

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА ЮРИДИЧНА АКАДЕМІЯ УКРАЇНИ
імені ЯРОСЛАВА МУДРОГО**

**ПРАВОВА ІНФОРМАЦІЯ
ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ
В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ**

Навчальний посібник

*За загальною редакцією
професора В.Г. Іванова*

**Харків
«Право»
2010**

*Рекомендовано до видання редакційно-видавничою радою
академії (протокол № 3 від 03.06.2009 р.)*

Рецензент: д-р техн. наук, проф. Н.В. Шаронова, завідувачка кафедри інтелектуальних комп'ютерних систем Національного технічного ун-ту “Харківський політехнічний інститут”.

Автори: **В.Г. Іванов**, д-р техн. наук, проф. (заг. ред., передм., гл. 1 у співавт.); **С.М. Іванов**, канд. техн. наук, доц. (гл. 8 у співавт.); **В.В. Карасюк**, канд. техн. наук, доц. (гл. 7, 8 у співавт.); **В.В. Комаров**, канд. юрид. наук, проф. (передм., гл. 1, 7 у співавт.); **Н.А. Кошева**, канд. техн. наук, доц. (гл. 6); **Ю.В. Ломоносов**, канд. техн. наук, доц. (гл. 4); **М.Г. Любарський**, д-р фізико-мат. наук, проф. (гл. 5); **М.В. Гвозденко** (гл. 3); **Н.І. Мазниченко** (гл. 2).

Правова інформація та комп'ютерні технології в юридичній діяльності: Навч. посіб. / В.Г. Іванов, С.М. Іванов, В.В. Карасюк та ін.; За заг. ред. В.Г. Іванова. – Х.: Право, 2010. – 240 с.

Розглянуто теоретичні й практичні питання ефективного використання комп'ютерних та інформаційних технологій у професійній діяльності юристів.

Для студентів гуманітарних і технічних вузів, які вивчають “Інформатику”, “Правову інформатику”, викладачів цих дисциплін, а також юристів-практиків.

СПИСОК СКОРОЧЕНЬ

АБД – автоматизований банк даних
АПС – автоматизовані інформаційно-пошукові системи
АРМ – автоматизоване робоче місце
АСКВД – автоматизовані системи контролю виконання документів
БД – база даних
ДПС – довідкова правова система
ЕД – електронний документ
ЕК – електронний каталог
ЕОМ – електронна обчислювальна машина
ЕЦП – електронний цифровий підпис
ІПІ – інтеграція права і інформатики
ІПС – інформаційно-пошукова система
ІТ – інформаційна техніка
“НАУ” – “Нормативні акти України”
ОІОТ – основи інформатики і обчислювальної техніки
ОС – операційна система
САБ – система автоматизації бібліотеки
САДП – системи автоматизації ділових процесів
СЕД – системи електронного документообігу
СІАЗ – системи інформаційно-аналітичного забезпечення
СУБД – системи керування базами даних
HTML – hyper text markup language – мова розмітки документів
HTTP – hyper text transfer protocol – протокол передачі гіпертексту

П Е Р Е Д М О В А

Комп'ютерні технології є незамінним ефективним засобом роботи сучасного юриста та основним способом удосконалення її організації.

Навчальна дисципліна “Правова інформація та комп'ютерні технології в юридичній діяльності” призначена для формування у студентів-юристів теоретичних знань і практичних навичок ефективного застосування комп'ютерних і інформаційних технологій у своїй майбутній професійній діяльності через уміле використання електронних документів та мережних ресурсів, електронних джерел навчання, офісного програмного забезпечення, мережних технологій і спеціалізованих програмних пакетів та баз даних правового призначення.

Актуальність і новизна цієї дисципліни визначається необхідністю вирішення важливого і нерозривного завдання – інформатизації права, з одного боку, і правозабезпечення інформатизації – з другого. Сучасна інформатика має зняти просторові, часові, змістові й технологічні обмеження в роботі з інформацією, надавши можливості якісно змінити професійне, економічне і культурне життя сучасної людини. До юридичних аспектів інформатики так само належать ті, що, торкаються вивчення прав, обов'язків та відповідальності суб'єктів, діяльність яких пов'язана з виробництвом, розповсюдженням та використанням виробництвом, розповсюдженням та використанням інформації, питання правового виховання членів інформаційного суспільства.

Потрібно знайти такі правові механізми, які забезпечать ефективне регулювання нового рівня суспільних відносин – інформаційних, що дозволить економічно ефективно розвивати цю сферу людської діяльності, а також протистояти різним характеристикам для неї порушенням і злочинам.

Перехід до усвідомлення таких реальностей зрушує і базові освітні орієнтири в юриспруденції.

Якщо навчальна дисципліна “Основи інформатики і обчислювальної техніки” дає студентам можливість одержати комплекс необхідних теоретичних знань про персональні ЕОМ, а також набути практичних умінь і навичок їх використання для

створення, зберігання, пошуку, обміну і представлення інформації різної фізичної природи, то спецкурс “Правова інформація та комп’ютерні технології в юридичній діяльності” має на меті знання обчислювальних і інформаційних систем в аспекті можливостей їх застосування в судочинстві, прокурорській і слідчій діяльності, судовій експертизі, господарській діяльності, державному управлінні.

Вивчення інформатики передбачає тісний зв’язок із загальними та спеціальними юридичними дисциплінами, який може бути досягнутий шляхом включення в зміст останніх окремих питань і тем, що торкаються застосування ЕОМ. Поява таких міждисциплінарних зв’язків предметів, що вивчаються, і математизація загальнонаукових і спеціальних дисциплін дозволить студентам гуманітарних вузів оволодіти сучасними методами і засобами наукової діяльності.

При цьому комп’ютер виступатиме переважно як засіб, інструмент навчання юридичних дисциплін і водночас як об’єкт вивчення – поглиблюватимуться знання про нього самого, закріпляться практичні навички роботи з ним і тим самим буде реалізований принцип безперервності та системності вивчення інформатики, що дасть можливість студентам юридичних вузів досягти необхідного сучасного рівня інформаційної компетентності для вирішення другої складової потенційного завдання інформатики – правозабезпечення інформатизації.

Навчальний посібник побудований на концептуальних принципах взаємодії і об’єднання “інтересів” права та інформатики, науковості, доступності, системності матеріалу й методичної послідовності його викладення.

Структура і зміст посібника спрямовані на вирішення основних завдань навчання, згідно з якими студент має ознайомитися з поняттями “правова інформатика” та “правова інформація”, математичними моделями, які використовуються в юридичній діяльності, основними цілями національної програми правової освіти населення, а також розглянути принципи побудови інформаційних систем державно-правового характеру; поглибити і розширити свої знання і уміння роботи у пакеті Microsoft Office, оволодіти організаційними, правовими та програмними засобами

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

Зважаючи на структуру та зміст навчального посібника, автори сподіваються, що він буде корисним досить широкому загалу читачів: студентам гуманітарних і технічних вузів, де вивчають інформатику і обчислювальну техніку як обов'язкову навчальну дисципліну; викладачам, які здійснюють теоретичну і практичну підготовку студентів з дисципліни "Інформатика і обчислювальна техніка"; викладачам інших дисциплін, що використовують персональні ЕОМ як інструмент навчання або підготовки навчальних матеріалів за своєю предметною галуззю; юристам, які самостійно набувають навиків інформаційної компетентності у своїй професійній діяльності.

Г л а в а 1

ПРАВОВА ІНФОРМАЦІЯ ТА ПРАВОВА ІНФОРМАТИКА

1.1.Інтеграція права й інформатики

Практика повсякденної діяльності людини і суспільства характеризується неухильним зростанням використання інформації і нових інформаційних технологій. Інформація – стратегічний ресурс суспільства, який визначає рівень розвитку держави, його економічний потенціал.

Інтенсивне зближення інтересів права й інформатики є об'єктивним і закономірним процесом, викликаним нагальною необхідністю у взаємному використанні новітніх досягнень цих наук, який має два взаємозв'язані аспекти: прикладний і змістовий. Тобто використання останніх досягнень у галузі інформаційних технологій, пристосованих або спеціально розроблених для розвитку й функціонування юридичної науки і практики, з одного боку, і юридичне закріплення питань, пов'язаних з упровадженням у певну сферу суспільних відносин цих інформаційних технологій, – з другого.

З розвитком інформаційного суспільства збільшуються потоки інформації, швидкість її обробки й розповсюдження, і у зв'язку з цим виникає потреба в захисті інтересів суб'єктів, які використовують інформацію у своїй діяльності. Тому важливо знайти такі правові механізми, які забезпечать правове регулювання інформаційних відносин, що дозволить економічно ефективно розвивати галузь людської діяльності виробництва й використання інформації цю, а також протистояти різним правопорушенням, пов'язаним з нею.

Розповсюдження електронних засобів фіксації, передачі й обробки інформації породжує безліч правових питань, що стосуються дотримання майнових і немайнових інтересів суб'єктів авторських прав. При захисті прав автора сайта виникає проблема ідентифікації мережних інформаційних ресурсів як об'єкта права: чи є вони різновидом бази даних або програмою для ЕОМ, чи можна віднести сайт до засобів масової інформації то-

що. Одним із найважливіших є питання безпеки й конфіденційності роботи в мережі Інтернет, іншими словами, захист комп'ютера від зараження вірусом, запобігання несанкціонованому доступу, недопущення перехоплення особистої електронної пошти, іншої секретної інформації.

Такі приклади можна продовжити, але головне полягає у тому, що інформаційні відносини все більше потребують правового впорядкування.

1.2.Правова інформатика

Перш за все слід сказати, що предмет інформатики особливий. Він не збігається з предметом суспільних наук чи з предметом системотехніки. Предмет інформатики складніший, він охоплює системи суспільно-технічної природи, що виникають штучно – шляхом соціального інженерного проектування.

Інформатика не є просто наукою про ЕОМ, як кібернетика і системотехніка, і не є наукою про передачу повідомлень каналами зв'язку, як канонічна теорія інформації. Це наука про інформаційно-соціальне середовище, у яке впроваджуються ЕОМ і в якому вони працюють як підсилювачі людського інтелекту. Традиційна теорія інформації наголошує на зв'язку одержувача з джерелом інформації. В основу інформатики покладено динаміку різних соціальних середовищ під дією інформації.

Інформатика – це фундаментальна галузь наукового знання, що формує системно-інформаційний підхід до аналізу навколишнього світу, вивчає інформаційні процеси й системи, методи й засоби одержання, перетворення, передачі, збереження й використання інформації у різних галузях соціальної практики.

Дослідження в правовій інформатиці повинні враховувати як інформаційні, так і правові аспекти об'єктів, явищ і процесів, що вивчаються. Інформаційні технології довгий час розглядалися правовою інформатикою тільки з погляду ефективності організації юридичної діяльності. Проте останнім часом необхідність взаємодії фахівців різних професійних галузей вимагає від юриста знання і розуміння всіх технічних і інформаційних особливостей об'єктів, що досліджуються.

У цьому сенсі правова інформатика є інструментальним засобом і джерелом знань, необхідних для вирішення безлічі проблем правового регулювання суспільних відносин.

Тому можна говорити, що правова інформатика як підгалузь загальної інформатики вивчає закономірності інформаційних процесів, проблеми створення, впровадження й ефективного функціонування комп'ютеризованих систем обробки правової інформації і, зокрема, системної інформатизації законотворчої, нормотворчої, правозастосовної та правоосвітньої діяльності, а також (опосередковано) проблеми нормативно-правового регулювання якісно нового виду суспільних відносин – інформаційних.

Це визначення узгоджується із Законом України “Про національну програму інформатизації” від 4 лютого 1998 р., де зазначено, що інформатизація – це сукупність взаємозалежних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, спрямованих на створення умов для задоволення інформаційних потреб громадян і суспільства на основі побудови, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, та застосування сучасної обчислювальної та комунікаційної техніки.

1.3. Поняття правової інформації

У загальноприйнятому значенні інформація – це дані, знання, повідомлення, які є об'єктом збереження, передачі й перетворення і допомагають розв'язати поставлене завдання. Інформація – це нові дані, які може використати людина для вдосконалення своєї діяльності та поповнення знань. Інформувати, в теорії інформації, означає повідомити щось, раніше невідоме.

У побуті ми часто вживаємо слово “дані” як синонім слова “інформація”, однак у науці вони істотно відрізняються одне від одного. Дані – це величини, їх відношення, словосполучення, факти, перетворення й обробка яких дозволяє одержати інформацію, а потім і знання про той чи інший предмет, процес або явище. Іншими словами, дані є тим матеріалом, після обробки якого створюється інформація. Інформація – це продукт взаємо-

дії даних і адекватних їм методів обробки.

Щодо правової інформації, то в широкому розумінні – це зміст даних (повідомлень), використання яких допомагає вирішити ту чи іншу правову задачу чи сприяє її вирішенню.

Множинність таких завдань, з одного боку, визначає різмаїття видів правової інформації та її джерел, з другого – зумовлює певні труднощі в її відокремленні від інших типів інформації (наукової, економічної, політичної тощо).

В юридичній практиці правовою інформацією визнають значеннєвий зміст правових норм. При цьому вважають, що останній міститься не тільки в актах вищих і місцевих органів влади та управління, а й у відомчих нормативних актах. Як джерело правової інформації розглядають також судову, арбітражну і нотаріальну практику.

Такий підхід до аналізу правової інформації правильний, але явно недостатній. У сфері юридичної діяльності використовується інформація, що міститься не тільки в правових нормах, а й у низці інших джерел. Приміром, при розкритті й розслідуванні злочинів. Тут поряд із інформацією, що міститься в нормах Кримінально-процесуального та Кримінального кодексів України, органи, що здійснюють оперативну діяльність, дізнання і слідства широко використовують інформацію з таких джерел, як сліди злочинів і злочинця, а також з образів, які залишилися у свідомості людей (потерпілого, свідка і самого злочинця). Це джерела спеціальної криміналістичної інформації, які є різновидом правової інформації, оскільки саме на її основі вирішують завдання з розкриття й розслідування злочинів. Самостійним видом правової інформації є, наприклад, кримінологічна інформація.

Такий підхід до визначення правової інформації знайшов своє відображення і в Законі України про інформацію, в якому зазначено, що правова інформація – це сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

1.4. Моделі та комп'ютерні технології в юридичній діяльності

Модель – це заміник об'єктів або явищ, тобто матеріальний чи уявний об'єкт, який у процесі дослідження замінює об'єкт-оригінал так, що його безпосереднє вивчення дає нові знання про об'єкт-оригінал.

Під моделюванням розуміють дослідження будь-яких явищ, процесів чи систем шляхом побудови й вивчення їх моделей, тобто об'єктів, що є уявними або матеріально реалізованими системами, кожна з яких, відображаючи чи відтворюючи об'єкт-оригінал, здатна замінювати його так, що її вивчення дасть нову інформацію про цей об'єкт.

Розрізняють:

а) моделі-аналоги, які є зменшеною копією системи, виконаної за допомогою фізичних і технічних засобів (моделі літаків, теплоходів або макети електростанцій, міст);

б) вербальні моделі – ті, що відтворюють систему за допомогою слів. Наприклад, різні статuti, розпорядження щодо експлуатації, законодавчі матеріали, процесуальні кодекси тощо;

в) знакові моделі – описують аналізовану систему за допомогою логічних і математичних символів. Знаковими є і блок-діаграми (блок-схеми), що зображують алгоритми рішення задач.

Модель повинна як можна докладніше, детальніше, точніше відображати процес або явище. Проте насправді кожна модель є лише спрощеним відображенням дійсності і в ній відбиваються тільки ті дані, що відповідають меті дослідження. Розклад руху літаків – теж модель, але вона, наприклад, не враховує впливу погодних умов на роботу аеропорту, оскільки останнє виходить за межі її призначення. Базовою мовою для моделювання може служити єдина міжнародна система символів блок-діаграм.

Так, у криміналістиці, наприклад, модель покликана відкрити можливості для одержання оперативно-розшукової або доказової інформації, а також для оцінки і дослідження цієї інформації у процесі оперативно-розшукової роботи, розслідувань і судового розгляду кримінальних справ. Таким чином, криміналістична математична модель може бути визначена як математичний опис речового до-

казу, зразка або іншого об'єкта криміналістичного дослідження, який є засобом фіксації об'єкта, здатний замінити його в процесі дослідження і відкриває можливості для одержання нової доказової або оперативно-розшукової діяльності.

Для криміналістики більш звичні фізичні моделі, які широко застосовують у доказуванні. Вони наочні і змістовні, хоча при математичному моделюванні наочність досить умовна. Однак такі моделі відкривають можливості для точного методу дослідження – математичного – дозволяють виявити та використати ті ознаки, що нерідко залишаються поза увагою, прихованими при фізичному моделюванні. Багато об'єктів не можуть вивчатися й використовуватися в криміналістичних цілях без їх математичного моделювання. До таких належать: дактилоскопічна реєстрація, вокалоскопія, інформаційно-пошукові й експертні системи, умови автотранспортної пригоди й т. ін.

Перспективним і актуальним бачиться застосування математичних моделей і комп'ютерних технологій у кримінальному і цивільному судочинстві. Правосуддя не може нормально функціонувати без підтримки одноманітних підходів до вирішення справ на всіх рівнях судової піраміди. Актам вищих судів додається велика сила зовсім не тому, що вони керуються іншими стандартами, ніж судді першої інстанції, а тому, що вони досягають ті ж об'єктивні закономірності глибше унаслідок тривалого й масштабнішого досвіду розгляду цивільних і кримінальних справ.

Якби вдалося створити великий комп'ютерний банк прецедентів і автоматично і правильно виділити істотні ознаки, які характеризують діяння і як достатньо доведений злочин, можна було б передбачати вирoki за конкретними справами і виключити суб'єктивний чинник. Тобто процес кваліфікації злочинів можна розглядати як формально-логічний процес (модель, алгоритм) "пізнання" судом юридичних властивостей факту через призму оцінки, даної законодавцем.

Кримінально-процесуальний кодекс України регламентує послідовність питань, що вирішуються судом при ухвалі вироку. Ця послідовність строго визначена Законом, вона не допускає ніяких змін. Сама форма вирішення цих питань близька до класич-

ної двозначної логіки: “так” – “ні”. Кожне питання повинно бути поставлене в такій формі, щоб на нього могла бути дана позитивна або негативна відповідь. Це безумовна модель, алгоритм і потім програма.

Такі завдання добре вирішуються з використанням моделей бінарного дерева (рис. 1.1.), у вузлах якого знаходяться відповідні кваліфікаційні питання, а стрілки указують на можливі відповіді на них.

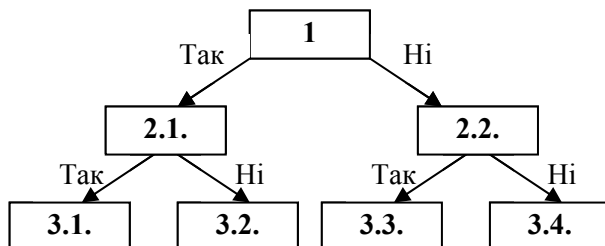


Рис. 1.1. Приклад моделі на основі бінарного дерева.

У такій схемі важливо не те, в якій послідовності з'ясовуються питання розмежування і кваліфікації, а те, аби жодне з них не було пропущено, щоб на кожне з них було дано відповідь, виходячи з фактичних матеріалів справи. Наприклад, початкові питання в цій моделі можуть звучати так: 1 – Чи завдано діяннями обвинуваченого шкоди чужому майну? 2.1. – Чи було це майно державним або громадським? І так далі. У разі негативної відповіді на друге питання відбувається перехід до іншої програми, що передбачає злочини проти особистої власності громадян.

Наявність у явищах соціально-правової дійсності статистичних закономірностей – одна з об'єктивних передумов для вибору і використання відповідних математичних методів і моделей, на основі яких може бути наданий кількісний опис об'єктів соціології права. Найважливіша роль тут належить методам теорії вірогідності і математичної статистики.

Статистичні закономірності виявляються і при вивченні проблеми правопорушень. Конкретні соціально-правові досліджен-

ня цього явища ґрунтуються на статистичному підході, а обробка статистичних даних, що цікавлять кримінолога, за допомогою обчислювальних машин значно збільшує обсяг інформації про причини й умови, які сприяють вчиненню злочинів, забезпечує вищу достовірність кінцевої інформації, дозволяє глибше аналізувати відповідні дані шляхом різних комбінацій статистичних показників.

Правильно побудовані і перевірені математичні моделі дають можливість точно вирішувати основне для кримінології питання – чи впливає певний соціальний чинник на стан і динаміку злочинності чи ні?

1.5. Національна програма правової освіти населення

Формування демократичної, правової, соціальної держави, засад громадянського суспільства зумовлює необхідність підвищення рівня правової культури населення. Для вирішення цього завдання, як сказано в Національній програмі правової освіти населення, затвердженій Указом Президента України від 18 жовтня 2001 р. № 992/2001, потребують вирішення на державному рівні питання подальшого розвитку правосвідомості населення, подолання правового нігілізму, задоволення потреб громадян у одержанні знань про право. Це може бути забезпечено, насамперед, шляхом удосконалення правової освіти населення.

Національна програма правової освіти населення передбачає створення необхідних умов для набуття широкими верствами населення правових знань та навичок у їх застосуванні, забезпечення доступу громадян до джерел правової інформації, а також визначає основні напрями правоосвітньої діяльності та першочергові заходи щодо їх реалізації.

Метою Програми є підвищення загального рівня правової культури та вдосконалення системи правової освіти населення, одержання громадянами необхідного рівня правових знань, формування у них поваги до права.

Цілком зрозуміло, що в сучасних умовах ефективна реалізація цієї мети можлива лише через запровадження новітніх інформаційних технологій, зокрема елементів дистанційного на-

вчання, які забезпечують доступ до віддалених джерел інформації з використанням комп'ютерних систем та телекомунікаційних засобів зв'язку (мережі Інтернет).

Українські юридичні ресурси в Інтернеті

Джерело інформації	Найменування сайта
<i>Бази законодавства</i>	
Інформаційно-пошукова система “Ліга”	www.liga.kiev.ua
Інформаційно-пошукова система “НАУ”	www.nau.kiev.ua
Верховна Рада України	www.rada.kiev.ua
Система правової підтримки ЛЮЦМАН online	Info.resourcecorp.net
Lex Info Sys – Інформаційна система про розвиток права у державах з перехідною економікою	www.lexinfosys.de
<i>Державні органи</i>	
Конституційний Суд України	www.constcourt.gov.ua
Верховний Суд України	www.scourt.gov.ua
Вищий господарський суд України	www.arbitr.com.ua
Харківський обласний суд	www.pravo.kharkov.com
Вища рада юстиції України	www.vru.gov.ua
Міжнародний комерційний арбітражний суд при Торговельно-промисловій палаті України	www.ucci.org.ua/arb/index.ru.html
Кабінет Міністрів України	www.nai.gov.ua/KM.htm
Головне керування державної служби України	www.elvisti.kiev.ua/GUDS/
Міністерство закордонних справ України	www.mfa.gov.ua
Міністерство внутрішніх справ України	www.mia.gov.ua
Сайт постійного представництва України в ООН	www.undp.org/missions/ukraine
<i>Юридичні організації</i>	
Українсько-Європейський консультативний центр з питань законодавства (UEPLAC)	www.ueplac.kiev.ua
Асоціація українських правників Америки (UABA – Ukraina America Bar Association)	www.brama.com/uaba/

Важливого значення у процесі поширення правових знань набувають юридичні клініки, які останнього часу створюються при юридичних ВНЗ України. У них разом із просвітницькою роботою здійснюється безоплатна правова допомога особам, які потребують соціального захисту та підтримки, а також отримання студентами старших курсів юридичних спеціальностей практичних навичок юриста. Типове положення затверджене наказом № 592 Міністерства освіти і науки України від 3 серпня 2006 р.

Метою юридичної клініки є:

- підвищення рівня практичних знань, умінь і навичок студентів юридичних спеціальностей;
- забезпечення доступу представників соціально уразливих груп суспільства до правової допомоги;
- формування правової культури громадян;
- підготовка та навчання студентів у дусі дотримання й поваги принципів верховенства права, справедливості й людської гідності;
- розширення співробітництва вищих навчальних закладів, що здійснюють підготовку фахівців-юристів, із судовими, правоохоронними органами, органами юстиції, державної влади й місцевого самоврядування, з іншими установами та організаціями;
- упровадження в навчальний процес елементів практичної підготовки студентів-правників у сфері юридичних послуг.

Для забезпечення діяльності юридична клініка оснащена комп'ютерами, що дозволяє працювати з правовими базами даних, мережею Інтернет, засобами телефонного зв'язку.

1.6. Інформаційні системи державно-правового характеру

Серед різних визначень поняття “система” найбільш універсальним слід визнати те, в якому під системою розуміється сукупність взаємопов'язаних об'єктів, підпорядкованих певній єдиній меті з урахуванням умов навколишнього середовища.

Структура й функціонування системи визначається поставленими перед нею цілями і завданнями.

Можна виділити наступні основні характеристики і властивості системи. Система є впорядкованою (а не хаотичною) сукупністю елементів. Як деталі, з яких складається автомобіль, будучи складеними разом, не утворюють автомобіль як систему, так і сукупність всіх норм, що визначають умови і обсяг покарання за різні види злочину, без відповідної їх систематизації не утворюють системи, яка називається “Кримінальний кодекс України”.

Елементи системи взаємозв’язані і взаємодіють у рамках цієї системи, будучи її підсистемами. Кожен елемент системи як підсистема характеризується функціональною самостійністю, якісною відособленістю, через що може розглядатися як самостійна система іншого рівня.

Система як ціле виконує певну функцію, яка не може бути зведена до функцій кожного окремо взятого її елемента.

Елементи системи (як підсистеми) можуть взаємодіяти як в рамках своєї системи, так і із зовнішнім середовищем і змінювати при цьому свій функціональний зміст або внутрішню будову.

Будь-яка цілеспрямована система є системою інформаційною, тобто її функціонування можливе тільки на основі прийому, створення, зберігання, передачі, обробки і видачі інформації. Можна говорити про чисто електронні системи керування (комп’ютерні, кібернетичні) або про змішані, людино-машинні системи.

Інформаційні системи державно-правового характеру є змішаними людино-машинними системами і належать до цілеспрямованих механізмів управління, тісно пов’язані з правом і через це виконують функцію регулятора суспільних відносин. Вони мають суб’єкти й об’єкти дії, канали прямих і зворотних зв’язків, за допомогою яких і здійснюються процеси збору, обробки та використання інформації і, зрештою, процеси управління.

Системи державно-правового характеру володіють всіма властивостями інформаційних систем.

Всі керовані системи, що функціонують у сфері юридичної діяльності, структурно можна поділити на суб'єкти і об'єкти керування або на підсистеми, що керують, і ті, якими керують (керовані).

Підсистеми, що керують, здійснюють керівні, регулівні та інші дії. До них належать відповідні органи державної влади, управління, суду, прокуратури, громадські організації тощо. Керовані системи піддаються керуючим діям. Об'єктом керування (керованою підсистемою) служить поведінка суб'єкта – підприємства, установи, організації, посадової особи, громадянина. Взаємодія і функціонування підсистем, що керують, і керованих здійснюється через інформаційні канали прямих і зворотних зв'язків.

Для прикладу розглянемо такий важливий суспільний інститут, як кримінальна юстиція. Будь-яка система кримінальної юстиції – апарат, за допомогою якого суспільство захищає правила поведінки, необхідні для охорони інтересів як окремої особи, так і всього суспільства. Система діє, використовуючи арешт, судове переслідування і засудження тих її членів, які порушують правила спільноти. Крім негайного покарання порушника закону будь-яка акція проти нього має три мети: 1) вилучити із суспільства людину, яка становить для нього небезпеку; 2) утримати решту членів суспільства від злочинної поведінки; 3) дати суспільству можливість зробити із злочинців законотворчих громадян.

Суб'єктами цієї системи є органи внутрішніх справ, прокуратури, суди, виправні заклади тощо; об'єктом дії – поведінка людей. Органи системи мають свої програми функціонування – насамперед юридичні й та інші. Ці органи виявляють злочини, адміністративні провини тощо, тобто по каналах прямого зв'язку до суб'єкта дії надходить різна соціально-правова інформація, що стосується поведінки людей. Органи юстиції (кожен по своїй лінії) збирають і обробляють цю інформацію та на її основі порушують і розслідують кримінальні справи, інші провини. Каналами зворотного зв'язку в систему надходить інформація про результати їх діяльності. Функціонування будь-якої системи правового характеру завжди пов'язане зі збором, обробкою та використанням інформації.

Контрольні питання

1. Якими об'єктивними факторами зумовлений процес інтеграції права та інформатики?
2. У чому принципова відмінність сучасної інформатики від інших технічних наук?
3. У чому полягає сутність правової інформатики?
4. Основні положення Закону України “Про Національну програму інформатизації”.
5. У чому відмінність даних та інформації?
6. Що розуміють під правовою інформацією?
7. Види правової інформації.
8. Дайте визначення поняття “модель” і “процес моделювання”.
9. Наведіть приклади використання моделювання і моделей в юридичній діяльності.
10. Дайте характеристику основних положень Національної програми правової освіти населення (НППОН).
11. Юридична діяльність як сукупність систем державно-правового характеру.

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ У ПІДГОТОВЦІ ЮРИДИЧНИХ ДОКУМЕНТІВ

2.1. Сучасні підходи до автоматизації документообігу

Інформаційний обмін є основою існування суспільства, тому що саме через нього реалізується дія суспільних відносин. Однією з форм інформаційного обміну є документообіг. Документообіг – це рух документів в організації з моменту їх одержання або створення до завершення виконання або відправлення. Перехід до інформаційного суспільства неминуче веде до розширення документообігу та його якісного ускладнення. Підвищення ефективності документообігу є одним із найважливіших завдань інформатики. Вирішується воно через автоматизацію роботи з документами і використання засобів обчислювальної техніки.

Механізм документообігу має декілька стадій. Перша стадія – створення документа. Далі – його транспортування (передача), впорядковане зберігання і відтворення (або інше застосування).

Не всі стадії документообігу автоматизуються однаково легко. Найпростіше автоматизується відтворення документів. Історично цей завершальний етап був автоматизований раніше за інших. Це відбулося ще на початку 80-х рр. XX ст., коли почалося впровадження друкувальних пристроїв, що підключаються до персональних комп'ютерів.

Пізніше, в другій половині 80-х рр., почалася автоматизація зберігання документів і керування доступом до них. Основним засобом автоматизації на цій стадії стали ранні системи керування базами даних (СУБД) і файлові системи персональних комп'ютерів.

Великий крок в автоматизації транспортування документів зроблено в 90-х рр. XX ст., коли основним засобом автоматизації стали мережні комп'ютерні служби. Створення комп'ютерних мереж і служб обміну даними зробили революційний переворот в

автоматизації діловодства. З'явилася можливість використовувати мережу для переміщення документів і централізованого стеження за ходом діловодного процесу.

Разом із цим з'явилися і проблеми, наприклад, правовий режим електронної копії документа. Технічне рішення цієї проблеми існує: будь-які дані, надані в електронній формі, можуть бути зашифровані й забезпечені електронним цифровим підписом (ЕЦП) – спеціальним кодом, який виключає сумніви щодо авторства і правильності змісту документа, що передається. Необхідною умовою переходу до автоматизованого документообігу є надання правового статусу електронним документам (ЕД). В Україні ця проблема була вирішена з ухваленням законів “Про електронні документи та електронний документообіг” та “Про електронний цифровий підпис”. Розмежування прав доступу до тих або інших документів при роботі в мережному середовищі стало ще однією суттєвою проблемою, яку теж вирішено – за допомогою системи спеціальних реєстраційних імен користувачів, паролів та криптографії.

Найважче автоматизувати процеси початкової стадії документообігу – створення документів. Вони далекі від остаточної автоматизації і понині. Пояснюється це просто. Чим більша творча складова того чи іншого процесу, тим важче його автоматизувати. Водночас, чим складніший інформаційний процес, тим вище ефективність від його автоматизації, хоч би й часткової. Процес автоматизації при створенні документа оснований на застосуванні стилів для оформлення деяких фрагментів документів та шаблонів документів. Причому є можливість використання як стандартних стилів та шаблонів, так і створення нових.

Наявність технологічної бази для розвитку систем автоматизації діловодства сприяла розробці окремих оригінальних інформаційних технологій роботи з документами, природа яких зумовлена потребою забезпечити користувача звичними атрибутами традиційного діловодства.

Чіткої класифікації систем завдань керування документами і застосування ІТ не існує. Наразі склався наступний загальний поділ.

Засоби автоматизації офісної діяльності (Office

Automation) – текстові редактори для підготовки і коригування документів, процесори електронних таблиць, програми генерації запитів за зразком із різних БД, мережні планувальники для призначення робочих зустрічей і нарад, засоби розробки і демонстрації презентацій, словники і системи перекладу, програми відсилки і прийому факсів, електронна пошта для обміну повідомленнями і пересилання файлів. Це можуть бути окремі пакети (Word, Word Perfect, Excel, Lotus 1-2-3 тощо), інтегрований пакет програм (MS Works) або узгоджений набір пакетів (Microsoft Office або Corel Perfect Office). 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 контроль за виконанням документів (нагадування про наближення строків закінчення виконання документа, повідомлення про прострочені документи тощо). Для цього в системах передбачається ведення журналу реєстрації і контролю або реєстраційно-контрольних карток документів. Такі системи побудовані на основі персональних СУБД 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 СУБД. Документи зберігаються або в базі даних, або у файловій системі. Електронні архіви забезпечують пошук як за атрибутами, так і за змістом документів і можуть включати функції контролю за виконанням документів.

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, струк-

туру проекту та склад робочих груп і “вміє” розсилати повідомлення належним чином згідно з їх 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, Novell Group Wize.

Системи автоматизації ділових процесів (САДП, системи автоматизації керування 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, керування проектами, робота з базами даних, об’єктно-орієнтоване програмування, CASE-технології.

Системи керування (електронними) документами (Electronic/Enterprise Document Management System) вважаються універсальними 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, сполучених 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

всередині 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 СУБД (Oracle, Informix, MS SQL Server, Sybase). Документи можуть зберігатися як у БД, так і у файловій системі. Обмін документами між користувачами здійснюється підсистемою обміну й маршрутизації документів, найчастіше роль цієї підсистеми виконують workflow-системи. Широко відомими прикладами таких систем є DOCS Open і Excalibur EFS.

Автоматизація документообігу є хоч і складним, проте дуже важливим елементом ефективності системи керування будь-яким господарським процесом, фінансово-господарською діяльністю підприємства, економікою країни. Ефективна організація електронного документообігу – запорука економічного зростання як окремого підприємства, так і держави в цілому.

2.2. Огляд сучасних систем електронного документообігу

Електронний документообіг являє собою сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Електронний документообіг – високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи різноманітних підприємств, організацій, установ, органів

державної влади і місцевого самоврядування. Ефективність керування підприємствами й організаціями не в останню чергу залежить від коректного вирішення завдань оперативного і якісного формування електронних документів, контролю їх виконання, а також продуманої організації їх збереження, пошуку і використання. Потреба в ефективному керуванні електронними документами і привела до створення систем електронного документообігу (СЕД).

Розвиток суспільних відносин вимагає розроблення, вдосконалення та оновлення науково-технічної та нормативно-правової бази України, створення спеціальних юридичних норм та правил регулювання сфери інформаційних документальних відносин. Верховною Радою України вже прийняті закони України: “Про електронні документи та електронний документообіг”, “Про електронний цифровий підпис”, “Про Національну програму інформатизації”, “Про телекомунікації”, “Про Національну систему конфіденційного зв’язку”, “Про захист інформації в інформаційно-телекомунікаційних системах” тощо. У цих документах визначені основні організаційно-правові засади електронного документообігу та використання електронних документів. Таким чином, застосування електронного документообігу є законодавчо підкріпленим та досить поширеним на підприємствах України.

У загальному випадку можна вважати, що СЕД – це організаційно-технічні системи, яка забезпечують процес створення, керування доступом і розповсюдження електронних документів у комп’ютерних мережах, а також забезпечують контроль над потоками документів в організації.

Суттєвою перевагою СЕД є можливість якісного й точно виконання безлічі завдань документообігу та опрацювання великих обсягів документів. Типи файлів, що, як правило, підтримують СЕД, включають: текстові документи, зображення, електронні таблиці, аудіо- та відеодані і веб-документи. Головне призначення СЕД – це організація збереження електронних документів, а також роботи з ними (зокрема, їх пошуку як за атрибутами, так і за змістом). У СЕД повинні автоматично від-

слідкуватися зміни в документах, терміни їх виконання, рух, а також контролюватися всі їхні версії. Комплексна СЕД має охоплювати весь цикл діловодства підприємства чи організації – від постановки завдання на створення документа до його списання в архів, забезпечувати централізоване збереження документів у будь-яких форматах, у тому числі складних композиційних документів. СЕД повинні поєднувати розрізнені потоки документів територіально віддалених підприємств у єдину систему і забезпечувати гнучке керування документами як за допомогою чіткого визначення маршрутів руху, так і шляхом вільної маршрутизації документів. У СЕД має бути реалізоване чітке розмежування доступу користувачів до різних документів залежно від їхньої компетенції, займаної посади і призначених повноважень. Крім того, СЕД повинна налаштовуватися на наявну організаційно-штатну структуру і систему діловодства підприємства, а також інтегруватися з існуючими корпоративними системами.

Основними користувачами СЕД є великі державні організації, промислові підприємства, банки і всі інші структури, чия діяльність супроводжується великим обсягом створюваних, оброблюваних і збережених документів.

Відповідно до основних принципів електронного документообігу він повинен функціонувати на таких засадах:

- 1) єдиноразова реєстрація документа;
- 2) можливість паралельного виконання різних операцій з метою скорочення часу руху документів і підвищення оперативності їх виконання;
- 3) безперервність руху документа;
- 4) єдина база документальної інформації для централізованого зберігання документів і виключення можливості дублювання документів;
- 5) ефективно організована система пошуку документа;
- 6) розвинена система звітності за статусами і атрибутами документів, що дозволяє контролювати поетапний рух документів.

Як показали дослідження, переважна більшість вітчизня-

них підприємств автоматизують свій документообіг з використанням пакета програмного забезпечення корпорації Microsoft, що пояснюється зручністю в експлуатації та широкими можливостями подальшого розвитку. Тому актуальним є огляд характеристик систем документообігу, що працюють на платформі Microsoft, визначення їх можливостей, технічних параметрів, вартості. Найцікавішими та поширеними СЕД на вітчизняному ринку є такі:

1. Система “Справа”. Виробником даної системи є компанія “Електронні офісні системи”. Система “Справа” призначена для автоматизації управлінської діяльності у вітчизняних міністерствах і відомствах, територіальних органах влади, на підприємствах різних сфер діяльності.

2. DocsVision 2.0 “Архів-Діловодство”. Виробником даної системи є компанія Digital Design. Система DocsVision 2.0 “Архів - Діловодство” являє собою закінчений додаток, призначений для створення архівів документів, автоматизації основних діловодних процедур і бізнес-процесів обробки документів в організації.

3. “Кодекс: Документообіг”. Компанією-виробником даної системи є ДП “Центр комп’ютерних розробок”. Система “Кодекс: Документообіг” – це комплекс взаємозалежних систем діловодства, банків документів і корпоративних сервісів, що забезпечують автоматизоване розв’язання задач діловодства і документообігу в органах державної влади й інших організацій.

4. “ГРАН-ДОК” для Microsoft Windows. Виробником даної системи є компанія Граніт-Центр. Система керування документами серії Documentum 4i дозволяє вирішувати широкий спектр задач автоматизації документообігу на підприємстві, пов’язаних з діяльністю різних підрозділів, а також автоматизувати типові бізнес-процеси.

5. LanDocs. Виробником даної системи є компанія Ланіт. Система LanDocs призначена для комплексної автоматизації процесів діловодства і ведення архіву електронних документів.

6. Lotus Notes. Виробником даної системи є компанія Lotus. Система Lotus Notes забезпечує розроблення і розміщення

прикладних програм групового забезпечення, дозволяє користувачам одержувати, відслідковувати, спільно використовувати і створювати інформацію для обробки документів.

7. OPTiMA-WorkFlow. Виробником даної системи є компанія OPTiMA. Система OPTiMA-WorkFlow призначена для керування процесами створення, обробки, тиражування і збереження документів, а також для автоматизації основних процедур сучасного діловодства й організації документообігу.

8. Documentum 4i. Виробником даної системи є компанія Documentum (Дистриб'ютор – компанія Документум Сервісіз). “Гран-Док” – система автоматизації діловодства і документообігу в державних і муніципальних структурах управління.

9. У судовій системі України використовується автоматизована система керування документообігом “Діловодство”.

Незважаючи на різноманіття систем автоматизації документообігу і діловодства, існують загальні вимоги, яким повинні відповідати ці системи:

- зручність і простота в адмініструванні та користуванні;
- масштабовуваність – здатність підтримувати будь-яку кількість користувачів; можливість нарощувати свою потужність має визначатися тільки потужністю відповідного апаратного забезпечення;
- розподіленість – підтримання роботи з документами в територіально розподілених організаціях та взаємодія з віддаленими користувачами;
- модульність – система має складатися з окремих модулів, інтегрованих між собою, що дає можливість замовникові вибирати й упроваджувати компоненти згідно зі своїми потребами;
- відкритість – наявність у системі відкритих інтерфейсів для можливої доробки та інтеграції з іншими системами;
- універсальність – можливість використання на різних апаратних платформах у середовищі різного системного програмного забезпечення.

Актуальність аналізу можливостей та характеристик різних систем автоматизації документообігу доводиться дослідженнями лабораторії інформаційних систем Московського фізико-

технічного інституту, метою яких було виявлення поточного стану ринку електронного документообігу, розповсюдженості систем і відношення користувачів щодо наявних систем. Під час досліджень було розглянуто десять російських і західних систем електронного документообігу, для оцінки опитано 239 фахівців різного профілю: користувачі систем електронного документообігу, адміністратори і технічні фахівці. На основі даних цього дослідження було створено математичну модель, відповідно до якої отримано загальний рейтинг розглянутих систем.

Таблиця 2.1.

