технологій¹.

Під час розслідування високотехнологічних злочинів все частіше виникає необхідність виявлення і вилучення слідів і речовинних доказів, представлених у вигляді інформації в обчислювальній чи телекомунікаційній системі, а також на магнітних носіях. У таких випадках з'являється потреба у спеціальних знаннях і навичках, основною процесуальною формою залучення яких є експертиза. Однак на сьогодні у спеціальній літературі та методології традиційних експертиз відсутнє єдине розуміння не

¹ Ще в 1982 році Верховний Суд СРСР визнав правомірним використання як доказів документів і висновків експертів, підготовлених засобами електронно-обчислювальної техніки, а Державний Арбітраж СРСР у 1979 році видав Інструктивні вказівки щодо використання як доказів з арбітражних справ документів, підготовлених за допомогою електронно-обчислювальної техніки.

тільки об'єктів і методів проведення експертиз такого роду, а й самої їхньої сутності¹. В одних випадках це призводить до необґрунтованого розширення кола об'єктів і вирішуваних задач у рамках традиційних криміналістичних експертиз, а в інших — суттєво звужує можливості застосування спеціальних пізнань при виробництві даного виду експертних досліджень.

У цьому контексті фахівці вводять поняття **комп'ютерно-технічної експертизи**, покликаної на основі спеціальних пізнань обізнаної особи-експерта вирішувати експертні питання відносно діянь, спрямованих проти інформаційної безпеки.

На даному етапі розглядаються такі *різновиди об'єктів комп'ютерно-технічних експертиз*:

- текстові і графічні документи (стандартні й електронні), виготовлені з використанням засобів автоматизації (обчислювальних систем, засобів передавання даних і копіювання інформації);
- програми для ЕОМ і допоміжна комп'ютерна інформація, необхідна для їхнього функціонування;
- відео- і звукозаписи, візуальна та аудіоінформація, представлена у форматі мультимедіа;
- комп'ютерні дані і відомості, представлені у форматах, що забезпечують їх автоматизоване збереження, пошук, оброблення і передавання (бази даних);
- фізичні носії інформації різної природи (магнітні, магніто-оптичні, оптичні та ін.).

Виходячи з цього, передбачається, що за допомогою комп'ютерно-технічних експертиз можуть виконуватись наступні *завдання*:

- 1) відтворення і роздрукування всієї або частини інформації, яка міститься на фізичних носіях, у тому числі в нетекстовій формі;
- 2) відновлення інформації, що раніше містилась на фізичних носіях і згодом стертої чи зміненої з різних причин;
- 3) встановлення часу введення, зміни, знищення або копіювання інформації;
- 4) розшифрування закованої інформації, підбір паролів і розкриття систем захисту інформації;
- 5) встановлення авторства, місця, засобу підготовки і способу виготовлення документів (файлів, програм);

¹ Згідно з Інструкцією про призначення та проведення судових експертиз, затвердженій Міністерством юстиції України 8.10.1998 р., технічна експертиза документів, фототехнічна експертиза, технічна експертиза матеріалів і засобів відеозвукозапису є підвидами криміналістичної експертизи, а експертиза комп'ютерної техніки і програмних продуктів розглядається як окремий вид.

б) з'ясування технічного стану, справності програмно-апаратних комплексів автоматизованих інформаційних систем, можливості їхньої адаптації під конкретного користувача.

У рамках дослідження комп'ютерної техніки, носіїв інформації, периферійного обладнання і програмного забезпечення можуть бути знайдені відповіді на такі *запитання*:

- які технічні несправності має даний комп'ютер (його окремі блоки та пристрої) і як ці несправності впливають на його роботу;
- чи використовуються представлені технічні пристрої в режимах, передбачених керівництвом з експлуатації, або вони підімкнені в режимах, які забезпечують додаткові, непередбачені стандартним варіантом можливості (наприклад, чи правильно підімкнений блок фіскальної пам'яті в контрольно-касовому апараті, побудованому на основі персонального комп'ютера);
- чи можливе вирішення певної задачі за допомогою даного програмного продукту;
- чи можна за допомогою даного програмного продукту реалізувати функції, передбачені технічним завданням на його розробку;
- які основні функції представленого програмного забезпечення, які його споживчі властивості, чи є воно небезпечним;
- чи перебуває представлене програмне забезпечення у стані, який забезпечує можливість його застосування на заданому комплексі технічних засобів або з певним іншим програмним забезпеченням;
- чи відповідає стиль програмування досліджуваного програмного продукту стилю програмування певної особи;
- за допомогою яких обчислювальних і програмних засобів створено програмне забезпечення;
- чи відповідають прийоми і засоби програмування, що використовувалися під час створення досліджуваного програмного продукту, прийомам і засобам, властивим даному програмісту;
- яка вартість програмного забезпечення або його окремих модулів (на час його придбання, вилучення, проведення експертизи);
- яка вартість комп'ютерної техніки (окремих комплектуючих) на час придбання (вилучення, проведення експертизи);
- яка орієнтовна дата створення обчислювального комплексу із заданими можливостями і дати виготовлення його окремих блоків;
- яка орієнтовна дата створення програмного забезпечення;
- яке призначення мають представлені бази даних, які їх споживчі властивості;

- чи існує на даному носії яка-небудь інформація, і якщо так, то яка;
- чи розміщено на представленому магнітному носії або у складі технічних засобів обчислювальної техніки інформаційне забезпечення, необхідне для вирішення певної функціональної задачі;
- чи існують на представленому магнітному носії файли з документами, які відносяться до тієї чи іншої сфери діяльності (наприклад, файли із зображеннями грошових знаків, кресленнями вибухових пристроїв, схемами електропроводки у будинку, бланками юридичних осіб і відбитками печаток, початковими текстами шкідливих програм мовою високого рівня і т. ін.);
- чи існує на даному носії інформація, яка свідчить про інформаційний обмін у якій-небудь мережі (зокрема, Інтернет) у заданий інтервал часу;
- чи існує на носії інформація, що її було знищено, і чи можна її відновити;
- чи можливе здійснення заданого виду діяльності з використанням представлених технічних засобів і розміщеного на них інформаційного і прикладного програмного забезпечення (наприклад, перехоплення електронної кореспонденції, підготовка і виготовлення підроблених грошових знаків);
- які наслідки (збитки) можуть бути від застосування комплексу технічних засобів, шкідливих програм у даній інформаційній системі, мережі.



Контрольні запитання і завдання

1. Які основні напрями автоматизації судових органів?
2. Схарактеризуйте інформаційні системи Верховного Суду України.
3. Які типові автоматизовані робочі місця працівників судів різного рівня?
4. Назвіть основні функції, що виконуються на АРМ судового виконавця.
5. Визначте основні типові функціональні підсистеми ІС державної судової адміністрації.
6. Визначте інформаційні зв'язки усередині КІС органів прокуратури і між нею та інформаційними системами інших органів і установ.
7. Яку структуру повинна мати КІС органів прокуратури?

8. Назвіть завдання, що розв'язуються в КІС органів прокуратури.

9. Схарактеризуйте систему Lotus Notes та її можливості для автоматизації документообігу.

10. Прокласифікуйте напрями комп'ютеризації судово-експертної діяльності.

11. Назвіть переваги, що їх надає використання комп'ютерних технологій у судовій експертизі.

12. Які завдання та об'єкти дослідження має комп'ютерно-технічна експертиза?



Література

1. Компьютерные технологии в юридической деятельности: Учеб. Пособие. / Под ред. проф. Н. Полевого, канд. юрид. наук В. Крылова. — М.: Изд-во БЕК, 1994. — 304 с.

2. Матеріали сайтів <http://www.expert.com.ua/>, <http://www.naiu.kiev.ua/visnik/>, <http://www.nicagora.euro.ru/>, <http://www.scourt.gov.ua/>, <http://www.supcourt.ru/it/>, http://www.ural-chel.ru/gubern/obl_sud/.



ІНФОРМАЦІЙНІ СИСТЕМИ ОРГАНІВ ВНУТРІШНІХ СПРАВ

9.1. ПРОБЛЕМИ І КОНЦЕПЦІЯ РОЗВИТКУ ІС ОВС УКРАЇНИ

Засоби обчислювальної техніки почали активно використовуватись в органах внутрішніх справ (ОВС) з 1960-х років. Здебільшого сфера їх застосування обмежувалась аналізом статистичної інформації, веденням криміналістичних та інших обліків і контролем за станом розгляду заяв і повідомлень про злочини.

Принципи побудови інформаційних систем ОВС відображали притаманний для того часу рівень розвитку технічних засобів і досягнень технології. Переважала централізована обробка інформації, за умов якої безпосередній доступ споживачів інформації (практичних працівників ОВС) до банків даних був неможливий або незручний. При цьому практично для кожної нової задачі розроблялись окремі проектні рішення, що призводило до дублювання інформаційних масивів, неузгодженості між ними і нерациональної організації інформаційної системи в цілому. Ефективність використання інформаційних систем знижувалась через відсутність зв'язку між базами даних різних регіонів і несумісність форматів зберігання даних.

Поступово склалася ситуація, коли програмно-технічна база інформаційних систем ОВС застаріла і перестала відповідати вимогам користувачів. Крім зазначених вище можна назвати такі важливі *недоліки*:

- дублювання процесів збирання та оброблення даних різними галузевими службами і на різних рівнях;
- недостатні повнота, вірогідність і захищеність даних;
- численність і недосконалість первинних облікових документів;
- слабкий інформаційний зв'язок між обліково-реєстраційними, оперативно-розшуковими та довідковими фондами різних служб;
- недосконалість організаційно-кадрового забезпечення інформаційних підрозділів МВС, ГУМВС, УМВС, УМВСТ та галузевих служб;

- нераціональне використання фінансових коштів на підтримку і розвиток інформаційних систем;
- недосконалість нормативно-правової бази.

Водночас загострення оперативного стану в Україні, збільшення обсягів інформації, що надходить і переробляється, зумовило гостру потребу в підвищенні ефективності всіх служб МВС на основі новітніх інформаційних технологій. Це підтверджується і нормативними документами, зокрема програмою боротьби з організованою злочинністю (Указ Президента України від 17.09.1997 р. № 837). Уже сьогодні в цьому напрямку спостерігаються певні позитивні тенденції, серед яких загальне підвищення комп'ютерної грамотності працівників міліції; збільшення переліку комп'ютерних інформаційних обліків (див. підрозд. 9.2); поширення використання сучасних засобів комп'ютерної техніки в діяльності всіх ланок ОВС; впровадження безпаліперових технологій оброблення інформації; створення комп'ютерної мережі обміну інформацією.