Загальна оцінка систем електронного документообігу

№ п/п	Система, компанія	Загальна оцінка, %
1	Євфрат, Cognitive Technologies	82
2	OfficeMedia, Інтертраст	81
	ЭСКАДО, Интерпроком ЛАН	81
3	ДЕЛО, ЭОС	79
4	Золушка, НТИЦ ИРМ	78
5	1С:Архив, 1С	77
6	Optima-Workflow, Оптима	73
	БОСС-Референт, Ай Ти	73
7	Эффект-офис, Гарант Интернешнл	72
8	LANDOCS, Ланит	67
9	PayDox, Интерфейс	62
10	ГранДок, Гранит Центр	57

2.3. Характеристика пакета Microsoft Office

Зібравши свої кращі програми в один уніфікований комплекс, компанія Microsoft створила багатоцільовий інструмент для обробки різноманітних даних, планування, спілкування й публікації в мережі. Пакет Microsoft Office на сьогоднішній день є

одним з найбільш популярних програмних продуктів на комп'ютерному ринку. Існують і інші пакети подібного призначення: Open Office, Star Office тощо. Пакет Microsoft Office набув популярності завдяки широкому спектру додатків і засобів, необхідних практично кожній організації чи окремому користувачеві. Пакет Microsoft Office існує в декількох версіях (97, 2000, XP, 2002, 2003, 2007, 2010) і редакціях, які розрізняються кількістю додатків і корисних утиліт, тобто обслуговуючих програм. Багато користувачів працюють лише з частиною можливостей Microsoft Office, деякі додатки не використовуються взагалі або використовуються частково.

Переваги пакета Microsoft Office і причини його популярності:

1. Основною перевагою програм пакета Microsoft Office є його інтегрованість, тобто пакет дозволяє спільно використовувати й легко переміщувати інформацію між різними додатками завдяки використанню технології OLE.

Технологія Object Linking and Embedding (OLE) ґрунтується на зв'язуванні і впровадженні об'єктів за допомогою буфера обміну, що дозволяє робити обмін об'єктами і даними різних типів між документами. Об'єктом будемо називати довільний елемент, створений в будь-якому одному додатку (додатку-джерелі), який можна помістити в документ іншого додатку (додатку-приймача). Причому зробити це можна так, що разом із даними, що вставляються, буде збережена інформація про додаток, який створив зазначений об'єкт. Згодом це дає можливість здійснювати редагування об'єкта засобами додатку, що створив його. Об'єкти можуть бути малюнком, текстом, діаграмою, електронною таблицею, навіть звуковим файлом або відеокліпом.

При створенні комплексних документів, які містять дані різних типів, можна використовувати три види обміну даними, які відрізняються можливостями при їх редагуванні в складі цього комплексного документа. Розглянемо особливості кожного з них:

1) статичне переміщення і копіювання об'єктів – статично скопійований (чи переміщений) фрагмент буде сприйнятий

як уведений із клавіатури. З ним можна виконувати будь-які дії, припустимі в даному додатку, але зв'язок із джерелом цих даних буде втрачений. Виконується шляхом звичайного копіювання об'єкта за допомогою буфера обміну або шляхом перетягування мишею. Обсяг файла-приймача збільшується тільки на обсяг вставленого фрагмента. Доцільно використовувати в тому випадку, якщо немає необхідності надалі редагувати вставлені дані. Наприклад, текстовий редактор Microsoft Word має дуже обмежені можливості у редагуванні растрового графічного малюнка, статично вставленого з будь-якої графічної програми (обсяг и, яскравість відображення, спосіб взаємодії з текстом і деякі інші). Якщо статично скопіювати таблицю з Excel в документ Word, то вона буде сприйнята як звичайна текстова таблиця, створена у Word, і якщо вихідні дані на листі Excel містили елементи таблиці з формулами, то текстова таблиця міститиме лише значення відповідних формул, і вміст цих елементів не буде автоматично перераховуватись зі зміною даних;

2) *впровадження (embed)* – дані, поміщені в документ, зберігають зв'язок з додатком-джерелом, але не з файлом-джерелом. У цьому випадку є можливість їх редагування в тому додатку, в якому ці дані були створені (тобто для редагування табличних даних, створених у Excel і поміщених у текстовий документ, буде завантажений додаток Excel). Подвійний щиголь на впроваджених даних дає можливість виправлення фрагмента у вікні програми-приймача, але за допомогою елементів керування (рядка меню і панелей інструментів) програми-джерела. Обсяг файла-приймача збільшується значно, на обсяг усього файла-джерела, а не тільки на обсяг впроваджених даних (тобто до файла-приймача додається повна копія файла-джерела). Виконується копіюванням виділеного фрагмента у файлі-джерелі в буфер обміну стандартними способами, а потім у файлі-приймачі – через команди: *Правка → Спеціальна вставка → Вставити*. У списку **“Как”** обрати формат, що містить слово **“объект”**. Документ, що містить впроваджені дані, простіше підтримувати і обмінюватися ним;

3) *зв'язування (link)* – дані не містяться в документі-

приймачі. Замість цього файл-приймач запам'ятовує джерело даних. Якщо фрагмент даних зв'язати з текстовим документом, то дані будуть виглядати так само, як ті, що введені з клавіатури, але при збереженні файла на диску замість даних у ньому буде інформація про те, як знайти ці дані у файлі-джерелі. Якщо відбудеться зміна даних у джерелі, вони відобразяться й у приймачі. Обсяг файла-приймача збільшується тільки на обсяг посилання на файл-джерело. Але необхідно пам'ятати, що при передачі даних потрібно передавати обидва файли. При зв'язуванні вихідний документ (тобто файл-джерело) не можна переміщати або перейменовувати (або після цього відновити зв'язки). Виконується: *Правка* → *Спеціальна вставка* → *Связать*. Далі – аналогічно впровадженню.

Підсумуємо вищенаведене: при статичній вставці файл-приймач, образно кажучи, не “пам'ятає” ні файла-джерела, звідки вставлялися дані, ні додатка, у якому ці дані були створені; при впровадженні файл-приймач “пам'ятає” додаток, у якому ці дані були створені, але не “пам'ятає” файла-джерела; при зв'язуванні файл-приймач “пам'ятає” і файл-джерело впроваджених даних, і додаток, у якому вони були створені.

Впровадження і зв'язування дозволяють вставляти в документ дані, з якими додаток-приймач не може працювати безпосередньо. При вставці в текстовий документ звуку чи відео в тексті з'являється позначка, щиглом по якій можна відтворити звук чи відео.

2. Незважаючи на інтегрованість пакета Microsoft Office, кожна програма може бути використана автономно.

3. Програми пакета Microsoft Office мають єдиний інтерфейс, що значно полегшує їх використання (загальні команди, системи меню, діалогові вікна і процедури). Таким чином, навчившись користуватися одним додатком, можна застосувати ці знання в роботі з іншим.

4. Ідеальна сумісність усіх додатків пакета Microsoft Office з ОС Windows і використання усіх функціональних можливостей ОС Windows та апаратних можливостей ПК (завдяки розробці однією фірмою – Microsoft).

5. Використання гіперзв'язків для створення динамічних документів. Гіперзв'язок може бути встановлено з веб-сторінкою, документом Microsoft Office, адресою електронної пошти шляхом приєднання до мережних ресурсів, текстом, графічним зображенням і багатьма іншими об'єктами. Щиголь по гіперзв'язку дозволить перейти до цих об'єктів.

6. Можливість збереження файлів у різних форматах, зокрема у форматі HTML, що дозволяє використовувати пакет для створення веб-сторінок, розташовуваних у Інтернеті.

2.4. Склад пакета Microsoft Office, стисла характеристика основних додатків

1. *Microsoft Word* – додаток для створення й обробки документів. Загальний вигляд вікна програми Microsoft Word представлений на рисунку 2.1.

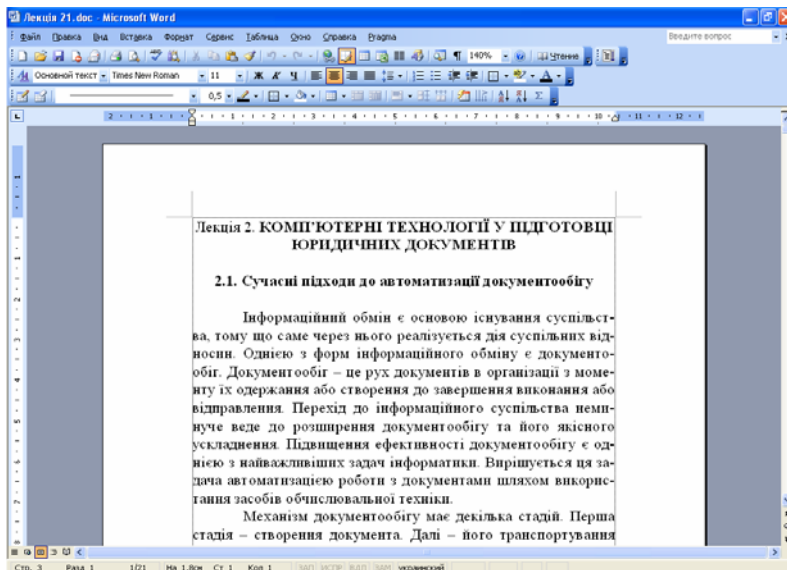


Рис. 2.1. Загальний вигляд вікна програми Microsoft Word.

Цей додаток формує за замовчуванням файли з розширенням doc, хоча користувач за своїм розсудом може зберігати файли з іншими розширеннями (dot – файл шаблону, rtf – текст у спеціальному форматі, що відключає макроси, txt – тільки неформатований текст, html – формат веб-сторінок та ін.). Документи, створені цим додатком, можуть містити текст, графіку, таблиці, звук, відеокліпи.

Microsoft Word забезпечує:

- введення, перегляд і редагування тексту;
- форматування символів тексту (використання різних шрифтів, їх обсягів, способу написання й кольору);
- зміну параметрів абзацу (його виділення, вирівнювання, міжрядковий інтервал);
- формування параметрів сторінки (обсяг паперу, орієнтація сторінки, поля і т. ін.);
- перевірку орфографії і граматики;
- виділення різних фрагментів тексту, їх копіювання, переміщення всередині документа і між додатками;
- тиражування документів;
- друк;
- формування, редагування, обробку таблиць;
- створення макросів (невеликих програм, що дозволяють автоматизувати виконання найбільш часто використовуваних дій);
- створення векторних графічних зображень і об'ємних текстових ефектів;
- підтримку формату HTML, що дозволяє здійснювати дизайн веб-сторінок і т. ін.

2. *Microsoft Excel* – програма керування електронними таблицями загального призначення, що використовується для обчислень, організації й аналізу ділових даних. Загальний вигляд вікна додатка представлений на рисунку 2.2.

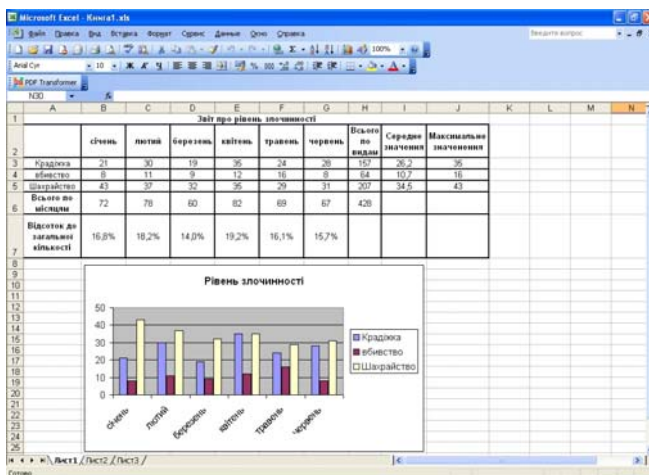


Рис. 2.2. Загальний вигляд вікна Microsoft Excel.

Це табличний процесор, орієнтований на обробку, в основному, числових даних, представлених у табличній формі. Дозволяє не тільки вводити дані в елементи таблиць, редагувати й форматовувати їх, а й застосовувати формули для опису зв'язку між значеннями в елементах таблиць. Розрахунок по заданих формулах виконується автоматично. Зміна значення в якому-небудь елементі таблиці приводить до автоматичного перерахунку значень всіх елементів таблиці, зв'язаних з нею формульними відносинами. Результати розрахунків можуть бути наочно проілюстровані діаграмами. Створена таблиця може бути надрукована. Створює файли з розширенням xls.

3. *Microsoft Access* – система керування базами даних (СУБД), яку можна використовувати для збереження, сортування й керування практично будь-якими типами даних. Створює та обробляє файли з розширенням mdb. Microsoft Access є реляційною СУБД, у якій логічно взаємозалежна інформація представляється у виді таблиці. Структура таблиці визначається сукупністю її стовпців і рядків, у кожному рядку таблиці містяться дані про один об'єкт бази даних. Записи можна порівнювати один з одним і з іншими джерелами даних для аналізу. Вміст такої бази може змінюватися в результаті сор-

тування запиту й інших операцій з даними. За допомогою СУБД Microsoft Access забезпечується рішення наступних основних задач:

- створення бази даних;
- занесення, редагування й видалення даних;
- упорядкування даних за будь-якими критеріями;
- вибір сукупності даних, що відповідають заданим критеріям;
- оформлення вихідних даних і т. ін.

4. *Microsoft Power Point* – засіб розробки демонстраційних матеріалів для електронної презентації з використанням слайдів (рис. 2.3.). Створює файли з розширенням ppt. Демонстраційний матеріал може містити текст, таблиці, діаграми, графіку, анімацію, звук та інші ефекти multimedia. Виходячи з того, що Power Point є складовою частиною пакета Microsoft Office, презентацію можна досить швидко підготувати, використовуючи фрагменти документів Microsoft Word, таблиць і діаграм Excel, даних Access. Створені в Microsoft Power Point презентації можна демонструвати на екрані ПК, моніторі великих обсягів чи декількох моніторах, на екрані за допомогою мультимедійного проектора чи діaproектора. Також можна вивести презентацію на друк при підготовці тез доповіді.

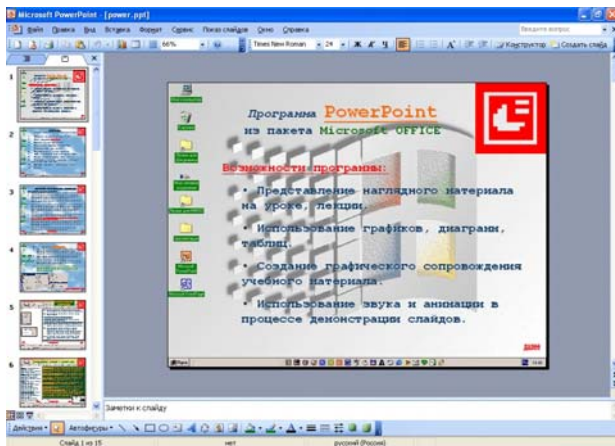


Рис. 2.3. Загальний вигляд вікна програми Power Point.

The screenshot shows the Microsoft Outlook 2010 application window. At the top, there's a ribbon with various tabs including 'Файл' (File), 'Правка' (Edit), 'Вид' (View), 'Справка' (Help), 'Действия' (Actions), and 'Оформление' (Appearance). Below the ribbon is a search bar and several quick launch icons. On the left side, there's a navigation pane with options like 'Почта' (Mail), 'Календарь' (Calendar), 'Контакты' (Contacts), 'Задания' (Tasks), 'Заметки' (Notes), and 'Список папок' (Folders). The main window area displays the 'Календарь' (Calendar) view for April 2010. A small calendar overview is visible on the left, showing the days of the month. The main calendar grid shows dates from 9 to 22, with the 26th of April highlighted. The status bar at the bottom indicates 'Всего элементов: 0' (Total items: 0).

Вирішення багатьох різноманітних завдань з планування й організації роботи можливе завдяки тому, що Outlook має наступні функціональні елементи:

- *Почта* – обробник повідомлень електронної пошти, але можуть оброблятися й документи, відправлені через локальну мережу;
- *Календарь* – календар і засіб створення розкладів, які повністю інтегровані з електронною поштою, контактами й ін-

шими засобами. Є можливість перегляду відомостей за конкретний день, тиждень, місяць;

- *Контакты* – поштова адресна книга з можливостями збереження відомостей про людей і організації, з якими відбувається спілкування;

- *Задачи* – призначений для планування конкретних робіт і контролю за їх виконанням;

- *Заметки* – використовують для запису питань, важливих думок, цінних зауважень, нагадувань і багато чого іншого, що звичайно записується в паперовий блокнот;

- *Дневник* – автоматично записуються вибрані користувачем дії, що мають відношення до вибраних контактів; ці дії розташовуються на часовій шкалі.

Усі названі елементи являють собою набір фільтрів єдиної бази, тобто вся інформація зберігається в одному масиві, робота з яким відбувається на основі визначеного набору файлів.

6. *Microsoft Front Page* – додаток, призначений для створення веб-публікацій. Не входить до стандартного складу пакета Microsoft Office, але його можливо придбати окремо. Дозволяє дуже легко створювати професійні веб-сайти навіть без знання мови HTML (або знання в мінімальному обсязі). Матеріали з файлів, підготовлених за допомогою додатків Microsoft Office або інших додатків, дуже просто перенести у веб-сторінки Front Page копіюванням за допомогою буфера обміну або механізму drag-and-drop, а програма самостійно генерує відповідний HTML-код. Під час роботи зразу можна бачити сторінку в тому вигляді, якою вона буде відображена у веб-браузері.

7. *Microsoft Office Publisher* – дозволяє створювати та редагувати буклети, брошури, оголошення, бюлетені, веб-вузли й т. ін.

8. Крім комплексу корисних додатків пакет Microsoft Office має *набір додаткових корисних утиліт*, які виконують обслуговуючі функції. Отримати доступ до цих утиліт можна наступним чином: *Пуск*→*Все программы*→*Microsoft Office*→*Средства Microsoft Office*. До складу утиліт входять:

- *Microsoft Access Snapshot Viewer* – засіб перегляду знімків звітів, містить копію кожної сторінки звіту Microsoft

Access з високою точністю відтворення, дозволяє переглядати та друкувати звіти Microsoft Access;

- *Microsoft Office Document Scanning* – забезпечує сканування багатосторінкових документів із застосуванням будь-якого встановленого сканера та розпізнавання тексту в графічних документах;


- *Microsoft Office Document Imaging* – дозволяє переглядати відскановані документи на екрані, здійснювати перекомпоновку багатосторінкових документів, виділення і обробку розпізнаного тексту, розстановку приміток у відсканованих документах і електронних факсах і відправку документів електронною поштою і факсом;

- *Microsoft Office Picture Manager* – робить можливим систематизацію, редагування та використання графічних файлів, забезпечує гнучкі засоби управління, редагування та сумісного використання рисунків. Можна корегувати вид рисунків, змінюючи наступні їх параметри: обсяг, яскравість і контрастність, колір, обрізання, поворот і відбиття, усунення ефекту червоних очей.

9. *Довідкова система програм пакета Microsoft Office.* Microsoft Office робить спілкування з довідковою системою простим, зрозумілим, комфортним, надаючи декілька зручних способів отримання інформації під час роботи в будь-якому додатку. Кожний з них має наступні інструменти:

- *Справка (F1)* – дозволяє або ввести питання самостійно, або обрати потрібне питання з відповідного розділу довідкової системи, скориставшись тематично підібраним змістом;

- *Помощник Microsoft Office* – відповідь на запитання, що цікавить. Містить дуже потужну базу даних відповідей на найпоширеніші запитання;

-  (*Что это такое?*) – така позначка з'являється в деяких вікнах діалогу; з її допомогою можна “вказати пальцем” на будь-який елемент додатка, якщо необхідно довідатися про нього докладніше;

- *Office в Інтернет* – забезпечує зв'язок з веб-вузлом Microsoft Office Online, який містить зовсім нові або оновлені відомості, які корпорація Microsoft постійно додає, а також має

можливість отримати рекомендації та поради від більш досвідчених користувачів.

Контрольні питання

1. Дайте визначення документообігу.
2. Назвіть стадії документообігу та розкажіть про можливості їх автоматизації.
3. Які причини, що сприяють процесу автоматизації документообігу? Обґрунтуйте власну думку.
4. Визначте поняття “електронний документообіг”.
5. Що собою являють системи електронного документообігу (СЕД)?
6. Назвіть найпопулярніші СЕД, які використовуються в Україні.
7. Які нормативні документи є підґрунтям для застосування електронного документообігу в Україні?
8. Чи вважаєте ви, що пакет Microsoft Office є однією з можливостей автоматизації процесу документообігу? Обґрунтуйте власну думку.
9. Які основні переваги пакета Microsoft Office і причини його популярності?
10. Назвіть відомі вам версії пакета Microsoft Office та його склад.
11. Дайте загальну характеристику додатку Microsoft Word, назвіть його основні можливості.
12. Визначте загальне призначення додатка Microsoft Excel та його можливості.
13. Стисло охарактеризуйте наступні додатки: Microsoft Access, Microsoft Power Point, Microsoft Outlook, Microsoft Office Publisher, Microsoft Front Page. У чому полягає загальне призначення кожного з них?
14. Які ще корисні утиліти є в складі пакета Microsoft Office?

ЗАСТОСУВАННЯ ПРОГРАМ ПАКЕТА MS OFFICE

3.1. Основні функціональні можливості текстового процесора MS Word при створенні юридичних документів

Microsoft Office Word – текстовий процесор, доступний під Windows і Apple Mac OS X. Дозволяє створювати документи високого ступеня складності. Підтримує технологію OLE, модулі сторонніх розробників, що підключаються, шаблони, захист документа, макроси та ін. Головні конкуренти – OpenOffice Writer, StarOffice Writer, Corel WordPerfect і Apple Pages.

Основні можливості редактора викладені в рамках дисципліни ОІОТ, тому розглянемо лише окремі прийоми роботи в Microsoft Word.

Поняття шаблону. Кожен документ Microsoft Word оснований на шаблоні. Шаблон – це бібліотека стилів, яка визначає основну структуру документа і містить його настройки, такі як елементи автотексту, шрифти, необхідні поєднання клавіш, макроси, меню, параметри сторінки, форматування і стилі. Шаблони дозволяють використовувати один і той самий стиль у різних текстових документах. Загальні шаблони, включаючи шаблон Normal.dot, містять настройки, доступні для всіх документів. Шаблони документів, наприклад, записок або факсів у діалоговому вікні *Шаблони*, містять настройки, доступні тільки для документів, оснований на відповідних шаблонах.

Користувач може одержати доступ до наступних шаблонів Microsoft Word:

- шаблони Microsoft Word на локальному комп'ютері – виконати *Файл*→*Створити* і в правій панелі вікна вказати *Шаблони на моєму комп'ютері*;

- шаблони Microsoft Office Online. Microsoft Office Online – це веб-вузол, створений компанією Microsoft на допомогу ко-

ристувачам Microsoft Office. На цьому вузлі розташовується довідка і підтримка, перевірка оновлень Microsoft Office, різні шаблони і пробні версії варіантів. Для доступу виконати *Файл→Создать* і в правій панелі вікна вказати *Шаблоны на узле Office Online*;

– створення файлу на підставі шаблону, розташованого на ваших веб-серверах. Для доступу виконати *Файл→Создать* і в правій панелі вікна вказати *На моих веб-узлах*. У полі *Имя файла* введіть Інтернет-адресу або адресу внутрішньої мережі і шлях до шаблону. Для відкриття натисніть кнопку *Открыть*;

– створення власного шаблону – ввести текст шаблону або відкрити документ, який треба перетворити на шаблон, виконати: *Файл→Сохранить как...* Указати *Тип файла→Шаблон документа* і дати шаблону ім'я. Доступ до створеного шаблону здійснюється так само, як і до шаблону на локальному комп'ютері.

Швидкий перехід по тексту – при роботі з багатосторінковими документами доводиться здійснювати перехід у межах тексту. Для швидкого переходу виконати *Правка→Перейти* (або натиснути комбінацію клавіш Ctrl+G). З'явиться вікно *Найти и заменить* з відкритою вкладкою *Перейти*. Дана вкладка дозволяє перейти до потрібної сторінки, закладки, рядка, виноска, розділу, примітки тощо.

Пошук фрагмента тексту – виконується в багатосторінкових документах по слову або словосполученню. Результат пошуку – виділене вказане слово або словосполучення на поточній сторінці або нижче по тексту. Для пошуку фрагмента виконати *Правка→Найти* і ввести слово або словосполучення для пошуку. Для підвищення релевантності пошуку можна натиснути кнопку *Больше* і виконати налаштування параметрів пошуку.

Закладка – використовується для прискореного доступу до найбільш використовуваних сторінок у багатосторінковому документі. Установіть курсор в місці, на яке буде здійснюватися перехід при використанні закладки, виконайте *Вставка→Закладка*. Введіть ім'я закладки. Ім'я закладки починається з літери і може містити тільки літери і цифри. Документ може ма-

ти декілька закладок. Для того, щоб скористатися закладкою, слід знов виконати *Вставка*→*Закладка*, вказати потрібну закладку, натиснути *Перейти*.

Гіперпосилання – текст документа може містити елементи (слова, символи, значки, малюнки і т. ін.), при натисканні на які буде здійснений автоматичний перехід на інший файл, який може знаходитися на вашому ПК, на ПК вашої локальної мережі або в Інтернеті, а також перехід в інший розділ поточного документа.

Існують два види гіперпосилань – абсолютне і відносне. Абсолютне гіперпосилання – це гіперпосилання, що містить повну адресу файла або веб-вузла. Наступна адреса є прикладом такої повної адреси в абсолютному гіперпосиланні: <http://www.microsoft.com/support>.

Відносне гіперпосилання містить адресу щодо адреси файла призначення. Адреса файла призначення також відома як база гіперпосилання.

База гіперпосилання – це спільно використовуваний у файлі шлях, що вказує на файл, у якому міститься гіперпосилання на файл призначення.

Наприклад, документ має наступну базу гіперпосилання: C:\Documents and Settings\Username\My Documents.

Документ “Sales.doc” розташований по наступному шляху: C:\Documents and Settings\Username\My Documents\April\Sales.doc.

Відносне гіперпосилання на документ містить тільки відносну адресу Sales.doc. Тому воно містить наступну адресу: April\Sales.doc.

Для створення гіперпосилання слід в потрібному місці документа виділити якийсь елемент документа (слово, позначку, літеру, малюнок тощо), викликати контекстне меню виділеного елемента, або ж просто викликати контекстне меню і виконати команду *Гиперссылка*. У переліку *Связать с...* задати об’єкт, на який посилається гіперпосилання – файл, веб-сторінку, новий документ, адресу електронної пошти. Для створення гіперпосилання на файл або веб-сторінку треба задати шлях до файла або адреси веб-сторінки. Щоб створити гіперпосилання на певному місці в поточному документі, це місце попередньо треба позна-

чити закладкою і послатися на неї.

Заміна слова в тексті – використовується у випадках некоректного перекладу або орфографічної помилки, що повторюється в тексті. Виконати *Правка*→ *Заменить*, ввести помилкове слово и слово, на яке його треба замінити. Залежно від вибору користувача відбудеться заміна або першого знайденого помилкового слова, або в усьому тексті. Заміна виконується тільки в тій графічній формі, в якій слово вказане у вікні *Заменить на...*

Вставка об'єкта в текстовий документ. Текстовий документ може бути оформлений різноманітними об'єктами – малюнками, таблицями, діаграмами, відеокліпами, аудіофрагментами тощо. Для їх вставки в текстовий документ виконати: *Вставка*→*Объект*.

Якщо об'єкт вже існує у вигляді файла відповідного типу, перейдіть на вкладинку *Создание из файла* и за допомогою кнопки “*Обзор*” вкажіть шлях до потрібного файлу та тип зв'язку з відповідним додатком. Текстовий редактор Word підтримує технологію OLE – технологію роботи з документом, складові частини якого (об'єкти) розроблені в різних додатках. Для подальшої роботи з упровадженими об'єктами Word автоматично завантажить потрібний додаток.

Якщо об'єкт треба створити, на вкладці *Создать* слід указати тип об'єкта і за допомогою відповідного додатка створити його або обрати із переліку наявних файлів.

Створення списків. Багаторівневі списки використовуються для переліку об'єктів за відповідною класифікацією. Наприклад:

1. Апаратна частина ПК
 - 1.1. Системна плата
 - 1.2. Накопичувачі
 - 1.3. Периферійні пристрої
2. Програмне забезпечення ПК
 - 2.1. Системне ПЗ
 - 2.1.1. Операційні системи
 - 2.1.2. Утиліти
 - 2.2. Інструментальне ПЗ

Для створення багаторівневого списку треба виділити

потрібні абзаци, які містять його елементи, викликати контекстне меню, виконати: *Список*. У вікні, що з'явилося, перейти на вкладку *Многоуровневый* і вибрати потрібний тип багаторівневого списку (в даному випадку другий тип).

Після цього слід виділити елементи другого рівня, викликати контекстне меню і виконати: *Увеличить отступ*. Аналогічно створюються елементи третього рівня (для їх створення потрібно двічі натиснути кнопку *Увеличить отступ*, оскільки при кожному її натисканні відбувається переміщення на наступний рівень).

Стильове форматування – це форматування тексту з використанням стилів. Якщо задати для абзаци потрібний стиль, то редактор автоматично відформатує цей абзац, вибравши певний шрифт, параметри абзаци, мову, обрамлення, нумерацію і т. ін. Якщо змінити характеристики стилю, то також автоматично зміняться відповідні характеристики всіх абзацив згідно з обраним стилем. У текстовому редакторі Word існує велика кількість стилів, але зазвичай використовуються наступні:

Заголовок 1 – для назви розділів;

Заголовок 2 – для назви параграфів;

Обычный – для звичайного тексту.

Для задання потрібного стилю слід установити курсор на відповідному абзаци. Потім задати потрібний стиль з розкритого списку в панелі інструментів або виконати: *Формат* → *Стили и форматирование* і в правій частині вікна вказати необхідний стиль.

Зміст документа – це список назв розділів, параграфів тощо із зазначенням сторінки. Для автоматичного створення змісту потрібно заголовки розділів і підрозділів виділити відповідними стилями. Заголовки розділів першого рівня (наприклад, ВВЕДЕННЯ, ВИСНОВОК, назви розділів) виділяємо стилем *Заголовок 1*, заголовки підрозділів – стилем *Заголовок 2* і т. д. Потім слід встановити курсор в місце формування змісту і виконати: *Вставка* → *Ссылка* → *Оглавление и указатели*. У вікні, що з'явилося, потрібно перейти на вкладку *Оглавление* і задати кількість рівнів змісту (якщо в документі є тільки розділи і підрозділи, то буде всього два рівні, якщо у підрозділах є парагра-

фи – це три рівні і т.д.).

Для автоматизації багаторазового виконання часто виконуваних з документом робіт створюються макроси, наприклад, для прискорення часто виконуваних операцій редагування або форматування, об'єднання декількох команд (для вставки таблиці з вказаними обсягами і межами і певним числом рядків і стовпців), спрощення доступу до параметрів у діалогових вікнах, автоматизації обробки складних послідовностей дій в документах тощо.

Макрос (або макрокоманда) – це послідовність заданих користувачем команд, що має ім'я і зберігається у формі стандартного програмного модуля на мові програмування Visual Basic for Application (VBA) або “Visual Basic для додатків”. VBA є середовищем програмування, розробленим спеціально для створення макросів у додатках. Це мова програмування, підтримувана всіма додатками пакета Microsoft Office. Макрос об'єднує всі інструкції в одному сценарії, який потім можна викликати за допомогою команди меню, кнопки панелі інструментів або комбінації клавіш. Список інструкцій, складових макросу, як правило, складається з макрооператорів.

Для створення макросів у Microsoft Word існують два методи:


1. Використання засобу для розробки макросу.

1. У меню *Сервіс* виконайте: *Макрос*→*Начать запись*.
2. У полі *Имя макроса* введіть ім'я нового макросу. Ім'я повинне починатися з букви, містити тільки букви і цифри.
3. У списку *Макрос доступен для* виберіть шаблон або документ, у якому зберігатиметься макрос.
4. Введіть опис макросу в поле *Описание*.
5. Якщо макросу не потрібно призначати кнопку панелі інструментів, команду меню або поєднання клавіш, натисніть кнопку **ОК**, щоб почати запис макросу.
6. Щоб призначити макросу кнопку панелі інструментів або команду меню, натисніть кнопку *Панели* і перейдіть на вкладку *Команды*. Виберіть записуваний макрос в списку *Команды* і перетягніть його на панель інструментів або в меню. Натисніть кнопку *Закрыть*, щоб почати запис макросу.

7. Щоб призначити макросу поєднання клавіш, натисніть кнопку *клавіатура*. Виберіть записуваний макрос в списку *Команды*, введіть поєднання клавіш у поле *Новое сочетание клавиш* і натисніть кнопку *Назначить*. Натисніть кнопку *Закрыть*, щоб почати запис макросу.

8. Виконайте дії, які слід включити в макрос.

При записі нового макросу допускається застосування миші тільки для вибору команд і параметрів. Для запису таких дій, як виділення тексту, необхідно використовувати клавіатуру. Наприклад, за допомогою клавіші F8 можна виділити текст, а за допомогою клавіші END – перемістити курсор у кінець рядка.

9. Для завершення запису макросу натисніть кнопку *Остановить запись* .

II. Програмування макросу за допомогою Visual Basic для додатків.

1. Виконайте: *Сервис*→*Макрос*→*Макросы*.

2. У списку *Макросы из* виберіть шаблон або документ, в якому зберігатиметься макрос.

3. У полі *Имя макроса* введіть ім'я нового макросу.

4. Натисніть кнопку *Создать*, щоб викликати редактор Visual Basic.

Поради щодо запису і використання макросів:

1. Перед записом макросу заплануйте заздалегідь кроки й команди, які він повинний виконати. Якщо під час запису буде допущена помилка, то в макросі також запишуться всі виправлення. Непотрібні інструкції можна буде прибрати пізніше шляхом редагування макросу.

2. Ім'я макросу повинне починатися з букви, в ньому не можна використовувати пропуски і символи пунктуації.

3. При створенні макросу, пов'язаного з форматуванням символів, для запису таких дій, як виділення тексту, не слід використовувати клавіші зі стрілками. Текст можна виділити за допомогою клавіші F8, а перемістити в початок і кінець рядка – за допомогою клавіш Home і End відповідно. Дії і параметри можна

обирати за допомогою миші, проте рухи миші не протоколюються. Наприклад, мишу не можна використовувати для виділення, копіювання, вставки і перетягування елементів. Для запису цих дій слід користуватися клавіатурою.

4. Якщо макрос викликає команду *Найти* або *Заменить*, натисніть кнопку *Больше* на вкладці *Найти* або *Заменить*, а потім виберіть параметр *Везде* в списку *Направление*. Якщо макрос виконує пошук тільки вперед або назад, то після досягнення кінця або початку документа Word припинить виконання макросу і запропонує продовжити пошук у частині документа, що залишилася.

5. Текст, що вводиться при створенні макросу, записується в ньому. Це дозволяє, наприклад, за допомогою макросу отримувати таблиці, в першому рядку яких (у так званій “шапці таблиці”) будуть представлені необхідні заголовки стовпців.

6. Перед використанням макросу, записаного в іншому документі, переконайтеся, що він не залежить від змісту цього документа.

7. Якщо певний макрос використовується надто часто, призначте йому кнопку панелі інструментів, команду меню або поєднання клавіш. Це дозволить швидко викликати макрос без відкриття діалогового вікна *Макросы*.

Захист документа. Засоби Word дозволяють захистити документ від:

- форматування і/або редагування. Виконати: *Сервис*→*Защитить документ*, у правій панелі вікна встановити потрібні режими і ввести пароль;

- відкриття. Виконати: *Сервис*→*Параметры*→*Безопасность* і встановити пароль для відкриття файлу. Там же задаються параметри сумісного використання для даного документа.

3.2. Робота з файлами інших форматів, що можуть містити текст

PDF (Portable Document Format) – це формат електронних документів, розроблений компанією Adobe Systems, переносимий формат документів, створений як засіб міжплатформеного обміну даними. У першу чергу, він призначений для представлення в електронному вигляді поліграфічної продукції; переважна частина сучасного професійного друкарського устаткування може обробляти PDF безпосередньо.

Формат не накладає ніяких обмежень на зовнішній вигляд документа. Документ у форматі pdf може містити текст, векторну і растрову графіку, шрифти, графіку, мультимедійні елементи, об'єднані довільно, що гарантує правильне відображення незалежно від операційної системи програмного забезпечення і призначених для користувача налаштувань конкретного комп'ютера. Саме ця властивість – зберігати початковий вигляд – і робить його привабливим. Необхідність швидкого переміщення по сторінках і об'єктах документа зумовила ієрархічну структуру даних PDF. На початку файлу знаходиться зміст, що показує де і які об'єкти у ньому розташовані, потім йдуть самі дані. Будь-які дії можливі за наявності всього PDF-файла, оскільки фрагмент даних, який знадобиться першим, може знаходитися в будь-якій його частині, у тому числі й у самому кінці файлу. Для документів з явним переважанням тексту і векторної графіки формат PDF, як правило, забезпечує помітне скорочення об'єму файлу (з відповідним скороченням часу пересилки по мережі і т. д.).

Для читання документів використовують як безкоштовну програму Adobe Acrobat Reader, так і сторонні розробки. Зазвичай програми перегляду розповсюджуються безкоштовно, а програми, що дозволяють не тільки переглядати, а й редагувати pdf-файли – на комерційній основі.

Формат PDF має наступні переваги:

– *кросплатформеність*: документ містить необхідні для правильного відображення елементи і виглядає однаково на будь-якій платформі й при будь-якому застосуванні. Кросплатформеність формату створює зручні умови для організації елект-

ронного документообігу;

- *компактність*: різні алгоритми компресії (архівації) дозволяють ефективно стискати як текст, так і графіку;

- *інтерактивність*: у pdf-файлі можна використовувати мультимедіа (відео-, аудіоролики), гіперпосилання, форми, дані з яких зберігаються в зовнішніх базах даних;

- *безпеку*: формат підтримує багаторівневий механізм захисту й перевірки достовірності. Є можливість встановити пароль на перегляд/редагування, створити електронний підпис для ідентифікації автора.

Недоліки у форматі також є. PDF охоплює безліч стандартів, що не дозволяє ефективно використовувати його в конкретних цілях. Наприклад, формат можна використовувати для створення сторінок або сайтів веб-сервером, але html справляється з цим завданням краще. PDF зберігає точну візуальну копію документа, але не його логічну структуру. Як наслідок, PDF достатньо складно редагувати.

Інші програми для роботи з PDF в Microsoft Windows

- Microsoft Office 2007 – у пакет оновлень SP2 вбудована функція експорту будь-яких документів у PDF, тобто перетворення pdf-файлів у doc не вимагає використання додаткових програм.

- Foxit Reader – умовно-безкоштовна програма для перегляду PDF-файлів у Microsoft Windows. Ємність програми складає 3,5 Мб, установки не вимагає.

- Sumatra PDF – вільна (GPLv2) програма для перегляду PDF-файлів у Microsoft Windows.

- ABBYY PDF Transformer – власна програма під Windows NT від 5.0 для створення і перетворення PDF-файлів з будь-якого офісного застосування і перетворення PDF-файлів в документи редагованих форматів (Microsoft Word, RTF і ін.).

- PDFCreator вільна програма для створення файлів PDF. Може використовуватися з будь-яким додатком Microsoft Windows, що має можливість друку документів.

- Scientific and technical documentation utility (STDU) Viewer – безкоштовна для некомерційного використання програма для читання PDF і DJVU файлів, Converter – платна про-

грама для перетворення формату DJVU в PDF.

Онлайнові

- Scribd

Формат DjVu (від фр. *deja vu* – вже бачене) графічний формат, розроблений фірмою AT&T, оптимізований для зберігання відсканованих документів. Існує два традиційні способи зберігання відсканованої книги: розпізнавання (OCR) з подальшою підготовкою повноцінного текстового електронного документа або скани – відскановані картинки, часто зібрані в pdf-документ. У першому випадку потрібно багато копіткої роботи, в другому – виходять файли обсягом у десятки і навіть сотні мегабайт. Компромісний варіант – це переклад відсканованих картинок у формат DjVu. При цьому текст і контрастні малюнки зберігаються із здатністю 300dpi, все решта вважається фоном і зберігається із зниженим дозволом. Це дозволяє стиснути електронний документ без втрати можливості його прочитання. Суть технології DjVu полягає в автоматичному діленні зображення на декілька ділянок (наприклад, текст, логотип фірми і растрова фотографія), для кожного з яких вибирається оптимальний для даного графічного образу алгоритм стиснення. Технологія DjVu забезпечує для файлів з чорно-білими монохромними зображеннями стиснення порядку 500:1. Виграш у обсяг і файла в порівнянні з форматом GIF складає в середньому 20 разів. У DjVu обсяг файла відсканованої книги можна одержати в межах декількох мегабайт, що цілком прийнятно. Особливого значення цей формат набуває для перенесення в мережу технічної, зокрема математичної літератури, де велику кількість схем і формул робить розпізнавання і переклад у текстовий формат практично нездійсненним. Він також ефективний у випадках, коли необхідно передати всі нюанси оформлення, наприклад, історичних документів, де важливе значення має не тільки зміст, а й колір і фактура паперу, дефекти пергаменту (тріщини, сліди від складання), виправлення, плями, відбитки пальців; сліди, залишені іншими предметами.

Формат DjVu стає фактичним стандартом для електронних бібліотек технічної і наукової літератури.

Величезна кількість книг у цьому форматі доступна в

файлообмінних мережах.

Формат оптимізований для передачі по мережі таким чином, що сторінку можна переглядати ще до завершення скачування. DjVu-файл може містити текстовий (OCR) шар, що дозволяє здійснювати повнотекстовий пошук по файлу. Крім того, DjVu-файл може містити вбудований інтерактивний зміст і активні ділянки посилання, що робить зручною навігацію в DjVu-книгах.

Програми для роботи з форматом DjVu

- **DjVu Browser plugin 6.1** – розроблений фірмою LizardTech, вільно поширюваний плагін для переглядання файлів формату djvu. Після установки DjVu файли відкриваються у вікні браузера (підійде майже будь-який – IE, Firefox, Safari).

- **DjVu Solo 3.1** – програма для створення DjVu - файлів. У DjVu можна перетворити графічні файли більшості популярних форматів (bmp, gif, jpeg, tiff і ін.) або безпосередньо отримати картинку зі сканера. Останнє не дуже зручно, оскільки відсутні навіть прості засоби роботи з графікою, що дозволяють, наприклад, обрізати чорні краї відсканованої картинки, повернути її тощо.

- **STDU Viewer ver 1.2** – нова програма для переглядання документів у djvu-, pdf- і tiff- форматах. Може служити не тільки для читання djvu, але і як компактна заміна Acrobat reader'у.

- **WinDjView-0.4.3** – зручна невелика програма для переглядання djvu-файлів.

- **DjVuReader v. 2.0.0.26** – зручна програма для переглядання DjVu.

- **DjVu Fancy Viewer** – програма-переглядач. Дозволяє створювати закладки в DjVu-документі і зберігати їх усередині djvu-файла. Може показувати здвоєні розвороти, красиво перегортає сторінки.

- **Any2djvu** – веб-сервер-сервіс, що здійснює перетворення практично будь-якого графічного формату в DjVu. Особливо корисне перетворення в DjVu форматів pdf, ps і ps.gz. Документи для перетворення можна не тільки завантажувати з власного комп'ютера, а й указувати url документа, що цікавить вас, у мережі.

CHM (Compiled HTML) – спочатку формат CHM був створений для формування зручної і функціональної довідкової системи до програм Windows. Цей формат часто використовується не тільки для створення хелп-систем до ПО, а й для видання книг в електронному вигляді. Найсильнішою стороною цього формату є наявність у CHM-файлах повнотекстового пошуку. Коротко файл CHM – це набір скомпільованих HTML-файлів, іншими словами, щось подібне до архіву з веб-сторінок. Діє CHM-файл за принципом архіву, стискає дані, що зберігаються в ньому, проте не всі, а тільки текстові або такі, що містять текст, відформатований за допомогою тегів HTML (HTML, TXT, CSS і файли інших форматів). Для читання файлів формату CHM використовуються програми CHMReader, FBReader та ін.

fb2 (FictionBook) – формат представлення електронних версій книг у вигляді XML-документів, де кожен елемент книги описується своїми тегами. Стандарт покликаний забезпечити сумісність з будь-якими пристроями і форматами. XML дозволяє легко створювати документи, готові до безпосереднього використання і програмної обробки (конвертації, зберігання, управління) у будь-якому середовищі. Документи, що зазвичай мають розширення .fb2, можуть містити структурну розмітку основних елементів тексту, деяку кількість інформації про книгу, а також вкладення з двійковими файлами, в яких можуть зберігатися ілюстрації або обкладинка. fb2 чудово дозволяє організувати структуру книги (розділи, підзаголовки, вірші, цитати тощо), вставляти в текст ілюстрації. Він без проблем читається як на РС, так і на КПК. Правильно підготовлений електронний текст у форматі FictionBook містить у собі всю необхідну інформацію про книгу – структурований текст, ілюстрації, інформацію про автора і видання, але не містить інформації про зовнішній вигляд документа. Як виглядатиме текст, отриманий з формату .fb2, залежить або від налаштувань програми-переглядача цього формату, або від параметрів, заданих при конвертації файла в інший формат. Для читання файлів формату .fb2 використовується програма FBReader, CoolReader та ін.

iSilo (Plam Os Platform /pdb - Palm Pilot Database format) – формат бази даних, використовується у всіх 3Com

PalmPilot, IBM Workpad і Macintosh/PC для збереження записів у базі даних. Обсяг одного запису може перевищувати 64 кб, є біти BackUp і т. д. Через в'ювер від iSilo книги у форматі PDB виглядають як у форматі СНМ. Які-небудь переваги цього формату для кінцевого користувача не відмічені, проте зустрічаються велими цікаві книги, скопійовані в PDB.

3.3. Використання можливостей Excel для статистичної обробки правових даних та побудова діаграм

Електронна таблиця – це засіб інформаційних технологій, прикладна програма, що дозволяє вирішувати наступні завдання:

- автоматизацію обчислень – автоматичну реалізацію обчислювальних завдань, які раніше можна було виконати тільки шляхом програмування;

- математичне моделювання – використання математичних формул дозволяє описати взаємозв'язок між різними параметрами системи або процесу. Можливість автоматичного обчислення формул і функцій при зміні значень вхідних у них операндів робить електронну таблицю зручним інструментом для організації чисельного експерименту:

- 1) підбір параметрів;
- 2) прогноз поведінки модельованої системи;
- 3) аналіз залежностей;
- 4) планування;

- використання електронної таблиці як бази даних. Електронні таблиці дозволяють виконувати дії, властиві СУБД, – пошук інформації за заданими умовами і сортування інформації;

- графічне представлення (у вигляді графіків, діаграм) числової інформації, що міститься в таблиці.

Одним із найпопулярніших табличних процесорів є MS Excel, що входить до складу пакета Microsoft Office.

Microsoft Excel – програма для роботи з електронними таблицями, створена корпорацією Microsoft для Microsoft Windows, Windows NT і Mac OS. Вона надає можливості економіко-статистичних розрахунків, графічні інструменти і мову ма-

кропрограмування VBA. Microsoft Excel входить до складу Microsoft Office, і на сьогоднішній день Excel є одним із найбільш застосовуваних у світі.

Версії Microsoft Excel для операційної системи Windows:

- 2001 р. – Excel 2002 (10) – Microsoft Office XP;
- 2003 р. – Excel 2003 (11) – Microsoft Office 2003;
- 2007 р. – Excel 2007 (12) – Microsoft Office 2007.

Створення і редагування таблиць. Документ Excel називається робочою книгою. Робоча книга – це набір робочих листів, розділених на рядки і стовпці, на перетині яких утворюються комірки. Імена рядків – це їх номери. Рядки мають номери від 1 до 65536. Імена стовпців – літери латинського алфавіту від **A** до **Z**, потім від **AA** до **AZ**, **BA** до **BZ** і т. д. Додати або видалити лист можна, викликавши контекстне меню ярлика листа в лівому нижньому кутку і виконавши команду *Додати* або *Удалити*. У комірку робочого листа можна вводити константи і формули. Константи розділяються на наступні категорії: числові значення, текстові значення, значення дат і часу, логічні значення і помилкові значення.

Якщо стандартна ширина стовпця недостатня для розміщення в ній даних, то Excel виводить або округлене значення, або рядок символів ####. Обсяг и комірок можуть бути змінені: встановити курсор на роздільнику заголовків стовпців або на роздільнику між номерами рядків і виконати буксирування.

Для розташування даних у комірці в декілька рядків треба викликати контекстне меню виділених комірок і виконати: *Формат ячеек*→*Выравнивание*, встановити: *Отображение*→*Переносит по словам* і змінити обсяг комірок. Вибір режиму *Автоподбор ширины* зменшує обсяг символів у виділеній комірці так, щоб вони повністю помістилися у комірці.

Для виділення блоку комірок треба виконати наступні дії:

- 1) виділення суміжних комірок – буксирування по комірках;
- 2) виділення несуміжних комірок – клацнути по першій комірці сукупності, потім при натиснутій клавіші [Ctrl] клацати по решті комірок сукупності;
- 3) виділення всіх комірок робочого листа – клацнути мишею по кнопці, розташованій на перетині адресних смуг.

3.2.1. Введення та редагування даних

Щоб почати редагування, слід клацнути по комірці, ввести дані. Для редагування змісту комірки двічі клацнути по комірці і внести виправлення. Для переміщення даних слід виділити комірку, підвести покажчик миші до межі виділеної комірки так, щоб курсор перетворився на звичайну стрілку миші, виконати буксирування до комірки, в яку переміщуються дані.

Для встановлення маркера заповнення виконати: *Сервис→Параметры→Правка→Перетаскивание ячеек*. При цьому в нижньому правому кутку виділеної комірки з'являється маленький чорний квадрат – маркер заповнення. При установці на маркер заповнення покажчик миші приймає вигляд тонкого чорного хрестика.

Маркер заповнення використовується для автоматичного введення в таблицю значень із списку автозаповнення, який створюється:

- вихідний список – *Сервис→Параметры→Списки* – виділити **НОВЫЙ СПИСОК** і ввести елементи списку, розділяючи їх комами;

- із значень, наявних у таблиці, виділити діапазон комірок, де містяться потрібні значення, виконати: *Сервис→Параметры→Списки→Импорт*.

Для використання списку автозаповнення слід ввести в комірку будь-який елемент із списку і відбуксирувати маркер заповнення в будь-якому напрямку, щоб ввести елементи списку в суміжні комірки.

Для використання автоматичного введення даних з постійною зміною слід ввести в першу комірку діапазону початкове значення, виділити діапазон для автоматичного заповнення даними і виконати: *Правка→Заполнить→Прогрессия*.

Дані в таблиці виводяться на екран у певному форматі. Якщо дані не відповідають заданому формату, то вони неправильно відображаються. Щоб установити потрібний формат, слід викликати контекстне меню комірок, виконати: *Формат ячеек→Число*.

3.2.2. Сортування й фільтрування даних

Сортування даних – це впорядкування записів у таблиці. Для виконання сортування слід виділити блок комірок, виконати: *Данные*→*Сортировка...*, задати порядок сортування.

Фільтрація даних – дозволяє знаходити і відбирати для обробки частину записів. Дані виводяться на екран у вигляді відфільтрованого списку, тобто лише ті рядки, які містять певні значення або відповідають певним критеріям. Excel містить два варіанти фільтрації: автофільтр і розширений фільтр.

1) автофільтр здійснює швидку фільтрацію списку відповідно до вмісту комірок або відповідно до простого критерію пошуку.

Для використання автофільтру потрібно:

- встановити курсор усередині таблиці;
- вибрати команди *Данные*→*Фильтр*→*Автофильтр*.

Заголовний рядок списку в режимі автофільтру містить у кожному стовпці кнопку зі стрілкою. Клацання розкриває списки, елементи якого беруть участь у формуванні критерію. Кожне поле (стовпець) може використовуватися як критерій;

○ розкрити список стовпця, по якому проводитиметься вибірка;

○ вибрати значення або умову і задати критерій вибірки в діалоговому вікні *Пользовательский автофильтр*.

Для відновлення всіх рядків початкової таблиці потрібно виділити рядок *Все в списке фильтра*, який розкривається, або виконати команду *Данные*→*Фильтр*→*Отобразить все*.

Для відміни режиму фільтрації потрібно встановити курсор усередині таблиці і повторно вибрати команду меню *Данные*→*Фильтр*→*Автофильтр (зняти прапорець)*.

Автофільтр можна використовувати для знаходження заданого числа найбільших або найменших елементів списку, пошуку порожніх комірок, текстових значень у заданому алфавітному діапазоні тощо;

2) розширений фільтр дозволяє формувати множинні критерії вибірки і здійснювати складнішу фільтрацію даних електронної таблиці із завданням набору умов відбору по декіль-

кох стовпцях. Фільтрація записів із використанням розширеного фільтру виконується так: виділивши комірку, слід виконати: *Данные* → *Фильтр* → *Расширенный фильтр*, у вікні *Расширенный фильтр* задати умови фільтрації.

3.2.3. Виконання обчислень в Excel

Формули – основний засіб аналізу даних робочого листа. Для введення формули в комірку слід ввести з клавіатури знак рівності, потім – формулу й натиснути [Enter].

Формула може містити знаки арифметичних операцій, посилання на комірку, константи, функції та імена. Арифметичні оператори формул мають вигляд: (+) – складання; (-) – віднімання; (/) – ділення; (*) – множення; (%) – відсоток; (^) – піднесення до степеня. Для зміни черговості виконання операторів у формулі використовуються круглі дужки.

Операндами формул в Excel зазвичай є посилання на комірку. У цьому випадку зміна змісту комірки автоматично приведе до відповідної зміни результату розрахунку за формулою. Введення посилання доцільно робити, виділяючи в таблиці потрібну комірку за допомогою миші.

Посилання в Excel бувають:

- відносні (= M1) – відносне посилання вказує на комірку, виходячи з її розташування відносно комірки, в якій знаходиться формула. При копіюванні формули в іншу комірку відносні посилання автоматично настроюються;

- абсолютні (= \$M\$77) – абсолютне посилання вказує на фіксовану комірку;

- змішані (наприклад, = \$M1 або = M\$1). Змішане посилання містить відносне й абсолютне посилання. Координата комірки, помічена знаком \$, є абсолютною і при копіюванні формули зберігається.

У формулі як операнди можуть бути використані імена комірок, діапазонів комірок і масиви.

Імена присвоюються таким чином: виділити комірку або діапазон і виконати: *Вставка*→*Имя*. Ім'я починається з літери і не містить пропусків. Для виконання однотипних операцій над

даними певного діапазону процес формування необхідних формул можна спростити, створивши для діапазону формулу масиву, яка буде пов'язана зі всіма його комітками.

Формула масиву може виконати декілька обчислень, а потім повернути одне значення або групу значень. Формула масиву обробляє декілька наборів значень, які називаються аргументами масиву. Кожен аргумент масиву повинен включати однакове число рядків і стовпців. Ця формула створюється так само, як і інші формули, з тією відмінністю, що для її введення використовуються клавіші [Ctrl]+[Shift]+[Enter].

Правила для формул масиву

1. Перед введенням формули масиву треба виділити комірку або діапазон комірок, які міститимуть результати. Якщо формула передбачає декілька значень, необхідно виділити діапазон такого ж обсягу і форми, як діапазон з початковими даними.

2. Натисніть клавіші [Ctrl]+[Shift]+[Enter] автоматично для фіксації введення формули масиву. При цьому Excel автоматично помістить формулу у фігурні дужки в рядку формул (не вводьте фігурні дужки вручну!).

3. У діапазоні не можна змінювати, очищати або переміщати окремі комірки, а також їх вставляти або видаляти. Усі комірки в діапазоні масиву треба розглядати як єдине ціле і редагувати всі разом.

4. Для зміни або очищення масиву треба виділити весь масив і активізувати рядок формул. Після зміни формули треба натиснути комбінацію клавіш [Ctrl]+[Shift]+[Enter].

5. Щоб перемістити вміст діапазону масиву, треба виділити весь масив і в меню *Правка* вибрати команду *Вирізати*. Потім виділіть новий діапазон і в меню *Правка* виберіть команду *Вставити*.

6. Вирізати, очищати або редагувати частину масиву не дозволяється, але можна призначати різні формати окремим коміткам у масиві.

Використання масивів

Одновимірні масиви

Використовуючи масиви, треба обчислити суму значень у рядках для кожного стовпця. Для цього:

1. Введіть у діапазон A1:D2 числові значення.
2. Виділіть діапазон A3:D3.
3. У рядку формул введіть $=A1:D1+A2:D2$.
4. Натисніть комбінацію клавіш [Ctrl]+[Shift]+[Enter].

	A3		fx {=A1:D1+A2:D2}			
	A	B	C	D		
1	5	10	15	20		
2	1	2	3	4		
3	6	12	18	24		
4						

Комірки A3:D3 утворюють діапазон масиву, а формула масиву зберігається в кожній комірці цього діапазону. Масив аргументів – це посилання на діапазони A1:D1 і A2:D2.

Двовимірні масиви

Масиви, які містять декілька рядків і стовпців, називаються двовимірними.

	A5		fx {=ЦЕЛОЕ(A1:D3)}			
	A	B	C	D		
1	1,2	2,3	6,5	1,8		
2	3,5	2,8	9,1	4,5		
3	2,6	3,5	7,9	6,4		
4						
5	1	2	6	1		
6	3	2	9	4		
7	2	3	7	6		
8						

Для поширення дії формули на декілька суміжних комірок слід встановити курсор на маркер і виконати буксирування. При

цьому слід пам'ятати, що при буксируванні по рядку в посиланнях на комірку змінюються імена стовпців, а при буксируванні по стовпцю – номери рядків. Якщо якийсь з параметрів імені комірки треба зафіксувати, щоб він не змінювався під час буксирування, поставте перед ним позначку \$, наприклад, B\$8 (закріплено 8-й рядок).

Для виконання складання даних, розташованих у суміжних комірках, можна скористатися функцією *Автосумма*: виділити комірки, які містять складові, й натиснути клавішу [Σ] в панелі інструментів.

3.2.4. Робота з майстром функцій

Ф у н к ц і ї – це спеціальні, заздалегідь створені формули, які дозволяють виконувати обчислення. Функція складається з двох частин: імені функції і аргументу. Аргумент функції вказується в дужках після імені функції. Функція може використовуватися самостійно або бути елементом формули.

Для самостійного використання функції слід виділити комірку, в якій буде розміщений результат, виконати: *Вставка*→*Функція* або натиснути відповідну кнопку на панелі інструментів, вибрати функцію із запропонованого списку і ввести аргумент. При введенні аргументу можна вказувати посилання на комірки таким чином:

- суміжні комірки – виділити буксируванням у таблиці або вказати ім'я першої комірки діапазону і через двокрапку (:) – ім'я останньої комірки діапазону (A5:M5);
- несуміжні комірки – виділити в таблиці комірки при натиснутій клавіші [Ctrl] або ввести посилання на комірки, розділяючи їх крапкою з комою (;) (M5;Z1);
- при введенні аргументів можна використовувати імена комірок і діапазонів – клавіша [F3] відкриває список існуючих імен у книзі.

Аргументи функції можуть бути як константами, так і формулами. Ці формули, у свою чергу, можуть містити інші функції. Функції, що є аргументом іншої функції, називаються вкладеними. У формулах Excel використовується до семи рівнів вкладення функцій.

3.2.5. Майстер діаграм. Види діаграм та основні етапи їх побудови

Діаграма – це графічно представлена залежність однієї величини від іншої. Діаграма використовується для графічного відображення й аналізу даних робочого листа. Діаграма й дані робочого листа, на основі яких побудована діаграма, будуть зв'язані один з одним незалежно від місця розміщення діаграми. Зміна даних в листі автоматично приведе до змін у діаграмі.

Створення діаграми за допомогою майстра діаграм. Для побудови діаграми в Excel слід скористатися майстром діаграм, який послідовно в чотирьох вікнах діалогу запрошує необхідну інформацію і створює відповідно до неї діаграму. Роботу треба виконувати в такій послідовності:

1. Виділити в робочому листі дані для побудови діаграми.

Текстові заголовки даних можна також включити у виділений діапазон.

2. Клацнути на кнопці *Мастер диаграмм* на панелі інструментів *Стандартная* або виконати: *Вставка*→ *Диаграмма*. У діалоговому вікні, що з'явилося, обрати потрібний тип і вид діаграми.

3. Натиснути *Далее*.

Вкладка *Диапазон данных* служить для визначення джерела даних діаграми. Перевірте діапазон комірок, що містять дані для побудови діаграми. У разі потреби вкажіть їх: введіть з клавіатури або за допомогою миші виділіть у робочому листі інший діапазон комірок. Якщо в діаграмі передбачається використання заголовків рядків і/або стовпців, то їх слід включити у виділений діапазон. Тут також можна вказати розташування рядків для діаграми:

- *Ряды в строках* – заголовки стовпців будуть розташовані на осі категорій, а заголовки рядків увійдуть до легенди, тобто кожен рядок буде окремим рядом даних.

- *Ряды в столбцах* – навпаки, заголовки стовпців увійдуть до легенди, а заголовки рядків будуть розташовані

ні на осі категорій. У цьому випадку окремим рядком буде стовпець.

Вкладка *Ряд* дозволяє видалити або додати ряд до діаграм, задати ім'я ряду (ввівши константу або посилання на відповідну комірку) і уточнити діапазон його значень.

4. Натиснути *Далее*. Наступне діалогове вікно надає можливості по оформленню діаграми: створення підписів осей, даних, назви діаграми, додавання та розміщення легенди.

5. Натисніть кнопку *Далее*. Задайте позицію створюваної діаграми.

Діаграму можна розмістити на тому ж листі, що й дані, або винести на окремий лист. У майбутньому позицію діаграми можна змінити.

Натиснення кнопки *Готово* в будь-якому вікні майстра діаграм дозволяє відмінити “проходження” решти вікон і створити діаграму з урахуванням заданих параметрів.

Діаграму, створену за допомогою майстра діаграм, можна в будь-який момент змінити.

Створення діаграми без допомоги майстра діаграм.

1. Виконайте: *Вид*→*Панели инструментов*→*Диаграммы*.

2. Виділіть у робочому листі діапазон комірок з даними для побудови діаграми. У виділений діапазон можуть входити також текстові заголовки рядків і стовпців.

3. Клацніть на стрілці поряд з кнопкою *Тип диаграммы*, оберіть потрібний тип діаграми. Для вставки діаграми можна також виділити відповідні дані в робочому листі і натиснути клавішу [F11]. Excel вставить у робочу книгу лист діаграм і створить із виділених даних діаграму на основі використовуваного за умовчанням формату.

Зміна параметрів діаграми, створеної будь-яким способом, можлива через контекстне меню.

3.4. Сумісне використання Word та Excel. Упровадження і зв'язування об'єктів між документами різних типів

Технологія OLE (*Object Linking and Embedding*) – технологія зв'язування і впровадження об'єктів розроблена корпорацією Microsoft.

OLE дозволяє передавати частину роботи від однієї програми редагування до іншої і повертати результати назад.

При використанні OLE в обміні інформацією беруть участь два додатки – додаток-джерело і додаток-приймач. Додаток-джерело використовується для створення і редагування OLE-об'єктів. Після того, як об'єкт створений, його поміщають у додатку-приймачі.

Зв'язування – OLE-зв'язаний об'єкт підключається до окремого файла. Керування відображенням OLE-об'єкта в додатку-приймачі здійснюється на основі інформації, що зберігається у файлі додатку-джерела. Якщо цей файл змінюється в додатку-джерелі, OLE-об'єкт відповідним чином оновлюється. OLE-об'єкт не міститься в документі-приймачі. Замість цього додаток-приймач запам'ятовує джерело об'єкта. Обсяг файла-приймача збільшується тільки на обсяг посилання на файл-джерело. Початковий файл повинен залишатися доступним на комп'ютері або в мережі і служити джерелом оригінальних даних. Для зв'язування таблиці Excel і документа Word треба:

- виділити таблицю в додатку-джерелі, викликати контекстне меню, виконати *Копировать*;

- відкрити документ Word, встановити курсор у місце вставки таблиці, виконати: *Правка*→*Специальная вставка*→*Связать*. Зазначити тип об'єкта, що зв'язується з документом.

Тепер при змінах у таблиці, що виконуються в Excel, ці зміни автоматично будуть відображатися в таблиці, що зв'язана з документом Word.

Впровадження – впроваджений OLE-об'єкт повністю міститься у файлі додатку-приймача, тому він не пов'язаний із зовнішнім файлом.

Об'єкт, поміщений в документ, “пам'ятає”, звідки він взявся. MS Office забезпечить можливість його редагування в тому додатку, в якому цей об'єкт був створений, а не в тому, в якому він зараз відображається. Обсяг файла-приймача збільшується на обсяг усього файла-джерела, а не тільки впроваджених даних. Для впровадження таблиці Excel в документ Word треба:

- виділити таблицю в додатку-джерелі, викликати контекстне меню, виконати: *Копировать*;

- відкрити документ Word, встановити курсор на місці вставки таблиці, виконати: *Правка→Специальная вставка→Вставить*. Зазначити тип об'єкта, що впроваджується в документ.

Для редагування впровадженого об'єкта необхідно виконати подвійний щиголь на впроваджених даних, що дасть можливість редагування фрагмента у вікні додатку-приймача, а за допомогою рядка меню і панелей інструментів – додатку-джерела. При відкритті файла на іншому комп'ютері впроваджений об'єкт можна буде переглядати, навіть не маючи доступу до початкових даних. Оскільки впроваджений об'єкт не має жодних зв'язків з початковим файлом, він не оновлюється при зміні початкових даних.

Буксирування є найпростішим способом створення OLE-об'єкта. За допомогою миші можна вибрати елемент у додатку-джерелі, відбуксирувати його в додаток-клієнт, після чого він автоматично стає OLE-об'єктом. При звичайному буксируванні виділеного об'єкта він стає OLE-впровадженим об'єктом. Якщо буксирування виділеного об'єкта здійснюватиметься при натиснутій клавіші [Ctrl] або [Shift], він стає OLE-зв'язаним об'єктом.

Впровадження і зв'язування дозволяють вставляти в документ дані, з якими додаток-приймач не може працювати безпосередньо. Наприклад, при вставці звуку чи відео в тексті з'явиться значок, клацнувши по якому можна відтворити необхідне – звук чи відео.

Контрольні питання

1. Яку альтернативу бланкам юридичних документів пропонує Microsoft Word?
2. Який елемент документа Microsoft Word дозволяє зв'язати документ з довідковими або додатковими матеріалами, а також здійснити перехід у межах документа? Порядок формування цього елемента.
3. Що таке макрос? Наведіть приклади використання макросів у юридичних документах.
4. Які засоби захисту документів надає Microsoft Word?
5. Наведіть приклади форматів файлів, що використовуються для створення електронних бібліотек.
6. Який з форматів файлів, що використовуються для створення електронних бібліотек, найбільш ефективний для збереження в електронному вигляді юридичних документів?
7. Що таке електронна таблиця? Можливості її застосування у юридичній діяльності.
8. Призначення фільтрації та сортування даних таблиці.
9. Розкрийте зміст понять “формула” і “функція”.
10. Дайте визначення поняття “діаграма”. Види діаграм.
11. Які засоби створення та оформлення діаграм?
12. Технологія OLE. Її призначення та використання в юридичній практиці.

ОСНОВИ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

4.1. Загальне уявлення про інформаційну безпеку

В обчислювальній техніці поняття “безпека” є дуже широким. Його слід розуміти як надійність роботи комп'ютера, що передбачає комплекс необхідних умов: а) схоронність цінних даних; б) захист інформації від внесення в неї змін неуповноваженими особами; в) збереження таємниці листування одержуваної інформації в електронному зв'язку. Охороняють безпеку громадян закони, але у сфері інформації, одержуваної з використанням обчислювальної техніки, систем та комп'ютерних мереж, правова практика поки що розвинута недостатньо. Законотворчий процес не встигає за розвитком технологій.

4.1.1. Кримінальна відповідальність

Розділ XVI Кримінального кодексу України “Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку” містить низку норм, які передбачають кримінальну відповідальність за вчинення злочинів у сфері використання комп'ютерних технологій. До них, зокрема, відносяться: ст. 361 КК України “Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку”; ст. 362 КК України “Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї”; ст. 363 КК України “Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється”.

4.1.2. Технологічні, організаційні, правові постулати захисту даних

Захист даних, захист інформації (data protection) – сукупність заходів і відповідних засобів, які забезпечують захист прав власності власників інформаційної продукції, у першу чергу – програм, баз і банків даних від несанкціонованого доступу, використання, руйнування або завдання шкоди в будь-якій іншій формі.

У галузі знань із захисту інформації сформульовано три основні постулати.

Перший постулат: *абсолютно надійний захист створити неможливо*. Система захисту інформації може бути, в кращому разі, адекватною потенційним загрозам.

Другий постулат: *система захисту інформації повинна бути комплексною: слід використовувати не тільки технічні засоби захисту, а й адміністративні та правові*.

Третій постулат: *система захисту інформації повинна бути гнучкою, здатною адаптуватися до умов, що змінюються*. Головна роль у цьому належить адміністративним (або організаційним) заходам, таким, наприклад, як регулярна зміна паролів і ключів, додержання строгого порядку їх зберігання, аналіз журналів реєстрації подій у системі, правильний розподіл повноважень користувачів і багато що інше.

Залежно від способів захисту всі заходи, спрямовані на запобігання злочинам, можна класифікувати на технічні, правові та організаційні.

Технічні заходи:

1) захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем; 2) організація обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок; 3) вживання конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів; 4) установка резервних систем електроживлення, оснащення приміщень замками, сигналізацією і багато що інше.

Правові заходи:

1) розробка норм, що встановлюють відповідальність за комп'ютерні злочини; 2) захист авторських прав; 3) удосконалення кримінального й цивільного законодавства, а також судочинства.

Організаційні заходи:

1) охорона обчислювального центру; 2) підбір персоналу, виключення випадків ведення особливо важливих робіт тільки

однією людиною; 3) наявність плану відновлення працездатності інформаційного центру після виходу його з ладу; 4) організація обслуговування обчислювального центру сторонньою організацією або особами, не зацікавленими в приховуванні фактів порушення роботи центру; 5) універсальність засобів захисту від усіх користувачів (у тому числі й вищого керівництва); 6) покладання відповідальності на осіб, які повинні забезпечити безпеку центру, вибір місця розташування центру тощо.

До основних видів порушень інформаційної безпеки можна віднести дані про типи атак.

Основні види порушень інформаційної безпеки

Джерело атак (назва)	Джерело атак (%)
Недобросовісні співробітники	81
Хакери	77
Конкуренти	44
Зарубіжні компанії	26
Зарубіжні уряди	21

Тип атаки	Частота виявлення (%)
Віруси	85
Зловживання в Інтернеті із боку співробітників	79
Несанкціонований доступ з боку співробітників	71
Відмова в обслуговуванні	27
Атаки зовнішніх зловмисників	25
Крадіжка конфіденційної інформації	20
Саботаж	17
Фінансові шахрайства	11
Шахрайства з телекомунікаційними пристроями	11

Обсяг втрат від атак за 2007 р. (у мільйонах доларів США)

Тип атаки	Обсяг втрат
Віруси	39,2
Зловживання в Інтернеті з боку співробітників	38,0
Несанкціонований доступ із боку співробітників	29,6
Відмова в обслуговуванні	12,2
Атаки зовнішніх зловмисників	9,1
Крадіжка конфіденційної інформації	78,7
Саботаж	31,1
Фінансові шахрайства	64,0
Шахрайства з телекомунікаційними пристроями	6,0

4.2. Види загроз для комп'ютерної інформації

Необхідність в інформаційній безпеці впливає із самої природи мережних служб, сервісів і послуг.

Потрібно чітко дотримуватися прийнятих протоколів обміну в мережі. Будь-яке розширення клієнтської програми може супроводжуватися певною загрозою. Рівень безпеки на кожному комп'ютері свій. Забезпеченням режиму безпеки займається системний адміністратор.

Загроза віддаленого адміністрування. Під віддаленим адмініструванням слід розуміти несанкціоноване керування віддаленим комп'ютером. Віддалене адміністрування дозволяє брати чужий комп'ютер під своє управління. Це може дозволити копіювати і модифікувати наявні на ньому дані, установлювати довільні програми, у тому числі й шкідливі, використовувати чужий комп'ютер для вчинення злочинних дій у мережі від імені його власника.

Загроза активного змісту. Активний зміст – це активні об'єкти, вбудовані у веб-сторінки. На відміну від пасивного змісту (текстів, малюнків, аудіокліпів тощо), акти-

вні об'єкти містять у собі не тільки дані, а й програмний код, що одержує клієнт веб-сторінки, яка завантажується. Агресивний програмний код, що потрапив у комп'ютер, здатний поводитися як комп'ютерний вірус чи як агентська програма. Так, наприклад, він може як руйнувати дані, так і взаємодіяти з віддаленими програмами і, таким чином, працювати як засіб віддаленого доступу чи готувати ґрунт для його установки.

Загроза перехоплення чи підміни даних на шляхах транспортування. З проникненням Інтернету в економіку дуже гостро постала загроза перехоплення чи підміни даних на шляху транспортування. Так, наприклад, розрахунки електронними платіжними засобами (картками платіжних систем) передбачають відправлення покупцем конфіденційних даних про свою картку продавцю. Якщо ці дані будуть перехоплені на одному з проміжних серверів, немає гарантії, що ними не скористається зловмисник. Крім того, через Інтернет передаються файли програм. Підміна цих файлів під час транспортування може призвести до серйозних негативних наслідків.

Загроза втручання в особисте життя. В основі цієї загрози лежать комерційні інтереси рекламних організацій. У наш час річний рекламний бюджет Інтернету складає кілька десятків мільярдів доларів США. У бажанні збільшити свої доходи від реклами безліч компаній організує веб-вузли, причому не стільки для того, щоб надавати клієнтам серверні послуги, скільки для того, щоб збирати про них персональні відомості. Ці відомості узагальнюються, класифікуються і поставляються рекламним і маркетинговим службам. Процес збору персональної інформації автоматизований і дозволяє без відома клієнтів досліджувати їх пріоритети, смаки, звички.

Загроза постачання даних неприйнятного змісту. Не вся інформація, яка публікується в Інтернеті, може вважатися суспільно корисною, і досить часто люди хочуть від неї захиститися.

У більшості країн світу Інтернет поки не вважається засобом масової інформації. Це пов'язано з тим, що постачальник інформації не займається її копіюванням, тиражуванням і поширенням, тобто він не виконує функцій ЗМІ. Усе це робить сам

клієнт у момент використання гіперпосилання. Тому звичайні закони про ЗМІ, які регламентують, що можна поширювати, а що ні, в Інтернеті поки не працюють.

Функції фільтрації інформації, що надходить, її змісту покладаються на браузер чи на спеціально встановлену для цієї мети програму.

Класифікація комп'ютерних злочинів базується на класифікації способів вчинення таких злочинів. Спосіб вчинення злочину є системою взаємозумовлених, рухомих, детермінованих дій, спрямованих на підготовку, здійснення і приховання злочину, зв'язаних з використанням відповідних знарядь і засобів, а також часу, місця, об'єктивної обстановки вчинення злочину та інших обставин, що цьому сприяють.

Комп'ютерні злочини за способом їх здійснення поділяються на:

- 1) методи перехоплення;
- 2) методи несанкціонованого доступу;
- 3) методи маніпуляції.

Комп'ютер є об'єктом правопорушення, коли мета злочинця – викрасти інформацію або завдати шкоди системі, що цікавить його. З комп'ютером як з об'єктом пов'язані такі види злочинів:

а) вилучення засобів комп'ютерної техніки. До цієї групи відносяться традиційні способи здійснення звичайних видів злочинів, у яких дії злочинця направлені на вилучення чужого майна;

б) розкрадання інформації;

в) розкрадання послуг (діставання несанкціонованого доступу до якоїсь системи з метою безвідплатного користування послугами, що надаються нею);

г) пошкодження системи. Дана група об'єднує злочини, здійснені з метою зруйнувати або змінити дані, що є важливими для власника одного або багатьох користувачів системи – об'єкта несанкціонованого доступу;

д) уївинг (заплутування слідів, коли метою атаки є прагнення приховати своє ім'я і місцезнаходження).

Слід зазначити, що об'єктом правопорушення може бути пристрій, що не є комп'ютером у загальноприйнятому ро-

зумінні цього слова, наприклад, стільниковий телефон, касовий апарат тощо.

Комп'ютери використовуються як засоби, що сприяють вчиненню злочину:

а) як засіб вчинення традиційних злочинів (як правило, шахрайство);

б) як засіб атаки на інший комп'ютер, засіб вчинення іншого комп'ютерного злочину.

Комп'ютер використовується як запам'ятовувальний пристрій (наприклад, після зламу системи створюється спеціальна директорія для зберігання файлів, що містять програмні засоби злочинця, паролі для інших вузлів, списки вкрадених номерів, кредитних карток і тощо).

Зарубіжними фахівцями розроблені різні класифікації способів учинення комп'ютерних злочинів. Нижче наведено назви способів учинення подібних злочинів, відповідних кодифікатору Генерального Секретаріату Інтерполу. Всі коди, які характеризують комп'ютерні злочини, мають ідентифікатор, що починається з літери Q. Для характеристики злочинів можуть використовуватися до п'яти кодів, розташованих у порядку убудови значущості.

- QA – несанкціонований доступ і перехоплення:

QAN – комп'ютерний абордаж; QAI – перехоплення; QAT – крадіжка часу; QAZ – інші види несанкціонованого доступу і перехоплення.

- QD – зміна комп'ютерних даних:

QDL – логічна бомба; QDT – троянський кінь; QDV – комп'ютерний вірус; QDW – комп'ютерний черв'як; QDZ – інші види зміни даних.

- QF – комп'ютерне шахрайство:

QFC – шахрайство з банкоматами; QFF – комп'ютерна підробка; QFG – шахрайство з ігровими автоматами; QFM – маніпуляції з програмами введення-виводу; QFP – шахрайства з платіжними засобами; QFT – телефонне шахрайство; QFZ – інші комп'ютерні шахрайства.

- QR – незаконне копіювання:

QRG – комп'ютерні ігри; QRS – інше програмне забезпечення; QRT – топографія напівпровідникових виробів; QRZ –

інше незаконне копіювання.

- QS – комп’ютерний саботаж:

QSH – з апаратним забезпеченням; QSS – з програмним забезпеченням; QSZ – інші види саботажу.

- QZ – інші комп’ютерні злочини:

QZB – з використанням комп’ютерних дошок об’яв; QZE – розкрадання інформації, що складають комерційну таємницю; QZS – передача інформації конфіденційного характеру; QZZ – інші комп’ютерні злочини.

Несанкціонований доступ і перехоплення інформації (QA) включає наступні види комп’ютерних злочинів:

QAH – “комп’ютерний абордаж” (хакінг – hacking): доступ у комп’ютер або мережу без права на те. Цей вид комп’ютерних злочинів зазвичай використовується хакерами для проникнення в чужі інформаційні мережі.

QAI – перехоплення (interception): перехоплення за допомогою технічних засобів без права на те. Перехоплення інформації здійснюється прямо через зовнішні комунікаційні канали системи або шляхом безпосереднього підключення до ліній периферійних пристроїв. При цьому об’єктами безпосереднього підслуховування є кабельні і дротяні системи, наземні мікрохвильові системи, системи супутникового зв’язку, а також спеціальні системи урядового зв’язку. До даного виду комп’ютерних злочинів також відноситься електромагнітне перехоплення (electromagnetic pickup). Сучасні технічні засоби дозволяють отримувати інформацію безпосередньо підключенням до комп’ютерної системи: її перехоплення здійснюється за рахунок випромінювання центрального процесора, дисплея, комунікаційних каналів, принтера і т. д. Усе це можна здійснювати, знаходячись на достатньому віддаленні від об’єкта перехоплення.

QAT – крадіжка часу: незаконне використання комп’ютерної системи або мережі з наміром несплати.

Зміна комп’ютерних даних (QD) включає наступні види злочинів:

QDL/QDT – логічна бомба (logic bomb), троянський кінь (trojan horse): зміна комп’ютерних даних без права на те через впровадження логічної бомби або троянського коня.

Логічна бомба полягає в таємному вбудовуванні в програму набору команд, який повинен спрацювати лише один раз, але за певних умов.

Троянський кінь – таємне введення в чужу програму таких команд, які дозволяють здійснювати інші програми, функції, що не планувалися власником, але одночасно зберігати і колишню працездатність.

QDV – вірус (virus): зміна комп'ютерних даних або програм без права на те через впровадження або розповсюдження комп'ютерного вірусу.

Комп'ютерний вірус – це спеціально написана програма, яка може “приписати” себе до інших програм (тобто “заражати” їх), розмножуватися і породжувати нові віруси для виконання різних небажаних дій на комп'ютері.

QDW – черв'як: зміна комп'ютерних даних або програм без права на те через передачу, впровадження або розповсюдження комп'ютерного черв'яка в комп'ютерній мережі.

Комп'ютерні шахрайства (QF) об'єднують у своєму складі різноманітні способи вчинення комп'ютерних злочинів:

QFC – комп'ютерні шахрайства, пов'язані з розкраданням готівки з банкоматів.

QFF – комп'ютерні підробки: шахрайства і розкрадання з комп'ютерних систем шляхом створення підроблених пристроїв (карток і ін.).

QFG – шахрайства і розкрадання, пов'язані з ігровими автоматами.

QFM – маніпуляції з програмами введення-виводу: шахрайства і розкрадання за допомогою неправильного введення в комп'ютерні системи або виводу з них через маніпуляції програмами. До цього виду комп'ютерних злочинів включається метод підміни даних кода (data diddling code change), яка зазвичай здійснюється при введенні-виводі даних. Це простий і тому часто вживаний спосіб.

QFP – комп'ютерні шахрайства і розкрадання, пов'язані із платіжними засобами. До цього виду відносяться найпоширеніші комп'ютерні злочини, пов'язані з крадіжкою грошових коштів, які складають близько 45% всіх злочинів, зв'язаних з вико-

ристанням ЕОМ.

QFT – телефонне шахрайство: доступ до телекомунікаційних послуг через посягання на протоколи і процедури комп'ютерів, що обслуговують телефонні системи.

Незаконне копіювання інформації (QR) складають наступні види комп'ютерних злочинів:

QRG/QRS – незаконне копіювання, розповсюдження або публікація комп'ютерних ігор та іншого програмного забезпечення, захищеного законом.

QRT – незаконне копіювання топографії напівпровідникових виробів: копіювання без права на те захищеної законом топографії напівпровідникових виробів, комерційна експлуатація або імпорту з цією метою без права на те топографії або самого напівпровідникового виробу.

Комп'ютерний саботаж (QS) складають наступні види злочинів:

QSH – саботаж з використанням апаратного забезпечення: введення, зміна, знищення комп'ютерних даних або програм; втручання в роботу комп'ютерних систем з наміром перешкодити функціонуванню комп'ютерної або телекомунікаційної системи.

QSS – комп'ютерний саботаж з програмним забезпеченням: знищення, пошкодження, погіршення або стримування комп'ютерних даних або програм без права на те.

До інших видів комп'ютерних злочинів (QZ) відносяться:

QZB – використання електронних дошок об'яв (BBS) для зберігання, обміну і розповсюдження матеріалів, що мають відношення до злочинної діяльності.

QZE – розкрадання інформації, що є комерційною таємницею: придбання незаконними засобами або передача інформації, що становить комерційну таємницю, без права на те або іншого законного обґрунтування з наміром заподіяти економічного збитку або одержати незаконні економічні переваги.

QZS – використання комп'ютерних систем або мереж для зберігання, обміну, розповсюдження або переміщення інформації конфіденційного характеру.

4.3. Засоби протидії загрозам для комп'ютерної інформації

Захист від віддаленого адміністрування. Ефективний захист від віддаленого адміністрування забезпечують два основні методи. Перший – встановлення на комп'ютері “жертви” програми (аналог сервера), з якого зловмисник може створити віддалене з'єднання в той час, коли “жертва” перебуває в мережі. Програми, що використовуються для цього, називаються троянськими. За своїми ознаками вони значною мірою нагадують комп'ютерні віруси. Другий метод віддаленого адміністрування оснований на використанні похибок (помилки), що є в програмному забезпеченні комп'ютерної системи – партнера по зв'язку. Мета цього методу – вийти за рамки спілкування з клієнтської (серверної) програми і прямо впливати на операційну систему, щоб через неї одержати доступ до інших програм і даних. Програми, що використовуються для експлуатації похибок комп'ютерних систем, називаються експлантами.

Захист від троянських програм. Для ураження комп'ютера троянською програмою хтось повинний її запустити на цьому комп'ютері. Тому варто обмежити доступ сторонніх осіб до мережних комп'ютерів звичайним адміністративним способом (фізичне обмеження доступу, пароль тощо). Звичайний метод установки троянських програм на чужих комп'ютерах пов'язаний із психологічним впливом на користувача. Треба умовити користувача зробити це самому. Найчастіше практикується розсилання шкідливих програм у вигляді додатків до повідомлень електронної пошти. У тексті повідомлення вказується, наскільки корисна і вигідна ця програма.

Рекомендації. Ніколи не запускайте нічого, що надходить разом з електронною поштою, незалежно від того, що написано в супровідному повідомленні (навіть від друзів).