Головною метою робіт, що проводяться, є забезпечення інформаційної підтримки діяльності ОВС:

- оперативне отримання працівниками та підрозділами ОВС повної інформації, необхідної для розкриття, розслідування, попередження злочинів і розшуку злочинців у систематизованому та зручному для користування вигляді;
- збирання та оброблення оперативної, оперативно-розшукової, оперативно-довідкової, аналітичної, статистичної і контрольної інформації для оцінювання ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях діяльності ОВС;
- ефективна інформаційна взаємодія з іншими правоохоронними органами і державними установами.



Інформаційний простір правоохоронних органів — приклад взаємодії

У 1997 році інформаційні системи Держкомкордону та МВС України було інтегровано в єдиний інформаційний простір. Основу ІС прикордонних військ України складає комплекс автоматизованого паспортного контролю «Кордон», який було адаптовано до нових пристроїв зчитування паспортів. ІС МВС України здійснює інформаційну підтримку в розкриванні та попередженні злочинів, установленні та розшуку злочинців, надає статистичні, аналітичні та довідкові дані. У результаті нова система прикордонного контролю дає змогу за лічені секунди одержувати інформацію про будь-який суб'єкт, який перетинає кордон України. У Німеччині час реакції подібної системи на запит оператора складає всього 1,5 с.

У сфері управлінської та контрольно-методичної роботи виконуються такі завдання комп'ютеризації:

- збирання і нагромадження даних про скоєні злочини;
- аналіз статистичної звітності за встановленими формами;
- контроль за дотриманням процесуальних строків, розглядом заяв громадян, виконанням планових заходів;
- складання управлінських документів;
- створення і використання баз даних (знань) та автоматизованих інформаційно-пошукових систем для одержання інформації про нормативні акти, наукову літературу, методичні розробки, матеріали передового досвіду слідчої та судової практики;
- нагромадження інформації про експертні установи, їх можливості, види експертиз, приблизні питання експертам та ін.;
- аналіз робіт з профілактики злочинів та оцінювання їх ефективності;
- аналіз інформації щодо нерозкритих злочинів минулих років, розробка рекомендацій щодо їх розкриття та використання типових ознак і ситуацій;
- формування моделей процесуальних дій зі збільшенням обсягу стандартної інформації стосовно розслідування різних видів злочинів;
- розробка методик розслідування кримінальних справ з комп'ютерних та інших видів злочинів.

У сфері розслідування злочинів автоматизації підлягають:

- процес слідчого виробництва з використанням баз процесуальних та інших документів, що оформляються на стадії попереднього розслідування;
- планування заходів по конкретних кримінальних злочинах;
- створення календарних планів і мережних графів розслідування;
- нагромадження та аналіз інформації з кримінальних справ, зокрема великого обсягу та багатоепізодних;
- складання слідчих та інших документів (у першу чергу, постанов щодо притягнення як обвинуваченого та висновків з обвинувачення) на основі даних, занесених у базу;
- передача до суду протоколів допитів, постанов та інших процесуальних документів на магнітних носіях та по каналах зв'язку;
- вибір та передача необхідної інформації для проведення відповідних заходів у ході оперативно-розшукової діяльності, її оформлення згідно з кримінально-процесуальним кодексом;
- зберігання та використання різноманітної довідкової інформації з кримінальних справ;

- контроль з боку керівників підрозділів за розслідуванням кримінальних справ на всіх етапах;
- організація та проведення бухгалтерських ревізій та експертиз, різноманітні розрахунки з кримінальних справ по економічних злочинах;
- використання у ході розслідування програм з методиками розслідування злочинів різних видів.

У цілому ІС МВС має структуру, адекватну адміністративно-територіальному розподілу і складається з підсистем відповідно до напрямків діяльності міністерства. Комплекс технічних засобів підтримує всі функції архітектури «клієнт—сервер» та «термінал—сервер» з урахуванням специфіки завдань, що виконуються на кожному рівні системи. Усі рівні комплектуються серверами баз даних і АРМ кінцевих користувачів.

Для інформаційного забезпечення ОВС України створюються дві категорії ІС за функціональним призначенням — загальновідомчі та галузеві. До **загальновідомчих ІС** належать:

- ІС оперативно-розшукового призначення, які містять дані, безпосередньо пов'язані з кримінальною або оперативно-розшуковою справою і використовуються багаторазово;
- спеціалізовані ІС оперативного оброблення інформації;
- ІС оперативно-довідкового призначення, які містять фактографічну інформацію про осіб, об'єкти та речі, що становлять оперативний інтерес;
- ІС кримінальної статистики, що містять інформацію про стан злочинності та результати боротьби з нею;
- адміністративно-управлінські ІС, які містять інформацію загальнодержавного та загальнослужбового використання.

До категорії **галузових ІС** належать такі, що не містять загальновідомчої інформації.

Доступ до ІС ОВС України здійснюється з відповідних АРМ безпосередньо або за допомогою засобів закритої відомчої електронної пошти через комутовані телефонні канали міжміської телефонної мережі, телефонної мережі «Іскра-2», телефонної мережі «Укрзалізниця», по виділених каналах зв'язку. Мережа має топологію типу «зірка» з Головним поштамтом в УОІ МВСУ і регіональними поштамтами в областях, до яких підключаються віддалені поштові відділення (абоненти). Абонентами електронної пошти ОВС України є підрозділи та окремі працівники органів внутрішніх справ.

Об'єднання АРМ у мережу дає змогу не тільки поєднати всі інформаційні ресурси, створити єдину розподілену базу даних, а

й забезпечити за допомогою засобів комунікації пошук і одержання необхідної фактографічної та документальної інформації з баз даних Інтерполу та інших структур.



Телекомунікації у діяльності ОВС — ще один напрям використання

Телекомунікації знаходять нові галузі застосування. Прикладом є спільний проект Міністерства юстиції та Міністерства оборони США з впровадження телемедицини для потреб військових та правоохоронців.

***Телемедицина** визначається як віддалене надання медичної допомоги за допомогою засобів телекомунікацій. Таким чином вирішуються проблеми для віддалених районів і, зокрема, для тюрем. Ув'язнені мають конституційне право на медичну допомогу, але її надання може вимагати значних витрат на доставку фахівців або конвоювання ув'язнених до спеціалізованих медичних закладів. Телемедицина забезпечує передавання лікареві інформації про особу, яка потребує лікування або діагностики. Формат передачі може варіюватись від повідомлень з результатами лабораторних тестів або зображеннями рентгенівських знімків до відеоконференції, у ході якої лікар може бачити на екрані і пацієнта, і показники діагностичних пристроїв. Ще одним напрямом є дистанційне керування лікарями широкого профілю з боку досвідчених спеціалістів.*

Крім зменшення витрат на медичну допомогу у закладах виконання покарань, телемедицина забезпечує зниження ризику порушення режиму під час зовнішніх консультацій, уникнення тривалих затримок під час надання медичних послуг, доступ до кращих спеціалістів, зменшення скарг на медичне обслуговування, скорочення потреби у фахівцях (один лікар може обслуговувати кілька віддалених районів).

Особливого значення в ІС ОВС має організаційно-кадрове забезпечення, у першу чергу інформаційна служба ОВС, яка складається з інформаційних підрозділів МВС, ГУМВС, УМВС, УМВСТ, міських, районних і лінійних ОВС (міськрайлінорганів) та галузевих інформаційних підрозділів. Інформаційні підрозділи відповідно до рівня ОВС мають у своєму складі відділи (відділення, групи, фахівців) за усіма напрямками роботи, а саме:

- оперативної інформації;
- оперативно-розшукової роботи з цілодобовим функціонуванням чергових інформаційних груп;
- оперативно-довідкової інформації;
- технічного обслуговування ІС і засобів оперативної поліграфії;

- супроводження та адміністрування ІС і банків даних, комп'ютерних мереж та телекомунікаційних систем;
- впровадження нових інформаційних технологій;
- збирання та оброблення статистичної інформації;
- архівної роботи;
- матеріально-технічного забезпечення.

В Управлінні оперативної інформації (УОІ) зберігається найбільша кількість інформаційних масивів у системі МВС України. Щорічно до цього управління звертаються сотні тисяч користувачів та кореспондентів. Це провідна організація, яка розробляє і впроваджує ІС в діяльність ОВС. Чергова частина УОІ цілодобово опрацьовує запити ОВС України на перевірку об'єктів обліку і видає рекомендації про їхню належність.

Підрозділи, що здійснюють збирання, нагромадження, оброблення та передавання інформації на всіх рівнях, несуть відповідальність за безпеку інформації. Організація загальної безпеки інформаційного забезпечення запроваджується і контролюється Управлінням справами і Центром технічного захисту інформації при МВС України, який визначає та впроваджує разом з інформаційною службою відповідні засоби захисту.

9.2. РІВНІ ТА СКЛАД ІНФОРМАЦІЙНИХ ОБЛІКІВ

Базовою ІС МВС є система автоматизованого ведення інформаційних обліків, які створюються для оперативного інформаційного забезпечення службової діяльності всіх підрозділів — від міськрайлінорганів до Міністерства внутрішніх справ. Більшість інформаційних обліків є загальновідомчими.

За *функціональною ознакою* обліки можна поділити на оперативно-довідкові, розшукові та криміналістичні. За *об'єктною ознакою* виокремлюють обліки осіб, злочинів (правопорушень) і предметів. Розрізняють також три рівні ведення інформаційних обліків.