Крім електронної пошти зловмисники використовують розповсюдження троянських програм через компакт-диски. Багато програм знаходяться в самому Інтернеті. Ніколи не встановлюйте непевірівених програм з компакт-дисків.

Захист від експлуатації помилок у програмному забезпеченні. Цей вид загроз майже безпечний для клієнтської сторони. Атакам програм-експлантів в основному піддаються сервери. Стратегія зломисників реалізується в три етапи.

На першому етапі вони з'ясовують склад програм і устаткування в локальній мережі “жертви”. На другому етапі розшукують інформацію про відомі помилки (похибки) в даних програмах. На третьому етапі готують програми-експланти (чи використовують раніше підготовлені кимось програми) для експлуатації виявлених похибок. Боротьба з цими загрозами може відбуватися на всіх трьох етапах.

Адміністрація серверів, насамперед, контролює звертання, мета яких полягає в з'ясуванні програмно-апаратної конфігурації сервера. Це дозволяє поставити порушника на облік задовго до того, як він зробить реальну атаку.

У найбільш відповідальних випадках використовують спеціально виділені комп'ютери чи програми, що виконують функції міжмережних екранів. Такі засоби також називають брандмауерами. Брандмауер займає положення між комп'ютерами, що захищаються, і зовнішнім світом. Він не дозволяє переглядати ззовні склад програмного забезпечення на сервері і не пропускає несанкціонованих даних і команд.

Захист від активного змісту. Сторона, яка захищається, повинна оцінити загрозу своєму комп'ютеру і, відповідно, настроїти браузер так, щоб небезпека була мінімальною. Якщо цінні дані чи конфіденційні відомості комп'ютер не містить, захист можна відключити і переглядати веб-сторінки в тому вигляді, який передбачив їх розробник. Якщо загроза небезпечна, необхідно виконати налаштування захисту в програмі Internet Explorer у діалоговому вікні *Параметри безпеки*.

Засоби захисту даних на шляхах транспортування. З проникненням комерції в Інтернет усе частіше виникає потреба проведення дистанційних ділових переговорів, купівлі через мережу програмного забезпечення та грошових розрахунків за поставлені товари й послуги, а отже, й захисту даних на шляхах транспортування. Одночасно з захистом

даних необхідно забезпечити посвідчення (ідентифікацію) партнерів по зв'язку і підтвердження (аутентифікацію) цілісності даних. Сьогодні в електронній комерції захищають і аутентифікують дані, а також ідентифікують віддалених партнерів за допомогою криптографічних методів, технологічно реалізованих в ЕЦП.

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо (Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”).

Усі програми кодування дозволяють привести початкову інформацію, що знаходиться в кодованому файлі, до вигляду, який не дозволяє використовувати закодовану інформацію за прямим призначенням. Для приведення закодованої інформації до початкового вигляду застосовують програми декодування. Програми кодування інформації переважно мають функції, що дозволяють декодувати дані, приведені до початкового вигляду. Розглянемо деякі з них.

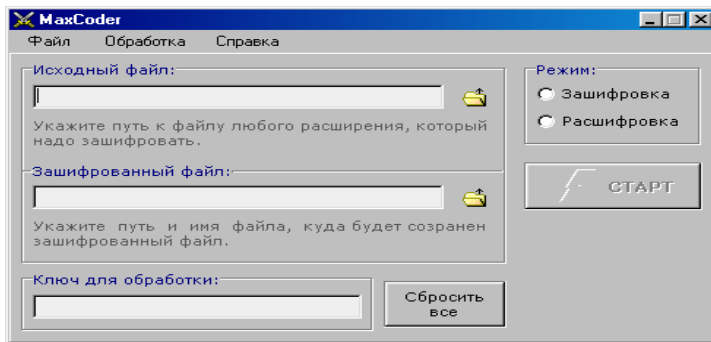


Рис. 4.1. Діалогове вікно програми кодування Maxcoder.

Інтерфейс програми містить три поля введення даних:

- початковий файл;
- зашифрований файл;

- ключ для обробки.

Виконання операцій кодування і декодування здійснюється достатньо швидко, що не вимагає жодних тимчасових витрат.

Програма кодування інформації SC схожа на програму кодування Maxcoder, проте існують відмінності у виборі ключових кодів.

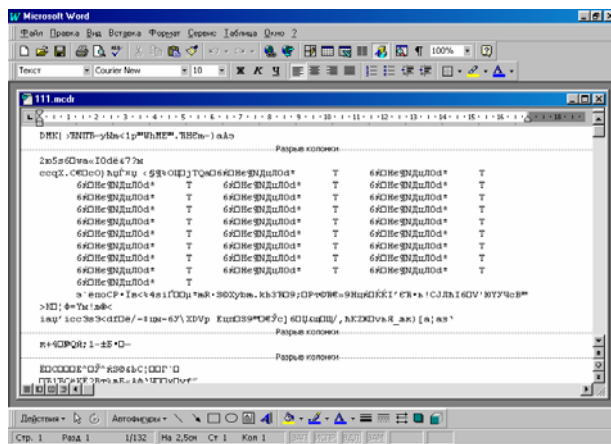


Рис. 4.2. Зашифрована програмою Maxcoder текстова інформація.

Signature Cryptographer (SC) – програма для захисту інформації у важливих файлах від несанкціонованого доступу. Захист здійснюється шляхом шифрування даних файла. Шифрувальник використовує як ключ зміст файлів замість рядка пароля. Таким чином, довжина пароля може досягати гігантських обсягів (або взагалі бути більше довжини шифрованого файла, що теоретично робить зашифрований файл незламуваним).

Замість довгих рядків пароля запам'ятати потрібно тільки ім'я файла, використаного для пароля. Спосіб шифрування файлів оснований на алгоритмі шифрування “Сигнатура”, детально описаному в інтерактивній довідковій системі. Шифрованим файлом може бути будь-який файл (*.EXE, *.DLL, *.TXT, *.DOC і ін.), що містить інформацію.

Після запуску програми (необхідно завантажити файл SC.exe) з'являється головне вікно Signature Cryptographer, загальний вид якого представлений на рис. 4.3.

У верхній частині вікна розташоване головне меню програми. За його допомогою можна викликати вікно налаштувань програми, переглянути файли допомоги.

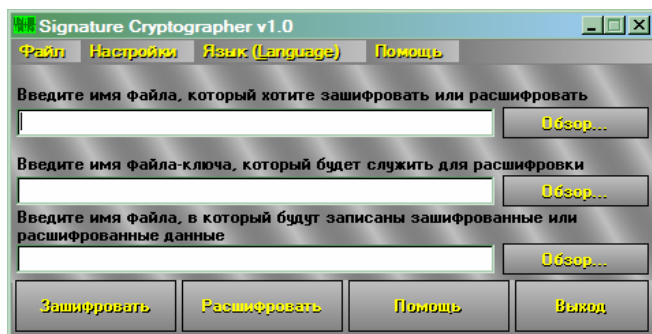


Рис. 4.3. Загальний вид вікна програми SC.

Головне вікно програми містить три поля введення, в які перед початком роботи потрібно ввести необхідні імена файлів.

У перше поле необхідно ввести ім'я наявного файла, який шифруватиметься або розшифровуватиметься (вхідний файл). Ім'я файла можна вводити як вручну, так через відповідну кнопку *Обзор*, вибравши потрібний файл із списку.

У другому полі повинне міститися ім'я наявного файла-ключа. Для введення значення в це поле можна так само скористатися відповідною кнопкою *Обзор*.

Третє поле залежно від налаштувань програми може заповнюватися автоматично. Воно містить ім'я файла, в який відбуватиметься запис зашифрованого або розшифрованого вхідного файла (вихідний файл). Якщо файл, указаний в цьому полі не існує, він буде створений, якщо існує перезаписаний, то всі попередні дані в ньому втратяться. Файл так само може бути вибраний за допомогою відповідної кнопки *Обзор*.

Вхідний файл може співпадати з вихідним файлом. У такому разі після роботи програми вхідний файл міститиме заши-

фровані або розшифровані коректно записані дані.

Шифрування за алгоритмом “Сигнатура” не відбувається з вмістом файла-ключа в чистому вигляді. Перед шифруванням всі дані у файлі-ключі обробляються алгоритмом, внаслідок чого виходить блок даних, рівний по довжині даним у файлі-ключі. Цей блок даних (далі – образ файла-ключа) використовується при шифруванні або розшифровці файла.

Слід зазначити, що образ файла-ключа (або його частини) створюється в оперативній пам’яті комп’ютера, а дані у файлі-ключі не змінюються.

Як приклад можна навести один із найбільш сильних засобів криптографічного захисту даних – програмний пакет PGP (Pretty Good Privacy).

PGP реалізує технологію криптографії з використанням ключів: користувач генерує пару віртуальних ключів, що складається із закритого ключа і відкритого ключа – чисел, зв’язаних певним математичним співвідношенням.

Закритий (секретний) ключ залишається у виключному доступі власника і зберігається в локальному файлі, захищеному паролем. Він використовується для розшифровки зашифрованої інформації, а також для її шифрування. Відкритий ключ використовується тільки для шифрування інформації: з його допомогою не можна провести дешифровку.

Відкриті ключі не слід тримати в таємниці: математика використовуваного криптографічного алгоритму така, що за відкритим ключем неможливо відновити закритий. Зазвичай користувач опубліковує свій відкритий ключ, роблячи його доступним будь-кому, хто захоче послати йому зашифроване повідомлення. Така людина зашифрує своє повідомлення вашим відкритим ключем користувача, при цьому ні той, хто надіслав зашифровану інформацію, ні будь-хто інший не може її розшифрувати. Тільки та людина, яка має секретний ключ, що відповідає відкритому ключу, може розшифрувати повідомлення. Очевидно, що секретний ключ має зберігатися його власником в секреті.

Величезною перевагою такого способу шифровки є те, що на відміну від звичайних методів шифрування, немає необ-

хідності шукати безпечний спосіб передачі ключа адресатові. Іншою корисною рисою таких криптосистем є можливість створити цифровий підпис повідомлення, зашифрувавши його своїм секретним ключем. Тепер за допомогою вашого відкритого ключа будь-хто зможе розшифрувати повідомлення і таким чином переконатися, що його зашифрував дійсно власник секретного ключа.

Ви можете опублікувати свій публічний ключ на своїй веб-сторінці або надіслати його електронною поштою своєму другу. Ваш кореспондент зашифрує повідомлення з використанням вашого відкритого ключа і відправить вам. Прочитати його зможете тільки ви з використанням секретного ключа. Навіть сам відправник не зможе розшифрувати адресоване вам повідомлення, хоча він сам написав його. Більш того, згідно із заявою експертів у галузі криптографії алгоритм шифрування, вживаний у PGP, робить практично неможливою розшифровку інформації без закритого ключа. Заступник директора агентства національної безпеки США Уїльям Кроуелл так охарактеризував надійність PGP: “Якщо всі персональні комп’ютери світу змусити працювати з єдиним повідомленням, зашифрованим PGP, розшифровка такого повідомлення в середньому потребуватиме часу, що у 12 мільйонів разів перевищує вік нашого Всесвіту”. Навіть якщо зважити на можливо завищений оптимізм американського чиновника, все одно залишається підстава говорити про великий запас надійності даної системи.

Захист від втручання в особисте життя. Збір відомостей про учасників роботи в Інтернеті. Крім засобів активного впливу, існують і засоби пасивного спостереження за діяльністю учасників мережі Інтернет. Вони використовуються рекламно-маркетинговими службами.

Відвідуючи веб-сторінки, ми бачимо майже на кожній рекламній оголошення (банери). При їх прийомі браузер установлює зв’язок з їх власником (рекламною системою) і непомітно для користувача реєструється в цій системі. Переходячи від однієї веб-сторінки до іншої, користувач створює свій психологічний портрет (він називається профілем). За характером відвіду-

ваних веб-вузлів і веб-сторінок віддалена служба здатна визначити стать, вік, рівень освіти, рід занять, коло інтересів, рівень добробуту і навіть характер захворювань особи. Варто де-небудь хоча б один раз зареєструватися під своїм ім'ям і прізвищем, і раніше зібрані абстрактні відомості набувають цілком конкретного змісту – так утворюються негласні персональні бази даних на учасників роботи в мережі Інтернет.

Джерела персональної інформації. Найбільш простим і очевидним джерелом для збору відомостей про активність клієнтів Інтернету є маркери “cookie”, що працюють у такий спосіб.

Відповідно до протоколу HTTP браузер може відправити серверу запит на постачання одного веб-ресурсу (документа HTML) і ніяк при цьому серверу не представитися. Іноді доцільно, щоб браузер серверу представлявся. Це корисно для Інтернет-магазинів.

Відповідно до протоколу HTTP сервер може передати браузеру невеликий пакет даних, у яких закодована інформація, потрібна серверу для ідентифікації браузера і настроювання на роботу з ним (доменне ім'я сервера і шлях доступу до веб-сторінки, для якої маркер був створений, а також час дії маркера). Цей пакет тимчасово запам'ятовується в оперативній пам'яті комп'ютера і виконує роль маркера (мітки). Якщо браузер знову звернувся до цього сервера, то він пред'являє йому раніше прийнятий маркер, і сервер відразу “розуміє”, з яким клієнтом він має справу.

Маркери можуть бути тимчасовими і постійними. Тимчасовий маркер зберігається в оперативній пам'яті доти, поки браузер працює. По закінченні його роботи всі тимчасові маркери, отримані від серверів, знищуються. Однак сервери залишають не тільки тимчасові, а й постійні маркери. Коли браузер завершує роботу, всі постійні маркери, що накопичилися в оперативній пам'яті, переносяться на твердий диск у вигляді файлів “cookie”. Так відбувається маркування твердого диска і комп'ютера клієнта. При виході в Інтернет відбувається зчитування маркерів з твердого диска в оперативну пам'ять, звідки браузер пред'являє їх

серверам, які їх поставили.

Фізичної загрози маркери “cookie” комп’ютеру не становлять – це файли даних, що не є програмним кодом. Але вони являють загрозу втручання в особисте життя.

Незаконний збір інформації може здійснюватися завдяки тому, що сервер у змозі прочитати не тільки свої маркери, а й ті, які встановили інші сервери. Практика використання маркерів для збору відомостей про користувачів Інтернетом в даний час знаходиться під пильною увагою фахівців-правознавців.

Інтернет – всесвітня інформаційна система загального доступу, логічно зв’язана глобальним адресним простором, базується на Інтернет-протоколі, визначеному міжнародними стандартами (Закон України “Про телекомунікації”).

У деяких країнах розробляються обмеження на використання маркерів “cookie” у зв’язку з тим, що сервер повинен мати об’єктивні засоби ідентифікації правового статусу клієнта, перш ніж розміщати на його комп’ютері маркери.

Браузер також легально поставляє інформацію з протоколу HTTP: повідомляє свою назву, номер версії, тип операційної системи комп’ютера і URL-адресу веб-сторінки, яку клієнт відвідав останньою.

Браузер Internet Explorer має спеціальні налаштування для відключення прийому маркерів “cookie” в діалоговому вікні *Параметри безпеки*. Найпростіше захистити папку C:\Windows\Cookies від запису. Час від часу видаляйте вміст папки.

4.4. Поняття про комп’ютерні злочини. Визначення, аналіз та фіксація слідів комп’ютерних злочинів

Термін “комп’ютерна злочинність” уперше з’явився в американській, а потім у зарубіжній пресі інших країн на початку 60-х років XX ст., коли були виявлені перші випадки злочинів, здійснених з використанням ЕОМ.

У квітні 2000 р. був розроблений проект Європейської конвенції про кіберзлочини, в якому поняття “злочин у сфері

комп'ютерної інформації” замінено терміном “кіберзлочин”.

Термін “кіберзлочин” охоплює будь-який злочин, який може здійснюватися за допомогою комп'ютерної системи або мережі в рамках комп'ютерної системи або мережі або проти комп'ютерної системи або мережі.

Для такої молододі держави, як Україна, комп'ютерна злочинність явище нове, але воно вже зумовило гострі проблеми, які потребують вирішення законодавчими і правоохоронними органами. Український законодавець у Розділі XVI Кримінального кодексу України визначив комп'ютерні злочини як злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж.

Комп'ютерний злочин – це суспільно небезпечне, карне діяння (дія або бездіяльність), предметом якого є комп'ютерна інформація, направлена на заподіяння шкоди. Необхідно відзначити, що комп'ютерні злочини мають високу латентність: тільки 10-15 % комп'ютерних злочинів стають відомими. За західними джерелами, середня банківська крадіжка із застосуванням електронних засобів складає близько 15 тис. доларів, а один із найгучніших скандалів пов'язаний із спробою викрасти 700 млн доларів з Першого національного банку в Чикаго.

Що стосується статистики злочинів у сфері використання банківських комп'ютерних систем по Україні, то її, по суті, немає, що, природно, не означає відсутності таких злочинів.

Мотиви злочинів. Основними цілями і мотивами вчинення злочинів у сфері комп'ютерної інформації виступають: користь (56,8%), хуліганські спонукання (17,1%), помста (12,7%), комерційне шпигунство або диверсія (9,1%).

Злочини у сфері використання комп'ютерних технологій у п'ять разів частіше здійснюються чоловіками. Більшість суб'єктів злочину мають вищу або незакінчену вищу технічну освіту (53,7%), а також іншу вищу або незакінчену вищу освіту (19,2%). Серед них переважають особи у віці від 30 до 45 років (46,5%), а також від 16 до 30 років (37,8%).

Для визначення, аналізу і фіксації слідів комп'ютерних злочинів необхідне отримання наступних даних: 1) уточнення

способу порушення цілісності (конфіденційності) інформації; 2) уточнення порядку регламентації власником роботи інформаційної системи; 3) уточнення кола працівників, що мають можливість взаємодіяти з інформаційною системою, в якій відбулися зміни цілісності (конфіденційності) інформації для визначення бази свідків і виявлення кола підозрюваних осіб; 4) уточнення даних про завдану шкоду.

Усі пристрої конкретної комп'ютерної системи підлягають огляду. Дії можуть проводитися з працюючою і непрацюючою комп'ютерною технікою. Якщо комп'ютер працює, то рекомендується:

- визначити, які програми виконуються;
- здійснити фотографування або відеозапис зображення на екрані;
- зупинити виконання програми;
- зафіксувати в протоколі результати своїх дій і реакції комп'ютера на них;
- визначити зовнішні пристрої комп'ютера – накопичувачі інформації і віртуальні диски;
- визначити наявність зовнішніх пристроїв віддаленого доступу до системи і визначити їх стан;
- роз'єднати мережні кабелі так, щоб ніхто не міг змінити або стерти інформацію в ході обшуку;
- скопіювати програми і файли даних, що зберігаються на віртуальному диску, на зовнішні носії;
- вимкнути з електромережі комп'ютер.

Якщо комп'ютер не працює:

- точно відобразити в протоколі і на схемі, що додається до нього, місцезнаходження комп'ютера і його периферійних пристроїв;
- точно описати порядок з'єднання між собою цих пристроїв з вказівкою особливостей; перед роз'єднанням кабелів корисно здійснити фотографування місць з'єднання і маркування кожного кабелю і пристрою, а також портів;
- роз'єднати пристрої комп'ютера;
- упакувати окремо носії на дискетах і магнітних стріч-

ках і помістити в оболонки для захисту від електромагнітної дії;

- упакувати кожен пристрій і сполучні кабелі;
- захистити і зафіксувати дисководи для транспортування.

Якщо буде потрібно включити комп'ютер, то це необхідно виконати за допомогою власної операційної системи.

Контрольні питання

1. Які сегменти входять до загального уявлення про інформаційну безпеку?
2. Визначте головні технологічні, організаційні та правові основи захисту даних.
3. Які існують види загроз для комп'ютерної інформації?
4. У чому полягає негативний вплив програм вірусів на комп'ютерні дані з точки зору інформаційної безпеки?
5. Назвіть основні групи комп'ютерних злочинів за класифікацією кодифікатора Генерального Секретаріату Інтерполу.
6. Які основні заходи вживаються для протидії загрозам комп'ютерної інформації?
7. Які програмні засоби існують для криптографічного захисту інформації?
8. У чому полягає принципова різниця між програмами криптозахисту?
9. Що можна віднести до джерел персональної інформації?
10. Сформулюйте поняття “ комп'ютерний злочин”.

ТЕХНІЧНЕ ТА ЮРИДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОННОГО ПІДПISУ

5.1. Електронний бізнес та електронна комерція

Перші електронні операції в Інтернеті були здійснені ще в 1995 р. Формально *електронний бізнес* є будь-якою трансакцією, здійсненою за допомогою функціональності інформаційної системи, після закінчення якої відбувається передача права власності або права користування реальним продуктом або послугою.

Разом з тим зараз відбувається поступова трансформація понять – активно вживається поняття “електронний бізнес”, яке слід розуміти як реалізацію ділової активності через Інтернет. Сьогодні спостерігається тенденція нарощування цього сервісу і поступового перетворення веб-вітрин на повноцінні інтернет-магазини. Це дозволяє бізнесу збільшити географію присутності на ринку, швидше реалізувати товар, послуги та отримати додатковий канал для маркетингу і реклами.

Проблема оплати за товар чи послугу вирішується масовим упровадженням електронних засобів платежу. Он-лайніві платіжні системи, що існують сьогодні, можна розділити на три види: *пластикові* (кредитні або дебетові) картки, *електронні чеки* та *цифрові гроші* (“електронний гаманець”). Головна проблема – це безпека електронних платежів. На користь її вирішення можна вважати появу протоколу SET (Secure Electronic Transactions – *безпечні електронні трансакції*) – міжнародного стандарту безпеки, який сьогодні є єдиним стандартом, прийнятим основними міжнародними платіжними системами для організації захищених платежів в Інтернеті.

Таким чином, сучасний електронний бізнес – це якісно нові технології, які дозволяють компанії досягти конкурентної переваги завдяки поліпшенню обслуговування своїх клієнтів та оптимізації бізнес-стосунків з партнерами. Інтернет-технології

є одним з основних, але не єдиним ключовим аспектом в електронному бізнесі.

Електронна комерція як один з елементів електронного бізнесу пов'язана з виконанням функцій маркетингу, включаючи продаж товарів і послуг через Інтернет споживачеві.

Залежно від використовуваної моделі бізнесу розрізняють системи B2B (Business to Business – ділові стосунки між компаніями), B2C (Business to Consumer – взаємодія компанії і кінцевого споживача), а також B2G (Business to Government – відносини комерційних структур і держустанов). Зараз все ширше для державного урядування використовується система G2G (Government to Government – відносини між держустановами).

5.2. Закон України “Про електронні документи та електронний документообіг”

Усі види бізнесу та урядування неможливі без документів. Електронний бізнес та сучасне урядування використовують *електронні документи*, визначення яких міститься в Законі України “Про електронні документи та електронний документообіг”, прийнятому 22 травня 2003 р. У ст. 5 вказано: “*Електронний документ* – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством”.

Важливим є те, що електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

При цьому “візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною” (ст. 5).

Одним із необхідних реквізитів звичайного документа є підпис або підпис з печаткою. Електронні документи теж потре-

бують підпису – електронного. У зазначеному Законі в ст. 6 це поняття визначається так: “Електронний підпис є обов’язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб’єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа. Відносини, пов’язані з використанням електронних цифрових підписів, регулюються законом”. При цьому “використання інших видів електронних підписів в електронному документообігу здійснюється суб’єктами електронного документообігу на договірних засадах”.

Крім того, електронний підпис Закон розглядає як засіб перевірки цілісності електронного документа. У ст. 12 вказано, що “перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису”.

Як технічно реалізується електронний підпис розглянемо в наступному підрозділі. У контексті теми, яка вивчається, важливим є поняття “електронний документообіг”, яке Закон визначає так: “Електронний документообіг (обіг електронних документів) – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.

Порядок електронного документообігу регламентується державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.”

У статтях 11 та 12 Закон також визначає порядок відправлення та передавання електронних документів, а також їх одержання: “Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ”.

Дуже важливим є визначення у Законі часу, коли був відправлений (ст. 11) та одержаний (ст. 12) електронний документ:

– “Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання”;

– “Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб’єктами електронного документообігу.

Якщо попередньою домовленістю між суб’єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа на папері. Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження”.

Зверніть увагу, що, як наголошено в ст. 11, “вимоги підтвердження факту одержання документа, встановлені законодавством у випадках відправлення документів рекомендованим листом або передавання їх під розписку, не поширюються на електронні документи. У таких випадках підтвердження факту одержання електронних документів здійснюється згідно з вимогами цього Закону”.

5.3. Поняття про електронний цифровий підпис

Закон України “Про електронні документи та електронний документообіг” доповнюється Законом України “Про електронний цифровий підпис”, прийнятим з ним одночасно, тобто 22 травня 2003 р. Цей Закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Зверніть увагу, що “дія цього Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису”.

Закон у ст. 1 визначає низку термінів і, що важливо, розрізняє поняття “електронний підпис” та “електронний цифровий підпис”:

- *електронний підпис* – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації підписувача цих даних;

- *електронний цифровий підпис* – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа”.

Щоб зрозуміти це визначення, розберемося з найважливішими поняттями, які воно містить.

Одним з основних реквізитів звичайних документів є рукописний підпис. Він підтверджує факт взаємозв’язку між відомостями, що містяться в документі, і особою, що підписала документ. В основу використання рукописного підпису як засобу ідентифікації покладено гіпотезу про унікальність особистих біометричних параметрів людини. Однак його ступінь захисту зовсім недостатній. Наприклад, на фінансових документах необхідна наявність двох рукописних підписів, а також печатки юридичної особи. Якщо й цього недостатньо, то засвідчують у нота-

ріуса чи використовують спеціальні бланки, що мають особливі засоби захисту.

Характерною рисою рукописного підпису є його нерозривний фізичний зв'язок з носієм інформації. Тобто рукописний підпис можливий тільки на документах, що мають матеріальну природу. Обидві сторони – учасники угоди повинні під час її складання бути присутніми, щоб особисто поставити свій підпис. Нерозривний зв'язок між підписом і матеріальним носієм документа зумовлює важливі відмінності між оригіналом та копіями документів, одержаними засобами копіювально-множної техніки. Копії мають певні особливості порівняно з оригіналами – меншу юридичну чинність, потребують додаткових процедур засвідчення.

Ще один недолік рукописного підпису – функціональний. Він пов'язаний з тим, що рукописний підпис забезпечує тільки ідентифікацію документа, тобто підтвердження його відношення до особи, яка поставила підпис, але ніякою мірою не забезпечує аутентифікації документа, тобто його цілісності та незмінності. Без спеціальних додаткових заходів захисту рукописний підпис не гарантує того, що документ не піддався змістовим змінам під час збереження чи транспортування.

На відміну від рукописного підпису, електронний цифровий підпис має не фізичну, а логічну природу – це просто послідовність символів, що дозволяє однозначно зв'язати автора документа, зміст документа та власника електронного цифрового підпису. Логічний характер електронного цифрового підпису робить його незалежним від матеріальної природи документа. Він дозволяє позначати й аутентифікувати документи, що мають електронну природу. Електронний цифровий підпис має наступні корисні властивості:

1) *можливість порівняти захисні властивості різних типів електронних цифрових підписів* – при використанні сертифікованих засобів електронного цифрового підпису його захисні властивості вище, ніж ручного. Їм можна дати об'єктивну (числову) оцінку, ґрунтовану не на гіпотезі про унікальність біометричних параметрів людини, а на строгому математичному аналізі. Звідси

впливає принципова можливість порівнянності захисних властивостей різних засобів електронного цифрового підпису;

2) *масштабованість* – з можливості об’єктивної оцінки захисних властивостей електронного цифрового підпису впливає можливість застосування найпростіших засобів електронного цифрового підпису в цивільному документообігу, де загроза підробки підпису невелика. А у випадках важливих та секретних документів – застосування інших, складних спеціальних засобів електронного цифрового підпису;

3) *дематеріалізація документа* – незалежність електронного цифрового підпису від носія дає можливість здійснювати договірні відносини між віддаленими юридичними та фізичними особами без прямого чи опосередкованого фізичного контакту між ними. Ця властивість, наприклад, лежить в основі електронної комерції;

4) *рівнозначність копій* – логічна природа електронного цифрового підпису дозволяє не розрізняти копій одного документа та зробити їх рівнозначними самому документу. Тобто будь-яка копія без додаткових заходів рівнозначна оригіналу.

Зверніть увагу на останній пункт. У ст. 8 Закону України “Про електронні документи та електронний документообіг” вказано, що “*оригіналом електронного документа* вважається електронний примірник документа з обов’язковими реквізитами, у тому числі з електронним цифровим підписом автора.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу”.

Є і недоліки цифрового підпису. Механізм підпису не знаходиться під безпосереднім контролем людини природними методами (наприклад, візуальними). Тому для використання електронного цифрового підпису необхідне спеціальне технічне,

організаційне і правове забезпечення.

Перейдемо до того, як здійснюється механізм електронного цифрового підпису. Якщо говорити стисло, то електронний цифровий підпис оснований на шифруванні.

5.4. Симетричні й несиметричні методи шифрування

З давніх часів застосовуються різні засоби шифрування повідомлень (загальний термін – *криптографія*). Належне шифрування має забезпечувати кожній зі сторін відносно впевненість у тому, що автором повідомлення дійсно є партнер (ідентифікація партнера) і що повідомлення не було змінене в каналі зв'язку (аутентифікація повідомлення).

Метод шифрування – це формальний алгоритм, що описує порядок перетворення повідомлення в зашифроване. Ключ шифрування є набором даних, необхідних для застосування методу шифрування.

Існує нескінченна безліч методів (алгоритмів) шифрування. Наприклад, ще Гай Юлій Цезар для зв'язку з Римським сенатом використовував метод *підстановки з ключем, рівним трьом*. У повідомленні кожен символ заміщався іншим символом, що відстоїть від нього в алфавіті на три позиції. Цей метод дуже простий. Зашифруємо, наприклад, слово “Гай”. Букви цього слова займають у алфавіті, відповідно, такі місця: 4, 1 та 14. Додаємо ключ, тобто число три. Одержуємо: 7, 4 та 17. На цих місцях в алфавіті стоять букви “е”, “г” та “м”, отже, слово “Гай” після шифрування набуде такого написання – “егм”.

Цей шифр можна легко зламати перебором усіх ключів: 1, 2, 3, ... На комп'ютері це займе дуже мало часу, тому що варіантів небагато. А саме – це кількість букв у алфавіті, тобто 33. Щоб підвищити захист, треба використовувати *багатоалфавітний ключ шифрування*, наприклад, 3-5-7. Це означає, що перший символ зміщується на три позиції, другий – на п'ять, третій – на сім. Потім процес циклічно повторюється. Тепер варіантів 33 у степені 3, тобто 35937. А якщо довжина ключа 12, то варіантів

більше ніж одиниця з 18 нулями. Легко віриться, та це й справедливо, що такий шифр зламати неможливо, навіть із застосуванням найновітнішої комп'ютерної техніки.

Розглянутий метод багатоалфавітної підстановки являє класичний приклад *симетричного шифрування*. Симетричність виявляється в тому, що обидві сторони використовують той самий ключ. Яким ключем повідомлення шифрувалося, тим же ключем і дешифрується. Це недолік, бо для використання симетричного алгоритму сторони повинні попередньо обмінятися ключами, а для цього потрібне пряме фізичне спілкування. Тому алгоритми симетричного шифрування прямо не використовуються в електронній комерції та сучасному урядуванні. Наприклад, кожному покупцю інтернет-магазину (їх тисячі) потрібно створити по ключу, десять ці ключі зберігати й невідомо як передавати.

В останні тридцять років з'явилися й одержали розвиток методи *несиметричної криптографії*. Саме на них і оснований електронний документообіг та електронний цифровий підпис зокрема.

Несиметрична криптографія використовує спеціальні математичні методи, на основі яких створено програмні засоби, які називаються засобами електронного цифрового підпису. Після застосування одного з таких засобів утворюється пара взаємозалежних ключів з унікальною властивістю: *те, що зашифровано одним ключем, може бути дешифровано тільки іншим і навпаки*. Власник пари ключів залишає один ключ собі, а інший ключ розсилає своїм адресатам. Публікація ключа може відбуватися прямим розсиланням, наприклад, електронною поштою або розміщенням ключа на своєму сайті, де його зможе одержати кожен бажаючий. Ключ, залишений для себе, називається *закритим* чи *особистим* ключем. Опублікований ключ називається *відкритим* чи *публічним*.

Закон України “Про електронний цифровий підпис” визначає ці поняття так: “*особистий ключ* – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису”.

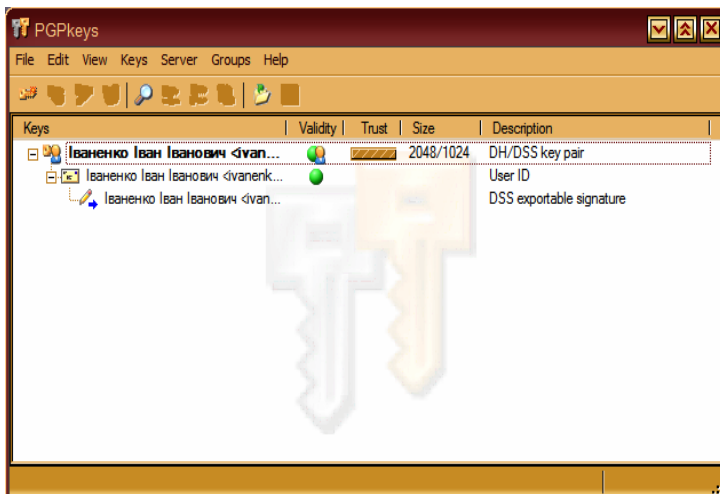


Рис. 5.1. Пара ключів несиметричного шифрування, створена за допомогою шифрувальної програми PGP 8.

Повідомлення (замовлення, договори, розпорядження тощо), які надсилаються власнику ключової пари, шифрують його відкритим ключем. Дешифрування виконується за допомогою закритого ключа.

Це можна уявити собі так. Відкритий ключ – це замочок, який сам замикається, а закритий ключ – це ключ від цього замочка. Адресат кладе своє повідомлення у коробочку та замикає тим замочком. Тепер добратися до повідомлення, тобто розшифрувати його, може лише власник закритого ключа.

Зверніть увагу на важливий аспект. Якщо власник ключів зашифрує повідомлення закритим ключем, то його може розшифрувати будь-яка людина, яка має відкритий ключ. Але якщо ключ підійшов, то це означає, що шифрувати міг тільки власник

закритого ключа, і тільки він. На цьому і базується електронний цифровий підпис.



Рис. 5.2. Так виглядає відкритий ключ, завантажений у поштовий агент MS Outlook Express для пересилки адресату.

А як організувати двосторонній обмін? Дуже просто – дві особи обмінюються своїми відкритими ключами. Кожен із них шифрує свої повідомлення відкритим ключем адресата. Як результат, зберігається таємниця листування. Ніхто, крім них, не може розшифрувати повідомлення, що до них надходять.

А як організувати двосторонній обмін з ідентифікацією? Тобто щоб додатково гарантувати, що повідомлення одному з

них надходять від другого. Теж дуже просто. Згадаймо знову про замочки – щоб переслати повідомлення, один із них замикає повідомлення у коробочку на два замочки – свій (закритий) та чужий (відкритий). Другий із них відкриває коробочку теж двома ключами – своїм (закритим) та чужим (відкритим). Тепер другий точно знає, що повідомлення прийшло від першого та його ніхто під час пересилання не міг розкрити.

Зауважте, що хоча на шляху від одного адресата до другого ніхто не зможе прочитати повідомлення, його зміст легко можна змінити. Як з цим боротися? Слід використовувати дайджест повідомлення.

5.5. Поняття про дайджест повідомлення

Дайджест повідомлення – це унікальна послідовність символів, що однозначно відповідає змісту повідомлення. Зазвичай дайджест має фіксовану ємність – 128 чи 168 бітів, що не залежить від довжини самого повідомлення. Дайджест вноситься до складу електронного цифрового підпису разом із відомостями про автора та зашифровується разом з ними.

Найпростіший прийом створення дайджесту – *контрольна сума символів*. Наприклад, якщо букві “а” відповідає в таблиці ASCII число 192, букві “б” – число 193, а букві “в” – 194, то контрольна сума тексту “абв” – $1 \cdot 192 + 2 \cdot 193 + 3 \cdot 194 = 1160$. Для великого за обсягом тексту це буде величезне число, тому, щоб одержати контрольну суму в 128 бітів, її переводять у двійковий вигляд, тобто який вона і має у комп’ютері, та беруть останні 128 знаків.

Зрозуміло, що при зміні змісту, навіть однієї букви, зміниться і контрольна сума. Множення на 1, 2, 3 і так далі у формулі для підрахунку контрольної суми необхідне для того, щоб не можна було переставити букви без зміни контрольної суми. Про правильну контрольну суму користувач довідається з підпису і, порівнявши їх, виявить стороннє втручання. Зрозуміло, що цю операцію комп’ютер робить автоматично.

Існують більш надійні способи, щоб зловмисник не зміг змінити повідомлення так, щоб зберегти контрольну суму, якщо шифр буде зламаний і контрольна сума стане відомою зловмис-

нику. Для цього використовують спеціальні *хеш-функції* (необоротні функції). Це означає, що за контрольною сумою легко знайти значення цієї функції – *хеш-код*. Але за хеш-кодом неможливо відтворити контрольну суму. Точніше, мільярди мільярдів контрольних сум дають точнісінько той самий хеш-код.

До речі, так зберігають паролі, наприклад, на інтернет-сайтах. Щоб їх не вкрали, зберігають лише хеш-коди. Самих паролів немає, так що й красти нічого. У разі перевірки пароля, наданого користувачем, обробляють пароль хеш-функцією, тобто одержують його хеш-код та порівнюють з хеш-кодом, який зберігають.

Повернемося до дайджесту повідомлення. Контрольна сума обробляється хеш-функцією, щоб утворити хеш-код (аутентифікацію повідомлення). Хеш-код так само унікальний для даного повідомлення, як і відбитки пальців для людини. Це і є дайджест повідомлення. Його називають *відбитком* чи *відтиском*. Іноді – *електронною печаткою*. Дайджест повідомлення приєднується до електронного підпису і стає його складовою частиною.

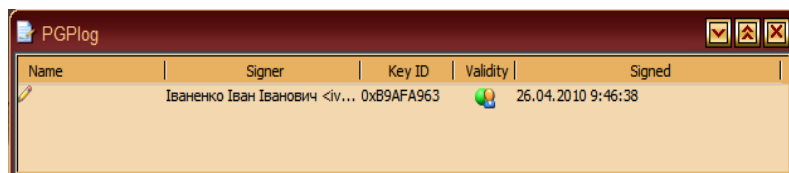


Рис. 5.3. Вікно шифрувальної програми PGP 8, в якому повідомляється, що підпис чинний і документ є аутентичним.

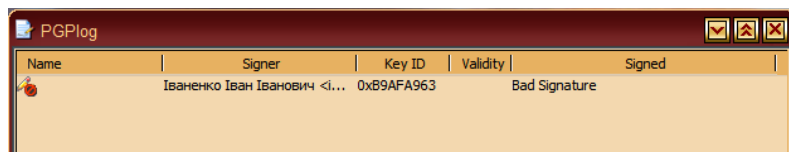


Рис. 5.4. Вікно шифрувальної програми PGP 8, в якому повідомляється, що підпис нечинний та/або документ є зміненим.

Сторона, що приймає повідомлення, розшифровує своє повідомлення, перевіряє електронний підпис за допомогою своєї

половини ключа, потім обробляє повідомлення тією ж хеш-функцією, що й відправник, після чого звіряє отриманий дайджест із тим, що містився в підписі. Якщо вони збіглися, значить, повідомлення не піддалося змінам у каналі зв'язку. Природно, що всі ці дії виконуються автоматично без участі самого користувача.

5.6. Поняття про криптостійкість засобів електронного цифрового підпису

Електронний цифровий підпис теж може бути підданий фальсифікації. Щоб його фальсифікувати, зловмисник повинний тим чи іншим способом одержати доступ до закритого ключа. У таких випадках говорять про *компрометацію закритого ключа*, з якої випливає *компрометація електронного підпису*. У ст. 1 Закону України “Про електронний цифровий підпис” це поняття визначається так: “*компрометація особистого ключа* – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа”.

Є традиційні й нетрадиційні способи компрометації. Традиційні – це викрадення ключа шляхом копіювання через несанкціонований доступ або викрадення устаткування чи викрадення через змову з особою, яка його використовує.

Захист від компрометації певною мірою забезпечує законодавство. У ст. 15 вказано: “Особи, винні у порушенні законодавства про електронний цифровий підпис, несуть відповідальність згідно з законом”.

Питаннями злому шифрів, розробкою методів, що дозволяють розшифровувати інформацію (знімати з неї захист) та оцінювати якість захисту інформації шифром (говорять: його *криптостійкість*) займається галузь криптографії – *криптоаналіз*.

Можливість злому шифру визначається продуктивністю обчислювальної техніки та ємністю ключа, яка вимірюється в бітах (двійкових розрядах). Чим більший ключ, тим більший час перебору можливих значень. Наприклад, дуже просто оцінюється криптостійкість симетричних ключів.

Якщо довжина ключа 40 бітів, то для його реконструкції треба перебрати 2^{40} чисел. Кілька сучасних комп'ютерів вирі-

шати цю задачу за добу. Якщо довжина 64 біти, то необхідна мережа з декількох десятків комп'ютерів. Задача вирішується протягом декількох тижнів. 128 бітів – час реконструкції у мільйони разів більше, ніж вік Всесвіту!

Щоб не заходити далеко, можна користуватися *принципом достатності шифрування та економічної доцільності* – повідомлення вважається досить захищеним, якщо його розшифровка потребує матеріальних витрат, які значно перевершують цінність інформації, яка міститься в повідомленні.

5.7. Технічне та юридичне забезпечення електронного цифрового підпису

Є простий прийом підміни відкритого ключа з метою створення помилкового (злочинного) каналу зв'язку. Припустимо, сторона А бажає перехопити чужі дані. Вона створює пару ключів і публікує відкритий ключ нібито від партнера В. Тоді всі повідомлення від партнера С до партнера В будуть легко перехоплюватися і читатися стороною А.

У відкритому ключі наводяться дані про власника, але в ньому нема засобів, які б свідчили, що ці дані не підмінені. Без вирішення цього питання механізм електронного цифрового підпису не може бути використаний ні в електронній комерції, ні в електронному документообігу. Тому Закон України “Про електронний цифровий підпис” та ще деякі державні законодавчі акти присвячені механізму підтвердження особи власника відкритого ключа, такому, як *сертифікація відкритих ключів*. У всіх випадках вказаний механізм ґрунтується на тому, що вводиться (призначається) додаткова сторона, яка засвідчує належність відкритого ключа конкретній юридичній чи фізичній особі.

У ст. 3 Закону зазначено, що електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо “електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифро-

вого підпису;

особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті”.

Основне поняття – “*посилений сертифікат ключа*” – визначено в ст. 1 Закону:

“*посилений сертифікат відкритого ключа* (далі – *посилений сертифікат ключа*) – сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом”.

У ст. 6 зазначено необхідні дані, що повинен містити сертифікат ключа, а в статтях 8, 9, 10 та 11 вказані вимоги до центрів сертифікації ключів та інших уповноважених на це органів, а також їх права та обов’язки.

Таким чином, особа, яка створила собі пари ключів, повинна звернутися в орган, уповноважений виконати сертифікацію, та отримати сертифікат ключа. Центр сертифікації перевіряє належність відкритого ключа заявнику і засвідчує цей факт додаванням до відкритого ключа свого підпису, зашифрованого власним закритим ключем. Будь-який партнер, бажаючи вступити в контакт із власником відкритого ключа, може прочитати запис, що засвідчений, за допомогою відкритого ключа центру сертифікації. Якщо цілісність запису не порушена і він довіряє центру сертифікації, то може використовувати відкритий ключ іншого партнера для зв’язку з ним.

Перший у світі закон про електронний цифровий підпис був прийнятий у березні 1995 р. Законодавчими зборами штату Юта (США).

Німецький закон про електронний цифровий підпис набув чинності в 1997 р. і став першим європейським законодавчим актом у цій сфері.

Комісія ООН з міжнародного торгового права розробила модельний закон, який запропоновано використовувати як основу при розробці національних законодавств. Цей закон опублікований у 1995 р.

Закони України “Про електронний цифровий підпис” та “Про електронні документи та електронний документообіг” від 22 травня 2003 р. повністю узгоджені зі стандартами міжнародного права.

Контрольні питання

1. Поясніть, що таке електронні бізнес і комерція та чим вони відрізняються?

2. Як визначає Закон України “Про електронні документи та електронний документообіг” поняття “електронний документ”?

3. Для чого за Законом України “Про електронні документи та електронний документообіг” потрібен електронний підпис?

4. Як трактує поняття “електронний документообіг” Закон України “Про електронні документи та електронний документообіг”?

5. Яким є порядок відправлення, передавання електронних документів та їх одержання за Законом України “Про електронні документи та електронний документообіг”?

6. Як визначає Закон України “Про електронний цифровий підпис” поняття “електронний підпис” та “електронний цифровий підпис”? Яка різниця між ними?

7. Які позитивні властивості має електронний підпис у порівнянні зі звичайним підписом? А які недоліки?

8. Що таке шифрування та ключ шифрування? Для чого застосовується шифрування?

9. Як буде виглядати слово “академія”, якщо б його зашифрував Гай Юлій Цезарь?

10. У чому різниця між симетричною та несиметричною криптографією?

11. Що таке закритий і відкритий ключі шифрування? Чим вони відрізняються?

12. Як за допомогою несиметричного шифрування організувати двосторонній обмін даними з ідентифікацією відправників?

13. Для чого потрібен дайджест повідомлення?

14. Як використовуються хеш-функції та хеш-код?

15. Які способи компрометації електронного підпису ви знаєте? Яке завдання науки криптоаналізу?

16. Для чого потрібна сертифікація відкритих ключів шифрування та який документ свідчить про її проведення?

17. Чи може електронний цифровий підпис за правовим статусом прирівнюватися до власноручного підпису?

18. Розкажіть про правове забезпечення цифрового підпису в міжнародному та вітчизняному законодавствах.

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАКОНОТВОРЧОЇ ТА ПРАВОЗАСТОСОВНОЇ ДІЯЛЬНОСТІ

Підвищення рівня обґрунтованості рішень, особливо державного значення, оперативність реагування органів влади на соціально-економічні процеси вимагають широкого використання сучасних наукових методів і засобів опрацювання інформації.

Необхідним є належне наукове обґрунтування проєктів нормативно-правових актів, зменшення впливу суб'єктивних чинників, скорочення технологічного циклу нормотворчого процесу, своєчасне й повне забезпечення органів державної влади, юридичних і фізичних осіб інформацією про чинні закони та підзаконні акти, їх тлумачення, а також збір даних зворотного зв'язку про практичні наслідки дії нормативних актів, аналіз, планування розробки нових, розгляд і схвалення відповідних змін до чинних законів та підзаконних актів.

З 1990 р. спільними зусиллями фахівців підрозділів Апарату Верховної Ради України, Національної академії наук України, Академії правових наук України, Дослідницької служби Конгресу США створена й розвивається комплексна багатофункціональна комп'ютеризована система інформаційно-аналітичного забезпечення (СІАЗ) законотворчої, правозастосовної та правоосвітньої діяльності, послугами якої щоденно користуються десятки тисяч державних і недержавних структур, юридичних та фізичних осіб як в Україні, так і за її межами.

Ця система має для України загальнодержавне, народногосподарське та міжнародне значення. Вона інтегрує десятки територіально рознесених автоматизованих комплексів інформаційно-аналітичного опрацювання даних, що забезпечують конвеєрну обробку та синхронізацію потоків інформації, оперативний контроль і прозорість законотворчого процесу, безперервне відстежування життєвого циклу кожного нормативно-правового акта.

6.1. Комп'ютерна мережа Верховної Ради України

Комп'ютерна мережа Верховної Ради України є ланкою CIA3. Це одна з найпотужніших мереж, що функціонують в органах державної влади, оснащена сучасною технікою, інформаційними ресурсами та програмними засобами.

Мережа розташована у приміщеннях Верховної Ради України, об'єднує понад 1500 робочих станцій і має доступ до глобальної мережі Інтернет, що дає можливість користувачам ознайомлюватись із законодавством України, брати участь у формуванні пропозицій до законопроектів, залучати необхідні світові інформаційні ресурси, здійснювати порівняльний аналіз нормативних актів України із законодавством інших країн, використовувати світовий досвід, гармонізувати законодавчу базу України з міжнародним правом. Доступ до інформації надається з робочих місць (комп'ютерів) секретаріатів комітетів, фракцій, груп та підрозділів Апарату Верховної Ради України.

6.2. Призначення та основні принципи побудови інтегрованої системи інформаційно-аналітичного забезпечення (CIA3) законотворчої діяльності Верховної Ради України

Призначення CIA3 полягає у виконанні наступних функцій:

- формування інформаційно-правової бази держави;
- поліпшення її якості;
- скорочення технологічного циклу законотворчого процесу, моделювання, аналізу, експертизи, обґрунтування з наступним прийняттям нормативних актів;
- своєчасне й повне інформування працівників структур державної влади, юридичних і фізичних осіб про чинні закони й підзаконні акти, їх роз'яснення і збір інформації про практичні наслідки їх дії.

Основні принципи побудови системи інформа-

ційно-аналітичного забезпечення законотворчої та правозастосовної діяльності визначаються великим обсягом опрацьовуваної інформації, складністю алгоритмів перетворення даних, значною кількістю користувачів. Вона належить до відкритих систем, безперервно обслуговує в реальному часі правотворчий та правозастосовний процеси. Опрацювання потоків інформації охоплює декілька етапів, кожний з яких має свої специфічні алгоритми й технологічні операції. Так, робота над законопроектом тільки в підрозділах Верховної Ради України складається з близько ста різних операцій опрацювання даних, кожна з яких є важливою в розробці якісного нормативно-правового акта. Системна інформатизація законотворчого процесу в українському парламенті дозволила впровадити сучасну організацію та технологію опрацювання даних, що охоплює використання нових методів і засобів, фіксацію та попередню підготовку інформації, зберігання, актуалізацію, запобіжне дублювання інформації на випадок можливих пошкоджень оригіналу й оперативне надання даних користувачам у потрібних їм аспектах. При цьому пропонуються різноманітні форми надання інформації: одержання твердих копій, видача на екран, компакт-диски та інші носії.

Створення та розвиток СІАЗ відбуваються із дотриманням низки загальновідомих *принципів*, які слід розрізняти кожний окремо.

Принцип системного підходу базується на системному аналізі об'єкта, потоків інформації, алгоритмів їх перетворення, а також системи в цілому, тобто на виборі цілей, засобів, етапів, критеріїв доцільності інших чинників, що впливають на функціонування системи. Ці чинники можуть мати правовий, політичний, економічний, соціальний, організаційний, технічний характер.

Сутність *принципу “нових завдань”* полягає в перебудові традиційних методів і прийомів керування відповідно до нових можливостей сучасних методів і засобів обробки даних, тобто в докорінній реорганізації всієї системи обробки інформації та керування на нових засадах. На практиці це означає, що аналіз існуючої системи керування виявляє об'єктивно необхідні нові ідеї, підходи, завдання, алгоритми, які можна реалі-

зувати в умовах функціонування комп'ютеризованої системи.

Створення загальнодержавної міжвідомчої СІАЗ – трудоємка і тривала робота, успішне здійснення якої залежить від додержання *принципу стадійності*. За цим принципом основні компоненти системи впроваджуються поетапно, послідовно, функції та потенційні можливості, закладені на попередньому етапі, реалізуються на наступному. Результатом цих дій є підвищення ефективності системи.

Принцип відкритості (незамкненості) полягає в можливості внесення до складу системи нових елементів (модулів) та використання системи або її окремих складових як ланки більш високого рівня ієрархії та інтеграції на міжвідомчому рівні. Це необхідно тому, що в процесі розвитку системи в цілому та окремих її компонентів постають нові проблеми, виникають потреби, пов'язані з кінцевим завданням управління. Необхідною умовою є швидка реакція СІАЗ на ці зміни, що забезпечує саме цей принцип.

Принцип гнучкості системи передбачає можливість зміни, адаптації структури системи та її складових, а також деяких функцій із затратною значно менших ресурсів порівняно зі створенням нових ланок або системи в цілому.

Принцип кооперування ресурсів реалізується через кооперування розробників та матеріальних ресурсів на міжгалузевому рівні для створення уніфікованих компонентів інтегрованої системи, оскільки важливою умовою злагодженого функціонування останньої потрібний єдиний підхід, а також технічне, інформаційне, програмне та методологічне поєднання всіх компонентів.

Для підтримки процесу розроблення та застосування законів, інших правових актів у складі системи інформаційно-аналітичного забезпечення законотворчої та правозастосовної діяльності розроблено й впроваджено низку забезпечувальних (забезпечують технологічний цикл законотворчої та правозастосовної діяльності) і спеціалізованих (функціональних) підсистем, автоматизованих робочих місць (АРМ).

Забезпечувальні підсистеми, кожна з яких,

виконуючи притаманне тільки їй завдання, у сукупності зумовлює функціонування всієї системи, це:

1. Підсистема інформаційного забезпечення – комплекс засобів знакового опису даних, а також форм їх подання та організації власне даних в обсязі, необхідному їй достатньому для функціонування системи, а також принципів, методів, способів, правил, схем, алгоритмів, за якими здійснюються збір даних, їх зберігання, пошук, контроль, редагування тощо.

2. Підсистема програмного забезпечення – сукупність комплексів, систем, бібліотек програм різного призначення, методів та засобів алгоритмізації.

3. Підсистема технічного забезпечення є сукупністю засобів, що реалізують процеси збору, обробки, зберігання, пошуку, відображення інформації, а також забезпечують зв'язок ланок системи організаційного керування між собою (ЕОМ, комп'ютерні мережі, периферійна та організаційна техніка, засоби зв'язку тощо).

Сукупність *функціональних підсистем* виконує всі функції керування, водночас кожна з них має власну цільову функцію.

“*Законопроект*” – підсистема, що обслуговує процес розроблення законодавчих актів від часу реєстрації початкового варіанта, вивчення проблеми, що потребує правового регулювання, збирання пропозицій, необхідної інформації із зовнішніх джерел, формування законопроектів до кінцевого юридичного оформлення. Вміст: тексти, порівняльні таблиці, інформаційно-аналітичні комплекси (планування законотворчої діяльності, реєстрація і контроль проходження законопроектів).

“*Рада*” – підсистема, що забезпечує голосування (підписання, анонімне, фракцій, груп), супроводження пленарних засідань Верховної Ради України, накопичення інформації про роботу народних депутатів під час обговорення законопроектів на сесії та проведення аналізу діяльності парламенту і фракцій народних депутатів, а також стенографування – комп'ютеризовану підготовку стенограм пленарних засідань Верховної Ради Украї-

ни в режимі реального часу.

“Еталонна база правової інформації” та її похідні охоплюють кінцеву продукцію нормотворчого процесу і дають змогу швидко здійснювати багатоваріантний пошук необхідних даних. Еталонна база даних нормативно-правових актів є автоматизованим фондом офіційних документів, що оперативно актуалізується (підтримується в контрольному стані) і захищена від пошкодження.

6.3. Загальноправові бази даних

Загальноправові бази даних є похідними від еталонної бази правової інформації і зорієнтовані на забезпечення правовою інформацією широкого кола користувачів за допомогою інформаційно-пошукових систем (ІПС) “НАУ”, “Ліга”, “Законодавство” та ін.

Згідно з основними вимогами ІПС має забезпечувати:

- швидкий, повний і точний пошук нормативних документів за реквізитами (дата видання, тип документа, орган влади), ключовими словами та кодами тематичного юридичного класифікатора. Редакції документів, зв’язки між документами – це ті тісно пов’язані з документами об’єкти, маніпулювання якими повинно бути передбачено в ІПС;
- автентичність знайдених документів, перегляд усіх їх редакцій, зумовлених внесенням змін;
- комфортність роботи користувача з програмним забезпеченням автоматизованих робочих місць;
- швидко актуалізацію текстів правових документів із внесенням змін і відповідних повідомлень про зміни та зі збереженням попередніх редакцій документів;
- збереження електронних архівів нормативних правових документів, що втратили чинність, та можливість науково-історичного аналізу їх змісту;
- автоматизацію перекладу правових текстів з української мови на іноземні.

6.4. Автоматизована інформаційно-пошукова система “Нормативні акти України”

6.4.1. ДПС як інструмент отримання інформації

Значення ефективної системи поширення правової інформації для сучасного цивільного суспільства важко переоцінити. Стає очевидним, що жодна реформа економічного і політичного устрою в країні в принципі неможлива без доступу мільйонів громадян і сотень тисяч підприємств до правової інформації. Згідно зі статтями 10 та 12 Закону України “Про інформацію” від 2 жовтня 1992 р. № 2657-ХІІ: “Право на інформацію забезпечується створенням механізму здійснення права на інформацію”. Це обумовлює використання ефективних інструментів для роботи з величезним масивом найрізноманітнішої правової інформації. Такі інструменти можуть бути створені лише на основі комп’ютерних технологій. Ними є автоматизовані інформаційно-пошукові системи – комп’ютерні довідкові правові системи. Комп’ютерна довідкова правова система – це програмний комплекс, що включає масив правової інформації і програмні інструменти, що дозволяють фахівцеві працювати з цим масивом інформації (проводити пошук конкретних документів або їх фрагментів, формувати добірки необхідних документів, виводити інформацію на друк і т. д.).

Перед кожним користувачем ДПС як при ухваленні рішення про вибір тієї або іншої системи, так і при використанні її в конкретній роботі постає питання визначення ключових властивостей систем, на які треба звернути увагу в першу чергу.

1. Якість інформаційного наповнення ДПС:

- повнота інформації;
- оперативність надходження нової інформації;
- достовірність інформації, її автентичність;
- якість юридичної обробки інформації в системах.

2. Якість комп’ютерних технологій, закладених у ДПС:

- пошукові і сервісні можливості;
- можливості використовуваної технології щодо передачі інформації та її актуалізації у користувача.

3. Загальний рівень сервісу і наявність додаткових послуг, що надаються користувачеві конкретною ДПС.

Пакети прикладних програм правових довідкових систем є ефективним інструментом роботи з великими обсягами законодавчої інформації, яка поступає безперервним потоком. Практично в усіх економічно розвинутих країнах є довідкові правові системи. У США – це Wru, Lexis та ін.; у Великобританії – Infolex, Prestel, Polis та ін.; в Італії – Italguire, Enlex; в Бельгії – Creodor; в Німеччині – Jurist, Lexinform та ін.; а Австрії – RDB; в Канаді – Datum; у Франції – Iretiv та ін.

6.4.2. Особливості АПС “Нормативні акти України”

Ця система є сучасним і простим засобом для роботи з правовою інформацією. Вона призначена для ведення, тиражування і використання електронної бібліотеки правової інформації, містить спеціалізоване програмне забезпечення із захистом і базу даних нормативних актів. База даних складається з автономних підсистем, кожна з яких містить документи певного типу. Відновлення бази здійснюється щотижня за допомогою спеціально організованого файлу – протоколу відновлень, який складається як із знову прийнятих, так і нової редакції раніше прийнятих документів. Протоколи відновлень надходять користувачеві від фірми “ІНФОРМТЕХНОЛОГІЯ” по мережі. Щоденно база даних поповнюється 70 - 100 документами.

Існують окремі бази даних з текстами документів: українською “НАУ-Експерт” (до складу “БД НАУ - Експерт” входить інтелектуальна надбудова “НАУ-Експерт”, що керує пошуком інформації у базі даних), російською (“НАУ - Русскоязычная”) та англійською (“NAU-English”) мовами (в офіційних та редакторських перекладах), а також збірник законів для КПК, смартфонів, флеш-карток – безкоштовна база даних, що вільно розповсюджується (містить Конституцію України, рішення Конституційного Суду України щодо тлумачення Конституції України, кодекси та основні закони України в поточній редакції).

Система має потужний пошуковий апарат та різноманітні

засоби відображення документів, кількість яких становить близько 100 000. ІПС містить:

1. Документи органів влади України:

- Верховної Ради України: Конституція, кодекси, закони, постанови;

- Президента: укази, розпорядження;

- Кабінету Міністрів: постанови, розпорядження, декрети;

- Конституційного Суду, Верховного Суду, Вищого господарського суду;

- Міністерств та відомств (зокрема, Державної податкової адміністрації, Національного банку, Державної митної служби, Фонду державного майна тощо).

2. Міжнародні угоди: двосторонні угоди України, міжнародні конвенції.

3. Органів влади СРСР та УРСР: чинні нормативні акти.

4. Документи регіонального законодавства.

5. Довідник органів влади.

6. Відомості про політичні партії і діячів.

7. Огляди преси тощо.

Особливості сервісів “НАУ”:

- відмінне структурування та відкритість інформації, що дозволяє знайти документ навіть без виклику пошуків;

- можливість пошуку документів за звичайною фразою природною мовою;

- повна історія статусу та редакцій нормативного акта (включаючи майбутні редакції);

- дослівне порівняння редакції кодексів та законів;

- добірки матеріалів (консультацій, судової практики, підзаконних актів) до статей кодексів та законів;

- ведення власної та/чи корпоративної бази;

- створення колекції власних пошукових запитів;

- використання маркерів, закладок, контролю документів;

- генерація щоденних та щотижневих звітів про зміни у законодавстві.

Система “НАУ” функціонує як на окремих персональних

комп'ютерах, так і в локальній мережі.

Система має багатовіконний інтерфейс із виділеним головним вікном (рис. 6.1.). Головне вікно відкривається в момент запуску системи і візуально відрізняється від інших вікон тим, що має у своєму лівому верхньому полі логотип “НАУ”. Закриття головного вікна здійснюється кнопкою в правому верхньому куті і спричиняє закриття всіх інших вікон продукту.

Крім головного вікна в процесі роботи можуть відкриватися наступні робочі вікна:

- вікна переліків знайдених документів;
- вікна текстової інформації;
- форми запитів на пошук і вивід інформації, експорт власної бази, а також вікна-повідомлення про помилки, попередження, запити на виконання операції, звіти про виконання операції.

Головне і робочі вікна програми мають ліву панель функцій вікна. Ліва панель у вікнах (крім форм запитів) може мати згорнутий і розгорнутий вигляд. Змінити вигляд можна кнопкою “Згорнути/Розгорнути” у верхньому лівому полі вікна.

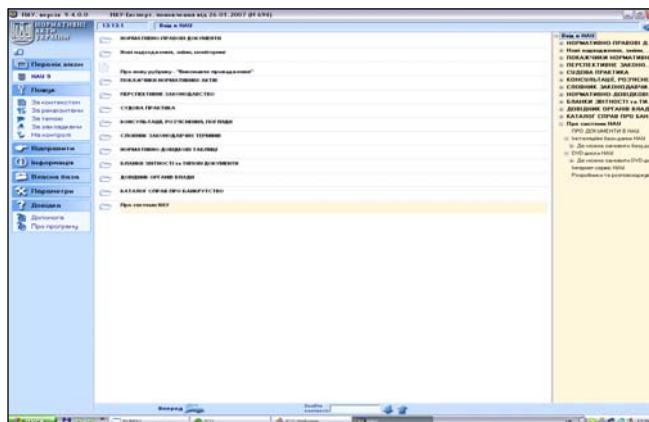


Рис. 6.1. Головне вікно АПС “НАУ”.

Групове меню “Перелік вікон” на лівій панелі вікон відображає поточний перелік відкритих вікон продукту. Перейти до потрібного вікна можна натисканням клавіші миші на відповідний пункт меню в переліку.

Форми запитів можна встановити в повноекранний режим або закрити кнопками в правому верхньому полі вікна. Режим згортання форм запитів не передбачений.

Форми запитів мають вбудовану допомогу. Детальні інструкції із заповнення пошукової форми можна отримати, вибравши групове меню “Допомога” на лівій панелі вікна форми. Допомогу із заповнення кожного параметра форми можна отримати, вибравши мишею відповідну назву параметра.

6.4.3. Функціональні можливості ІПС

База даних має ієрархічну структуру, що дає змогу легко орієнтуватися в її змісті та швидко знаходити потрібні розділи. Документи систематизовано за типами, тематикою, офіційними публікаціями, хронологією надходження.

У будь-якому розділі бази працюють універсальні пошуки:

- за словом чи контекстом у тексті (рис. 6.2.);
- за контекстом у назві;
- за датою.

Передбачено функціональні клавіші: [F6] – пошук за словом у тексті, [F7] – пошук за контекстом у назві, номері, [F8] – пошук за контекстом у тексті, [F9] – пошук за датою // інтервалом дат. При пошуку за контекстом можна також перевіряти інтервал дат. Важливо, що при пошуку за контекстом слова треба набирати слова без закінчень. Існує 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 також знайти за допомогою спеціальних пошуків за їх реквізитами: видавцем, номером, датою, назвою, видом, статусом, відомостями про реєстрацію (рис. 6.3.).

Для формування пошукового запиту надається можливість користуватися словниками всіх можливих значень реквізитів.

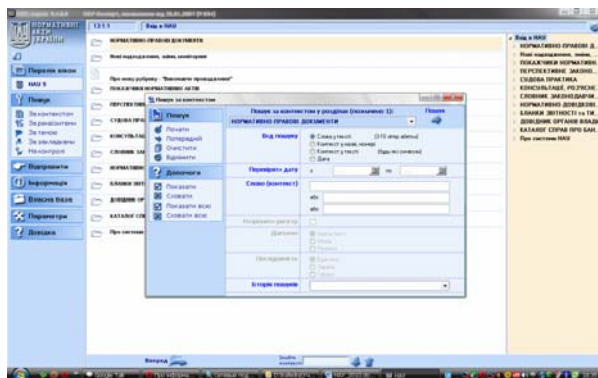


Рис. 6.2. Вікно пошуку за контекстом в АПС “НАУ”.

При введенні або зміні якого-небудь реквізиту програма миттєво перераховує будь-яку комбінацію реквізитів, допомагаючи звужувати поле пошуку.

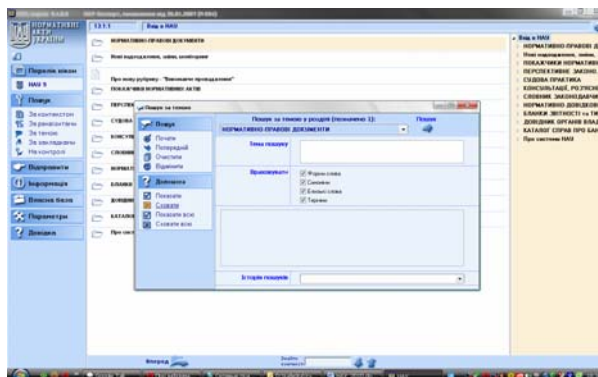


Рис. 6.3. Вікно пошуку за тематикою в АПС “НАУ”.

6.4.4. Робота зі знайденою інформацією

Списки знайдених документів можна: відсортувати за датою чи типом, а також провести серед них додатковий пошук.

Будь-яку знайдену інформацію (списки, тексти, довідки) можливо роздрукувати, встановивши шрифти, сторінки, колонти-тули, експортувати у Word, записати у файл, помістити у буфер обміну для передачі в іншу програму, зберегти у власній базі.

У текстах документів є можливість поставити свій коментар у будь-якому місці, виділити маркером будь-які фрагменти.

За допомогою ПС “НАУ” можна отримати відомості про публікації, добірки судової практики до нормативних актів, добірки консультацій та коментарів до нормативних актів, створити пошуки документів за зв’язками та посиланнями.

6.4.5. Створення власної бази

Програма дозволяє користувачеві створити власну базу (чи декілька баз) з довільною структурою. У власній базі можна вмістити та організувати за тематиками: власні тексти та файли; посилання на документи основної бази; посилання на розділи та рубрики основної бази; закладки-коментарі до текстів; колекції пошукових запитів.

У власній базі автоматично працюють універсальні пошуки. Власними базами можна обмінюватися з іншими користувачами “НАУ”.

6.4.6. Елементи інтелектуального пошуку: підсистема “Експерт”

Існує 10 версій інсталяційних баз даних “НАУ”, які розрізняються за складом інформації, мовою документа, сервісними можливостями, а також збірник законів для КПК, смартфонів, флеш-карток – безкоштовна база даних, що вільно розповсюджується. Містить Конституцію України, рішення Конституційного Суду України щодо тлумачення Конституції України, кодекси та найважливіші закони України в поточній редакції. До складу БД “НАУ-9” входить інтелектуальна надбудова “НАУ-Експерт”, що при керуванні пошуком інформації у базі даних “розуміє” при-

родну мову пошукового запиту, а саме враховує форми слів, відмінки, синоніми, забезпечує розпізнавання нормативно визначених термінів, аналіз змісту словосполучень, оцінює ступінь відповідності результатів пошуку запиту.

З жовтня 2007 р. почалося розповсюдження нового унікального за своїми інформаційними та сервісними можливостями продукту “МЕГА-НАУ”. Це інтегрований банк даних, який об’єднує базу судових рішень (1,5 млн рішень 650-ти судів України) і базу правової та аналітичної інформації “НАУ-Експерт”. Система унікальна за обсягом інформації (близько 2 млн документів) і за системою зв’язків, що інтегрує судові рішення і нормативні акти в єдиний аналітичний комплекс.

6.5. Всесвітня електронна мережа правових документів

У сучасних умовах міждержавного співробітництва законотворча та правозастосовна діяльність потребує використання міжнародної системи правової інформації. Створення в 1976 р. Міжнародної правової бази даних у Правничій бібліотеці Конгресу США було мотивоване бажанням задовольнити таку потребу. База виправдала себе як простий та ефективний засіб швидкого та безпосереднього доступу до складових частин правового середовища різних країн і з часом перетворилася на світову електронну мережу правових документів (Global Legal Information Network – GLIN, www.glin.gov). Систему створено на принципах достовірності джерел, простоти пошуку юридичних документів, багатонаціональної орієнтації.

Згідно з ідеологією та технологією, прийнятою у проєкті GLIN, Апаратом Верховної Ради України здійснено опрацювання “Відомостей Верховної Ради України”, з використанням тезауруса GLIN готуються реферати законів України, постанов Верховної Ради України, відбувається обмін ними через мережу Інтернет.

Використання інформаційної системи GLIN, правових баз даних Російської Федерації, Євросоюзу, інших держав розглядається як складова частина інформаційно-аналітичного забезпечення законодавчої та правозастосовної діяльності, як засіб розши-

рення меж інформаційного забезпечення українського парламенту, реалізації міжпарламентських інформаційних обмінів, гармонізації законодавства України з міжнародним законодавством.

Таким чином, аналітик має можливість знайти документи, що цікавлять його, як з-поміж законодавчих актів України, так і в законодавчій базі іншої країни (або країн), отримати переклад іноземного документа українською мовою, зберегти його у вигляді файла або надрукувати.

Контрольні питання

1. Визначте поняття “інформаційно-пошукова система”.
2. Назвіть основні вимоги до комп’ютеризованої системи правової інформації.
3. Визначте роль інформаційно-пошукових систем у правовій сфері.
4. Що таке нормативна правова інформація. Які основні її класифікації існують у правовій науці?
5. Що таке автоматизована інформаційна система?
6. Наведіть основні класифікації автоматизованих інформаційних систем.
7. З яких складових утворюється база даних?
8. Які функціональні можливості системи?
9. Як налагоджується система (здійснюється установка шрифту, мови повідомлень)?
10. Перегляд бази даних.
11. Пошук документів у базі.
12. Пошук документів по картотеці.
13. Робота зі списком документів.
14. Робота з текстом документа (використання гіперпосилання, створення і використання закладок, пошук за контекстом, видача інформації про документ, копіювання у власну базу, друк).
15. Створення і робота з власною базою.

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ У ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

7.1. Комп'ютерні технології фіксування судового процесу

Одним із напрямів інформатизації судів є використання комп'ютерних систем фіксації судового процесу. Технічна фіксація судових процесів здійснюється комп'ютерними системами, які дозволяють крім аудіозапису судового процесу отримувати анотацію (журнал, формуляр тощо) подій судового процесу, згідно із аудіозаписом.

Технічний комплекс фіксування ходу судового процесу (далі – комплекс звукозапису) – це сукупність апаратно-програмних засобів, приладів і відповідних інструкцій, що забезпечують належне фіксування, зберігання, копіювання (дублювання) та використання інформації, яка відображає хід судового засідання (судового процесу).

Системи технічної фіксації судових процесів забезпечують такі техніко-технологічні функції:

- 1) реєстрацію вербальної процесуальної складової, яка переважно є доказами;
- 2) створення в реальному або відкладеному часі формуляра судового процесу, який відображає всі основні події судового процесу й нерозривно пов'язаний з фонограмою;
- 3) запис фонограми й нерозривно пов'язаного з нею формуляра на компакт-диск, що не перезаписується;
- 4) підтвердження фонограми електронним підписом, який об'єктивно виключає будь-яку модифікацію фонодокумента та забезпечує його легітимність;
- 5) стенографування за допомогою спеціального програмно-апаратного модуля транскрайбера;
- 6) захист системи від знищення даних і керуючих програм;

- 7) запис звуку з різних мікрофонів по окремих каналах;
- 8) аудіоконтроль процесу запису з можливістю відтворення запису для постійного контролю;
- 9) підтримка роботи в комп'ютерній мережі та можливість зберігання даних технічної фіксації судових процесів на сервері.

На сьогоднішній день у судах використовуються, в основному, такі системи технічної фіксації судових засідань:

- цифровий магнітофон “Тритон” (застосовується в місцевих загальних судах);

- система технічного фіксування судового процесу “СРС-Феміда” (застосовується в місцевих та апеляційних господарських судах);

- система технічного фіксування судового процесу “Оберіг” (застосовується в судах загальної юрисдикції).

Основне завдання систем технічної фіксації судових засідань – належне фіксування, зберігання, копіювання та використання інформації, яка відображає хід судового засідання.

Перед початком судового процесу секретар судового засідання проводить підготовку обладнання, на якому здійснюватиметься фіксування судового процесу, зокрема, перевіряє комплекс звукозапису на відсутність ознак несправності та втручання в роботу його конструкції.

У разі наявності ознак втручання, порушення цілісності пломб, несправності комплексу звукозапису секретар зобов'язаний терміново повідомити про це адміністратора та суддю. Те ж саме секретар повинен зробити і в разі виявлення будь-яких ознак несправності безпосередньо під час фіксування судового процесу.

Секретар не повинен залишати комплекс звукозапису, в якому він зареєструвався, без нагляду, передавати іншим особам пароль або електронний ключ та допускати інших осіб до роботи із системою.

Перед тим як завершити роботу комплексу звукозапису, необхідно його заблокувати або вийти з відповідної програми та завершити сеанс роботи з операційною системою Windows.

Оригінал фонограми повинен зберігатися тимчасово в

комп'ютері чи пристрої, яким безпосередньо робилося фіксування, і не може бути стертим до створення архівної та робочої копій.

Паралельно із записом перебігу судового засідання секретар має вести журнал судового засідання за допомогою спеціальної програми, при цьому повний перебіг процесуальної дії не фіксується. Вимоги до журналу судового засідання визначаються процесуальним законодавством.

Після закінчення судового засідання секретар зберігає та роздруковує журнал судового засідання, підписує його і приєднує до справи, а також створює архівну та робочу копії фонограми судового засідання.

Архівна копія фонограми – запис на відповідному носії комплексу звукозапису, що має статус оригіналу та призначений для довготривалого зберігання в архіві. Архівні копії використовуються у разі недостатності, пошкодження або знищення робочих копій та для вирішення спірних питань.

Робоча копія фонограми – запис на відповідному носії комплексу звукозапису або на комп'ютері архіваріуса. Робоча копія призначена для поточної роботи, наприклад, для створення копій сторонам процесу, прослуховування суддями тощо.

Для кожної судової справи виділяються два компакт-диски: один – для архівної копії, другий – для робочої копії. На ці диски записуються всі фонограми судових засідань у справі. У разі, якщо фонограми засідань не вміщуються на один компакт-диск, виділяються додаткові.

Після створення архівної та робочої копій фонограм із записом перебігу судового засідання компакт-диски повинні пакуватися в конверти. До маркування конверта компакт-диска входять такі відомості: номер судової справи, серійний номер компакт-диска, дата судового засідання, підпис секретаря, примітка.

Архівні копії мають зберігатися в архіві, робочі – у спеціальному конверті разом зі справою. Знищуються вони разом зі справою після закінчення встановленого терміну зберігання справи.

Повноваження щодо створення архівних та робочих копій, підтримання архіву, виготовлення з архівних даних робочих

копій та копій на вимогу учасників процесу, підготовка дисків з фонограмами для передачі в інший суд, ознайомлення учасників процесу з фонограмами покладаються на архіваріуса суду відповідно до “Інструкції про порядок фіксування судового процесу технічними засобами”, яка була затверджена наказом Державної судової адміністрації України 21 липня 2005 р.

7.2. Основні програми фіксування судового процесу

Програма звукозапису судових засідань “Тритон”. Для технічного фіксування судового процесу застосовуються комплекси звукозапису двох типів: персональний комп’ютер зі спеціальним обладнанням і програмним забезпеченням та цифровий магнітофон “Тритон”.

Персональний комп’ютер зі спеціальним обладнанням та програмним забезпеченням складається з:

1) апаратних засобів:

– персонального комп’ютера (мінімальна конфігурація: процесор не менше P300, оперативна пам’ять не менше 32 Мб, твердий диск не менше 1 GB (700 Мб вільного місця), звукова плата, пристрій CD-RW);

- мікшера (може бути вбудований у системний блок);
- від 1 до 6 мікрофонів, приєднаних до мікшера;
- навушників;
- динаміків;
- блоку безперебійного живлення;

2) програмних засобів:

- програми “Діловодство суду”;
- спеціальної програми звукозапису.

Цифровий магнітофон “Тритон” складається з:

1) апаратних засобів:

- блоку цифрового магнітофона;
- від 1 до 6 мікрофонів, приєднаних до блоку;
- клавіатури;
- навушників;
- блоку безперебійного живлення.

2) програмних засобів:

– спеціальної програми звукозапису.

Систему технічного фіксування судового процесу “SRS Femida” використовують лише у Верховному Суді України, Вищому господарському суді України, в системі господарських судів України, а також у судах апеляційної інстанції.

Особливістю системи є якісний цифровий аудіозапис судового процесу і можливість одержання текстових звітів на комп’ютері за допомогою програм. Система забезпечує повну фіксацію судового процесу завдяки одержанню фонограми виступів кожного учасника й електронного протоколу судового засідання. Має відповідні ступені захисту і не може бути відкорегована. Система також дозволяє секретарям безпосередньо під час судового засідання формувати в напівавтоматичному режимі короткий протокол процесу. Роботу системи можна порівняти з функціями звичайного відеомагнітофона або диктофона, однак її перевага полягає в тому, що аудіо-відеозапис розбивається на відрізки, що відповідають подіям судового процесу – це дозволяє надалі швидко знайти необхідний фрагмент.

Отримана інформація зберігається на твердому диску системи і дублюється на компакт-диску, що долучається до справи. Комплекс включає в себе як апаратні, так і програмні рішення. Так, у системі зведена до мінімуму ймовірність видалення збереженої раніше інформації – це досягається за рахунок багаторазового дублювання інформації на двох твердих дисках одночасно. Комплекс оснащений устаткуванням безперебійного живлення. Якщо в процесі судового засідання раптово виключиться електрика, то система IS Meshanics SRS Femida зможе працювати ще приблизно 40 хвилин.

Програма звукозапису судових засідань “Оберіг” призначена для технічної фіксації судового процесу в зручному інтерфейсі, дозволяє секретареві (відповідальній особі) в ході засідання формувати протокол звукозапису.

Результатом роботи є фонограма, розмічена відповідно до подій судового процесу і протокол, в якому відображається в хронологічній послідовності: час початку/кінця всіх виступів, коментарі до кожного з них, які за потреби робить секретар, но-

мер компакт-диска, на який здійснюється запис, а також інша необхідна інформація.

Фонограма з відповідним протоколом судового засідання зберігається у вигляді електронного документа на твердому диску комп'ютера, який може копіюватися засобами “Оберіг” на будь-який змінний носій.

Програма створення протоколу засідання містить шаблони всіх основних дій, які можуть відбуватися під час засідання, і список дійових осіб. Перелік шаблонів за бажанням можна редагувати або поповнювати.

Прослуховування отриманих фонограм з компакт-диска здійснюється на звичайному комп'ютері після активації рядка події протоколу. Протокол може створюватися як одночасно із звукозаписом, так і після звукозапису.

7.3. Правові засади фіксування судового процесу технічними засобами

Відповідно до п. 7 ч. 3 ст. 129 Конституції України, пунктів 10, 11 ст. 6 та ст. 197 Цивільного процесуального кодексу України, ст. 41 Кодексу адміністративного судочинства України, ст. 4⁴ Господарського процесуального кодексу України, п. 4 ст. 9, п. 14 ст. 126 Закону України “Про судоустрій в Україні” реалізація принципу гласності судочинства забезпечується за допомогою повного фіксування судового процесу технічними засобами.

Згідно зі ст. 129 Конституції України та ст. 6 ЦПК України фіксування судового процесу технічними засобами є однією з гарантій гласності судового процесу як засадничого принципу правосуддя. Порядок фіксування судового засідання технічними засобами встановлюється процесуальним законодавством (ст. 197 ЦПК України, “Інструкцією про порядок фіксування судового процесу технічними засобами”, затвердженою наказом Державної судової адміністрації України від 21 липня 2005 р. № 84 “Про затвердження Інструкції про порядок фіксування судового процесу технічними засобами”).

Фіксування судового засідання технічними засобами здійснює секретар судового засідання або інший працівник суду

(ч. 11 ст. 6 ЦПК України), завдяки чому воно є офіційною формою фіксації судового процесу технічними засобами. Поряд із цим є неофіційні форми фіксації судових процесів. Наприклад, відповідно до ст. 6 ЦПК України учасники цивільного процесу та інші особи, присутні на відкритому судовому засіданні, мають право робити письмові записи, а також використовувати портативні технічні аудіопристрої. Для цього не потрібна згода учасників процесу та постановлення про це ухвали суду. Натомість проведення в залі судового засідання фото- і кінозйомок, відео-, звукозапису із застосуванням стаціонарної апаратури, а також транслявання судового засідання по радіо і телебаченню допускається на підставі ухвали суду за наявності згоди на це осіб, які беруть участь у справі.

Фіксування судового процесу у процесуально-правовому аспекті означає відбиття, закріплення юридично значущих дій суду, інших учасників судового процесу у відповідних процесуально-документальних формах для забезпечення їх вірогідності з точки зору об'єктивності засобів фіксації судового процесу та визначення процесуальних наслідків цих дій при розгляді справи по суті та на наступних стадіях судового процесу. При такому підході фіксація судового процесу означає обов'язковість процесуально-документального оформлення актів-документів, які фіксують процесуальні дії суду, сторін та інших учасників судового процесу, а також обставини, факти при розгляді справи, тобто мова йде про письмову фіксацію в судочинстві у межах, визначених законодавством.

Процесуальні кодекси не містять уніфікованого стандарту фіксування судового процесу. Наприклад, відповідно до статей 4⁴, 81¹ ГПК України судовий процес фіксується технічними засобами та відображається у протоколі судового засідання в порядку, встановленому кодексом. Про судові засідання, огляд і дослідження письмових або речових доказів за їх місцезнаходженням складається протокол. Господарський суд може здійснювати стенографічний, а також аудіо- чи відеозапис судового засідання. ЦПК України передбачає правило повного фіксування судового засідання (ст. 197 ЦПК України). Аналогічне правило містить і Кодекс адміністративного судочинства України (ст. 41).

Повне фіксування судового засідання можна розглядати з фактичної та юридичної сторін. З фактичної сторони повне фіксування судового засідання – це фіксація ходу судового засідання в цілому, без певних обмежень, що дозволяє відтворювати повний зміст тих чи інших процесуальних дій. Крім того, повнота фіксації означає таку форму фіксації, яка дозволяє відтворювати не лише зміст процесуальних дій у судовому засіданні, а й форму їх усного викладення та інші обставини, в тому числі нормально-церемоніальну, або ритуальну сторону процесу. Використання технічних засобів фіксації, виходячи з технологічних можливостей технічного обладнання, дозволяє вирішувати це завдання.

Що стосується суто процесуального аспекту фіксування судового засідання, то він зводиться до фіксації та можливості відтворення тих процесуальних дій, які безпосередньо впливають на розгляд справи по суті або на динаміку судочинства та рух справи. Тобто завдяки технічним засобам у судовому засіданні фіксації підлягають усі факти процесуальної поведінки суду та учасників процесу, навіть і та інформація, яка не має процесуального значення.

Оскільки не вся інформація, що міститься в технічному записі, має значення для вирішення справи і може використовуватися як доказ, правило про фіксацію судового засідання технічними засобами слід розглядати також як гарантію публічних інтересів правосуддя. Мова йде не лише про підвищену надійність звукозапису, а й про те, що така форма фіксації судового засідання запобігає з боку учасників судового процесу тим чи іншим перекручуванням ходу судового засідання або фальсифікації, що не виключається при протокольній фіксації судового засідання, та підвищує певною мірою довіру до суду.