Основою системи збирання, контролю та використання інформації є **територіальний (районний) рівень**, з якого інформація передається до вищих рівнів. На цьому рівні ведуться загальновідомчі інформаційні обліки, які використовуються в міськрайліноорганах, а також у спеціалізованих підрозділах міліції:

1) підрозділами оперативної інформації — заяви та повідомлення про скоєні злочини та пригоди; затримані та зареєстровані особи; невідкладні дії чергового при отриманні повідомлень про правопорушення та пригоди, ведення оперативних планів тощо; табельна

зброя, спеціальні засоби, засоби індивідуального захисту та активної оборони; оперативна інформація щодо осіб, які підозрюються в скоєнні злочинів, осіб певних категорій, членів злочинних угруповань; криміногенні об'єкти; вилучені та викрадені речі; спецапарат;

2) карним розшуком — особи криміногенних категорій, члени злочинних угруповань та інші, які становлять оперативний інтерес; особи, які оголошені в розшук; невпізнані трупи та невідомі хворі; викрадені та вилучені номерні речі, автотранспорт, зброя; криміногенні об'єкти; спецапарат; оперативна інформація;

3) службою боротьби з економічною злочинністю (БЕЗ) — оперативна інформація щодо осіб, які підозрюються у скоєнні злочинів, які здійснюють незаконні валютні операції, про фальшивомонетників і т. ін.; способи скоєння розкрадань, злочинів у валютній та кредитно-фінансовій сферах; об'єктів господарської діяльності, які потребують оперативного нагляду; вилучений та викрадений автотототранспорт; спецапарат;

4) слідством — особи, що притягуються до кримінальної відповідальності; кримінальні справи та їхній рух; речові докази;

5) експертно-криміналістичною службою — сліди, вилучені з місць подій та знаряддя скоєння злочинів; фотороботи підозрюваних осіб; дактилоскопія; фото- та відеотеки; вилучена фальшива валюта; кулегільзотека;

6) адміністративною службою міліції — розташування сил та засобів; індивідуальна та відомча зброя; об'єкти дозвільної системи; адміністративні правопорушення; паспортна реєстрація громадян; особи, які відбули покарання в місцях позбавлення волі;

7) службою ДАІ — зареєстрований автотототранспорт; викрадений і вилучений автотототранспорт; власники посвідчень водія; дорожньо-транспортні пригоди; адміністративні правопорушення тощо;

8) службою охорони — стан і характеристики об'єктів, що охороняються;

9) службою виконання покарань — спецконтингент; спецапарат; оперативна інформація; порушення режиму утримання; результати перевірок явок з повинною;

10) службою пожежної охорони — пожежі; протипожежний стан об'єктів.

Порядок формування інформаційних обліків галузевими службами, відповідальність за їх актуальність, вірогідність та використання регламентується відповідними наказами.

На **регіональному (обласному) рівні** ведуться інформаційні обліки, які є складовими загальновідомчих інформаційних підсистем і

використовуються службами ГУМВС, УМВС, УМВСТ. Тут інтегрується інформація, яка надходить з міськрайлінорганів та установ виконання покарань, має регіональний характер і стосується:

- надзвичайних подій;
- злочинних та адміністративних правопорушень;
- підприємств, організацій та установ, що становлять оперативний інтерес;
- зареєстрованого автотранспорту;
- зареєстрованої вогнепальної та газової зброї;
- викрадених, загублених і вилучених предметів злочинного посягання, зокрема номерних та безномерних речей, антикваріату, автотранспорту, вогнепальної та газової зброї, документів, криміналістичних обліків (кулегільзотеки, слідотеки, відбитки пальців рук тощо);
- осіб — які скоїли злочини, які скоїли адміністративні правопорушення, які зникли безвісті, які становлять оперативний інтерес, злочинців, оголошених у розшук, наркоманів, невпізнаних трупів та невідомих хворих;

а також:

- обліків адресних бюро;
- оперативно-довідкових і дактилоскопічних картотек;
- обліків адміністративно-управлінського призначення (нормативно-законодавчі акти, розпорядчі документи, накази);
- обліків спеціалізованого призначення галузевих служб (кадрові, господарчі, бухгалтерські тощо);
- обліків архівів та спецфондів.

На регіональному рівні інформація контролюється на повноту, вірогідність, актуальність та захищеність і обробляється. Також забезпечується зв'язок з центральним рівнем і з територіальними правоохоронними органами та іншими установами держави.

Центральний (державний) рівень інтегрує ІС ОВС загальновідомчого значення та галузевих служб МВС України. Тут забезпечується контроль, нагромадження та оброблення інформації, що використовується під час аналізу, планування, прийняття рішень та проведення у межах України оперативно-розшукових, слідчих та інших спеціальних заходів з боротьби зі злочинністю, міжвідомчий та міжрегіональний інформаційний зв'язок, міждержавний обмін інформацією. До складу інформаційних обліків цього рівня належать:

- 1) банки кримінологічної інформації, що містять відомості про:
 - надзвичайні події;
 - нерозкриті тяжкі та резонансні злочини;

- викрадені, загублені та вилучені предмети, знаряддя скоєння злочинів, речові докази, зокрема номерні речі, антикваріат, автотранспорт, вогнепальну зброю, документи, криміналістичні обліки;
 - викрадені та вилучені наркотичні речовини;
 - об'єкти виготовлення, перероблення, зберігання та використання наркотичних речовин;
 - осіб таких категорій: особливо небезпечних рецидивістів; злочинців-гастролерів; злочинців, оголошених у міждержавний розшук; організаторів і членів злочинних угруповань, кілерів; які були засуджені за злочини, пов'язані з наркотиками, торговців та розповсюджувачів наркотичних речовин з міжрегіональними та міжнародними зв'язками; схильних до вчинення злочинів, пов'язаних з посяганнями на інтереси держави; які пропали безвісті; невідомих хворих;
- 2) банк оперативно-довідкової інформації, що містить дані алфавітного та дактилоскопічного обліків раніше засуджених осіб;
 - 3) банк статистичної інформації, що містить дані про стан злочинності та результати боротьби з нею;
 - 4) банк спеціальної інформації, що містить повідомлення спецапарату та іншу оперативну інформацію загальноповідомчого значення;
 - 5) банк паспортної реєстрації громадян;
 - 6) банк з інформацією про зареєстрований автотранспорт;
 - 7) банк з інформацією про зареєстровану вогнепальну зброю;
 - 8) банки даних адміністративно-управлінського призначення;
 - 9) банки даних спеціалізованого призначення галузевих служб;
 - 10) банки даних архівів та спеціальних фондів.

Повнота даних на кожному рівні за категоріями обліку визначається відповідними нормативними документами.



Перевірка кримінальної статистики — досвід поліції Нью-Йорка

Поліцейський департамент м. Нью-Йорк використовує для запису інформації щодо злочинів он-лайн систему скарг (On-Line Complaint System, OLCS). Для складання тижневих звітів відділків про злочини, скоєні на підвідомчих територіях, застосовується комп'ютеризована статистична система COMPSTAT (Computerized Statistics System). Звіти містять дані щодо головних категорій кримінальних злочинів — навмисних і ненавмисних вбивств, зґвалтувань, грабунків, злочинних нападів, крадіжок зі зломом, значних злодійств, викрадень транспортних засобів. Ці звіти відіграють важливу роль при аналізі криміналь-

них тенденцій, моніторингу проблем і дій відділків та оперативних підрозділів, плануванні використання поліцейських ресурсів. Дані про роботу всіх агентств включаються до щорічного Управлінського звіту мера, який видається згідно з Хартією міста.

У 1997 році був започаткований аудит звітних даних, який виконує Офіс Ревізора штату Нью-Йорк (Підрозділ управлінського аудиту та державних фінансових послуг, *Division of Management Audit and State Financial Services*). Мета аудиту — перевірка узгодженості даних і тенденцій, представлених у звіті мера, з даними системи COMPSTAT і перевірка цих даних на предмет правильності, повноти і надійності. Крім порівняння даних, випадкова статистична вибірка даних із системи звірюється з документами відділків (по випадково вибраних відділках у випадковій послідовності за випадково вибрани тижні). У 1999 році розбіжність між даними документів і системи OLCS з одного боку та даними COMPSTAT з іншого склали 18 злочинів і були визнані несуттєвими (1,6 % порівняно з верхньою межею у 4,9 % при 95-відсотковому рівні впевненості). Перевірка стосується також процедур контролю даних у системі COMPSTAT, а в разі визнання їх недостатніми, оцінюється, наскільки вони впливають на достовірність даних.

9.3. ОПЕРАТИВНО-РОЗШУКОВІ ОБЛІКИ

9.3.1. ІС «Інтегрований банк даних»

ІС «Інтегрований банк даних» (ІБД) призначена для оперативного забезпечення працівників і підрозділів ОВС інформацією для розшукової діяльності, розслідування і попередження злочинів, надання аналітичної, статистичної та контрольної інформації для розробки і прийняття обґрунтованих оптимальних рішень на всіх рівнях управління.

Система містить інформацію про осіб криміногенних категорій (особливо небезпечні рецидивісти, «гастролери», оголошені у міждержавний розшук, бродяги); нерозкриті тяжкі злочини, викрадену, вилучену, знайдену зброю; номерні речі; транспортні засоби, викрадені в Україні та країнах СНД. Передбачається поєднання обліків зареєстрованого та викраденого транспорту, що дасть змогу виявляти викрадений транспорт на етапі реєстрації, підвищити достовірність масивів і надавати на запити ОВС більш повну інформацію.

В ІБД ведуться інформаційні обліки «Особа», «Річ», «Зброя», «Угон», «Злочин», «Антикваріат», при цьому можна включати додаткові інформаційні обліки, не порушуючи існуючі об'єкти.

ІБД забезпечує пошук:

- осіб за фрагментами установчих даних, описами, дактило-формулами;
- злочинів за документами, описами;
- територіальних об'єктів за фрагментами установчих даних;
- антикваріату за фрагментами установчих даних, описами;
- автотранспорту за фрагментами установчих даних (номера агрегатів або державними номерними знаками);
- номерних речей за фрагментами установчих даних (безпосередньо речі або її номерної деталі);
- зброї за фрагментами установчих даних (безпосередньо зброї або її номерної деталі).

Для отримання інформації за вмістом ІБД призначена підсистема оброблення запитів абонентів у режимі безпосереднього доступу до ІБД через телефонні канали зв'язку. Оперативно-розшукову інформацію можна одержати також в черговій частині УОІ МВС України.

9.3.2. ІС «Розшук»

ІС «Розшук» призначена для централізованого збирання інформації від ініціаторів розшуку про осіб, що розшукуються і встановлюються, які оголошені в регіональний, державний, міждержавний розшук, її оброблення та надання за запитами працівників ОВС, інших зацікавлених міністерств і відомств. Функціонування ІС (рис. 9.1) регламентовано Законом України від 18.02.1992 р. **«Про оперативно-розшукову діяльність»** і відповідними наказами та розпорядженнями МВС України.

Інформація збирається ініціаторами розшуку на регіональному рівні в управліннях (відділеннях) оперативної інформації (УОІ/ВОІ) ГУ-УМВС, обробляється і передається каналами електронної пошти до УОІ МВС України для об'єднання з інформацією, яка надійшла з інших регіонів. Концентрація інформації про розшукові справи в УОІ МВСУ дає можливість вчасно надсилати відомості про осіб, оголошених у міждержавний розшук на території України, до Головного інформаційно-обчислювального центру МВС Російської Федерації і стежити за передорученням розшуку. Інформація про осіб, що розшукуються в країнах СНД, надходить в електронному вигляді і інтегрується до банку даних. Після узагальнення вся інформація розсилається електронною поштою в УОІ/ВОІ ГУ-УМВС України. Отже, кожна інформаційна служба областей України має загальний масив інформації про осіб, оголошених у регіональний, державний і міждержавний розшук.