Таким чином, технологія фіксації судового засідання технічними засобами безпосередньо впливає на визначення процесуального режиму технічного запису як доказу, а також на якість, достовірність та повноту цього доказу для розгляду справи та забезпечення процесуальних прав учасників судового процесу.

Виходячи з процесуального режиму та значущості техні-

чного запису, технічні засоби фіксування судового засідання мають відповідати вимогам надійності та простоти використання персоналом суду і забезпечувати легітимність звукозапису.

Цифрові засоби фіксації та їх використання потребують програмного й технічного забезпечення, які унеможливають несанкціонований доступ до систем фіксації та вплив технічних чинників на процедуру запису, а також відповідних заходів технічної та правової безпеки. Системи фіксації повинні мати і запобіжники втручання в об'єктивність запису, які виключали б навіть теоретичну ймовірність монтажу, а саме – механічне опломбування; енергозалежний календар, годинник; відсутність засобів редагування і вилучення записів; наявність електронного підпису; наявність пристрою для швидкого копіювання записів на одноразові носії (CD-диски). На даний час порядок фіксування судового засідання технічними засобами та вимоги щодо технічних засобів фіксування передбачено Інструкцією про порядок фіксування судового процесу технічними засобами, затвердженою наказом Державної судової адміністрації України від 21 липня 2005 р.

Правовий режим фіксування судового процесу технічними засобами визначається процесуальним законодавством. Так, відповідно до ч. 2 ст. 197 ЦПК України технічне фіксування судового засідання здійснює секретар або за розпорядженням головуючого інший працівник апарату суду (в будь-якому випадку це повинні бути працівники, які пройшли відповідне навчання).

На вимогу особи, яка бере участь у справі, або за ініціативою суду здійснюється повне чи часткове відтворення технічного запису судового засідання (ч. 3 ст. 197 ЦПК України). Як правило, така необхідність виникає при співставленні показань свідків та при застосуванні ч. 7 ст. 191 ЦПК України або ч. 4 ст. 182 ЦПК України тощо. Відтворення технічного запису судового засідання можливе і поза межами судового засідання з метою ознайомлення зі змістом запису (ч.1 ст.199 ЦПК України).

Носій інформації, на який здійснювався технічний запис судового засідання, є додатком до журналу судового засідання і після закінчення судового засідання він долучається до матеріалів справи.

Відповідно до процесуального законодавства особа, яка бере участь у справі, має право отримати роздруківку технічного запису судового засідання (повне або часткове роздрукування за плату) та копію інформації з носія, на який здійснювався технічний запис (безоплатно). Щодо отримання копії носія, на який здійснювався технічний запис, то відповідно до Інструкції про порядок фіксації судового процесу технічними засобами за заявою осіб, які беруть участь у справі, архіваріус створює копії фонограми для зазначених осіб. Обсяг плати за роздрукування технічного запису судового засідання відповідно до ч. 6 ст. 197 ЦПК України встановлюється Кабінетом Міністрів України. Відповідно до постанови Кабінету Міністрів України від 15 лютого 2006 р. № 151 “Про встановлення обсягів плати за роздрукування технічного запису судового засідання в адміністративних та цивільних справах та видачу дубліката виконавчого листа або судового наказу” плата за роздрукування однієї сторінки тексту на папері формату А4, що повністю або частково відтворює технічний запис судового засідання, встановлюється в обсяг і п’яти гривень.

7.4. Електронне (віртуальне) судочинство

У зв’язку з введенням у судочинство України фіксування судового засідання за допомогою звукозаписувальних технічних засобів у плані висунення проблеми мова може йти і про певні перспективи “електронізації” судових процесів завдяки ширшому використанню у майбутньому комп’ютерних та телекомунікаційних технологій, які мають забезпечити інформаційну підтримку електронного (віртуального) судочинства. Ця проблема стала майже головним питанням модернізації цивілістичних процесів в багатьох країнах (США, Канада, Нова Зеландія, Австрія, Італія, Англія, Німеччина тощо). Мова йде перш за все про електронну форму представлення документів до суду, викликів і повідомлень сторін, вірогідність та доказову силу електронних документів тощо, що забезпечує електронне документування судового діловодства відповідно до вимог процесуального законодавства. У більш широкому аспекті впровадження інформаційно-

комп'ютерних технологій, по суті, означає і більш широке поняття електронного (віртуального) судочинства як системи не лише фіксації судових процесів, а й способів комунікації учасників судочинства, проведення дистанційного розгляду судових справ, функціонування банку даних справ та судових рішень, автоматичного формування статистичної звітності про діяльність судів, розподіл навантаження на суддів тощо.

Причинами пошуку альтернатив традиційним формам судочинства стали неефективність процедур судочинства, невдачі його реформ та сподівання, що завдяки використанню комп'ютерних технологій підвищиться якість правосуддя. Щодо цього висловлюється впевненість, що електронне судочинство має переваги, які виявляться значно пізніше. Воно в більшій мірі гарантуватиме доступ до правосуддя, швидкість розгляду справ судами, сприятиме підвищенню якості судових рішень, контролю сторін за розглядом справи та економії судових витрат, посилить змагальність та публічність судових процесів. Інформаційні технології у майбутньому стануть фундаментом судової системи, що викличе радикальні зміни у процесуальному праві. На думку прихильників такого підходу, традиційний судовий розгляд стає застарілим, оскільки існує обладнання, необхідне для проведення віртуальних судових процесів, а програмне забезпечення вдосконалюється досить швидко. Так, за прогнозами, в межах десяти років систему віртуального цивільного процесу можна вдосконалити без великих фінансових вкладень з боку судів, адвокатів та сторін. Враховуючи те, що цифрова інформація майже безкоштовна, має великий ступінь збереженості, може передаватися на велику відстань, у перспективі слід очікувати, що в судових процесах будуть не лише використовуватися електронні комп'ютерні технології як такі, а й те, що основні процесуальні дії, в тому числі особисті пояснення і сам судовий розгляд, будуть здійснюватися через мультимедійну презентацію. Так, наприклад, електронний протокол судового процесу буде реєструвати докази, які мають надати сторони, показання свідків будуть записані до початку судового розгляду та розглянуті адвокатами сторін, як і інші документальні дані. Оскільки всі докази будуть зібрані, обмін ними та іншими змагальними паперами здійсне-

ний, то кожне питання підготовки справи до судового розгляду, в принципі, може бути вирішене до судового розгляду, а можливість тих чи інших несподіванок у ході судового розгляду буде повністю ліквідовано. На розгляд суду при цьому може бути покладено лише огляд мультимедійної презентації, допит свідків під присягою у звичний спосіб або у спосіб відеоконференції незалежно від місця знаходження свідка, проведення крос-допитів сторін та їх адвокатів для захисту мультимедійних презентацій судового розгляду.

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

Як приклад застосування нових електронних технологій можна навести новели ЦПК Німеччини. Цей кодекс передбачає можливість участі у судовому засіданні учасників процесу завдяки використанню відео- та аудіозасобів (параграф 128а), використання електронних документів (параграф 130а), вручення та доставку документів (параграф 174 ч.ІІІ), ознайомлення з матеріалами в електронній формі справи, огляд електронних документів (параграф 371 ч.1 п.ІІ), трансляцію зображення та звуку судового розгляду в залі судового засідання представників та помічників сторін, які під час судового розгляду знаходяться в іншому місті (параграф 128а). У такому випадку зображення та звук судового розгляду транслюється в зал судового засідання та місцезнаходження сторін, представників та адвокатів. Якщо стосовно підготовчих процесуальних документів, доданих до них клопотань, заяв сторін, а також пояснень, висловлювань, висновків і заяв третіх осіб передбачена письмова форма, то достатнім і належним за процесуальним законодавством Німеччини визнається викладення документа в електронній формі, якщо такий документ може бути оброблений судом (параграф 130а).

Застосуванню й упровадженню нових комунікаційних технологій значну увагу було приділено при останній новелізації

цивільно-процесуального законодавства Англії. У 1991 р. в Англії був створений спеціальний Судовий комітет з інформаційних технологій. Вже до кінця 1995 р. Комітет ініціював проведення 25 пілотних проектів з питань сервісу інформаційних технологій у судочинстві. Правила цивільного судочинства 1998 р. Англії передбачили можливість подання до суду документів в електронній формі, впровадження телекомунікацій у судочинство тощо. Відповідно до правила 32.3. PD, Annex 3 RCP суд може дозволити свідку давати покази через відеозв'язок або інші засоби комунікацій. Так, у справі *Polanski v Conde Nast Publications Ltd* (2005) 1 WLR 637 позивачу, який піддавався ризику екстрадиції в США, якщо б він в'їхав до Англії, було дозволено давати свідчення по відеозв'язку. В Англії доктрина процесуального права впровадження нових телекомунікацій та інформаційних технологій розглядає як суттєвий крок до якості та доступності правосуддя.

Активні кроки у застосуванні комп'ютерних технологій у судочинстві зроблено в Бельгії. З 2008 р. тут діє проект "Фенікс", який передбачає єдину, синхронну та структурну комп'ютеризацію судової системи. У зв'язку з цим Палатою представників Бельгії був ухвалений закон щодо проведення електронних судових розглядів, який передбачає відповідні зміни у Судовому кодексі та Кримінальному процесуальному кодексі Бельгії та прийняття інших підзаконних актів. Аналогічні тенденції відбуваються і в інших країнах.

Так чи інакше проблема електронних (віртуальних) судових процесів виникає і буде виникати. Але у даній час спостерігається неоднозначне ставлення до законодавчих нововведень у різних країнах та їх оцінка. Одна точка зору зводиться до того, що електронізація судочинства призводить до формалізації і може бути загрозою для проведення ефективних реформ правосуддя, є деструктивною, оскільки створює складні теоретичні та прикладні проблеми. Мова йде, зокрема, про перегляд основних принципів судочинства – доступності правосуддя, змагальності, усності, безпосередності тощо. Інша точка зору зводиться до того, що судовий процес відбувається з застосуванням систем передачі інформації і, по суті, є інформаційною системою, яка може

інтерпретуватися як система комп'ютерної електронної інформації. Виходячи з цього, стверджується, що теоретично і практично існує наявна сумісність між процесуальними реаліями та електронними технологіями.

Проблема електронного (віртуального) судочинства – це проблема, яка лише починає засвоюватись у юридичній науці і практиці судочинства. В основному, електронізація судочинства у даний час стосується електронних форм як виду процесуальної інформації та окремих випадків електронного (віртуального) процесу з використанням відеоконференцз'язку, які, за великим рахунком, по суті є додатковими стосовно існуючих традиційних процедур взаємодії суду та учасників судового процесу. Відповідь на питання сумісності електронних технологій з принципами судового процесу дасть час.

Використання технологій відеоконференцз'язку в судовій владі дозволяє підвищити ефективність використання часу, фінансових і людських ресурсів, збільшити кількість розглянутих справ за інтервал часу, скоротити терміни розгляду справ.

Для практичного судочинства застосування відеоконференцз'язку дає наступні можливості:

- проведення касаційних і наглядових судових процесів з використанням відеотехнології для взаємодії суддів, прокурорів і адвокатів, що знаходяться в залі судового процесу з одним або декількома засудженими в одній або декількох виправних установах в реальному часі;

- допит свідків за програмою їх захисту (із спотворенням голосу і приховуванням очей) за кримінальним або іншим судовим діловодством відповідно до українських і міжнародних правових актів;

- консультації, наради, семінари суддів і співробітників апарату суду з колегами з одного або декількох судів;

- інтерактивне дистанційне навчання співробітників судів загальної юрисдикції і виправних установ служби виконання покарань.

7.5. Комп'ютерні технології забезпечення розгляду судових справ

Відповідно до Положення про Державну судову адміністрацію, затвердженого постановою Кабінету Міністрів України від 14 січня 2009 р. №14, Державна судова адміністрація організовує в установленому порядку створення, впровадження та функціонування Єдиної судової інформаційної системи, Єдиного державного реєстру судових рішень, інших реєстрів та інформаційних систем, забезпечення ведення яких належить до її повноважень.

Відповідно до покладених на ДСА України завдань та з урахуванням галузевої структури визначено пріоритетні напрями інформатизації:

1. Автоматизація процесів документообігу:

а) для судів

- автоматизація процесів реєстрації та створення документів;
- забезпечення технологічних процесів проходження судових справ;
- контроль дотримання процесуальних термінів;
- контроль виконання документів;
- технічне фіксування (аудіо-, відеозапис) та протоколювання судового процесу;
- автоматичний розподіл судових справ до розгляду;
- формування статистичної звітності на базі первинної

інформації.

б) для ДСА

- формування статистичної, фінансової звітності, моніторинг стану організаційного та, зокрема, матеріально-технічного забезпечення судів.

Автоматизація процесів документообігу, в тому числі:

- автоматизація процесів реєстрації та створення документів;
- контроль виконання документів.

2. Функціонування порталу судової влади.

3. Функціонування Єдиного державного реєстру судових рішень.

4. Функціонування системи обліку суддівських кадрів:

а) для суддів – доступ до баз даних судових справ та Єдиного державного реєстру судових рішень; інформаційного масиву судової практики; нормативно-правових баз даних та інших інформаційних ресурсів;

б) для адвокатів – доступ до інформації по справах за участю адвоката;

в) для сторін судового процесу – своєчасне і надійне інформування про хід судової справи; доступ до інформації по справі.

Відповідно до Положення про Єдину судову інформаційну систему України (ЄСІС) інформатизація діяльності судів та Державної судової адміністрації – це використання сукупності нормативно-правових, програмно-технічних та телекомунікаційних засобів, що забезпечують збирання, накопичення, аналіз та зберігання інформації судової діяльності.

Завданням ЄСІС є забезпечення інформаційної та технологічної підтримки судочинства на принципах дотримання балансу між потребою громадян, суспільства і держави у вільному обміні інформацією шляхом створення умов для сприяння законності й обґрунтованості прийнятих судових рішень, скорочення строків розгляду судових справ, забезпечення оперативного доступу суддів і працівників апаратів судів до чинного законодавства та судової практики, забезпечення об'єктивного аналізу судової практики, підвищення інформованості суспільства про діяльність судів, забезпечення прозорості й відкритості стану системи правосуддя в Україні.

Єдина судова інформаційна система передбачає забезпечення та доступ даних до віртуальних підсистем, якими є наступні:

- Підсистема “Судове діловодство та документообіг”. Встановлюється на всіх об'єктах автоматизації та призначена для забезпечення судового діловодства на всіх стадіях судового процесу, починаючи з надходження судової справи до суду, закінчуючи її передачею до архіву та зберіганням; автоматизації проце-

сів проходження процесуальних документів; забезпечення загального діловодства і забезпечення документообігу внутрішніх та зовнішніх документів; здійснення процесуального контролю та контролю виконання документів та відстеження життєвого циклу справ та документів; здійснення обліку та контролю використання бланків суворої звітності при видачі (виготовленні) копій судових рішень.

- Підсистема “Судова статистика”. Встановлюється в судах, ДСА, ТУ ДСА, радах суддів та призначена для забезпечення формування статистичної та аналітичної інформації щодо стану здійснення судами правосуддя.

- Підсистема “Планування та розподіл судових справ”. Встановлюється в судах та призначена для автоматичного розподілу судових справ, що надійшли до суду, та складання попереднього графіка призначення справи до розгляду. Підсистема інтегрована з підсистемою “Судове діловодство та документообіг”.

- Підсистема “Кадри”. Встановлюється у кадрових підрозділах ДСА, Вищій раді юстиції, кваліфікаційних комісіях суддів, радах суддів та призначена для організації обліку суддівських кадрів та ведення кадрової роботи по інших категоріям працівників.

- Підсистема “Фінансовий блок”. Встановлюється в ДСА, судах, радах суддів та призначена для забезпечення організації бюджетних процесів, доступу до звітів та статистичної інформації щодо фінансового забезпечення судів.

- Підсистема “Аналітика”. Встановлюється на робочих місцях керівного складу суддів, ДСА, Ради суддів України та призначена для формування інформаційно-аналітичних звітів з різних аспектів діяльності судів, починаючи з аналізу матеріального, кадрового та іншого забезпечення, закінчуючи узагальненням оцінки діяльності судів, суддів, ДСА, з метою виявлення проблемних ділянок діяльності судової системи та підтримки управлінських рішень.

- Підсистема “Законодавство та право”. Встановлюється в судах, ДСА, Раді суддів України та призначена для надання оперативного й зручного доступу до законодавства та ін-

ших нормативних та правових актів в електронному вигляді.

- *Підсистема “Матеріально-технічне забезпечення”*. Встановлюється в ДСА України, ТУ ДСА, судах та призначена для обліку і організації керування об’єктами нерухомості судів і ДСА, матеріально-технічними, інтелектуальними та іншими ресурсами, що потребують обліку, організації збереження та поставок.

- *Підсистема “Протоколювання та звукозапис судового процесу”*. Встановлюється в судах та призначена для ведення аудіо-протоколу судових засідань, прослуховування звукозаписів судових засідань та, при необхідності, створення друкованих протоколів. Система протоколювання повинна бути інтегрована з підсистемою діловодства та документообігу (створення нового протоколу не повинно вимагати повторного введення інформації стосовно справи).

- *Підсистема відеоконференцв’язку*. Призначена для забезпечення проведення судових засідань без залучення до зали суду підсудних, які знаходяться в слідчому ізоляторі або свідків з інших населених пунктів; оперативного проведення нарад у віддаленому режимі.

- *Підсистема “Судова практика”*. Встановлюється на робочих місцях суддів, може бути доступна адвокатам та іншим громадянам та призначена для узагальнення судової практики і підтримки процесу прийняття судових рішень суддею в рамках єдиних підходів використання положень права. Система судової практики може передбачати два рівні: перший – судової практики суду; другий – загальної судової практики. Система забезпечить технічну можливість публікації та узагальнення судової практики.

- *Підсистема “Довідникова підсистема”*. Встановлюється на робочих місцях всіх працівників суду і ДСА та призначена для надання інформації стосовно діяльності судів і ДСА, пошуку контактів та адрес організацій судової системи та організацій, що забезпечують роботу судової системи, іншої інформації, яка потрібна в судах в процесі їх діяльності.

- *Інтернет-портал судової влади*. Доступний всім громадянам України через мережу Інтернет та призначений для забезпечення потреби в інформації щодо діяльності судової системи.

- *Єдиний державний реєстр судових рішень*. Призначений для публікації судових рішень судів загальної юрисдикції, крім судових рішень, які містять інформацію, що є державною таємницею.

- *Звернення громадян*. Встановлюється в судах, ДСА України, ТУ ДСА та призначена для автоматизованої реєстрації відомостей про скарги, пропозиції, заяви (далі – звернення) громадян (організацій та установ), постановки їх на контроль, аналізу своєчасного розгляду звернень, формування довідок і статистичних матеріалів про роботу зі зверненнями громадян.

- *Інформаційний кіоск*. Встановлюється в судах та призначений для надання громадянам, відвідувачам суду, інформації про діяльність суду.

- *Адміністрування підсистем*. Встановлюється у адміністратора ЄСІС, деякі блоки – в ТУ ДСА і судах та призначена для супроводу роботи ЄСІС, забезпечення її працездатності.

- *Інформаційне забезпечення*. Встановлюється у адміністратора ЄСІС та призначена для забезпечення єдиних підходів ведення судової інформації та уніфікації інформації та інформаційних потоків в судовій системі.

- *Комплексна система захисту інформації (КСЗІ)*. Встановлюється у всіх суб'єктів, які використовують підсистеми ЄСІС, та призначена для забезпечення розмежування доступу до інформації та її захисту.

- *Система автоматизації документообігу “Деловодство”*. Впроваджується в судах України, центральному апараті Державної судової адміністрації України, а також в територіальних управліннях Державної судової адміністрації. Система дозволяє автоматизувати практично всі аспекти роботи суду, починаючи з первинної реєстрації документів і ведення журналів, і закінчуючи автоматизованою підготовкою рішень, автоматичною відправкою їх в ЄДРСР, обміном справами і документами між вказаними судами і автоматичною побудовою статистичного звіту.

Існуючий програмний комплекс забезпечує: а) створення, друк, реєстрацію і збереження в базі даних всіх документів, що стосуються справ, за підрозділами, видами і категоріями; б) облік

вхідної і вихідної кореспонденції, розпоряджень тощо з можливістю швидкого пошуку документа і справи; в) виготовлення дублікатів документів.

Комплекс має редактор текстів, що дозволяє виконувати виготовлення нових документів на основі стандартних зразків (шаблонів), які знаходяться в базі даних, а також нових нестандартних документів і створення на їх основі зразків для подальшої роботи. При введенні документа за шаблоном заповнюються поля введення документа, які пов'язані з базою даних. При збереженні документа інформація з полів введення документа відразу зберігається в потрібних полях бази даних. Система дозволяє формувати електронний архів, що дає можливість повністю автоматизувати процес пошуку старих документів і видачі довідок, копій і дублікатів документів. При введенні здійснюється орфографічний контроль документа.

За допомогою механізму зразків (шаблонів) система дозволяє створювати реєстраційні картки необхідного вигляду, реєструвати в системі потрібні види документів і вести за ними реєстри з можливістю отримання будь-яких звітів. Пошук документа здійснюється за всіма параметрами (дата, прізвище, вид документа, реєстровий або системний номер тощо) і в різних діапазонах значень (повна відповідність, інтервал “від” – “до”, більше або менше вказаного значення щодо чисельних параметрів пошуку).

Програма дозволяє використовувати єдину систему класифікації документів і має можливість контекстної індексації документів, що забезпечує проведення контекстного пошуку документа разом з пошуком за вибраними реквізитами документів.

Особливо важливо, що система передбачає можливість автоматичного контролю процесуальних строків розгляду справ, виконання документів і формування всіх форм звітності. Крім того, дозволяє в автоматичному режимі централізовано або децентралізовано вести поштові реєстри по документах, що відправляються з організації і роздруковувати їх. Існує можливість друкувати поштові адреси на конверти. Для зручності введення адрес у довідник організацій в систему інтегрований довідник поштових індексів України, що дозволяє в автоматичному режи-

мі за індексом заповнювати місто, область. І навпаки, за назвою населеного пункту знаходити індекс організації.

Практичне значення має генератор звітів, який дозволяє формувати наявні звіти, описувати запит і форму вихідного документа для обробки і аналізу будь-якої інформації з бази даних. У поєднанні з системою синхронізації баз даних генератор звітів забезпечує автоматичне формування і відправку інформації в інші віддалені підрозділи або організації в обраному форматі і з вказаною періодичністю.

Система забезпечує достатній контроль доступу і захист інформації. Мова йде як про захист інформації в цілому, так і розмежування доступу співробітників до інформації через систему паролів. Розмежування доступу здійснюється як на рівні пунктів меню системи, так і на рівні підрозділів, окремих документів і справ. Система адміністрування користувачів дозволяє виконувати підключення нових користувачів, установку персональних паролів і прав доступу користувачів до баз даних, її складових частин і окремих елементів.

Особливе значення має синхронізація баз даних у межах системи. Перш за все завдяки системі реплікації баз даних “РЕПА” в автоматичному режимі засобами електронної пошти можливо передавати дані (документи і справи в електронному вигляді) між віддаленими підрозділами, організаціями. Також передбачено збір інформації з регіонів на центральний рівень, а також підтримка на регіональному рівні актуальних загальнодержавних довідників.

У складі комплексу поставляється спеціалізована програма “СИРКО”, що дозволяє за вказаним розкладом проводити контроль цілісності бази даних, автоматичне створення резервних копій. Про результат роботи програма повідомляє адміністратора системи за допомогою log- файла та електронної пошти.

Система автоматизації документообігу “Деловодство” підтримує інтеграцію системи з комплексом звукозапису “Обе-ріг”. Модуль звукозапису системи забезпечує:

- запис фонограми звукового засідання авторизованим користувачем системи з використанням механізму електронного підпису;

- формування журналу (протоколу) засідання під час звукозапису з автоматичною прив'язкою записів журналу (протоколу) до відповідних місць фонограми;
- редагування журналу (протоколу) засідання;
- друк і збереження в системі журналу (протоколу) засідання;
- виготовлення копій фонограми і журналу (протоколу) засідання за замовленням користувачів і запис їх на компакт-диски;
- забезпечення прослуховування копій звукозапису і синхронного перегляду журналу (протоколу) засідання на персональних комп'ютерах, не обладнаних системою і комплексом звукозапису;
- облік у системі створених копій звукозапису засідання.

Система резервного копіювання баз даних (СРКБД) "СИРКО". Розроблена для автоматизованої перевірки і резервного копіювання SQL – баз даних клонів Interbase - Interbase 6, Firebird, Yaffil, а також для можливості віддаленого контролю виконання вказаних завдань за допомогою електронної пошти.

Основні функції програми:

- запуск в зазначений час;
- перевірка цілісності бази даних;
- створення резервної копії бази даних;
- контрольне відновлення з резервної копії бази даних;
- порівняння структури робочої бази даних з еталонною;
- відсилання звіту про результати роботи електронною поштою за вказаними адресами;
- можливість автоматичного відключення користувачів від бази даних перед перевіркою бази;
- компоненти консолі бази даних;
- менеджер користувачів;
- диспетчер користувачів, підключених до бази даних;
- перевірка бази (Validation) в ручному режимі;
- резервне копіювання/відновлення (BackUp/Restore) бази в ручному режимі;
- рестарт бази даних у ручному режимі;

- відключення бази даних у ручному режимі;
- вбудований компаратор баз даних, що працює як у ручному, так і в автоматичному режимах. У автоматичному режимі використовується для порівняння структури відновленої бази з еталоном.

Програма реплікації документів в електронному вигляді між базами даних автоматизованої системи “Деловодство” “РЕПА”. Програма реплікації документів в електронному вигляді між базами даних автоматизованої системи “Деловодство” РЕПА дозволяє судам оперативно отримувати всю інформацію у справах, що їх цікавить, отримувати практику судочинства, будувати звітність для оцінки якості роботи суддів тощо.

Основні функції програми:

- дозволяє передавати дані (документи і справи в електронному вигляді) між видаленими підрозділами і організаціями в автоматичному режимі засобами електронної пошти;
- забезпечує збір інформації з регіонів на центральний рівень;
- забезпечує підтримку актуальних загальнодержавних довідників на регіональному рівні.

Автоматизована система документообігу в адміністративних судах (АС ДАС) призначена для автоматизації процесів проходження процесуальних документів, загального діловодства і документообігу внутрішніх та зовнішніх документів, здійснення процесуального контролю та контролю виконання документів, відстеження порядку проходження справ та документів, розподілу судових справ і матеріалів між суддями, формування звітності суду про стан здійснення правосуддя, передачу справ до електронного архіву тощо.

Положення про АС ДАС затверджено наказом судової адміністрації України № 129 від 3 грудня 2009 р.

Система забезпечує:

- контроль за дотриманням процесуальних строків при розгляді судової справи та автоматичне інформування головної у справі суддю, суддю-доповідача, голову суду та заступника голови (голову судової палати) про наявні та потенційні проблеми дотримання процесуальних строків;

- використання електронного цифрового підпису (ЕЦП) для засвідчення документа, що набуває офіційного статусу;
- оперативний пошук справ та документів за реквізитами;
- індексацію документів та контекстний пошук за текстами документів;
- видачу судових рішень (копій) та формування виконавчих листів на підставі наявних у Системі даних;
- зберігання текстів судових рішень та інших документів, створених у Системі;
- відправку електронних копій судових рішень до Єдиного державного реєстру судових рішень;
- надання особам інформації про стан розгляду справ щодо них;
- формування звітності суду про стан здійснення судочинства тощо.

Для отримання інформації у суді в системі АС ДАС функціонує підсистема електронного довідника. Електронний довідник встановлюється на окремому комп'ютері в холі суду для забезпечення оперативного надання інформації щодо дати надходження справи до суду, номера справи, сторін та інших учасників у справі, дати та часу призначення справи до розгляду, зали судового засідання, дати розгляду справи, а також резолютивна частина рішення у справі (крім рішень у справі, яка слухалась у закритому судовому засіданні) та інформація про надходження апеляційних чи касаційних скарг та їх розгляду за окремою справою. Для отримання інформації необхідно ввести мінімальний набір даних щодо номера справи або дати прийняття судового рішення, або найменування однієї зі сторін у справі.

Забезпечення захисту інформаційних ресурсів Системи здійснюється шляхом застосування засобів і методів технічного захисту інформації, впровадження організаційних та інженерно-технічних заходів комплексної системи захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого доступу до неї, її модифікації або спотворення.

7.6. Відеоконференцзв'язок у судовій системі

Однією із форм використання інформаційних технологій у судовій системі є можливість відеоконференцзв'язку.

Відеоконференція – це технологія, яка дозволяє візуалізувати відносини, обмінюватися даними і спільно обробляти їх в інтерактивному режимі, використовуючи можливості звичного всім комп'ютера, максимально наближаючи спілкування на відстані до реального живого спілкування. Для проведення відеоконференцій використовується спеціальна технологія – відеоконференцзв'язок. Взаємодію в режимі відеоконференцій також називають сеансом відеоконференцзв'язку.

Існують дві основні технічні проблеми, що гальмують розвиток відеоконференцзв'язку. Перша полягає в пропускну здатності каналу зв'язку. Аналогові телефонні лінії цілком підходять для передачі аудіосигналу, але вони не в змозі забезпечити якісну трансляцію потоку відеоінформації. Друга проблема – швидкість обробки аудіо- й відеопотоку, тобто час кодування передаваної і декодування отримуваної інформації.

Вирішити проблему обробки інформації дозволяють два основні підходи – програмний і апаратний. Програмний ґрунтується на спеціалізованому програмному забезпеченні, що використовує для реалізації алгоритмів кодування/декодування центральний процесор комп'ютера.

Другий підхід орієнтується на використання спеціалізованого апаратного забезпечення з попередньо встановленим на заводі програмним забезпеченням. Ці “закінчені рішення” мають високі якісні характеристики, але й високу вартість. Якщо поєднати два вищеописані підходи, то можна отримати достатньо гнучкий програмно-апаратний комплекс з належною якістю зв'язку і прийнятною ціною. Такі рішення і є найбільш поширеними.

Для організації відеоконференції між двома точками необхідно:

- у кожній з точок повинен бути термінал відеоконференцзв'язку. Це може бути самостійний пристрій або комп'ютер з відповідним програмним забезпеченням і, можливо, спеціальною платою;

- ці дві точки повинні бути з'єднані відповідною мережею, зазвичай по IP або ISDN.

Для організації відеоконференцій з повноцінною участю декількох сторін (більше двох) необхідна наявність спеціальних пристроїв для багатоточкових відеоконференцій. Їх зазвичай називають MCU (Multipoint Conference Unit).

Для якісної відеоконференції необхідне виконання наступних правил:

- мати типове обладнання прийому / передачі;
- гарантовані високошвидкісні канали зв'язку (послуга зв'язку);
- стабільне і надійне електроживлення телекомунікаційного обладнання і відеоконференцзв'язку;
- оптимальні шумо- та ехопоглинаючі особливості приміщення;
- правильне розташування обладнання відеоконференцзв'язку по відношенню до світлового фону приміщення;
- коректну настройку телекомунікаційного обладнання і відеоконференцзв'язку по обслуговуванню якості з пріоритизацією передачі даних.

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

рішення представники сторін знову отримали доступ до відеоконференції, і судом було оголошено рішення у справі. Рішення третейського суду видане сторонам також і в паперовому вигляді з підписами суддів і печаткою.

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

7.7. Голосові портали в судовій діяльності

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

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

Абсолютно нові можливості відкрилися з появою у 1998–1999 рр. реально працюючих технологій синтезу і, що найважли-

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

Одним з основних завдань судової влади є підвищення відкритості і прозорості судової діяльності. Рішення цієї задачі можливе тільки з використанням сучасних комп'ютерних і інформаційних технологій. Тому вельми цікавим у зв'язку з цим є впровадження і використання окремими судами інноваційного рішення “Голосовий портал суду”.

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

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

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

“Голосовий портал” може обробляти п'ять запитів, що поступають одночасно. Проте можливості системи Авауа допускають значне масштабування числа запитів.

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

7.8. Реєстр судових рішень

Єдиний державний реєстр судових рішень (далі – Реєстр) – автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень почав свою роботу з червня 2006 р. на веб-сайті державного підприємства “Судовий інформаційний центр” (<http://www.reyestr.court.gov.ua/>). Використання Реєстру передбачено Законом України “Про доступ до судових рішень” від 22 грудня 2005 р. № 3262-IV.

Передбачений повний і загальний доступ до Реєстру. Повним доступом можуть скористатися лише судді, оскільки при цьому надається вся інформація про судову справу і про учасників судового процесу, тобто й така, що може бути конфіденційною. Загальний доступ, який відкритий для широкого загалу, не містить даних (імен, номерів телефонів, автомобілів, адрес), які дозволяють ідентифікувати особу.

На початок 2009 р. до Реєстру внесено близько 2,7 млн документів. На жаль, з великої кількості судів інформація до Реєстру на початок 2009 р. ще не надійшла. База включає судові рішення, прийняті після першого червня 2006 р. Щорічно в Україні приймається близько 5 млн таких рішень, із них лише близько 1 % не буде розміщено в Єдиному реєстрі. Переважно це закриті судові рішення з грифом “цілком таємно”, які містять державну таємницю.

Доступ до рішень у Реєстрі виконується наступним чином.

1. Веб-сторінка доступу на сайт <http://reyestr.court.gov.ua/> / reyestr/frame.php.

2. Вхід у Реєстр через “Загальний доступ”. Відкриється форма для запиту.

3. Обов’язкові поля для заповнення: “Дата ухвалення судового рішення”. Якщо невідома точна дата, необхідно виставити приблизні числа прийняття документа.

4. Результатом пошуку буде впорядкований перелік справ, які відповідають запиту, або повідомлення, що не знайдено жодного документа.

5. Для доступу до тексту документа необхідно клацнути

мишею на полі “№ рішення”. Отриманий текст можна скопіювати чи зберегти для подальшої роботи.

7.9. Єдиний державний реєстр виконавчих проваджень

Єдиний державний реєстр виконавчих проваджень (далі – Єдиний реєстр) – це комп’ютерна база даних, створена за допомогою автоматизованої системи, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення та надання відомостей про виконавчі дії. Прийнятий відповідно до:

- “Положення про Єдиний державний реєстр виконавчих проваджень”, затверджене наказом Міністерства юстиції України від 20 травня 2003 р. № 43/5 “Про затвердження Положення про Єдиний державний реєстр виконавчих проваджень” і зареєстроване в Міністерстві юстиції України 21 травня 2003 р. № 388/7709;

- наказу Міністерства юстиції України від 28 травня 2004 р. № 634/7 “Про здійснення контролю за впровадженням Єдиного державного реєстру виконавчих проваджень у регіонах”;

- наказу Міністерства юстиції України від 24 лютого 2006 р. № 13/5 “Про внесення змін до Положення про Єдиний державний реєстр виконавчих проваджень та встановлення обсягів оплати за його експлуатацію”;

- наказу Міністерства юстиції України від 24 липня 2008 р. № 1270/5 “Про внесення змін до деяких нормативно-правових актів Міністерства юстиції України”;

- наказу Міністерства юстиції України від 25 липня 2008 р. № 1293/5 “Про встановлення обсягів плати за користування Єдиним державним реєстром виконавчих проваджень”.

Результатом пошуку за вказаними параметрами будуть знайдені в базі Єдиного реєстру записи про суб’єктів, найменування яких містять у собі всі слова, вказані в параметрах пошуку.

Якщо в параметрах пошуку вказано лише код ЄДРПОУ або ІдН, результатом пошуку будуть знайдені в базі даних Єди-

ного реєстру записи про суб'єктів, які мають вказаний у параметрах пошуку код ЄДРПОУ або ІдН.

Якщо в параметрах пошуку крім найменування вказано ще й код ЄДРПОУ або ІдН суб'єкта, то результатом пошуку будуть знайдені в базі даних Єдиного реєстру записи про суб'єктів, які містять у найменуванні всі слова, вказані в параметрах пошуку, та разом з тим мають вказаний у параметрах пошуку код ЄДРПОУ або ІдН. Наприклад, якщо параметрами пошуку вказати: “Веселка” (найменування) 12345678 (код ЄДРПОУ), то результатом пошуку будуть лише суб'єкти з кодом ЄДРПОУ 12345678, найменування яких містять слово “Веселка”.

Загальні правила формування параметрів пошуку суб'єкта в базі даних Єдиного реєстру:

1) необхідно вказувати лише ті атрибути (найменування чи ПІБ або кілька значущих слів з найменування чи ПІБ, код ЄДРПОУ чи ІдН), які точно містяться в реєстровому записі про суб'єкта, якщо такий запис є в базі даних Реєстру;

2) не потрібно вказувати атрибути, які запис про суб'єкта може не містити взагалі або містити в іншій формі;

3) не потрібно в параметрах пошуку вказувати організаційно-правову форму юридичної особи, оскільки можливе різне написання однієї організаційно-правової форми, наприклад: “Товариство з обмеженою відповідальністю” або “ТОВ“, або “ТзОВ”, або навіть “ООО” (якщо має місце порушення Закону про державну мову);

4) значущими символами у найменуванні або ПІБ суб'єкта є символи кирилиці та цифри.

Слова в найменуванні суб'єкта та в параметрах пошуку відокремлюються одне від одного пробілом.

За параметром пошуку “Каштан” не буде знайдено запису в базі даних Єдиного реєстру, в якому найменування суб'єкта було помилково зареєстровано без пробілу між організаційно-правовою формою та назвою: ТОВ “Каштан”, але будуть знайдені суб'єкти з найменуванням ВАТ “Каштан”, “Каштан” комунальне підприємство тощо.

На результат пошуку не впливають: порядок слів у параметрах пошуку, регістр літер у найменуванні або ПІБ, наявність

або відсутність дефісів, тире, ком, лапок, апострофів, дужок, крапок, двокрапок, зірочок, символу “№”, більше ніж один підряд символ пробілу тощо. Алгоритм пошуку просто ігнорує (“викидає”) вказані символи з параметрів пошуку.

5. Якщо точні назва або ПБ суб’єкта невідомі і є впевненість у правильності лише частини слова з назви або ПБ, можливе використання у параметрах пошуку так званих шаблонних символів:

- символ “_” заміняє собою один будь-який значущий символ у слові;
- символ “%” заміняє собою будь-яку кількість символів у слові.

Наприклад, за параметром запиту “%Ірпін%” будуть знайдені такі суб’єкти: “ДПІ м.Ірпінь”, “ДПІ міста Ірпіня”, “Ірпінська міська санітарно-епідеміологічна станція” тощо.

6. Для поля “Тип особи” у параметрах пошуку краще вказувати значення “Усі типи”. У цьому разі будуть знайдені всі записи про суб’єктів – фізичних осіб або підприємців – фізичних осіб незалежно від того, з яким значенням поля “Тип особи” (“Юридична особа” або “Фізична особа”) вони були зареєстровані в базі даних Єдиного реєстру.

7. Для поля “Категорія майна” у параметрах пошуку краще вказувати значення “Усі типи”. У цьому разі будуть знайдені всі записи про арештоване у ході ведення ВП майно боржника, арешт на яке було накладено шляхом винесення “Постанови про арешт майна боржника та оголошення заборони на його відчуження”, “Постанови про відкриття виконавчого провадження (з одночасним накладенням арешту на майно боржника)”, складання “Акта опису й арешту майна”.

8. Пошук у Єдиному реєстрі функцією “Пошук ВП за боржником”, а також пошук при формуванні “Витяг з ЄДРВП” та “Витяг з ЄДРВП щодо арештованого майна” видає як результат лише виконавчі провадження, які перебувають у стані виконання, тобто для яких було зареєстровано “Відкриття ВП”, однак не було зареєстровано “Закінчення ВП”.

Пошук у Єдиному реєстрі при формуванні “Витяг з ЄДРВП на запит державних органів” та “Довідка з ЄДРВП” по-

вертає як результат усі зареєстровані в базі даних Єдиного реєстру виконавчі документи та виконавчі провадження, незалежно від їх стану.

7.10. Нотаріальні реєстри

Визначальним фактором нотаріального процесу є інформаційний аспект змісту нотаріальної діяльності, тому серед сукупності різних технологічних та організаційних рішень певне місце повинні зайняти комп'ютерні технології.

Нотаріальний реєстр – центральна база даних, у яку вноситься інформація певного виду. Бази окремих реєстрів зв'язані одна з одною; при цьому використовуються єдині словники: адміністративно-територіального устрою України, суб'єктів, документів.

Державне підприємство “Інформаційний центр” створено за наказом Міністерства юстиції № 76/5 від 9 грудня 1997 р. постановою Кабміну України № 1272 від 14 липня 1999 р. Держінформ’юст визначено адміністратором реєстрів, функціонування яких належить до компетенції Мін’юсту, таких як:

- *Державний реєстр обтяжень рухомого майна* – (чинний з 1 березня 1999 р.) для забезпечення переважного права заставодержателя у задоволенні вимог за рахунок рухомого майна боржника.

- *Єдиний реєстр довіреностей* – започаткований у червні 1998 р. Мета створення – профілактика злочинів проти власності шляхом накопичення та використання нотаріусами, органами ДАІ та іншими правоохоронними органами відомостей про посвідчені доручення. За даними Єдиного реєстру доручень можна перевірити чинність доручення, посвідченого в будь-якому регіоні України. На підставі спільного наказу МВС та Мін’юсту від 21 січня 1999 р. № 4/5/39 “Про спільну діяльність щодо виявлення викрадених транспортних засобів та уникнення їх незаконного придбання і реалізації” ДАІ МВС України надано доступ до Єдиного реєстру доручень.

- *Єдиний реєстр спеціальних бланків нотаріальних документів* впроваджено в серпні 1997 р. для надання нотаріусам та

правоохоронним органам можливості перевірки дійсності нотаріальних документів, виконаних на спеціальних бланках. У реєстрі також містяться відомості про недійсні бланки: викрадені, зіпсовані, анульовані та відсутні.

– *Єдиний реєстр нотаріусів України* введений в дію в серпні 1997 р. Забезпечує упорядкування обліку державних та приватних нотаріусів України, містить відомості про нотаріальні округи, державні нотаріальні контори, державних та приватних нотаріусів України.

– *Єдиний реєстр заборон відчуження об'єктів нерухомого майна* запроваджений з травня 1997 р. Мета створення – підвищення рівня захисту майнових прав та інтересів громадян і організацій шляхом накопичення та використання нотаріусами України, а також правоохоронними органами даних про заборони відчуження та арешти нерухомого майна юридичних та фізичних осіб.