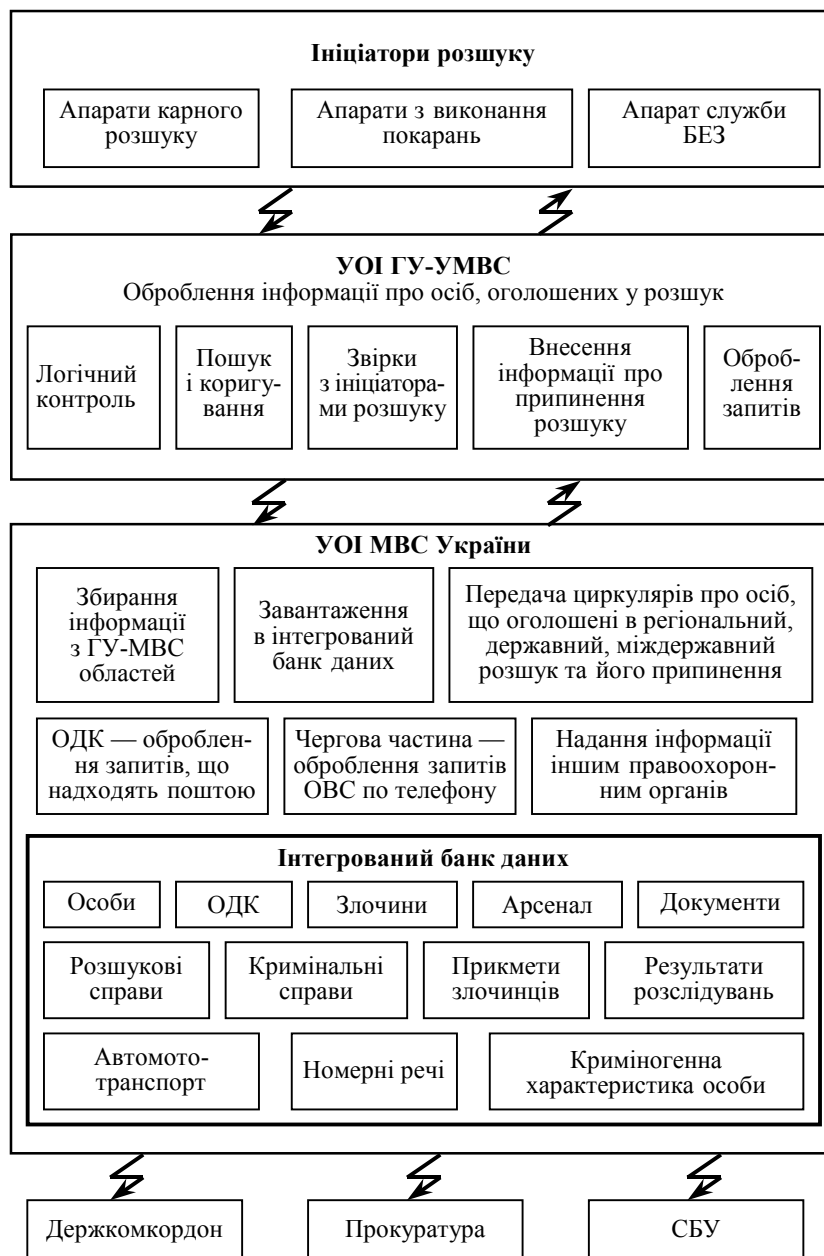


Рис. 9.1. Функціонування ІС «Розшук»

9.3.3. ІС «Пізнання»

ІС «Пізнання» призначена для обліку осіб, зниклих безвісті, невпізнаних трупів, невідомих хворих; проведення пізнавальних заходів щодо цих категорій осіб в автоматизованому режимі; надання рекомендацій на проведення пізнавальних заходів.

Документом для формування бази даних та оброблення запитів є пізнавальна карта, яка надсилається з УОІ ГУ-УМВС в областях до МВСУ. Запити на перевірку надсилаються поштою, телеграфом або електронною поштою.

Для системи характерні нагромадження і зберігання великих обсягів інформації; розширені можливості доступу до даних; підтримка значної кількості типів даних, у тому числі широкого спектра промислових стандартів графічних об'єктів; забезпечення багатокористувацького режиму роботи.

Основні складові системи:

1) підсистема авторизації користувачів, що забезпечує захист від несанкціонованого доступу;

2) підсистема вводу, що дає змогу нагромаджувати інформацію і здійснювати її логічний контроль;

3) підсистема пізнання;

4) підсистема резервного копіювання/відновлення, яка забезпечує можливість відновлення системи в разі виникнення збоїв.

До банку даних вводяться такі характеристики осіб, які варіюються для різних категорій останніх і об'єднані у *логічні групи*:

- установчі дані — ОВС, що надав інформацію, дактилоформула, формула обліку, стать, дата зникнення (виявлення), дата народження (смерті), вік, зріст (довжина трупа), національність (расовий тип), розмір голови, розмір ноги, група крові, місце зникнення (виявлення), прізвище, ім'я, по батькові, фотографія, дата фотографування;

- характерні прикмети — місцезнаходження прикмети (двозначний числовий код області тіла людини), опис прикмети відповідно до словника прикмет, текстова фабула, що доповнює й уточнює прикмету;

- стан зубів — зубна формула (опис стану кожного зуба відповідно до словника);

- особливості зовнішності — словесний портрет зовнішності особи за словником зовнішності;

- одяг — вид, колір, матеріал одягу за відповідними словниками, а також текстова фабула, що уточнює і доповнює інформацію про одяг;

- хвороби;
- додаткові відомості. Для безвісті зниклих — місце народження, місце мешкання, професія, обставини зникнення, дані про судимість, можливе місце мешкання. Для невпізнаних трупів — стан трупа, причина смерті, дата розтину трупа, час поховання (дата), місце поховання (номер могили);
- додаткові дані — дата подачі заяви; дата заведення пошукової справи; номер справи; дата надання оперативної інформації; ОВС, що надав інформацію; дата постановки на облік в області; дата перевірки за обліками області; дата постановки на облік у МВС; дата перевірки за обліками у МВС; дата направлення інформації до Москви; особа, яка здійснювала перевірку правильності заповнення документа; дата постановки на облік у БД; користувач, який здійснив введення інформації.

Для перевірки правильності заповнення пізнавальної карти, коригування даних, зняття осіб з обліку та підрахунку статистики підсистема вводу забезпечує пошук за номером і датою заведення справи, ОВС, що надав інформацію, датою зникнення (виявлення), датою постановки на облік, статтю, прізвищем, ім'ям, по батькові (для безвісті зниклих). У разі зняття осіб з обліку фізичне видалення інформації з бази не відбувається, що дає змогу поновити інформацію в разі помилкового зняття з обліку, переглянути інформацію і сформувати повні статистичні дані.

Процес пізнання заснований на порівнянні прикмет та інших характеристик облікових об'єктів. Для підвищення ефективності і достовірності прикмети і характеристики розділено на дві групи залежно від ідентифікаційної цінності.

Першу групу складають прикмети, які дають можливість з високою ймовірністю відсіяти об'єкти з великими розбіжностями — категорія обліку, стать, дата зникнення (виявлення), вік, зріст (довжина трупа), істотні характерні прикмети (наприклад, ампутації).

До другої групи входять прикмети, що дають змогу в сукупності з іншими прикметами цієї групи визначати основних кандидатів для остаточної ідентифікації: стан зубів, характерні прикмети, особливості зовнішності, одяг.

Процес ідентифікації організовано в три етапи:

- 1) вибірка об'єктів на основі прикмет з першої групи;
- 2) робота з одержаною вибіркою — для кожного об'єкта обчислюється сумарний коефіцієнт відповідності його параметрів (прикмет і характеристик) параметрам об'єкта, що ідентифікується;

3) упорядкування вибірки за зменшенням сумарного коефіцієнта відповідності або будь-якої його складової (наприклад, за складовою, утвореною завдяки аналізу одягу), візуальний аналіз експерта, ухвалення рішення в кожному конкретному випадку, яке фіксується в БД. Експерт також може надати рекомендацію на проведення пізнавальних дій. Після підтвердження з ОВС про проведені дії, в разі впізнання, цей факт записується у БД, особа автоматично знімається з обліку і у подальших процедурах пізнання системою до уваги не береться.

9.3.4. ІС «Арсенал»

Єдина система централізованого номерного обліку вогнепальної зброї у системі МВС України «Арсенал» створена з метою здійснення всебічного контролю за зброєю згідно з дорученням Кабінету Міністрів України.

ІС «Арсенал» створено на базі наявного в УОІ (ВОІ) ГУМВС, УМВС масиву «Мисливець», який регламентується наказом МВС України № 170-93. У ній містяться дані про вогнепальну, пневматичну, калібру понад 4,5 мм та швидкістю польоту кулі понад 100 м/с зброю; холодну зброю; спеціальні засоби самооборони, заряджені речовинами сльозоточивою та подразнюючою дії (газові пістолети та револьвери, що перебувають у користуванні громадян і організацій); дані про зброю органів внутрішніх справ, військових частин, навчальних закладів системи МВС та про зброю, що зберігається на складах військових баз МВС. Реквізитами, що зберігаються, є вид зброї, серія, марка, модель, номер, калібр, рік випуску, призначення, право власності, дата видачі дозволу, область, орган, який видав дозвіл, прізвище, ім'я та по батькові власника, дата народження, відомості про зняття з обліку, дата введення/коригування даних.

Структурно ІС «Арсенал» поділяється на підсистеми обласного і державного рівня. Обмін інформацією між ними здійснюється каналами електронної пошти.

Система забезпечує пакетне введення інформації у формати вхідних документів; інтерактивне введення інформації; коригування бази даних; пошук документів за номерами, серіями; пошук документів за фрагментами установчих даних. За допомогою інформації з ІС «Арсенал» встановлюється належність зброї за її номерами, контролюється переміщення зброї від одного власника до іншого.

9.3.5. ІПС за прізвищами та дактилоскопічним обліком криміногенних осіб

«ІПС за прізвищами та дактилоскопічним обліком криміногенних осіб» містить обліки оперативно-довідкової картотеки (ОДК) та дактилоскопічні обліки Управління оперативної інформації та державного науково-дослідного експертно-криміналістичного центру МВС України і забезпечує:

- зберігання, нагромадження, ведення, автоматизований облік та видачу у встановленому порядку ОВС, СБУ, прокуратурі, судам та іншим правоохоронним органам оперативно-довідкової інформації на осіб (у тому числі іноземців та осіб без громадянства), які скоїли злочини на території України, були заарештовані, засуджені, затримані за бродяжництво, зникли від слідства та суду;

- ідентифікацію осіб, які приховують свої біографічні дані від правоохоронних органів;

- пошук злочинців за слідами, виявленими на місці злочину.