– *Реєстр прав власності на нерухоме майно* чинний з 1 жовтня 2002 р. Забезпечує захист права власності на нерухоме майно фізичних та юридичних осіб. Цей реєстр містить відомості про зареєстровані права власності, суб'єктів прав, об'єкти нерухомого майна, правовстановлюючі документи, на підставі яких здійснено реєстрацію прав власності. Технологічні та технічні засоби ведення реєстру забезпечують довічне зберігання та достовірність інформації.

Щодо технологічних особливостей використання вказаних реєстрів слід зазначити, що всі вони побудовані за клієнт-серверною технологією. Реєстратори, тобто державні нотаріальні контори, та приватні нотаріуси, що уклали відповідні угоди з адміністратором реєстрів (Державне підприємство “Інформаційний центр”), мають повний прямий доступ до баз даних єдиних реєстрів через комп'ютерну мережу, вносять відповідно з установленим порядком записи про набуття чинності та припинення дії документів і перевіряють дійсність документів шляхом запитів до єдиних реєстрів. Адміністратор здійснює комплекс організаційних заходів щодо забезпечення захисту інформації, яка міститься в єдиних реєстрах.

7.11. Автоматизована система ведення Державного земельного кадастру

Україна як одна з найбільших країн Європи має могутній земельно-ресурсний потенціал. Із 60,3 млн га земель держави майже 70 % складають сільськогосподарські угіддя, а 10 млн га – лісові. Близько 2,3 млн га (4 %) знаходиться під забудовою.

Земельним кодексом України передбачена система державної реєстрації державних актів на землю у складі Державного реєстру земель. У ст. 193 Земельного кодексу України надане наступне визначення: “Державний земельний кадастр – це єдина державна система земельно-кадастрових робіт, яка встановлює процедуру визнання факту виникнення або припинення права власності і права користування земельними ділянками та містить сукупність відомостей і документів про місце розташування та правовий режим цих ділянок, їх оцінку, класифікацію земель, кількісну та якісну характеристику, розподіл серед власників землі та землекористувачів”.

Складовими частинами земельного кадастру є: а) державна реєстрація землекористувачів; б) кількісний облік земель; в) характеристика якості земель; г) економічна оцінка землі; д) кадастрові земельні карти.

Сьогодні, коли ми говоримо про кадастр, то маємо на увазі кадастрову інформацію в середовищі сучасних інформаційних технологій.

Передбачається, що структура бази даних буде мати чотири реєстри:

1. *Реєстр земельних ділянок, який являє собою таблицю, що включає кадастрові номери земельних ділянок та їхні певні характеристики.*

2. *Реєстр власників і користувачів.* Тут також використовується унікальний номер: для фізичних осіб – ідентифікаційний код, який надає податкова інспекція, для юридичних осіб – це код ЗКПО, який надає статуправління.

3. *Реєстр правових документів* має код документа і його атрибути.

4. *Реєстр прав на земельну ділянку.* Містить всі правові

документи, пов'язані як із земельними ділянками, так і з власниками чи користувачами. За станом на 1 травня 2008 р. в електронному кадастрі вже перебуває 10,8 млн записів, до Державного реєстру земель внесено 7,4 млн земельних ділянок.

7.12. Інформаційно-аналітичні системи криміналістичних обліків

Система “АБД”. Аналітична підтримка правоохоронної діяльності спирається на потужні інформаційні бази даних, у яких накопичено інформацію у значних обсягах для оперативно-службової діяльності підрозділів МВС. У центральному апараті МВС України створена структурована гетерогенна комп'ютерна мережа, інформаційною магістраллю якої є оптоволоконинне кільце, до якого через комутаційне обладнання під'єднано локальні мережі галузевих служб МВС. Оперативно-розшукову діяльність забезпечує *інтегрований банк даних*, який складається з відомостей про:

- осіб криміногенних категорій;
- осіб, які допускають немедичне вживання наркотичних засобів, психотропних речовин і перебувають на диспансерному обліку;
- психічно хворих, які становлять небезпеку для оточення;
- утримувачів притонів;
- осіб, які займаються проституцією;
- осіб, затриманих за бродяжництво;
- інших категорії осіб, які перебувають на обліку в органах внутрішніх справ і схильні до вчинення злочинів;
- викрадені транспортні засоби;
- викрадені мобільні телефони;
- зареєстровану в Дозвільній системі МВС мисливську, спортивну, газову зброю громадян і організацій, табельну зброю ОВС, МО, Держприкордонслужби, СБУ, Держмитслужби, Державного департаменту з питань виконання покарань, Керування державної охорони, а також викрадену, вилучену номерну зброю;

- розшук злочинців та держборжників в Україні та СНД, безвісти зниклих;
- викрадені, вилучені предмети антикваріату;
- втрачені паспорти.

Крім того, для інформаційно-аналітичного забезпечення оперативних підрозділів ОВС використовується підсистема “ОРІОН” обласного та центрального рівнів, яка містить систематизовані, оперативні відомості стосовно осіб та тяжких злочинів, учинених на території України.

На даний час усі УМВС провадять оперативно-довідковий облік, використовуючи єдине для всіх структур програмне забезпечення. В інформаційній мережі ОВС України функціонують такі основні інформаційні системи: “Інтегрована інформаційно-пошукова система органів внутрішніх справ України” (“ІПС ОВС”), “Оперативно-довідкова картотека” (“ОДК”), “Автоматизований банк даних” (“АБД-центр”) та підсистеми: “Розшук”, “Пізнання”, “Міжвідомчий банк даних” (“МБД”), “Наркобізнес”, “Арсенал”, “Оазис”, “Втрачені паспорти”, система АІС “Інтегрований національний банк даних про транспортні засоби” та інші.

Інформаційна система “Автоматизований банк даних” (“АБД-центр”) забезпечує збір, обробку та аналіз інформації, яка регламентується відповідними наказами МВС України на вищому рівні МВС. На рівні обласних УМВС використовується версія цієї системи “АБД-область”, а на рівні районних підрозділів – “АБД-район”.

Автоматизований банк даних призначений для оперативного забезпечення працівників і підрозділів ОВС інформацією для розшукової діяльності, розслідування і попередження злочинів у повному і зручному для використання вигляді, надання аналітичної, статистичної та контрольної інформації.

Інформаційна система “АБД” забезпечує ведення таких інформаційних фондів: “Особа”, “Річ”, “Зброя”, “Угон”, “Злочин”, “Антикваріат”.

Інформаційна система дає змогу залучати додаткові інформаційні обліки, не порушуючи існуючих об’єктів.

Автоматизований банк даних забезпечує:

- інтерактивне введення інформації до форматів вхідних

документів;

- введення зображень усіх видів об'єктів “АБД”;
- налагодження пакетного обміну інформацією щодо необхідних форматів;
- коригування записів передбази, що не пройшли контроль.

7.13. Системи “Фоторобот і портретна ідентифікація”, “АР” (автоматичні пістолети)

Система АПС ПОРТРЕТ/У призначена для складання композиційних портретів (фотороботів). Для складання композиційного портрета (фоторобота) відбирається група портретів з необхідними ознаками зовнішності.

Режим складання словесного портрета в діалоговому режимі з пред'явленням свідкові типових малюнків елементів обличчя дозволяє оперативно провести опитування свідка і скласти з його слів словесний портрет.

Для пошуку портретів за описом здійснюється пошук портретів у базі даних на основі класифікаційного аналізу ідентифікаційних ознак портретних зображень і ознак зовнішності, а також їх упорядкування за ступенем подібності з портретом. Пошук портретів у базі даних здійснюється автоматично.

Складання фотороботів здійснюється з елементів зовнішності портретів групи подібності.

База даних підзвітних осіб містить крім портретів наступну інформацію: реєстраційний номер; прізвище, ім'я, по батькові; повну дату народження; код підрозділу, у якому особа стоїть на обліку.

Можливий пошук у базі за зазначеними реквізитами. У разі вибору якого-небудь запису бази відтворюється відповідний портрет.

Система АРМ “АР” (автоматичні пістолети) дає змогу вводити та переглядати параметри пістолетів, здійснює автоматичний пошук за такими параметрами:

- конструктивні особливості моделі;
- сліди на стріляній кулі;
- сліди на стріляній гільзі.

Дає змогу переглянути зображення пістолетів різноманітних систем. Має інтуїтивно зрозумілий інтерфейс і не створює труднощів при роботі з нею.

7.14. Автоматизація судово-експертних досліджень. Система “Автоекс”

Практика судово-експертних досліджень свідчить, що підвищення їх ефективності та наукової обґрунтованості нерозривно пов'язане з підвищенням рівня автоматизації інформаційного забезпечення цього виду юридичної діяльності.

Комп'ютерна техніка використовується у різних за змістом і метою напрямках.

1. Для автоматизації збору й обробки експериментальних даних, одержуваних у ході досліджень. Таке устаткування в більшості випадків являє собою вимірювально-обчислювальні комплекси, змонтовані на базі приладів і ПК. Для аналізу використовуються внутрішні технологічні банки даних, що містять або набори специфічних фізико-хімічних параметрів, які характеризують речовини й матеріали, або спектрограми об'єктів, записані безпосередньо на магнітних носіях.

2. АПС (автоматизовані інформаційно-пошукові системи) за конкретними об'єктами експертизи призначені для автоматизації деяких допоміжних обліків, таких, наприклад, систем, як “Метали” (містять відомості про склади металів і сплавів та галузі й сфери їх застосування); “Волокно” (характеристики текстильних волокон); “Марка” (характеристики автоемалі); “Взуття” (характеристики підшов взуття) тощо. Такі банки даних легко тиражувати. Вони можуть працювати як ізольовано, так і будучи вбудованими у вимірювально-обчислювальні комплекси.

3. Системи аналізу зображень. До них належать програми, що дозволяють проводити діагностичні й ідентифікаційні дослідження, наприклад, дактилоскопічні, трасологічні, портретні, складання композиційних портретів та ін. Деякі з цих систем використовуються для криміналістичної реєстрації.

4. Програмні комплекси або окремі програми виконання

допоміжних розрахунків за відомими формулами й алгоритмами, які необхідні, в першу чергу, у технічних експертизах, наприклад, для моделювання умов пожежі або вибуху для розрахунку кількісних характеристик процесів їх виникнення й розвитку. Велика кількість допоміжних розрахунків необхідна в автотехнічних, електротехнічних, технологічних експертизах. Спеціалізовані пакети прикладних програм створені також для розрахунків планово-економічних і бухгалтерських експертиз тощо.

5. Розробка програмних комплексів автоматизованого вирішення експертних завдань, що включають підготовку самого експертного висновку. Найпростішим прикладом є автоматизована експертна методика “Автоекс”: у програму закладені основні формули автотехнічних досліджень, які використовуються при вирішенні завдань у справах про наїзди на пішоходів.

Система “Автоекс” призначена для використання в експертних дослідженнях наїздів транспортних засобів на пішоходів. Ця система має досить високу ступінь автоматизації – від введення вхідних даних до отримання тексту експертного висновку. Система дає змогу відповісти на питання, які стосуються механізму дорожньо-транспортної пригоди: про швидкість автомашини, зупиночний шлях, положення автомобіля і пішохода в певні моменти часу та параметри дорожньо-транспортної пригоди; про наявність у водія технічної можливості не допустити наїзд транспортного засобу екстреним гальмуванням; про дослідження наїздів з обмеженою видимістю для водіїв. У системі передбачений контроль правильності введення вхідних даних. Експертний висновок, що автоматично формується системою, складається з текстової частини, математичних формул для обчислень параметрів пригоди, необхідних розрахункових таблиць. У цілому необхідно зазначити високу ефективність використання системи “Автоекс” завдяки засобам автоматизації та великій кількості автотехнічних експертиз, що проводяться останнім часом.

Для автоматизації експертних досліджень існують й інші програми, такі як: “Очевидець”, “FRO – ФОТОРОБОТ”, “Почерк”, “Oldman”, “Ирис”, “Мак”, “CHANGE”, “LEFTH”, “AGE.SEX”, “Дактоексперт”, “Дермалог”, “DEX”, “Сонда”, “Дактаузор”, “Холмс”, “Кортик”, “Авто”, “REFERENCE

MENAGER”, “MANEVR”, “СПИРТ”, “Бібліотека”, “FARM” тощо. Ці програми впроваджені у практику не так широко, як описані вище.

7.15. Експертиза фонограм усного мовлення, дактилоскопічна експертиза, ідентифікація почерку оператора ЕОМ

Експертиза фонограм. Звукові сліди в криміналістиці – досить новий вид інформації. У кримінальному процесі засоби, на яких зафіксовані звукові сліди, називаються матеріалами звукозапису (ст. 85 КПК України). Сучасні технічні засоби дають змогу на різноманітних матеріалах - носіях фіксувати звукові сліди злочинів, наприклад, хуліганські дії особи в квартирі, офісі, на вулиці, факти нанесення образи словами, вимагання хабара, погрози вбивством та ін. У цьому разі матеріали звукозапису в кримінальному судочинстві використовуються як речові докази, які можуть бути засобами для розкриття злочинів і викриття винних (ст. 78 КПК України). Перед експертом фонограми слідчий ставить декілька запитань: про ідентифікацію людини, голос якої записаний на носієві; про зміст сказаного; про додаткові звуки, що є у запису, та їх ідентифікацію тощо. Відеофонічна експертиза проводиться за допомогою комп’ютерних програм та спеціалізованого обладнання комп’ютерів.

Програма “PINGUIN– IP” – відкритий графічний інструментальний засіб для обробки та аналізу зображень (призначена для проведення відеофоноскопичних експертних досліджень).

Програма “EXPAD” – автоматизоване робоче місце експерта-криміналіста на базі персонального комп’ютера, що забезпечує введення фонограм у пам’ять ПК та проведення їх криміналістичного дослідження.

Дактилоскопія. Найефективнішим для ідентифікації слідів осіб, вилучених з місця вчинення злочину, залишається дактилоскопічний фонд. Саме тому було створено центральну автоматизовану дактилоскопічну систему. Сьогодні існує центральний банк даних (2,6 млн дактокарт осіб, що стоять на обліку) та встановлено в підрозділах інформаційної служби

УМВС областей спеціалізовані графічні станції для поточного введення дактокарт, що надходять на облік, завантаження їх до центрального банку даних та виконання ідентифікаційних завдань. Для проведення дактилоскопічних досліджень використовують автоматизовані дактилоскопічні інформаційно-пошукові системи “DEX” (Україна), “Морфо” (Франція), “NEC” (Японія), “Принтрак” (США), “Дермалог” (Німеччина), “Сонда” (Росія), “Папілон” (Росія), “Дактомат” (Білорусь) тощо.

Ідентифікація за клавіатурним почерком. Методи ідентифікації і аутентифікації, які базуються на використанні особистих ідентифікаторів, мають недоліки, пов’язані з необхідністю використання атрибутивних та пізнавальних характеристик. Ці недоліки зникають при використанні біометричних методів ідентифікації. Важливе місце серед біометричних підходів займають методи аналізу динамічних образів особистості (аутентифікація за динамікою рукописного підпису, клавіатурним почерком, особливостями роботи з комп’ютерною мишею тощо). Біометричні методи можна реалізувати за допомогою стандартних засобів мультимедіа. Наприклад, дослідження показали, що клавіатурний почерк конкретного користувача має високу стабільність. Це дозволяє за ним з високою достовірністю ідентифікувати користувача ПК.

Під поняттям “клавіатурний почерк” розуміємо систему індивідуальних особливостей набору і динаміки відображення літер, слів і речень на клавіатурі. Застосування методу ідентифікації за клавіатурним почерком виправдано щодо користувачів з великим досвідом роботи з комп’ютером, у яких вже сформувався власний почерк роботи на клавіатурі (програмістів, секретарів).

Вже існують розроблені програмні комплекси, що базуються на ідентифікації за методом клавіатурного почерку.

Контрольні питання

1. Відповідно до яких нормативних актів України відбувається повне фіксування судового процесу технічними засобами?
2. Техніко-технологічні функції системи технічної фіксації судових процесів.

3. Назвіть системи технічної фіксації судових засідань.
4. Назвіть складові електронного (віртуального) судочинства.
5. Які, на ваш погляд, переваги електронного (віртуального) судочинства.
6. Які, на ваш погляд, недоліки електронного (віртуального) судочинства.
7. Назвіть можливості, які дає судочинству застосування відеоконференцзв'язку.
8. Назвіть підсистеми Єдиної судової інформаційної системи.
9. Назвіть пріоритетні напрями інформатизації судової системи України.
10. Назвіть можливості системи автоматизації документообігу “Діловодство”.
11. Забезпечення гласності судового процесу з використанням “Голосового порталу”.

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

8.1. Поняття про глобальну комп'ютерну мережу Інтернет

У суспільстві склалося неоднозначне ставлення до глобальної комп'ютерної мережі Інтернет і тих технологій, що вона підтримує. Одні вважають, що це всесвітня комунікаційна мережа; другі – величезне інформаційне звалище; треті – мегамаркет без обмежень; четверті – ідеальне середовище для злочинців; п'яті – що це необмежене джерело інформації тощо. Тому надано сучасне техніко-технологічне визначення.

Інтернет (Internet) – мережа передачі даних, що має глобальну децентралізовану архітектуру, розвинені методи адресації і передачі інформації на основі протоколів TCP/IP між одно- і різнотипними мережами передачі даних, комп'ютерними системами і різноманітним термінальним (кінцевим) устаткуванням і забезпечує доступ до величезної кількості розподілених інформаційних ресурсів та надання різноманітних інформаційних послуг. Підкреслимо, що Інтернет є мережею, яка об'єднала існуючі мережі у різних частинах і країнах світу.

Розвиток мережі почався на початку 60-х рр. XX ст. Для створення надійної, безвідмовної мережі зв'язку під егідою агентства перспективних розробок міністерства оборони США (Defence Advanced Research Project Agency – DARPA) почалася розробка і впровадження глобальної військової комп'ютерної мережі, яка з'єднувала дослідні лабораторії на території США. За іменем агентства вона отримала назву ARPANet.

З 1974 р. для мережі використовуються протоколи IP (Internet Protokol) – міжмережний протокол та TCP (Transmission Control Protokol) – протокол керування передачею. Протоколи TCP/IP, які використовуються зараз, були написаними у 1981 р. Протоколи TCP/IP одержали статус стандарту США.

У 1990 р. Міністерство оборони США приймає рішення

побудувати власну мережу на основі ARPANet. Відбувається поділ наявної мережі на ARPANet і MILNet. Вводиться система доменних імен – Domain Name System (DNS), число хостів невідпинно зростає.

З 1991 р. починається активне комерційне використання Інтернету.

Днем народження українського Інтернету вважається 2 грудня 1992 р. Саме у цей день, після переговорів, що велися більше ніж рік із структурами в американському уряді, які відповідають за адміністрування Інтернету, був делегований домен для України – .UA. На 2004 р. в українському сегменті працювало більше 400 провайдерів, число користувачів складало приблизно 3,5 млн осіб. У 2005 р. кількість користувачів в Україні становила приблизно 4 млн осіб, на кінець 2006 р. – 4,5 млн (це 12-те місце у світі), весною 2008 р. – 7,7 млн користувачів. Загальна кількість користувачів у світі становить на початок 2009 р. приблизно 1 млрд, а кількість сайтів – приблизно 110 млн.

8.2. Технологічні та соціальні аспекти Інтернету

Технологія передачі інформації в мережі Інтернет побудована за принципом комутації пакетів. Визначальними для цієї технології є два поняття: протокол і адреса.

Протокол – це узгоджені правила взаємодії між двома хостами (таким терміном називають будь-які комп'ютери, що підключені до мережі, незалежно від типу, принципів дії та ін.). Стандартний протокол забезпечує “порозуміння” між хостами в мережі і сумісність програм та даних за системою кодування і форматом.

У системі протоколів TCP/IP протоколи IP відповідають за адресацію у мережі, а TCP – забезпечують доставку повідомлень за потрібною адресою.

IP виконує маршрутизацію даних між хост-машинами. Дані по мережі передаються частинами, які називаються дайтаграмами (datagrams). Мережі об'єднуються в Інтернеті за допомогою IP-маршрутизаторів (routers). Якщо одержувач дайтаграми знаходиться у другій мережі, то IP направляє дайтаграму на локальний

маршрутизатор. Якщо цей маршрутизатор не під'єднаний до даної мережі, то цю даятаграму посилають на інший маршрутизатор. Так продовжується доти, поки вона не досягне мережі одержувача. IP вибирає маршрут виходячи з інформації, яка знаходиться у таблиці маршрутизації.

TCP має механізм, який гарантує, що дані передаються без помилок, повністю і в потрібній послідовності. TCP посилає дані у вигляді сегментів, направляє їх по IP, який забезпечує їх маршрутизацію. З іншого боку, TCP сприймає вхідні сегменти від IP, визначає, який додаток є приймачем даних, і передає їх цьому додатку в такому порядку, в якому їх було отримано з TCP.

Адреса – це унікальний ідентифікатор хоста у мережі Інтернет. Уся мережа поділена на частини, які називаються доменами. Домени можуть мати субдомени (домени нижнього рівня), які, у свою чергу, можуть поділятися на субдомени. Адміністратор домену виконує присвоєння імен комп'ютерам. Назви доменів верхнього рівня є стандартизованими, серед них є домени для кожної країни. Імена можуть складатися з двох, трьох, чотирьох або п'яти міток. Стандарти Інтернету дозволяють мітки довжиною до 63 символів та імена до 255 символів. Наприклад, *jug-academy.kharkov.ua* – це і'мя домену, що належить Національній юридичній академії, складається з трьох міток. Доменні імена маршрутизатори перетворюють на числові адреси. Вони вже називаються IP-адресами. IP-адреса складається з чотирьох чисел (номерів), записаних через крапки. Наприклад: 10.106.1.1. Крайнє ліве число позначає адресу мережі верхнього рівня; числа, що стоять праворуч, означають більш дрібні ділянки мережі і так далі, поки не дійдемо до конкретного комп'ютера.

У мережі для користувачів підтримується низка послуг (їх також називають сервісами чи службами). Кожна послуга – це певні можливості для користувача під час роботи з мережею. Практично всі послуги мережі побудовані на принципі “клієнт–сервер”. Сервер (у мережі Інтернет) – це комп'ютер або програма, здатні надавати клієнтам (у міру надходження від них запиту) деякі мережні послуги.

Клієнт – прикладна програма, завантажена в комп'ютер користувача, яка забезпечує передачу запитів до сервера й

одержання відповідей від нього.

Соціальне значення мережі визначається тими можливостями, що їх може надати мережа для користувачів. Ці можливості реалізовані через сервіси. Різні сервіси мають різні прикладні протоколи. Найпоширенішими з них є наступні:

- *Електронна пошта (e-mail)* – для обміну електронними повідомленнями (листами) і невеликими блоками даних.

- *Телеконференції (usenet)* – спосіб спілкування користувачів мережі у рамках обраних дискусійних груп (групи новин).

- *Списки розсилки (maillists)* – спосіб спілкування через електронну пошту всіх, хто підписався на певний список розсилки.

- *Переміщення файлів (ftp)* – копіювання файлів даних із серверів у мережі на власний комп'ютер.

- *Віддалений доступ (telnet)* – спосіб керування іншим комп'ютером у мережі, яким дозволено це робити, де б він не знаходився.

- *Всесвітня павутина World Wide Web(WWW)* – спосіб доступу до інформаційних ресурсів у мережі, який реалізує концепцію гіперпосилань.

- *Gopher* – засіб розподіленого пошуку і передачі файлів у мережі.

- *IRC (Internet Relay Chat)* – спосіб спілкування з іншими користувачами мережі у режимі реального часу.

- *ICQ (I Seek You)* – безоплатна система Інтернет-пейджингу (передачі коротких повідомлень у мережі), у якій кожен користувач має свій унікальний номер.

- *VoIP (Voice over Internet Protocol; IP-телефонія)* – система зв'язку, яка забезпечує передачу голосу людини через мережу Інтернет.

- *Інтернет-аукціон (Internet auction)* – електронна торговельна система, у якій продаж товарів виконується безпосередньо між користувачами мережі.

- *Інтернет-радіо або веб-радіо (realaudio)* – технологія передачі поточкових аудіоданих через мережу Інтернет.

- *IP-телебачення (Internet Protocol Television, скорочено IPTV)* – система передачі телевізійних програм через Інтернет із забезпеченням додаткових послуг з вибору контенту й ке-

рування його подачею.

- *Інтернет-реклама* – медійна реклама, яка розміщується на сайтах в Інтернеті. Аналогічна рекламі у друкованих ЗМІ, але наявність у банері гіперпосилання та можливість анімаційного зображення значно розширюють можливості її дії.

- *MUD і MOO (Multi User Dungeon* – гра серед багатьох користувачів у мережі й *Object-Oriented MUD* – об’єктно-орієнтований світ користувачів) – гра рольового характеру серед користувачів для проведення дозвілля. У віртуальному світі MOO створюються об’єкти і визначаються їх властивості і зв’язки, що можуть застосовуватися навіть у освітніх цілях.

8.3. Правова характеристика базових понять

Визначення основних понять Інтернет-технологій наведено в Законі України “Про телекомунікації”. Основні з них такі:

- *адреса мережі Інтернет* – визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв;

- *адресний простір мережі Інтернет* – сукупність адрес мережі Інтернет;

- *домен* – частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється;

- *домен.UA* – домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів для обслуговування адресного простору українського сегмента мережі Інтернет;

- *домен другого рівня* – частина адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у цій мережі;

- *Інтернет* – всесвітня інформаційна система загального доступу, яка логічно зв’язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

- *провайдер телекомунікацій* – суб’єкт господарювання,

який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.

8.4. Пошук інформації у мережі

Пошукова система – це веб-сайт, який надає можливість пошуку інформації в мережі Інтернет. Більшість пошукових систем шукає інформацію на сайтах всесвітньої павутини, але існують системи, які здатні шукати файли на ftp-серверах, товари в Інтернет-магазинах, інформацію у групах новин usenet тощо. Існують кілька моделей роботи пошукових систем. За популярністю використання варто виділити дві моделі: каталоги (довідники, директорії) і пошукові машини (індекси або пошукові покажчики).

Пошукові каталоги. Каталоги в WWW представляють систематизовану за тематичними розділами інформацію про сторінки в мережі. Звичайно це багаторівнева класифікація посилань, побудована зверху вниз. По суті, пошукові каталоги є предметними каталогами й аналогічні бібліотечним каталогам. Вони являють собою набори посилань на сайти, організовані за змістовими властивостями. Каталоги можна назвати пошуковими деревами, тому що вони розгалужуються в міру уточнення теми. На основній сторінці пошукового каталогу знаходиться список великих тематичних категорій, наприклад: Комп'ютери й Інтернет (Computers & Інтернет). Кожен запис у списку – це гіперпосилання, за яким можна перейти до наступної сторінки пошукового каталогу, на якому дана тема представлена детальніше, наприклад: Інформатика (Computer Science) або Програми (Software). Продовжуючи вибір теми, можна дійти до останнього рівня – списку конкретних веб-сторінок і далі серед них вибрати потрібні ресурси.

Пошукові машини. Дуже часто виникає потреба в механізмі пошуку актуальної, унікальної, спеціальної інформації, що не охоплена і не може бути охоплена пошуковими каталогами. Для цього використовуються програмні засоби автоматичного пошуку. Задача пошукової машини (search engine) – знайти кваліфікованому користувачеві будь-яку інформацію,

якщо вона існує.

При пошуку веб-ресурсів користувач складає запит на пошук за допомогою ключових слів. Пошукова система повинна знайти веб-сторінки, що відповідають запиту. У результаті користувач має одержати гіперпосилання і короткі відомості про знайдені ресурси.

Мащини пошуку розрізняються мовами запиту, зонами пошуку, глибиною пошуку всередині документа, методами ранжування і пріоритетів, тому застосування різних пошукових машин дає, відповідно, різні результати.

Пошуковий двигун – комплекс програм, який забезпечує функціональність пошукової системи. Критеріями якості роботи пошукової системи є релевантність (тобто ступінь відповідності запиту і знайденого матеріалу), повнота бази, врахування морфології мови. Індексція інформації виконується пошуковими роботами. Використовуються двигуни, які ґрунтуються на технології RSS, а також такі, що базуються на роботі з XML-даними різних типів. Пошукові сервери збирають і зберігають характеристики переглянутих документів у своїх базах даних. Завдяки наявності каталогів можна вести спрямований пошук потрібних даних, переглядаючи їх вміст.

Контекстний пошук, тобто пошук за змістом документів, пошукові сервери виконують, використовуючи власні бази даних.

8.5. Основні пошукові портали

Найбільш популярні пошукові системи в Інтернеті: Google, Yahoo, Msn, Aol, Ask, Altavista, Excite, Lycos, All The Web; українські – Uaport, Poshuk, El.visti, Meta, Uaportal, Bigmir, Echo та ін.

У мережі Інтернет багато сайтів правової тематики. Українські юридичні ресурси в Інтернеті можна класифікувати наступним чином:

Бази законодавства:

- LIGAOnline–www.liga.net – база законодавства компанії “ЛігаБізнесІнформ”.

- “АТ Інформтехнология”–www.nau.kiev.ua – розроблювач популярної програми “Нормативні акти України”.

- “Сервер Верховної Ради України” – www.rada.gov.ua – безкоштовна база законодавства, інформація про юридичні видання, посилання на зарубіжні законодавства.

- “Сервер законодавчих актів України на Trifle.Net” (відомий також як база законодавства на сервері Apex) – www.apex.dp.ua.

Каталоги юридичної інформації:

- Розділ “Ukraine/Law” на Yahoo!-(англ.)

dir.yahoo.com/Government/Law/.

- “BRAMA: Ukrainian Law and Legal Matters” – www.brama.com (англ.) каталог української юридичної інформації

- “FindLaw:Ukraine-(engl.)” – www.findlaw.com, довідник ресурсів Інтернету юридичної тематики.

- “Ukraine at “CEE Source: Central and East European Legal, Political, Business and Economics WWW Resources” – (англ.) www.law.gonzaga.edu – розділ про Україну в базі даних по праву, політиці й економіці країн Центральної і Східної Європи.

- Розділ “Правительство” на “Ping:” – www.topping.od.ua.

Державні органи:

- “Перелік серверів державних органів” на сайті Верховної Ради України – portal.rada.gov.ua.

- “Кабінет Міністрів України” – (укр.) інформація про Кабінет Міністрів України – www.kmu.gov.ua/.

- “Головне керування державної служби України” – www.guds.gov.ua/.

- “Міністерство закордонних справ України” – www.mfa.gov.ua/.

- “Міністерство внутрішніх справ України” – (англ.,укр.) – www.mvs.gov.ua/.

- Сайт постійного представництва України в ООН – www.un.org.ua/.

- “Національний банк України” – www.bank.gov.ua.

- “Інформаційний центр Міністерства юстиції України” – www.informjust.kiev.ua.

8.6. Новітні пошукові технології

Зважаючи на стан розвитку інформаційних технологій, покращення надання та обробки інформації в мережі пов'язують з використанням парадигми багатоагентних систем. Передбачається, що пошукові системи на їх основі зможуть вийти на новий рівень ефективності. У розвитку систем пошуку й обробки Інтернет-ресурсів почали використовувати засоби штучного інтелекту. Відомі пошукові системи, які працюють на цих засадах: Autonomy, Webcompass, Marri, Daml, Ontoseek та ін. Вони, як правило, працюють з онтологіями для інтелектуальної обробки Інтернет-ресурсів. Саме тому з розвитком агентних технологій на основі методів і засобів штучного інтелекту пов'язують перспективи переходу від простору даних до простору знань у глобальних і локальних мережах.

8.7. Автоматизований бібліотечний комплекс Академії

Бібліотечний комплекс реалізований на базі прикладної програми “Система автоматизації бібліотеки” (САБ-2), яка функціонує у середовищі Windows 2000 і підтримує клієнт-серверну технологію обробки даних.

Користувачі системи розділені на дві категорії: а) внутрішні користувачі – персонал бібліотеки, представники якого мають прямий доступ до всіх баз даних; б) зовнішні користувачі, що одержують доступ до бази даних системи в он-лайнному режимі (через веб-сайт бібліотеки) читання.

Структура електронного каталогу в системі САБ-2 побудована згідно з прийнятими правилами ведення карткових каталогів, книг обліку і звітності. Загальний електронний каталог (ЕК) включає три великих розділи:

- бібліографічні описи неперіодичних видань (ЕК-Н);
- бібліографічні описи періодичних видань (ЕК-П);
- аналітичні описи статей та інших складових частин видань (ЕК-С).

На веб-сайті бібліотеки крім доступу до зазначених компонентів ЕК забезпечується доступ до специфічної довідкової

інформації статичного і динамічного характеру.

У всіх режимах пошуку застосовується однакова за структурою екранна форма, у якій для введення даних при формуванні пошукового запиту використовуються п'ять рядків (у першому режимі) або три рядки (у другому і третьому режимах). Кожен рядок введення даних складається з чотирьох сегментів, у які вводяться наступні дані: 1) ім'я обраного пошукового параметра; 2) значення обраної кількісної умови ($=$, \leq , \geq , \diamond); 3) значення пошукового параметра, що задається; 4) логічна умова, що задається, "И" або "ИЛИ".

Рис. 8.1. Вигляд екранної форми запиту на пошук видання.

Усі величини, крім значень пошукових параметрів, вибираються користувачем зі списків, що випадають (полів і умов), а значення пошукових параметрів вводяться користувачем за його розсудом. При цьому користувачеві доцільно увійти у відповідний довідник і переконатися в наявності тих значень пошукових параметрів, які він планує задати.

Список параметрів, що вибираються для включення в пошуковий запит, містить 12 параметрів: автор, вид видання, рік видання, видавництво, індекс ББК, індекс УДК, ключове слово,

основна назва, предметна рубрика, серія або ISSN, навчальна дисципліна (“тематика”), мова видання (рис. 8.1.).

У системі передбачено чотири формати видачі на екран результатів пошуку, які відрізняються своєю повнотою.

Крім того, кожний бібліотечний опис книги супроводжується “кнопками” для формування замовлення на одержання цього видання і для виклику повнотекстового документа (якщо такий міститься на сервері бібліотеки).

8.8. Локальні комп’ютерні мережі юридичних установ та організацій. Інформаційні сервіси в локальній мережі Національної юридичної академії України

Як приклад локальної комп’ютерної мережі розглянемо мережу Національної юридичної академії України ім. Ярослава Мудрого. Основою локальної мережі є оптичний кабель (10700 метрів), що з’єднав всі корпуси академії і став основою єдиної мультисервісної локальної комп’ютерної мережі (така її офіційна назва). На початок 2009 р. до мережі підключені комп’ютерні класи в учбових корпусах (головному та Інституті прокуратури). Закінчуються роботи з підключення оптичним кабелем гуртожитків. Загалом у мережі є більше 700 робочих місць (значну частку із них складають робочі місця у студентських гуртожитках). Основою мережі є багатофункціональний двопроцесорний сервер HP ProLiant DL380 з двома процесорами Intel Xeon® 3 GHz, дисковий масив ємністю 540 Gb з можливістю нарощування до 1 Tb. Для перетворення оптичної інформації функціонують чотири медіаконвертори D-Link, два керовані комутатори, 20 медіаконверторів по окремих корпусах та об’єктах і 18 звичайних комутаторів.

Створене інформаційне середовище в змозі потенційно забезпечити всі наявні сучасні й перспективні інформаційні сервіси.

У мережі можна скористатися такими сервісами:

- автоматизація проведення модульного контролю знань студентів;
- оперативний облік успішності та відвідувань студентів;

- доступ з усіх робочих місць до сайта бібліотеки;
- надання послуг IP-телефонії;
- 88 каналів цифрового TV;
- електронна пошта;
- файлообмінні послуги користувачам;
- доступ до електронних копій раритетних видань;
- доступ до ресурсів мережі Інтернет;
- доступ до інформаційної бази правничих документів,

яка поновлюється з сервера Верховної Ради України;

- інші послуги обслуговуючого характеру.

Також виконується підготовка передумов для реалізації елементів дистанційного навчання.

У мережі Інтернет Академія представлена власним сайтом. Веб-сайт Академії розміщений на головному сервері і цілодобово доступний в Інтернеті. Адреса сайта www.jur-academy.kharkov.ua. Сайт має сучасний дизайн, достатньо деталізований і відповідає сучасним вимогам щодо наявності елементів інтерфейсу. Також на сайті є власна пошукова система.

Контрольні питання

1. Сформулюйте визначення глобальної мережі Інтернет.
2. З якого часу Україна має власний домен в Інтернеті?
3. У чому полягає принцип комутації пакетів?
4. Що собою являє поняття “протокол передачі даних у мережі”?
5. Які протоколи покладено в технологічну основу роботи мережі Інтернет?
6. У чому полягає призначення протоколів IP?
7. У чому полягає призначення протоколів TCP?
8. Яким чином ідентифікуються хости в мережі?
9. Чому в Інтернеті набула поширення клієнт-серверна технологія?
10. Назвіть формат адреси хоста в Інтернеті (у доменній формі та у вигляді IP-адреси).
11. Зазначте особливості адресації користувачів сервісу e-mail.

12. У чому полягає призначення сервісу переміщення файлів? Назвіть його характеристики.

13. Яке призначення сервісу e-mail? Назвіть його характеристики.

14. Назвіть характеристики сервісу телеконференцій. У чому його призначення?

15. Для чого застосовується сервіс списків розсилки? Які його характеристики?

16. Які послуги надає сервіс віддаленого доступу? Назвіть його характеристики.

17. Яке призначення і характеристики сервісу IRC?

18. Сервіс ICQ – його призначення і характеристики.

19. Назвіть призначення і принципи організації мережі WWW.

20. Назвіть призначення і характеристики сервісу VoIP.

21. Назвіть призначення і характеристики сервісу IPTV.

22. Наведіть законодавче визначення поняття “домен”.

23. Назвіть нормативний документ, що визначає основні поняття Інтернет-технологій.

24. Що собою являють пошукові каталоги в WWW?

25. Що собою являють пошукові машини в WWW?

26. Які пошукові портали вам відомі?

27. Парадигма багатоагентного пошуку. В чому є її сутність?

28. На якій технології побудовано бібліотечний комплекс академії?

29. Якою є структура пошукового запиту в бібліотечному комплексі?

30. Для чого застосовуються логічні умови в запитах до бібліотечного комплексу?

31. Які параметри можуть бути включені в пошуковий запит?

32. Назвіть сервіси, що надаються користувачам локальної мережі Академії.

33. Опишіть структуру веб-сторінки Академії в Інтернеті.

СЛОВНИК ТЕРМІНІВ

F

fb2 (FictionBook) – формат представлення електронних версій книг у вигляді XML-документів, де кожен елемент книги описується своїми тегами.

G

Gopher – засіб розподіленого пошуку файлів у мережі і передачі їх.

I

ICQ (I Seek You) – безоплатна система Інтернет-пейджингу (передачі коротких повідомлень у мережі), у якій кожен користувач має свій унікальний номер.

IP-адреса (Internet Protocol address) – ідентифікатор (унікальний номер), що використовується для адресації комп'ютерів та пристроїв у мережі TCP/IP (наприклад, мережі Інтернет).

IP-телебачення (Internet Protocol Television, скор. – IPTV) – система передачі телевізійних програм через Інтернет із забезпеченням додаткових послуг із вибору контенту і керуванням його подачею.

IRC (Internet Relay Chat) – спосіб спілкування з іншими користувачами мережі у режимі реального часу.

iSilo (Plam Os Platform /pdb – Palm Pilot Database format) – формат бази даних, використовується у всіх 3Com PalmPilot, IBM Workpad і Macintosh/PC для збереження записів у базі даних.

M

Microsoft Access – система керування базами даних, яку можна використовувати для збереження, сортування й керування практично будь-якими типами даних.

Microsoft Excel – програма керування електронними таблицями загального призначення, що використовується для розрахунків, організації й аналізу ділових даних. Входить до складу Microsoft Office.

Microsoft Front Page – додаток, призначений для створення веб-публікацій.

Microsoft Office Publisher – програма, що дозволяє створювати та редагувати буклети, брошури, оголошення, бюлетені, веб-вузли й т. ін.

Microsoft Outlook – є комбінацією програми обробки електронної пошти і менеджера особистої інформації або могутнього багатофункціонального органайзера.

Microsoft Power Point – засіб розробки демонстраційних матеріалів для електронної презентації з використанням слайдів.

Microsoft Word – додаток для створення й обробки документів.

P

PGP – програма, яка реалізує технологію створення електронного підпису на документах.

Q

QA – несанкціонований доступ і перехоплення.

QD – зміна комп'ютерних даних.

QF – комп'ютерне шахрайство.

QR – незаконне копіювання.

QS – комп'ютерний саботаж.

QZ – інші комп'ютерні злочини.

R

RSS (Really Simple Syndication) – сімейство XML-форматів, що використовується для публікації та постачання інформації, яка часто змінюється, наприклад, нових записів у блозі, заголовків новин, анонсів статей, зображень, аудіо- і відеоматеріалів. Документ у стандарті RSS (інколи називають “стріч-

кою”, “веб-стрічкою” або “каналом”) складається з повного або часткового тексту і метаданих (дати й авторства).

S

Signature Cryptographer – програма для захисту інформації у важливих файлах від несанкціонованого доступу.

“SRS-Femida” – система фіксування ходу судового процесу, що забезпечує якісний цифровий аудіозапис судового процесу і можливість одержання текстових звітів на комп’ютері за допомогою програм.

V

VBA (Visual Basic for Application, Visual Basic для додатків) – середовище програмування, розроблене спеціально для створення макросів у додатках. Підтримується всіма додатками пакета Microsoft Office.

VoIP (Voice over Internet Protocol; IP-телефонія) – система зв’язку, яка забезпечує передачу голосу людини по мережі Інтернет.

X

XML (Extensible Markup Language) – розширювана мова розмітки – стандарт побудови мов розмітки ієрархічно структурованих даних для обміну між різними додатками, зокрема, через Інтернет. XML - документ складається із текстових знаків, у найпростішому випадку, – ASCII, і придатний до читання людиною.

А

Автентичність інформації у ДПС – властивість, яка гарантує, що суб'єкт або ресурс ідентичний заявленим.

АПС (автоматизовані інформаційно-пошукові системи) – сукупність програмно-апаратних засобів, призначених для автоматизації діяльності, пов'язаної зі зберіганням, передачею і обробкою інформації.

Архівна копія фонограми – запис на відповідному носії комплексу звукозапису, що має статус оригіналу та призначений для довготривалого зберігання в архіві.