Порядок ведення оперативно-довідкових і дактилоскопічних обліків регламентований наказом МВСУ від 2.03.95 р. № 138 «Про порядок ведення персонального оперативно-довідкового і дактилоскопічного обліків в органах внутрішніх справ України».

Інтегрована ІС базується на масиві даних комп'ютерних систем УОІ МВСУ та даних, нагромаджених у вигляді облікових карток за прізвищами, дактилокарт і слідів, вилучених з місць скоєння злочинів експертно-криміналістичними підрозділами ОВС.

Дактилоскопічна за прізвищами та оперативно-довідкові картотеки нагромаджують такі дані:

- основні установчі дані — прізвище, ім'я, по батькові (в тому числі і російською мовою), дата і місце народження, дактилоформула;

- додаткові установчі дані — місце проживання, професія, місце роботи, посада, національність, громадянство;

- відомості про арешт, судимість;

- відомості про притягнення до кримінальної відповідальності;

- відомості про місце та час відбування покарання, переміщення, дату і підставу звільнення;

- номери слідчих та архівних справ;

- відомості про перебування у розшуку (коли, ким оголошений, у зв'язку з чим), відомості про РС та КС, призупинення (дата), запобіжні заходи;

- відомості про затримання;

- дактилоскопічну інформацію.

Обсяг оперативно-довідкової картотеки за прізвищами складає близько 5 млн карток. Щорічно до картотеки надходить близько 250 тис. нових карток, 260 тис. коригувань, приблизно 250 тис. карток, які втратили актуальність, знімається з обліку. Обсяг дактилоскопічної картотеки складає близько 2,6 млн дактилокарт, а обсяги вилучених з місць скоєння злочинів слідів, які нагромаджуються в експертно-криміналістичних підрозділах ОВС України — орієнтовно 500 тис.

9.3.6. ІС «ОАЗИС»

ІС «ОАЗИС» призначена для збирання, оброблення та аналізу даних про фінансову діяльність підприємств, що ведуть протизаконну діяльність, в інтересах оперативних і слідчих служб ОВС.

Система дає змогу:

- створити банк даних підприємств, що ведуть протизаконну діяльність, із забезпеченням доступу до цієї інформації представників слідчих та оперативних органів;
- сформувати список фіктивних підприємств, яким було перераховано гроші за продукцію з урахуванням ціни, що падає або зростає;
- встановити закономірність переказу грошових коштів на кореспондентські рахунки іноземних банків;
- простежити на етапі збирання матеріалів оперативної перевірки рух грошових коштів на рахунки конкретних підприємств;
- згрупувати підприємства по областях та банках, що їх обслуговують;
- створити АРМ оперативно-слідчого працівника шляхом підключення до банків даних ДПА.

ІС «ОАЗИС» складається з кількох частин (робоче місце користувача, робоче місце адміністратора тощо), які здатні взаємодіяти між собою за допомогою комп'ютерної мережі.

9.4. ІС ДЕРЖАВНОЇ АВТОМОБІЛЬНОЇ ІНСПЕКЦІЇ

Основними функціями ІС ДАІ МВС України є інформаційне забезпечення діяльності ДАІ та інформаційна взаємодія її служб з іншими службами забезпечення правопорядку та безпеки громадян. Основні *напрямки застосування інформаційних технологій* такі:

- реєстраційна, екзаменаційна і дозвільна діяльність;
- управління дорожнім рухом;

- телевізійний нагляд за дорожнім рухом (попередження, виявлення, фіксація, припинення і профілактика порушень правил дорожнього руху (ПДР));
- залучення учасників дорожнього руху, які порушили ПДР, до адміністративної відповідальності;
- облік та аналіз відомостей про виявлені порушення ПДР;
- контроль за заходами із забезпечення безпеки руху з метою зменшення кількості і ваги наслідків дорожньо-транспортних пригод;
- контроль своєчасності проходження державного технічного огляду;
- оперативне керування підрозділами ДАІ;
- розкриття злочинів, пов'язаних з використанням автотранспортних засобів;
- доведення до співробітників ДАІ сигнальної інформації щодо фактів одержання дублікатів посвідчень водія і реєстраційних документів, спроби постановки на облік викраденого транспортного засобу та ін.;
- правозастовна діяльність підрозділів ДАІ;
- облікова, статистична та аналітична діяльність співробітників ДАІ;
- видача довідкової інформації;
- підготовки звітної документації.

Згідно з наведеним переліком виокремлюють такі *типові підсистеми ІС ДАІ*:

1) «Учасник дорожнього руху» забезпечує інформаційну підтримку екзаменаційної і дозвільної діяльності ДАІ шляхом автоматизації задач прийому кваліфікаційних іспитів; підготовки, виготовлення, видачі і наступного оперативного контролю документів на право керування транспортним засобом; введення, оброблення, збереження та видачі інформації про складання іспитів і видані документи;

2) «Автомобіль» — забезпечує реєстраційну і дозвільну діяльність, а також контроль за своєчасним проходженням технічного огляду;

3) «Дорога» — призначена для керування дорожнім рухом — управління транспортними потоками та експлуатацією комплексу телеавтоматичної системи керування рухом транспорту, а також інформаційного забезпечення учасників дорожнього руху;

4) «Адміністративна практика» — реалізує функції, пов'язані із залученням учасників дорожнього руху, які порушили ПДР, до адміністративної відповідальності;

5) «Чергова частина» — автоматизує оперативне керування підрозділами і диспетчеризацію транспортних засобів;

6) «Розшук» — призначена для інформаційного забезпечення служб, що займаються розкриттям злочинів, пов'язаних з використанням автотransпортних засобів, і містить комплекс задач з реєстрації та обліку пошукової роботи підрозділів ДАІ;

7) «Розрахунки» — вирішує задачі контролю за своєчасністю оплати виставлених рахунків;

8) «Стратегічне керування» — призначена для:

- аналізу статистики, класифікації і кластеризації дорожньо-транспортних пригод, порушень ПДР, інтенсивності трафіка дорожнього руху;

- ведення динамічних картографічних об'єктів інтегрованої БД, що описують аварійність, криміналізацію і щільність дорожнього трафіка;

- автоматизованої розробки методичних рекомендацій і профілактичних заходів на основі результатів аналізу (реорганізація дорожнього руху, складання маршрутів патрулювання і місць постів пікетів, управління інвестиціями в дорожню інфраструктуру та ін.);

- моделювання організації дорожнього руху, в тому числі в екстремальних ситуаціях;

- складання багатовимірних аналітичних і статистичних зведень і звітів.

9.5. ЄДИНА ДЕРЖАВНА АВТОМАТИЗОВАНА ПАСПОРТНА СИСТЕМА УКРАЇНИ

9.5.1. Мета створення і структура ЄДАПС

Основною характерною рисою роботи паспортної служби України є великий обсяг інформації, що нагромаджується та обробляється. Для паспортно-візових підрозділів районних і міських УВС він складає від десятків тисяч до кількох мільйонів документів, а для обласних адресних бюро і централізованих картотек МВС — мільйони і десятки мільйонів документів. Зрозуміло, що за таких обсягів інформації швидке й ефективне оброблення даних, у тому числі оперативних запитів, практично неможливе.

Сьогодні багато країн світу (за неофіційними даними, близько 50) перейшли до використання автоматизованих паспортних сис-

тем, що забезпечують облік громадян, які проживають у цих країнах. В основу цих систем покладено банк даних про населення, який заповнюється при одержанні або заміні паспорта, при зміні громадянства або місця проживання, та автоматизоване оформлення машинозчитуваних паспортних документів — традиційних паспортів-книжок і паспортних карток та віз (проїзних документів) у вигляді пластикових карток.

У 1995 році Інститутом кібернетики ім. В. М. Глушкова НАН України разом з МВС України, Інститутом проблем реєстрації інформації НАН України і Міжнародним центром інформаційних технологій «INT» було розпочато розробку проекту ***Єдиної державної автоматизованої паспортної системи (ЄДАПС) України***. Концепція створення ЄДАПС була затверджена Постановою Кабінету Міністрів від 20.01.1997 р. № 40.

ЄДАПС є базовою системою обліку громадян, які проживають в Україні, і найважливішою складовою Державного реєстру фізичних осіб. Її створення визначено як один із напрямів інформатизації діяльності органів державної влади та органів місцевого самоврядування у рамках завдань Національної програми інформатизації.

Головною метою створення ЄДАПС України є підвищення ефективності роботи паспортних підрозділів органів внутрішніх справ, удосконалення інформаційного забезпечення діяльності правоохоронних та інших органів, у функції яких входить облік населення України, підтримка прийняття рішень у сфері демографічної і соціальної політики держави. Впровадження ЄДАПС означає приведення паспортної системи у відповідність з вимогами Конституції України та світовою практикою і сприятиме підвищенню рівня безпеки громадян і держави в цілому.

За логічною структурою ЄДАПС являє собою трирівневу інформаційно-аналітичну систему.

Місцевий рівень ЄДАПС — це автоматизовані системи паспортних відділень районних УВС, які повинні забезпечувати вирішення таких задач:

- введення даних з первинних документів (заяв про отримання паспорта, прописку, виписку), контроль і передача їх на вищі рівні системи;
- введення в базу даних оцифрованих за допомогою сканера фотографій або фотографування за допомогою цифрової відеокамери;
- введення в базу даних за допомогою сканера оцифрованих особистих підписів;

- ведення бази даних про отримання і заміну паспортів громадянина України і паспортів для виїзду за кордон, прибуття і вибуття громадян, зміни їх сімейного стану і т. ін.;

- автоматизація документообігу (формування і друк адресних листків прибуття і вибуття, статталонів до них, звітів про роботу та ін.) і забезпечення безпаперової технології оброблення даних;

- взаємодія з іншими системами обліку громадян (реєстр платників податків, реєстр населення, системи військового обліку, охорони здоров'я тощо);

- інформаційне обслуговування запитів користувачів системи.

Регіональний рівень ЄДАПС — це автоматизовані системи адресних бюро обласних УВС, які складаються з робочих станцій працівників довідкової служби адресного бюро і регіонального центру автоматизованої підготовки паспортів. На цьому рівні забезпечується:

- інформаційне обслуговування запитів користувачів системи;

- введення в базу даних оцифрованих фотозображень за допомогою сканера з фотографії або фотографування за допомогою цифрової відеокамери;

- введення в базу даних за допомогою сканера оцифрованих особистих підписів;

- автоматизоване внесення паспортних даних (текст, фотографія, особистий підпис) в паспорт або паспорт-картку методом комп'ютерного друку з подальшим ламінуванням;

- контрольне зчитування надрукованого паспорта-картки або сторінки паспорта для виїзду за кордон;

- облік використаних бланків паспортів;

- взаємодія з іншими системами обліку громадян обласного рівня.

Державний рівень ЄДАПС — це автоматизована система рівня МВС, яка підтримує центральну базу даних про громадян, що проживають в Україні, а також бази даних спеціального призначення (оперативно-довідкові, пошукові та інші картотеки). На цьому рівні виконуються:

- отримання даних про прибуття і вибуття громадян за формами адресних листків з АС паспортних відділень, їх автоматизована перевірка по спеціалізованих базах даних МВС і запис в центральну базу даних;

- отримання заяв про видачу паспортів громадян України і паспортів для виїзду за кордон з місцевого рівня, їх автоматизована перевірка по спеціалізованих базах даних МВС, передача даних в АС адресних бюро для автоматизованого оформлення паспортів;

- отримання даних з нижніх рівнів про оформлені та видані громадянам паспорти і внесення їх в центральну базу даних (реєстрація видачі паспортів);
- інформаційне обслуговування запитів користувачів системи;
- ведення оперативно-довідкових і пошукових картотек у взаємодії зі спеціалізованими базами даних МВС України;
- інформаційно-аналітична підтримка прийняття рішень стосовно широкого кола соціальних питань, пов'язаних зі структурою, міграцією та динамікою розвитку населення.

Через мережу віддалених терміналів користувачами системи на державному рівні, крім органів МВС, можуть бути також служби інших відомств (СБУ, МЗС, суду і прокуратур, Мінстата, Мінфіну та ін.) за згодою МВС.

Отже, місцевий рівень є основним для введення і первинного оброблення інформації. Особисті дані громадян заносяться до бази даних цього рівня і через регіональний рівень передаються в базу даних центрального рівня для оброблення та виготовлення паспортів (у майбутньому — і свідоцтв про народження). Після одержання підтвердження дані автоматично фіксуються в базах даних усіх рівнів і стають доступними для використання в інших системах. Регіональний рівень забезпечує підтримку бази даних з обліковою інформацією про громадян, які проживають у відповідному регіоні. Завданням центрального рівня є ведення інтегрованої бази даних та управління всіма вузлами системи. У разі надходження запитів від суб'єктів нижчих рівнів стосовно окремої особи на центральному рівні проводиться верифікація отриманої інформації. За позитивних результатів перевірки відбувається запис (або модифікація) в базу даних центрального рівня, повідомлення про це автоматично передається на відповідні регіональний та місцевий рівні.

Реалізацію основних завдань центрального рівня покладено на головний центр паспортизації — ВАТ «Київське підприємство обчислювальної техніки і інформатики» (ВАТ «КП ОТІ»), яке на перших етапах створення ЄДАПС виконує функції головного обчислювального центру, а з розширенням системи буде реорганізоване у самостійний орган управління.

Функціонально ЄДАПС складається з окремих підсистем, які поступово впроваджуються на різних рівнях і мають взаємодіяти між собою. *Основні підсистеми ЄДАПС* забезпечуватимуть:

- підсистема ідентифікації особи — підготовку, введення, оброблення і зберігання, оперативний пошук і перевірку ідентифікаційної інформації;

- підсистема обліку громадян — підготовку, введення, оброблення і зберігання облікової інформації; контроль за додержанням громадянами правил паспортної системи;
- підсистема документування громадян — підготовку і формування інформації, необхідної для виготовлення/заповнення паспортів/документів, що посвідчують особу; автоматизований контроль проходження документів по всьому технологічному ланцюгу від замовлення до виготовлення і доставки документів замовникові;
- підсистема запитів та аналізу даних — оперативний пошук і отримання облікової інформації про громадян у рамках повноважень користувачів; формування аналітичних і статистичних зведень для прийняття управлінських рішень і сприяння проведенню різноманітних державних і регіональних заходів;
- підсистема взаємодії із зовнішніми системами — обмін інформацією і взаємодію з іншими загальнодержавними системами та авторизованими зовнішніми користувачами;
- підсистема контролю доступу і захисту інформації — контроль функціонування програмно-апаратних засобів та управління роботою системи в цілому; контроль доступу і захист від несанкціонованого доступу; надійність, безпеку і цілісність інформації, що зберігатиметься в системі.

Центральною частиною ЄДАПС є потужний обчислювальний комплекс головного центру паспортизації, який каналами зв'язку з'єднується з підпорядкованими центрами регіонального рівня. Взаємодія на місцевому і на регіональному рівнях забезпечується за клієнт-серверною технологією з використанням потужних серверів та спеціалізованих АРМ.

Особливістю ЄДАПС є використання спеціалізованого технічного забезпечення. Насамперед це пристрої, які забезпечують введення графічних даних (фотокарток і особистих підписів), а також друк даних і їх контрольне зчитування.

9.5.2. Інформаційне забезпечення ЄДАПС

Основними складовими інформаційного забезпечення ЄДАПС є уніфіковані первинні документи, передбачені законодавчими актами; система класифікації і кодування; проблемно орієнтована база даних; нормативно-довідкова інформація; технічна, нормативно-методична документація та інструкції.

Згідно з Постановою Кабінету Міністрів від 28.09.1996 р. № 1182 «Питання паспортизації громадян» у рамках впровадження ЄДАПС передбачається виготовлення паспорта громадя-

нина України у вигляді картки розміром 54,0 × 85,6 або 74,0 × 105,0 мм. Паспорт-картка повинен мати такі самі елементи даних, як і паспорт громадянина України: Державний герб України, оцифровану фотографію власника і його персональні дані (прізвище, ім'я, по батькові, стать, місце і дата народження, ідентифікаційний номер, дата видачі і код органу, що його видав), особистий підпис, найменування установи, що видала картку, і підпис посадової особи. Також на паспорт-картку (на чіп) заносяться машинозчитувані дані (місце мешкання, відношення до військової служби, група крові, сімейний стан, дані про дітей та ін.). У зоні розміщення ідентифікатора особи можуть бути розміщені інші дані біометричної ідентифікації або елементи захисту за умов, що вони не будуть затемнювати ідентифікатор особи.

Виготовлення/заповнення паспорта-картки здійснюється за спеціальними технологіями із застосуванням багатокольорового лазерного друку на попередньо задрукованому синтетичному матеріалі та термоламінації.



ЄДАПС — паспорт громадянина України

Паспортна система — комплекс заходів з обліку населення за місцем проживання та забезпечення видачі паспортів.

Положення про паспорт громадянина України затверджено постановою Верховної Ради України від 2.09.1993 р. № 3423. Бланки паспортів виготовляються за єдиними зразками, затвердженими постановами Кабінету Міністрів України: у формі паспортної книжечки — 4.06.1994 р. № 353 та 30.12.1997 р. № 1489-74 (нова редакція); у формі паспортної картки — 30.06.1998 р. № 986-40.

Видачу паспортів громадянина України у вигляді паспортної книжечки розпочато у травні 1995 року і на сьогодні завершено.

Термін впровадження паспортів громадянина України у вигляді картки буде визначено Кабінетом Міністрів України у міру створення ЄДАПС. Паспорти у формі картки впроваджуватимуться шляхом введення нового бланка паспорта, а не шляхом обміну паспортів.

Нині існує низка міжнародних стандартів на машинозчитувані паспорти і паспортні картки. Ще у 1968 році в рамках діяльності Міжнародної організації цивільної авіації було розглянуто пропозиції щодо запровадження машинозчитуваного паспорта або паспортної картки, які у наступному могли б замінити традиційний паспорт з метою прискорення перевірки, що здійснюється при паспортному контролі. З 1.01.1985 р. за рішенням Ради ЄС запроваджено єдиний європейський паспорт, в якому відомості наводяться так само, як і в документі Міжнародної організації цивільної авіації Дос 9303. Досвід використання таких документів свідчить, що ви-

датки на їх виготовлення не набагато більші, ніж на звичайні. Додаткові витрати на спеціальне зчитувальне обладнання компенсуються зростаючим ступенем безпеки, швидкістю та точністю перевірки і гнучкістю оброблення персональних даних. В Україні запроваджено сім машинозчитуваних документів (шість типів паспортних документів та машинозчитувана візова етикетка). Постановою Кабінету Міністрів України від 28.06.1997 р. № 636 затверджено порядок заповнення машинозчитуваної зони документів, що посвідчують особу.

У БД ЄДАПС зберігаються такі *основні реквізити*:

- 1) текстова інформація:
 - ідентифікаційний номер;
 - прізвище, ім'я та по батькові (державною мовою з обов'язковою транслітерацією за допомогою літер англійського алфавіту та за бажанням особи — мовою легалізованих національних меншин);
 - дата народження;
 - місце народження;
 - стать;
 - дата реєстрації та адреса місця постійного проживання;
 - прізвища, ім'я та по батькові, що використовувалися раніше;
 - відомості щодо перебування раніше в іноземному громадянстві;
 - відомості про видачу паспорта та його дублікатів;
 - відомості про місце роботи/навчання;
 - відомості про сімейний стан — відомості про дружину/чоловіка та дітей;
 - відомості про освіту;
 - відомості про видачу документів, що посвідчують особу, та про документи для виїзду за кордон (паспорт громадянина України для виїзду за кордон, проїзний документ дитини, дипломатичний паспорт, службовий паспорт, посвідчення особи моряка) — серія і номер, орган і дата отримання, термін дії;
 - відомості про відношення до військової служби;
 - відомості про вибуття;
 - відомості про смерть або про зникнення безвісти;
- 2) службова інформація (потреба особливої допомоги, пов'язаної з інвалідністю, тимчасові обмеження у праві виїзду за кордон);
- 3) графічна інформація — ідентифікатор особи; дані біометричної ідентифікації; зразок особистого підпису.



ЄДАПС — два ідентифікатори

Ідентифікатор особи — відтворений у паспорті (документі) відцифрований образ особи.

Ідентифікаційний номер особи — цифровий код, що складається із десяти символів і присвоюється кожній особі згідно з визначеною системою кодування, на підставі даних про дату народження та стать особи.

Крім цього у базі містяться дані про паспорти, посвідчення та інші документи, що були видані в установленому порядку: тип документа, номер документа, дата видачі власникові, термін дії, орган, що видав документ, стан документів (виготовлений, транспортування, обмежене використання, вилучений, загублений, знищений), системна службова інформація.

База даних нормативно-довідкової інформації складається з:

- класифікаторів (словників-кодіфікаторів) і довідників — одиниць адміністративно-територіального устрою; паспортних відділень України; органів РАГС; судів загальної юрисдикції; військових комісаріатів; країн світу, дипломатичних представництв та консульських установ України за кордоном; поштових відділень; пунктів пропуску через державний кордон; прізвищ, імен, по батькові (чоловічих і жіночих); статі, освіти, сімейного стану, відношення до військової служби; причин отримання і заміни паспорта; причин відмови в отриманні або заміні паспорта; причин прибуття і вибуття громадян; цілей і обмежень виїзду за кордон та ін.;
- таблиці транслітерації назв і власних імен;
- інформаційно-пошукових тезаурусів.

Цільовий банк даних створюється на центральному рівні. Передбачається також ведення резервного банку даних, територіально віддаленого від центрального вузла з міркувань безпеки.

9.6. ГЕОГРАФІЧНІ ІНФОРМАЦІЙНІ СИСТЕМИ ОВС УКРАЇНИ

Злочинність — це людське явище, отже, розподіл злочинів за територією не може бути довільним. Для того щоб відбувся злочин, злочинець і його об'єкт (жертва або річ) повинні, принаймні тимчасово, перебувати в одному місці. Місце порушення закону визначається багатьма факторами, починаючи від місця появи жертви до географічної зручності для злочинця. Отже, розуміння цих факторів може допомогти у правоохоронній діяльності. Донедавна з цією ме-

тою працівники ОВС устромляли кнопки у настінні карти. Сучасні географічні інформаційні системи дають змогу використовувати різноманітні електронні карти. Головна відмінність ГІС — зв'язок між геометрією картографічної інформації та атрибутивними даними у табличній формі. Цей зв'язок дає можливість переходити від одного подання даних до іншого або сполучати їх.

У діяльності органів внутрішніх справ ГІС використовуються для автоматизованого нагромадження, обліку й аналізу різноманітної інформації про події на території, підвідомчої ОВС, а також планування дій щодо розшуку злочинців, припинення злочинних акцій, масових безпорядків тощо.

Види карт і зображень на них залежать від *задач, що вирішуються*:

- візуалізація географічних аспектів подій. Навіть найпростіші електронні карти підвищують достовірність інформації про підвідомчу територію за рахунок прив'язки до картографічної бази даних і наочного її відображення (рис. 9.2, *а*). Це дає можливість полегшити аналіз інформації про правопорушення, оперативно прийняти рішення щодо вживання заходів з урахуванням особливостей території, оптимізувати сили і засоби, проконтролювати рух мобільних об'єктів, спрямувати патрулі тощо;

- аналіз криміногенної ситуації. З цією метою використовуються карти щільності злочинів (кількості злочинів на один квадратний кілометр з виділенням кварталів, районів тощо — рис. 9.2, *б*). Відповідні значення відображаються різними кольорами або їх відтінками. Карти щільності дають можливість розглянути проблему в цілому, без деталізації щодо окремих злочинів. Окремим випадком використання таких карт є сполучення даних з різних джерел, що дає змогу простежити взаємозв'язок між рівнем злочинності та визначеними факторами, наприклад, демографічними показниками;

- визначення «гарячих точок» — осередків з великою концентрацією злочинів для спрямування додаткових сил (поліцейських патрулів). Хоча розподіл злочинів по території можна простежити і на простій карті, множина злочинів за однією адресою на ній може бути подана однією точкою, тому їх слід виділяти спеціальним способом (рис. 9.2, *в*). Якщо дані щодо криміналу подаються як суцільні ділянки, як «гарячі» виділяють ділянки з більшою кількістю злочинів на квадратний кілометр. Їх поєднання з позначками окремих злочинів дає змогу виділити адреси, за якими скоєно численні злочини. Водночас на подібних картах не всі виділені зони є дійсно «гарячими» — у виділення можуть попадати райони, де не зареєстровано правопорушень;

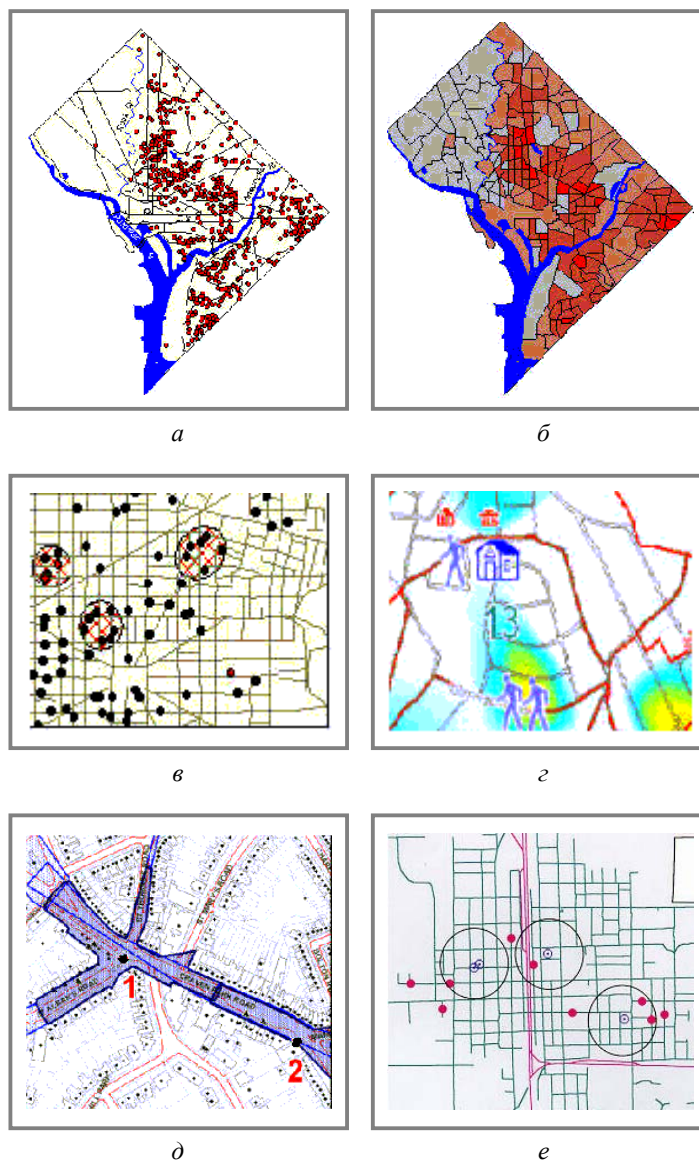


Рис. 9.2. Електронні карти для візуалізації географічних аспектів подій (а); аналізу криміногенної ситуації (б); визначення «гарячих точок» (в); надання

зведень патрулям (з); розміщення камер спостереження (д);
оцінки близькості розміщення об'єктів (е)

- надання патрулям зведень щодо недавніх тенденцій у злочинах. Такі карти містять спеціальні символи, що позначають місця скоєння злочинів протягом кількох попередніх днів, а також градієнтні лінії, що вказують тенденції злочинності за попередні тижні (рис. 9.2, з);

- розміщення камер спостереження для збільшення їх покриття і врахування обмежень на їх використання. Така карта може показувати ділянку покриття камери з виділенням зони, в якій злочинець може бути ідентифікований, а одержані зображення можуть бути використані як докази, а також дерева, дорожні знаки та інші перешкоди (рис. 9.2, д);

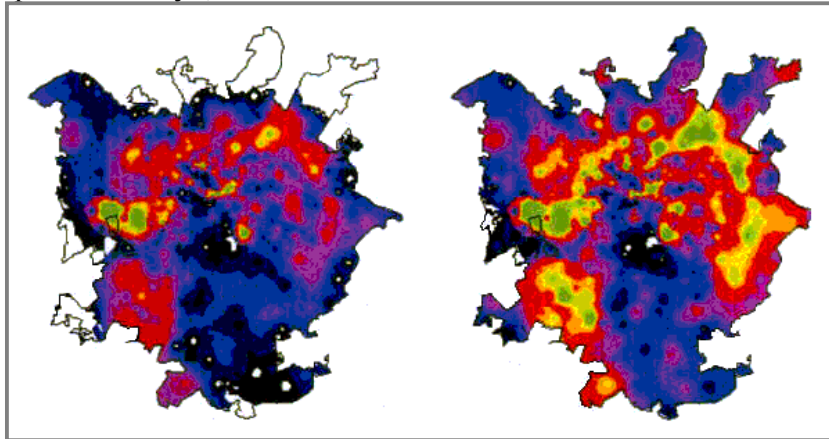
- оцінювання близькості розміщення об'єктів. Об'єкти, відстань між якими встановлюється, можуть бути різноманітними, наприклад, школи і місця продажу алкогольних і тютюнових виробів, дошкільні заклади і місця мешкання осіб, які відбули покарання за сексуальне насильство над дітьми (рис. 9.2, е);

- дослідження тенденцій скоєння злочинів відносно місць мешкання злочинців з можливим співставленням їх з демографічними факторами. Кожний район показується кольором, який відображає порівняння між кількістю мешканців, що скоїли злочини у минулому (відбули покарання), загальною кількістю таких осіб і кількістю правопорушень. Для аналізу може подаватись кілька карт одночасно;

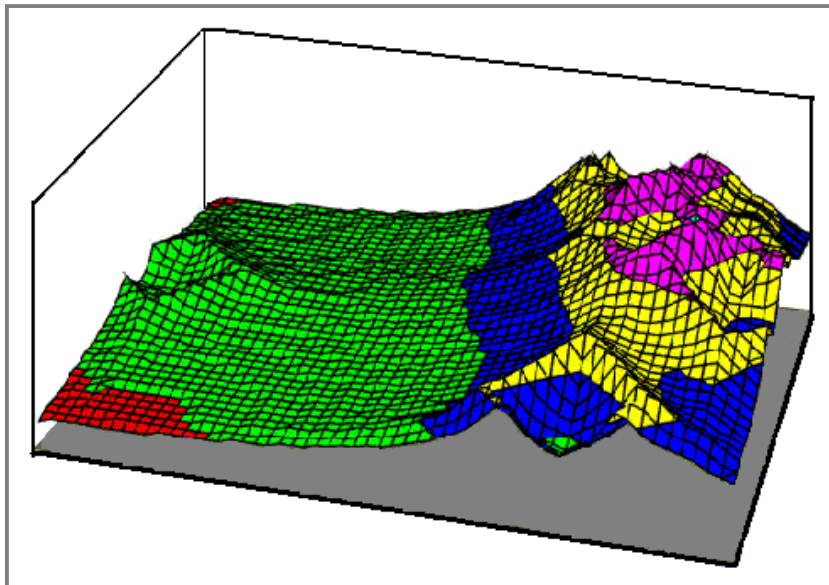
- вивчення географічних тенденцій і змін їх у часі. З цією метою здійснюється інтерполяція даних — території з однаковим рівнем злочинності показуються одним кольором. Окремі злочини не позначаються. Таким чином можна виявити місця концентрації злочинної діяльності без прив'язки до географічних місць (районів). Порівняння двох або більше карт за різні періоди дає змогу виявити як загальні тенденції (зменшення/збільшення кількості правопорушень), так і зміни їх географічного розподілу, які можна зіставити, наприклад, із приростом населення (рис. 9.3, а);

- аналіз викрадень автомобілів. За думкою багатьох аналітиків, місце, де було знайдено автомототранспорт, може бути більш красномовним під час розслідування злочину, ніж місце самого угону. За відсутності альтернативного засобу пересування злодій найбільш ймовірно залишить автомобіль поблизу певного місця призначення, наприклад, майстерні, де автомобілі розбирають на частини. Таким чином, карта щільності

розшуканих автомобілів на квадратний кілометр дає змогу зосередити пошук;



a



б

Рис. 9.3. Електронні карти:
а — для вивчення географічних тенденцій злочинності;
б — для вивчення поведінки серійних злочинців

- визначення шаблонів поведінки серійних злочинців. Карті, що використовуються з цією метою, мають допомогти зробити висновок щодо місця мешкання злочинців на основі місця скоєння ними злочинів за припущення, що між цими місцями є взаємозв'язок. Злочинці, як і інші люди, мають повсякденне життя — їздять на роботу, роблять покупки і т. ін. — у межах деякого звичного осередку, найчастіше навколо своєї оселі. Така зона лежить в основі ділянки їх злочинної діяльності. ГІС визначають цю ділянку і з урахуванням того, що злочини практично не здійснюються у безпосередній близькості від місця мешкання, оцінюють ймовірність проживання злочинця в кожній точці (вертикальна вісь на тривимірній карті, рис. 9.3, б). Зіставлення одержаних даних з картою районів (вулиць і будинків) і врахування географічних чинників дає змогу звузити сферу пошуку.

Крім підготовки статистичних і аналітичних звітів для ОВС, ГІС можуть використовуватись для підготовки даних для іншої аудиторії — політичних діячів, преси, широкої громадськості. Прикладом є сайт ARJIS (The Automated Regional Justice Information System, Автоматизована регіональна правова ІС, <http://www.arjis.org>), де доступна інформація про правопорушення в окрузі Сан Дієго. Інформація, що відображається на карті, залежить від вибраних користувачем налаштувань (рис. 9.4).



Приклад ГІС — система «Граніт»

Інтегрована система колективної безпеки громадян міста «Граніт» призначена для передачі сигналів екстреного виклику з будь-якого стаціонарного або мобільного об'єкта з автоматичним визначенням місця розташування останнього, прийняття рішень із службового реагування на ситуацію та надсилання вказівок оперативним підрозділам.

Основним об'єктом спостереження і контролю системи є зареєстровані та незареєстровані абоненти. Незареєстрованими абонентами є громадяни та їхнє майно, які не мають охоронних засобів системи, але можуть звернутись до неї по допомогу. Зареєстрованими абонентами (користувачами) є громадяни та організації, які бажають одержати додаткове забезпечення безпеки — датчики контролю за змінами нормального стану навколишнього середовища і функціонування людини.

Сигнали тривоги від датчиків передаються патрульними станціями сил реагування, абонентськими і вузловими станціями (ре-

трансляторами) до центру оброблення інформації та управління системою по каналах радіо- і телефонного зв'язку. Основним елементом відображення інформації, що надходить, є електронна карта міста. Аналіз повідомлень, прийняття рішень по них і видачу вказівок та рекомендацій силам реагування здійснюють оператори системи за допомогою СППР. Алгоритми підтримки прийняття рішень передбачають визначення найближчих до місця виникнення сигналу тривоги груп реагування, формування запитів до бази даних щодо розміщення або характеристик місця виникнення тривожної ситуації, видачу відповідей черговому оператору тощо. Сферою застосування системи є правоохоронна діяльність, медичні служби, пожежна охорона, екологічні організації, служби міського господарства та ін. Відповідні фахівці складають сили реагування.

ГІС ОВС України розробляються Інститутом передових технологій разом з УОІ МВСУ на основі програмного продукту американського Інституту спостереження за навколишнім середовищем (Environmental Systems Research Institute, ESRI, <http://www.esri.com/>) ArcView.

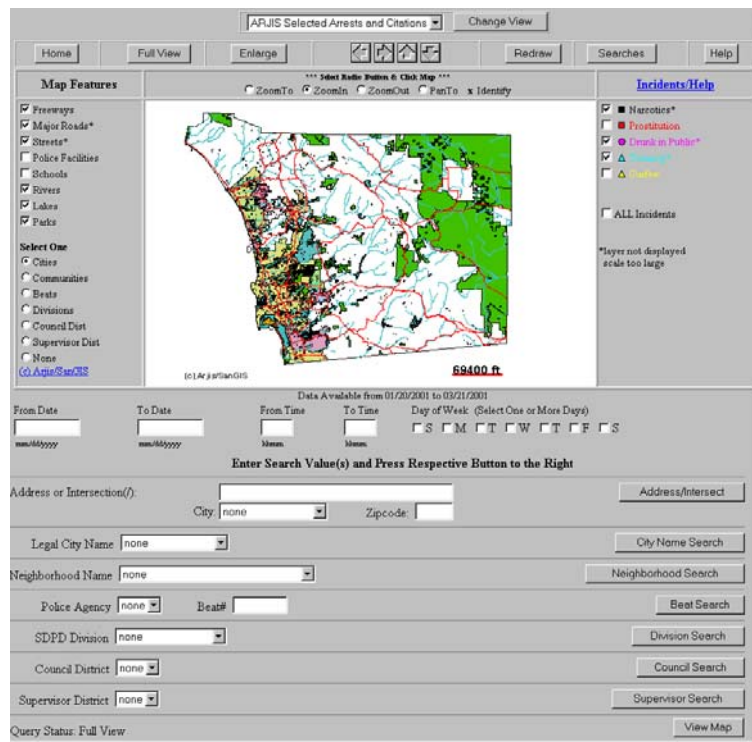


Рис. 9.4. Частина Web-сторінки системи ARJIS

У системах використовуються цифрові бази та електронні карти, розроблені в Укргеодезкартографії. Можливі актуалізація і спостереження за картографічною базою даних із використанням космічних знімків високого дозволу (2—3 м).

До складу ГІС ОВС України входять такі *функціональні модулі*:

- бази даних підвідомчої території;
- сервер оперативної бази даних;
- модуль оперативного керування ситуацією на підвідомчій території з АРМ оперативного чергового та АРМ збирання інформації та обліку конкретних подій;
- модуль розв'язування аналітичних задач та упорядкування звітів.

До складу функціональних модулів можуть входити *підмодулі*:

- картографічної інформації (бази додаткових даних про територію);

- доступу до спеціальної інформації (органів МВС, СБУ, податкової міліції, митниці, Міністерства надзвичайних ситуацій тощо) баз даних території (прикордонні райони, морські об'єкти тощо);

- відстеження і зв'язку з мобільними об'єктами;
- прогнозування і моделювання.

Під час роботи з ГІС з бази даних керування територією інформація надходить до модуля оперативної бази даних, звідки передається до функціональних модулів. У модулі оперативного керування територією відбувається координатна прив'язка подій до геокодованої картографічної електронної основи. У результаті на екрані АРМ оперативного чергового на електронній карті автоматично з'являється умовне позначення події. Далі залежно від виду події (рухливі — викрадення або статичні — пограбування, пожежа тощо) починає працювати АРМ вирішення оперативних задач: визначення особливостей місця події; визначення найкоротшого шляху для патрульної мобільної групи; визначення зон перехоплення; виділення в зоні спостереження особливих об'єктів (кількість жителів будинку, селища, наявність піднаглядних осіб тощо); оперативне формування протоколу події і проектів наказів оперативного чергового для керування силами і засобами.

На підставі записаних даних про оперативний стан у модулі вирішення аналітичних задач і звітів можуть бути підготовлені статичні звіти за той чи інший період по різних видах подій і районах території. Може бути проведений порівняльний аналіз за злочинами, визначена їх кореляція з піднаглядними особами, транспортними розв'язками, наявністю зброї, наркотиків тощо. На АРМ прогнозування можна побудувати тривимірні моделі за обраними статистичними даними, скласти необхідний маршрут, визначити місця охорони і спостереження, розрахувати необхідні сили і засоби.



Контрольні запитання і завдання

1. *За якими напрямками у діяльності ОВС застосовуються інформаційні технології?*
2. *Які ІС ОВС України є загальновідомчими?*
3. *Схарактеризуйте організаційне забезпечення ІС ОВС України.*
4. *Які обліки ведуться на територіальному рівні?*
5. *Які обліки ведуться на регіональному рівні?*

6. Які обліки ведуться на центральному рівні?
7. Схарактеризуйте:
 - а) ІС «Інтегрований банк даних»;
 - б) ІС «Розшук»;
 - в) ІС «Пізнання»;
 - г) ІС «Арсенал»;
 - д) «ІПС за прізвищами та дактилоскопічним обліком криміногенних осіб»;
 - е) ІС «ОАЗИС».
8. Які типові прикладні підсистеми виокремлюють в ІС ДАІ?
9. Які задачі вирішуються: а) на місцевому рівні ЄДАПС; б) на регіональному; в) на державному?
10. Визначте функціональну структуру ЄДАПС.
11. Яку структуру має БД ЄДАПС?
12. Назвіть складові бази даних нормативно-довідкової інформації ЄДАПС.
13. Які задачі ОВС вирішують за допомогою ГІС?



Література

1. Компьютерные технологии в юридической деятельности: Учеб. пособие. / Под ред. проф. Н. Полевого, канд. юрид. наук В. Крылова. — М.: Изд-во БЕК, 1994. — 304 с.
2. Матеріали сайтів <http://www.compulog.ru/komit/infores>, <http://www.insoft.ru/insoft/gibdd>, <http://www.kmu.gov.ua/>, <http://www.ncjrs.org/>, <http://www.ojp.usdoj.gov/cmrc>.
3. Саницький В. А. та ін. Система інформаційного забезпечення ОВС України: Навч.-практ. посібник. — К.: Редакційно-видавничий відділ МВС України, ТОВ «АНЕТКС», 2000. — 144 с.