Б

Багатоагентні системи (Multi-agent system) – системи, основними компонентами яких є множина програмних модулів (інтелектуальних агентів), які виконують свої функції на вузлах комп'ютерної мережі у взаємодії між собою та серверною частиною системи.

Бібліотечна система – систематизована сукупність електронного каталогу та електронних документів, які об'єднані за тематичними та іншими ознаками, має додаткові сервіси і можливості, що спрощують пошук документів і роботу з ними. Сучасні бібліотечні системи побудовані за клієнт-серверною технологією і використовуються в локальних чи глобальних мережах.

Браузер (browser) – програма для комп'ютера або іншого електронного пристрою (смартфона, мобільного телефона), під'єданого до Інтернету, яка дає можливість шукати та переглядати інформацію на веб-сторінці.

Буфер – сегмент пам'яті для тимчасового збереження даних.

В

Веб-сторінка – текстовий файл, що містить опис зображення документа мовою гіпертекстової розмітки – HTML (Hyper Text Markup Language). Сторінка може містити не тільки форматований текст, а й графічні, звукові та відеооб'єкти. Найважли-

віщою рисою веб-сторінок є гіпертекстові посилання. Передбачається, що веб-сторінка розміщується на сайті в Інтернеті.

Вербальні моделі – моделі, що відтворюють систему за допомогою слів. Наприклад, різні статuti, розпорядження щодо експлуатації, законодавчі матеріали, процесуальні кодекси тощо.

Віддалений доступ (telnet) – сервіс в Інтернеті, спосіб керування комп'ютером у мережі іншим комп'ютером, якому дозволено це робити, де б він не знаходився.

Відеоконференцз'язок (ВКС) – телекомунікаційна технологія інтерактивної взаємодії двох і більш видалених абонентів, при якій між ними можливий обмін аудіо- та відеоінформацією в реальному масштабі часу з урахуванням передачі керуючих даних.

Відеоконференція – інформаційна технологія, що забезпечує одночасно двосторонню передачу, обробку, перетворення і представлення інтерактивної відео- та звукової інформації на відстань у реальному режимі часу за допомогою апаратно-програмних засобів обчислювальної техніки. Між двома та більше абонентами для проведення відеоконференцій використовуються така технологія, як відеоконференцз'язок.

Відкритий (публічний) ключ – а) один з пари ключів несиметричного шифрування, технології створення ЕЦП, який його власник відкрито розсилає своїм адресатам; б) параметр криптографічного алгоритму перевірки ЕЦП, доступний суб'єктам відносин у сфері використання ЕЦП.

Візуальна форма електронного документа – відображення даних, які містять документ, електронними засобами або на папері у формі, придатній для сприймання його змісту людиною.

Власна база ДПС – сервіс, призначений для самостійного створення власної ієрархічної бази даних, яка може зберігати як власні документи користувача, так і посилання на документи головної бази даних ДПС.

Всесвітня павутина World Wide Web (WWW) – сотні мільйонів пов'язаних між собою документів, розміщених на комп'ютерах, що знаходяться на всій земній кулі, які реалізують доступ до інформаційних ресурсів у мережі через концепцію гіперпосилань.

Г

Гіперзв'язок – елемент (текстовий, графічний і т. д.), вибір якого дозволить перейти до іншого об'єкта (файла, фрагмента файлу, веб-сторінки, деяких сервісів Інтернету і т. д.).

Голосовий портал – інтелектуальна голосова комерційна система масового обслуговування телефонних абонентів, яка забезпечує автоматичну обробку телефонних дзвінків за допомогою комп'ютерів.

Д

Дайджест повідомлення (електронна печатка) – унікальна послідовність символів, що однозначно відповідає змісту повідомлення; є обов'язковим елементом ЕЦП і вказує на зміни у змісті повідомлення, якщо такі були.

Дані – величини та їх відношення, словосполучення, факти, перетворення й обробка яких дозволяє одержати інформацію, а потім і знання про той чи інший предмет, процес або явище; слугують матеріалом, з якого внаслідок обробки даних створюється інформація.

“Діловодство” – система автоматизації документообігу, що дозволяє автоматизувати практично всі аспекти роботи суду, починаючи з первинної реєстрації документів і ведення журналів і закінчуючи автоматизованою підготовкою рішень, автоматичною відправкою їх в ЄДРСР, обміном справами і документами між вказаними судами і автоматичною побудовою статистичного звіту.

Дистанційне навчання – одержання освіти на основі сучасних педагогічних та інформаційних методів через застосування телекомунікаційних технологій.

Діаграма – графічне зображення даних робочого листа.

Документообіг – рух документів в установі, організації з моменту їх одержання або створення до завершення виконання або відправлення.

Домен – частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслугову-

ється групою серверів доменних імен та централізовано адмініструється.

Доменні імена (доменна адреса) – унікальне алфавітно-цифрове ім'я, що ідентифікує конкретний вузол Інтернету. Кожне доменне ім'я відповідає одній або декільком IP-адресам; одній IP-адресі можуть відповідати декілька доменних імен.

Достовірність інформації у ДПС – тексти повинні надходити до бази з перевірених джерел, перевірятися на предмет відповідності оригіналові і бути автентичними йому.

ДПС (довідкова правова система) – програмний комплекс, що включає масив правової інформації і програмні інструменти, що дозволяють фахівцям працювати з цим масивом інформації (проводити пошук конкретних документів або їх фрагментів, формувати добірки необхідних документів, виводити інформацію на друк тощо).

Е

Електронна комерція – один з елементів електронного бізнесу, пов'язаний із виконанням функцій маркетингу, включаючи продаж товарів і послуг через Інтернет.

Електронна пошта (e-mail) – популярний сервіс в Інтернеті, що робить можливим обмін даними будь-якого змісту (текстові документи, аудіо- та відеофайли, архіви, програми) через мережу.

Електронна таблиця – засіб інформаційних технологій, прикладна програма, що дозволяє вирішувати різні обчислювальні задачі, сортування, фільтрацію даних тощо.

Електронне (віртуальне) судочинство – проведення судового процесу з використанням сучасних комп'ютерних та телекомунікаційних технологій.

Електронний бізнес – будь-яка трансакція, здійснена за допомогою функціональності інформаційної системи, після закінчення якої відбувається передача права власності або права користування реальним продуктом або послугою.

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи

обов'язкові реквізити документа.

Електронний документообіг (обіг електронних документів) – сукупність процесів створення, обробки, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності, а в разі необхідності з підтвердженням факту одержання таких документів.

Електронний підпис – а) обов'язковий реквізит електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу. Накладанням електронного підпису завершується створення електронного документа; б) дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

Електронний цифровий підпис (ЕЦП) – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. ЕЦП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Електронні архіви – системи автоматизації, призначені, насамперед, для фізичного збереження електронних копій документів та їх пошуку.

ЄСІС (Єдина судова інформаційна система України) – система інформатизації діяльності судів та державної судової адміністрації на підставі використання сукупності нормативно-правових, програмно-технічних та телекомунікаційних засобів, що забезпечують збирання, накопичення, аналіз та зберігання інформації судової діяльності.

3

Закладки до документів довідкової правової системи – створюються користувачем для здійснення швидкого переходу до обраного фрагмента тексту за допомогою функції “Пошук за

закладками” в головному вікні системи ДПС “НАУ”. У тексті можна встановити закладку з власним коментарем.

Закритий (особистий) ключ – один з пари ключів несиметричного шифрування технології створення ЕЦП, який його власник залишає собі.

Засоби юридичної діяльності – норми права, юридична техніка й різні предмети матеріального світу, що забезпечують досягнення мети юридичної діяльності. Ці предмети виступають як засоби збору й обробки інформації, засоби захисту, охорони і нападу (ЕОМ, зброя, аудіо-, відеотехніка).

Змістовий аспект ІІІ – юридичне закріплення питань, пов’язаних із впровадженням у певну сферу суспільних відносин інформаційних технологій.

Знакові моделі – описують аналізовану систему за допомогою логічних і математичних символів.

I

Інтеграція права і інформатики (ІІІ) – об’єктивний закономірний процес інтенсивного зближення інтересів права і інформатики, викликаний нагальною необхідністю взаємного використання новітніх досягнень цих наук.

Інтегрований банк даних нормативних документів – інтегрований банк даних МЕГА-НАУ, який об’єднує базу судових рішень НАУ-Судові рішення та базу правової і аналітичної інформації НАУ-Експерт, містить великий обсяг інформації та систему зв’язків, яка інтегрує судові рішення й нормативні акти в єдиний аналітичний комплекс.

Інтелектуальний пошук – одержання інформації за смисловим змістом.

Інтернет – всесвітня інформаційна система загального доступу, логічно зв’язана глобальним адресним простором, базується на Інтернет-протоколі TCP/IP, визначеному міжнародними стандартами, забезпечує обмін даними між комп’ютерами в мережі.

Інтернет-аукціон (Internet auction) – електронна торговельна система, в якій продаж товарів виконується безпосеред-

ньо між користувачами мережі.

Інтернет-радіо або веб-радіо (realaudio) – технологія передачі поточкових аудіоданих через мережу Інтернет.

Інтерфейс – правило взаємодії та обміну даними між та всередині апаратного та програмного комплексів ЕОМ, а також людиною та ЕОМ.

Інформатизація – сукупність взаємозалежних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, спрямованих на створення умов для задоволення інформаційних потреб громадян і суспільства на основі розбудови, розвитку й використання інформаційних систем, мереж, ресурсів та інформаційних технологій застосуванням сучасної обчислювальної та комунікаційної техніки.

Інформатика – фундаментальна галузь наукового знання, що формує системно-інформаційний підхід до аналізу навколишнього світу, вивчає інформаційні процеси й системи, методи й засоби одержання, перетворення, передачі, збереження й використання інформації у різних галузях соціальної практики.

Інформаційні відносини – відносини в суспільстві, які виникають із приводу змісту, збереження, передачі й використання інформації.

Інформація – а) дані, знання, повідомлення, які є об'єктом збереження, передачі й перетворення і допомагають вирішити певне завдання; б) нові дані, які може використати людина для вдосконалення своєї діяльності та поповнення знань.

К

Клієнт – прикладна програма, завантажена в комп'ютер користувача, яка забезпечує передачу запитів до сервера й одержання відповідей від нього.

Ключ шифрування – набір даних, необхідних для застосування методу шифрування.

Коментар до документа ДПС – функція “Коментар до документа” дає можливість отримати додаткові відомості аналітичного характеру, що стосуються змісту, статусу, редакцій документа тощо.

Комп'ютерний злочин – суспільно небезпечне, карне діяння (дія або бездіяльність), предметом якого є комп'ютерна інформація, направлена на заподіяння шкоди.

Компрометація електронного підпису – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа.

Контроль документів ДПС – забезпечує можливість швидко визначити зміни в документах, які попередньо встановлено на контроль. Контролюється внесення змін у текст документа або інформація про його опублікування.

Криптоаналіз – галузь криптографії, яка займається розробкою методів, що дозволяють розшифровувати інформацію та оцінювати якість захисту інформації шифром (його *криптостійкість*).

Криптографічний захист інформації – вид захисту інформації, що реалізується перетворенням інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Криптографія – наука про методи шифрування.

Криптостійкість – якість захисту інформації шифром.

М

Макрос – набір команд і інструкцій, що виконуються як одна команда у додатках Microsoft Office.

Маркери ДПС – виділений кольором фрагмент тексту.

Медіаконвертор – пристрій, призначений для перетворення сигналу одного виду в інший. Найчастіше середовищем розповсюдження сигналів є мідні дроти, оптичні кабелі та радіоканали. У кожному з названих середовищ сигнали представлені різними видами. Їх взаємне перетворення виконують медіаконвертори.

Метод шифрування – формальний алгоритм, що описує порядок перетворення повідомлення в зашифроване.

Моделі-аналоги – зменшені копії системи, виконаної за допомогою фізичних і технічних засобів (моделі літаків, теплоходів або макети електростанцій, міст).

Модель – матеріальний чи уявний об’єкт, який у процесі дослідження замінює об’єкт-оригінал так, що його безпосереднє вивчення дає нові знання про об’єкт-оригінал.

Н

Національна програма правової освіти населення – програма, що передбачає створення необхідних умов для набуття широкими верствами населення правових знань та навичок у їх застосуванні, забезпечення доступу громадян до джерел правової інформації, а також визначає основні напрями правоосвітньої діяльності та першочергові заходи щодо їх реалізації.

Несиметричне шифрування – шифрування та розшифрування проводиться різними ключами, які створюють взаємозалежну пару ключів – особистий та відкритий.

Нотаріальний реєстр – центральна база даних, у яку вноситься певна інформація. Бази окремих реєстрів зв’язані одна з одною; використовуються єдині словники: адміністративно-територіального устрою України, суб’єктів, документів.

О

Об’єкти юридичної діяльності – явища, процеси і предмети, щодо яких здійснюється правове втручання.

“Оберіг” – система фіксування ходу судового процесу, що забезпечує створення фонограми, розміченої відповідно до подій судового процесу і протоколу, в якому відображається в хронологічній послідовності: час початку / кінця всіх виступаючих, коментарі до кожного виступу, які за необхідності робить секретар, номер компакт-диска, на який здійснюється запис, а також інша необхідна інформація.

Онтологія – модель детальної формалізації галузі знань з допомогою концептуальної схеми. Така схема містить структури даних, які описують всі релевантні класи об’єктів, їх зв’язки та правила виводу знань, що прийняті у цій галузі.

Оперативність надходження нової інформації до ДПС – щоденне поновлення баз даних.

Особистий (закритий) ключ – параметр криптографічного алгоритму формування ЕЦП, доступний тільки підписувачу.

П

Переміщення файлів (ftp - file transfer protocol) – сервіс в Інтернеті, призначення якого полягає в копіюванні файлів даних із серверів у мережі на власний комп'ютер.

Повнота інформації у ДПС – показник, що характеризує міру достатності інформації для вирішення різних завдань.

Посилений сертифікат відкритого ключа – сертифікат ключа, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом.

Пошукова система – служба в Інтернеті, яка надає можливість пошуку інформації на сайтах, а також (можливо) у групах обговорення та ftp-серверах.

Пошуковий апарат ДПС – програмний інструмент, який дозволяє користувачеві працювати з масивом правової інформації (пошук за: контекстом, реквізитами, темою, закладками, документами на контролі).

Пошуковий робот (спайдер) – програма, що є складовою частиною пошукової системи і призначена для обходу сторінок Інтернету з метою занесення інформації про них (ключових слів) у пошуковий каталог.

Пошукові запити довідкової правової системи – спеціальні елементи пошуків за їх реквізитами: видавцем, номером, датою, назвою, видом, статусом, відомостями про реєстрацію.

Правова інформатика – комплексна наукова дисципліна, що вивчає закономірності інформаційних процесів, проблеми створення, впровадження й ефективного функціонування комп'ютеризованих систем обробки правової інформації і, зокрема, системної інформації законотворчої, нормотворчої, правозастосовної та правоосвітньої діяльності, а також проблеми нормативно-правового регулювання нового класу суспільних відносин – інформаційних.

Правова інформація – а) зміст даних (повідомлень), використання яких допомагає вирішити ту чи іншу правову задачу

чи сприяє її вирішенню; б) *(законодавче визначення)* 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. Правовій інформації притаманні ті самі властивості, що і звичайній.

Правовий режим фіксування судового процесу – сукупність нормативно закріплених умов фіксування судового процесу. Визначається п. 7 ч. 3 ст. 129 Конституції України, п. 10, 11 ст. 6 та ст. 197 Цивільного процесуального кодексу України, ст. 41 Кодексу адміністративного судочинства України, ст. 4-4 Господарського процесуального кодексу України, п. 4 ст. 9, п. 14 ст. 126 Закону України “Про судоустрій в Україні”, п. 28 ст. 4 постанови Кабінету Міністрів України від 14 січ. 2009 р. № 14 “Про затвердження Положення про Державну судову адміністрацію України”.

Прикладний аспект ІІІ – використання останніх досягнень у галузі інформаційних технологій, пристосованих або спеціально розроблених для розвитку й функціонування юридичної науки і практики.

Протокол ІР (Інтернет-протокол) – мережний протокол, який визначає маршрутизацію передачі інформації та відповідає за адресацію пакетів.

Протокол зв’язку – набір стандартних правил представлення інформації, передачі сигналів, ідентифікації та виявлення помилок, необхідний для обміну інформацією.

Протокол комунікаційний – обумовлені наперед правила передачі даних між двома пристроями. До основних параметрів, які описує протокол, відносяться: тип перевірки помилок, що використовується при передачі; метод компресії (стискання) інформації (якщо такий є); спосіб визначення передавальним пристроєм факту завершення передачі; *П.к.* є одним із протоколів зв’язку.

Протокол мережний – оснований на стандартах набір правил, що визначає принципи взаємодії комп’ютерів у мережі; задає загальні правила взаємодії різноманітних програм, мережних вузлів чи систем і створює таким чином єдиний простір пе-

редачі; *П.м.* є одним із протоколів комунікаційних.

Протокол TCP – Transmission Control Protocol (Протокол керування передачею) – один з основних мережних протоколів Інтернету, призначений для керування передачею даних в мережах і підмережах TCP/IP.

Р

Реквізити правових документів – найбільш усталені структурні елементи нормативних правових актів: видавець, номер, дата, назва, вид, статус, відомості про реєстрацію.

Робоча копія фонограми – запис на відповідному носії комплексу звукозапису або на комп'ютері архіваріуса.

С

Сайт (веб-сайт) – сукупність веб-сторінок, доступних у мережі Інтернет, об'єднаних як за змістом, так і навігаційно; фізично *с.* може розміщуватися як на одному, так і на декількох серверах; за ним закріплена унікальна IP-адреса.

Сервер – комп'ютер або програма, здатні надавати клієнтам (у міру надходження від них запиту) деякі мережні послуги.

Сервіси ДПС – особливі інструменти, які дозволяють не лише знайти потрібні документи, але й зручно працювати з ними.

Сертифікації відкритих ключів – процедура підтвердження особи власника відкритого ключа в Центрі сертифікації.

Симетричне шифрування – шифрування, яке проводиться тим самим ключем, що й розшифрування.

Система – сукупність взаємопов'язаних об'єктів, підпорядкованих певній єдиній меті з урахуванням умов навколишнього середовища.

Система електронного документообігу – організаційно-технічна система, яка забезпечує процес створення, керування доступом і розповсюдження електронних документів у комп'ютерних мережах, а також забезпечує контроль над потоками документів в організації.

Системи державно-правового характеру – цілеспрямовані механізми управління, тісно пов'язані з правом, виконують

функцію регулятора суспільних відносин.

Списки розсилки (maillists) – сервіс в Інтернеті; спосіб спілкування через електронну пошту всіх, хто підписався на певний список розсилки.

Суб'єкти юридичної діяльності – юристи і їх об'єднання.

Т

Телеконференції (usenet) – сервіс в Інтернеті; спосіб спілкування користувачів мережі у рамках обраних дискусійних груп (груп новин).

Технології OLE (Object Linking and Embedding) – методи зв'язування і впровадження об'єктів за допомогою буфера обміну, які дозволяють здійснювати обмін об'єктами і даними різних типів між документами.

“Тритон” – система фіксування ходу судового процесу з використанням цифрового магнітофона.

Ф

Фіксування судового процесу – а) *(у процесуально-правовому аспекті)* відбиття, закріплення юридично значущих дій суду, інших учасників судового процесу у відповідних процесуально-документальних формах для забезпечення їх вірогідності з точки зору об'єктивності засобів фіксації судового процесу та визначення процесуальних наслідків цих дій при розгляді справи по суті та на наступних стадіях судового процесу; б) *(у технічному аспекті)* фіксування, зберігання, копіювання (дублювання) та використання інформації, яка відображає хід судового засідання (судового процесу) з використанням сукупності апаратно-програмних засобів, приладів і відповідних інструкцій.

Фільтрація – швидкий спосіб виділення із списку підмножини потрібних даних для подальшої роботи з ними.

Формат СНМ (Compiled HTML) – набір скомпільованих HTML-файлів, подібний архіву з веб-сторінок; діє СНМ-файл за принципом архіву, стискає дані, що зберігаються в ньому, але не всі, а тільки текстові або такі, що містять текст, який

відформатований за допомогою тегів HTML (HTML, TXT, CSS і файли інших форматів).

Формат DjVu (від фр. *deja vu* – вже бачене) – графічний формат, розроблений фірмою AT&T, оптимізований для зберігання відсканованих документів.

Формат PDF (Portable Document Format) – формат електронних документів, розроблений компанією Adobe Systems і створений як засіб міжплатформеного обміну даними. У першу чергу призначений для представлення в електронному вигляді поліграфічної продукції. Значна кількість сучасного професійного друкарського устаткування може обробляти PDF безпосередньо.

Формула масиву в Microsoft Excel – обробляє декілька наборів значень, що називаються аргументами масиву.

Формули Excel – вираз, що починається із знаку рівності і складається з числових величин, адрес комірок, функцій, імен, які сполучені знаками арифметичних операцій. Результатом виконання формули є значення, яке виводиться в комірці, а сама формула відображається в рядку формул. Якщо значення в комірках, на які є посилання у формулах, змінюються, то результат зміниться автоматично.

Функціональні клавіші – клавіші на клавіатурі комп'ютера (зазвичай позначаються FN), які можуть бути запрограмовані так, щоб викликати команду операційної системи або прикладних програм для виконання певних дій.

Функція в Microsoft Excel – об'єднання декількох обчислювальних операцій для розв'язання певної задачі. Функції в Microsoft Excel являють собою формули, що мають один або декілька аргументів, тобто числові значення або адреси комірок.

X

Хост – узагальнена назва будь-якого комп'ютера, підключеного до мережі, незалежно від типу, принципів дії, призначення.

Ц

Центр сертифікації – організація, яка замається сертифі-

кацією (підтвердженням належності до заявника) відкритого ключа.

Ш

Шаблон – бібліотека стилів, яка визначає основну структуру документа і містить його настройки: елементи автотексту, шрифти, необхідні поєднання клавіш, макроси, меню, параметри сторінки, форматування і стилі.

Штучний інтелект (Artificial intelligence) – розділ інформатики, що займається формалізацією методів постановки та рішення задач, які нагадують методи, що використовує людина.

Ю

Юридична клініка – некомерційна організація при юридичних ВНЗ України, яка веде просвітницьку роботу і здійснює безоплатну правову допомогу особам, які потребують соціального захисту та підтримки, на базі якої студенти старших курсів юридичних спеціальностей набувають практичних навичок роботи юриста.

Юридична обробка інформації в системах – багатоетапний процес підготовки та контролю вхідних правових документів: загальний аналіз нормативних актів, виявлення прямих і непрямих зв'язків між документами і правовими нормами, унаслідок чого документи в ДПС зв'язані перехресними посиланнями, що не обмежуються випадками очевидних згадувань одного документа в іншому.

СПИСОК ЛІТЕРАТУРИ

- Вопросы кибернетики и права: Сб. – М.: Наука, 1967.
Правовая кибернетика: Сб. – М.: Наука, 1973.
- Гаврилов О.А. Математические методы и модели в социально-правовых исследованиях. – М.: Наука, 1980. – 183 с.
- Компьютерные технологии в юридической деятельности: Учеб. и практ. пособие / Под ред. Н. Полевого, В. Крылова. – М.: БЕК, 1994. – 304 с.
- Коваленко М.М. Комп'ютерні віруси і захист інформації. – К.: Наук. думка, 1999. – 262 с.
- Гаврилов О.А. Курс правовой информатики: Учеб. для вузов. – М.: НОРМА-М, 2000. – 432 с.
- Ситник В.Ф. Основы інформаційних систем: Навч. посіб. – 2-ге вид., переробл. і допов. – К.: КНЕУ, 2001. – 420 с.
- Береза А.М. Електронна комерція: Навч. посіб. – К.: КНЕУ, 2002. – 236 с.
- Основы информатики та обчислювальної техніки: Навч. посіб. / Иванов В.Г., Карасюк В.В., Гвозденко М.В.; За заг. ред. В.Г. Иванова. – К.: Юрінком Інтер, 2004. – 328 с.
- Навчально-методичний посібник для самостійної роботи та практичних занять з навчальної дисципліни “Правова інформація та комп'ютерні технології в юридичній діяльності” / Уклад.: В.Г. Иванов, С.М. Иванов, В.В. Карасюк та ін. – Х.: Нац. юрид. акад. України, 2009. – 48 с.
- Будапештская инициатива “открытый доступ” [Электронный ресурс]. – Режим доступа: URL: <http://www.soros.org/openaccess/ru/read.shtml>. – Загл. с экрана.
- Копанова В. Бібліотека в системі наукової електронної комунікації // Бібл. вісн. – 2007. – № 5. – С. 3-9.
- е-будущее и информационное право / Брыжко В.М., Цимбалюк В.С., Орехов А.А., Гальченко О.Н.; Под ред. Р.А. Калужного, М.Я. Швеца. – К.: Интеграл, 2002. – 264 с.
- Денисова О.О. Інформаційні системи і технології в юридичній діяльності : Навч. посіб. – К.: КНЕУ, 2003. – 315 с.
- Інформаційно-пошукова система “Нормативні акти України”: Навч.-практ. посіб. / Иванов В.Г., Карасюк В.В., Гвозден-

ко М.В. – Х.: Нац. юрид. акад. України, 2000. – 30 с.

Інформаційно-пошукова система “АБД – Район”: Навч.-практ. посіб. з дисципліни “Правова інформація та комп’ютерні технології в юридичній діяльності”/ Іванов В.Г., Карасюк В.В., Гвозденко М.В. та ін. – Х.: Нац. юрид. акад. України, 2000. – 44 с.

Комп’ютерні технології у підготовці юридичних документів: Навч. посіб. / Іванов В.Г., Карасюк В.В., Гвозденко М.В. –Х.: Нац. юрид. акад. України, 2001. – 113 с.

Правова інформатика: Підруч. / За ред. В. Дурдинця, Є. Мойсеєва та М. Швеця. – 2-ге вид., допов. та переробл. – К.: ПанТот, 2007. – 524 с.

Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2002. – 496 с.

Крылов В.В. Расследование преступлений в сфере информации. – М.: Городец, 1998. – 264 с.

Основи сучасної криптографії / Баби́чев С.Г., Гончаров В.В., Серов Р.Е. – М.: Гаряча Лінія-Телеком, 2001.

Криміналістична інформатика: Курс лекцій / Хахановський В.Г., Тебякін О.М., Поліщук Ю.В.; За заг. ред. В.Г. Хахановського. – К.: НАВСУ, 2002.

Інформатика: Базовый курс / Симонович С.В. и др. – СПб.: Питер. – 2007. – 428 с.

Правова інформатика: Підруч. – У 2-х т. / За ред. В.Я. Тація, Я.Ю. Кондратьєва, М.Я. Швеця. – К.: Парлам. вид-во, 2004. – Т. 1. – 416 с.

Основи Інтернет-технологій: Підруч. / Бредіхін В.М., Карасюк В.В., Карпухін О.В., Міщеряков Ю.В.; За ред. О.В. Карпухіна. – Х.: Компанія СМІТ, 2009. - 384 с.

Матеріали сайтів: <http://www.nau.kiev.ua>;
<http://www.liga.kiev.ua>.
<http://www.informjust.kiev.ua>;
<http://www.mijust.gov.ua>;
<http://www.rada.gov.ua/>.

ДОДАТКИ

ФРАГМЕНТИ НОРМАТИВНИХ ДОКУМЕНТІВ ЗА ТЕМАМИ

Додаток 1.

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

*(Із змінами та доповненнями станом
на 5 березня 2009 року)*

Розділ XVI

ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

1. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, —

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, —

караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися

певною діяльністю на строк до трьох років та з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи.

Примітка. Значною шкодою у статтях 361-363¹, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

(В ред. від 23.12.2004 р. // ВВР України. – 2005. – № 6. – Ст. 139)

Стаття 361¹. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, —

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, —

караються позбавленням волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, які є власністю винної особи.

(В ред. від 23.12.2004 р. // ВВР України. – 2005. – № 6. – Ст.139)

Стаття 361². Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. Несанкціоновані збут або розповсюдження інформації

з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, —

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, —

караються позбавленням волі на строк від двох до п'яти років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

(В ред. від 23.12.2004 р. // ВВР України. – 2005. – № 6. – Ст. 139)

Стаття 362. Несанкційовані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

1. Несанкціоновані зміна, знищення або блокування інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, —

карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років з конфіскацією програми або технічних засобів, за допомогою яких було вчинено несанкціоновані зміна, знищення або блокування інформації, які є власністю винної особи.

2. Несанкціоновані перехоплення або копіювання інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мере-

жах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені собою, яка має право доступу до такої інформації, —

карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи.

3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, —

карається позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програми або технічних засобів за допомогою яких було здійснено несанкціоновані дії з інформацією, які є власністю винної особи.

(В ред. від 23.12.2004 р. // ВВР України. – 2005. – № 6. – Ст. 139)

Стаття 363. Порухення правил експлуатації

Електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється Порухення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, —

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

(В ред. від 23.12.2004 р. // ВВР України. – 2005. – № 6. – Ст.139)

Стаття 363¹. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих си-

стем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, —

карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, —

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років та з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено масове розповсюдження повідомлень електрозв'язку, які є власністю винної особи.

(В ред. від 23.12.2004 р. // ВВР України. – 2005. – № 6–Ст. 139)

Д о д а т о к 2.

ЦИВІЛЬНИЙ КОДЕКС УКРАЇНИ

№435-IV, 16.01.2003, Кодекс України, Верховна Рада України

(Відомості Верховної Ради України (ВВР), 2003, №40-44, ст.356)

КНИГА ЧЕТВЕРТА

Право інтелектуальної власності

Г л а в а 35

ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Стаття 418. Поняття права інтелектуальної власності

1. Право інтелектуальної власності - це право особи на

результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності, визначений цим Кодексом та іншим законом.

2. Право інтелектуальної власності становлять особисті немайнові права інтелектуальної власності та (або) майнові права інтелектуальної власності, зміст яких щодо певних об'єктів права інтелектуальної власності визначається цим Кодексом та іншим законом.

3. Право інтелектуальної власності є непорушним. Ніхто не може бути позбавлений права інтелектуальної власності чи обмежений у його здійсненні, крім випадків, передбачених законом.

Стаття 419. Співвідношення права інтелектуальної власності та права власності

1. Право інтелектуальної власності та право власності на річ не залежать одне від одного.

2. Перехід права на об'єкт права інтелектуальної власності не означає переходу права власності на річ.

3. Перехід права власності на річ не означає переходу права на об'єкт права інтелектуальної власності.

Стаття 420. Об'єкти права інтелектуальної власності

1. До об'єктів права інтелектуальної власності, зокрема, належать:

- літературні та художні твори;
- комп'ютерні програми;
- компіляції даних (бази даних);
- виконання;
- фонограми, відеограми, передачі (програми) організацій мовлення;
- наукові відкриття;
- винаходи, корисні моделі, промислові зразки;
- компонування (топографії) інтегральних мікросхем;
- раціоналізаторські пропозиції;
- сорти рослин, породи тварин;
- комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення;
- комерційні таємниці.

**ПРАВО ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА
ЛІТЕРАТУРНИЙ, ХУДОЖНІЙ ТА ІНШИЙ ТВІР
(АВТОРСЬКЕ ПРАВО)**

Стаття 433. Об'єкти авторського права

1. Об'єктами авторського права є твори, а саме:
 - 2) комп'ютерні програми;
 - 3) компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;
 - 4) інші твори.
2. Твори є об'єктами авторського права без виконання будь-яких формальностей щодо них та незалежно від їх завершеності, призначення, цінності тощо, а також способу чи форми їх вираження.
3. Авторське право не поширюється на ідеї, процеси, методи діяльності або математичні концепції як такі.
4. Комп'ютерні програми охороняються як літературні твори.
5. Компіляції даних (бази даних) або іншого матеріалу охороняються як такі. Ця охорона не поширюється на дані або матеріал як такі та не зачіпає авторське право на дані або матеріал, що є складовими компіляції.

Д о д а т о к 3 .

ЗАКОН УКРАЇНИ
Про внесення змін до Закону України “Про авторське
право і суміжні права”

№2627-III, 11.07.2001, Закон, Верховна Рада України (*Ві-
домості Верховної Ради України (ВВР), 2001, №43, ст.214*)

Верховна Рада України **постановляє:**

Внести до Закону України “Про авторське право і суміжні права” (Відомості Верховної Ради України, 1994 р., № 13, ст. 64) зміни, виклавши його у такій редакції:

ЗАКОН УКРАЇНИ **Про авторське право і суміжні права**

Стаття 18. Авторське право на комп'ютерні програми

Комп'ютерні програми охороняються як літературні твори. Така охорона поширюється на комп'ютерні програми незалежно від способу чи форми їх вираження.

Стаття 24. Вільне копіювання, модифікація і декомпіляція комп'ютерних програм

1. Особа, яка правомірно володіє примірником комп'ютерної програми, має право без зр. и автора або іншої особи, яка має авторське право на цю програму:

1) внести до комп'ютерної програми зміни (модифікації) з метою забезпечення її функціонування на технічних засобах особи, яка використовує ці програми, і вчинення дій, пов'язаних з функціонуванням комп'ютерної програми відповідно до її призначення, зокрема запис і збереження в пам'яті комп'ютера, а також виправлення явних помилок, якщо інше не передбачено ур. ою з автором чи іншою особою, яка має авторське право;

2) виготовити одну копію комп'ютерної програми за умови, що ця копія призначена тільки для архівних цілей або для заміни правомірно придбаного примірника у випадках, якщо оригінал комп'ютерної програми буде втраченим, знищеним або стане непридатним для використання. При цьому копія комп'ютерної програми не може бути використана для інших цілей, ніж зазначено у цьому пункті та пункті 1 цієї частини, і має бути знищена у разі, якщо володіння примірником цієї комп'ютерної програми перестане бути правомірним;

3) декомпілювати комп'ютерну програму (перетворити її з об'єктного коду у вихідний текст) з метою одержання інформації, необхідної для досягнення її взаємодії із незалежно розробленою комп'ютерною програмою, за дотримання таких умов:

а) інформація, необхідна для досягнення здатності до взаємодії, раніше не була доступною цій особі з інших джерел;

б) зазначені дії здійснюються тільки щодо тих частин комп'ютерної програми, які необхідні для досягнення здатності до взаємодії;

в) інформація, одержана в результаті декомпіляції, може використовуватися лише для досягнення здатності до її взаємодії з іншими програмами, але не може передаватися іншим особам, крім випадків, якщо це необхідно для досягнення здатності до взаємодії з іншими програмами, а також не може використовуватися для розроблення комп'ютерної програми, схожої на декомпільовану комп'ютерну програму, або для вчинення будь-якої іншої дії, що порушує авторське право;

4) спостерігати, вивчати, досліджувати функціонування комп'ютерної програми з метою визначення ідей і принципів, що лежать в її основі, за умови, що це робиться в процесі виконання будь-якої дії із завантаження, показу, функціонування, передачі чи запису в пам'ять (збереження) комп'ютерної програми.

2. Застосування положень цієї ст. не повинно завдавати шкоди використанню комп'ютерної програми і не повинно обмежувати законні інтереси автора та (або) іншої особи, яка має авторське право на комп'ютерну програму.

Д о д а т о к 5 .

ЗАКОН УКРАЇНИ

Про Національну програму інформатизації

№74/98-ВР, 04.02.1998, Закон, Верховна Рада України
(Відомості Верховної Ради (ВВР), 1998, №27-28, ст.181)
(Із змінами, внесеними згідно із Законом
№2684-ІІІ від 13.09.2001, ВВР, 2002, №1, ст.3)

Цей Закон визначає загальні засади формування, виконання та коригування Національної програми інформатизації.

Р о з д і л І

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Основні терміни та поняття

У цьому Законі наведені нижче терміни та поняття вживаються у такому значенні:

база даних - іменована сукупність даних, що відображає

стан об'єктів та їх відношень у визначеній предметній області;

база знань - масив інформації у формі, придатній до логічної і смислової обробки відповідними програмними засобами;

геоінформаційні системи - сучасні комп'ютерні технології, що дають можливість поєднати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо);

засоби інформатизації - електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій;

інформатизація - сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

інформаційна послуга - дії суб'єктів щодо забезпечення споживачів інформаційними продуктами;

інформаційна технологія - цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

інформаційний продукт (продукція) - документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

інформаційний ресурс - сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

інформаційний суверенітет держави - здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави;

локалізація програмних продуктів - приведення програмних продуктів, які використовуються в Україні, у відповідність із законами України та іншими нормативно-правовими актами, стандартами, нормами і правилами, що діють в Україні;

нерезиденти - юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням за межами України, які створені й діють відповідно до законодавства іноземної держави, у тому числі юридичні особи та інші суб'єкти підприємницької діяльності, створені за участю юридичних і фізичних осіб;

окреме завдання - комплекс проектів інформатизації, взаємопов'язаних і взаємопор. жених за термінами реалізації, складом виконавців та спрямованих на досягнення конкретних цілей;

проект інформатизації - комплекс взаємопов'язаних заходів, як правило, інвестиційного характеру, що узгоджені за часом, використанням певних матеріально-технічних, інформаційних, людських, фінансових та інших ресурсів і мають на меті створення заздалегідь визначених інформаційних і телекомунікаційних систем, засобів інформатизації та інформаційних ресурсів, які відповідають певним технічним умовам і показникам якості;

резиденти - юридичні особи, суб'єкти підприємницької діяльності, що не мають статусу юридичної особи (філії, представництва тощо), з місцезнаходженням на території України, які здійснюють свою діяльність відповідно до законодавства України.

Д о д а т о к 6 .

ЗАКОН УКРАЇНИ

Про інформацію

№2657-XII, 02.10.1992, Закон, Верховна Рада України
(*Відомості Верховної Ради (ВВР), 1992, №48, ст.650*)

(*Вводиться в дію Постановою ВР*

№2658-XII від 02.10.92, ВВР, 1992, №48, ст.651)

Стаття 22. Правова інформація

Правова інформація - це сукупність документованих або

публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативні правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

З метою забезпечення доступу до законодавчих та інших нормативних актів всім громадянам держава забезпечує видання цих актів масовими тиражами у найкоротші строки після набрання ними чинності.

Д о д а т о к 7 .

ЗАКОН УКРАЇНИ

Про електронні документи та електронний документообіг

№851-IV, 22.05.2003, Закон, Верховна Рада України
(*Відомості Верховної Ради (ВВР), 2003, №36, ст.275*)
(*Із змінами, внесеними згідно із Законом*
№2599-IV від 31.05.2005, ВВР, 2005, №26, ст.349)

Цей Закон встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

Р о з д і л І

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:
адресат - фізична або юридична особа, якій адресується електронний документ;

дані - інформація, яка подана у формі, придатній для її оброблення електронними засобами;

посередник - фізична або юридична особа, яка в установ-

леному законодавством порядку здійснює приймання, передавання (доставку), зберігання, перевірку цілісності електронних документів для задоволення власних потреб або надає відповідні послуги за дорученням інших суб'єктів електронного документообігу;

обов'язковий реквізит електронного документа - обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;

автор електронного документа - фізична або юридична особа, яка створила електронний документ;

суб'єкти електронного документообігу - автор, підписувач, адресат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу.

Стаття 2. Сфера дії Закону

Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Стаття 3. Законодавство про електронні документи та електронний документообіг

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про телекомунікації", "Про обов'язковий примірник документів", "Про Національний архівний фонд та архівні установи", цим Законом, а також іншими нормативно-правовими актами.

(Частина перша ст. 3 із змінами, внесеними згідно із Законом №2599-IV від 31.05.2005)

Якщо міжнародним договором України, згода а на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.

Р о з д і л ІІ

ЕЛЕКТРОННИЙ ДОКУМЕНТ

Стаття 5. Електронний документ

Електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Стаття 6. Електронний підпис

Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом.

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Стаття 8. Правовий статус електронного документа та його копії

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;
2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди и, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

Р о з д і л І І І

ЗАСАДИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Стаття 12. **Перевірка цілісності електронного документа**

Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису.

Д о д а т о к 8 .

ЗАКОН УКРАЇНИ

Про електронний цифровий підпис

№852-IV, 22.05.2003, Закон, Верховна Рада України
(*Відомості Верховної Ради (ВВР), 2003, №36, ст.276*)

Цей Закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Дія цього Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

Якщо міжнародним договором, згода а на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються у такому значенні:

електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

сертифікат відкритого ключа (далі – сертифікат ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

посилений сертифікат відкритого ключа (далі – посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

акредитація – процедура документального засвідчення

компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

блокування сертифіката ключа – тимчасове зупинення чинності сертифіката ключа;

підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;

послуги електронного цифрового підпису – надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;

надійний засіб електронного цифрового підпису – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється у порядку, визначеному законодавством.

Стаття 2. Суб'єкти правових відносин у сфері послуг електронного цифрового підпису

Суб'єктами правових відносин у сфері послуг електронного цифрового підпису є:

підписувач;

користувач;

центр сертифікації ключів;

акредитований центр сертифікації ключів;

центральний засвідчувальний орган;

засвідчувальний центр органу виконавчої влади або ін-

шого державного органу (далі – засвідчувальний центр);
контролюючий орган.

Стаття 3. Правовий статус електронного цифрового підпису

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

Стаття 4. Призначення електронного цифрового підпису

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

Стаття 6. Вимоги до сертифіката ключа

Сертифікат ключа містить такі обов'язкові дані:

найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);

зазначення, що сертифікат виданий в Україні;
унікальний реєстраційний номер сертифіката ключа;
основні дані (реквізити) підписувача – власника особистого ключа;

дату і час початку та закінчення строку чинності сертифіката;

відкритий ключ;
найменування криптографічного алгоритму, що використовується власником особистого ключа;

інформацію про обмеження використання підпису.

Посилений сертифікат ключа, крім обов'язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника.

Д о д а т о к 9 .

ЗАКОН УКРАЇНИ

Про телекомунікації

№1280-IV, 18.11.2003, Закон, Верховна Рада України
(*Відомості Верховної Ради (ВВР), 2004, №12, ст.155*)

(*Із змінами, внесеними згідно із Законами*

№1876-IV від 24.06.2004, ВВР, 2004, №48, ст.526

№2119-IV від 21.10.2004, ВВР, 2005, №2, ст.34

№2285-IV від 23.12.2004, ВВР, 2005, №7-8, ст.162

№2505-IV від 25.03.2005, ВВР, 2005, №17, №18-19,
ст.267

№3200-IV від 15.12.2005, ВВР, 2006, №14, ст.116

№3317-IV від 12.01.2006, ВВР, 2006, №18, ст.155

№3375-IV від 19.01.2006, ВВР, 2006, №22, ст.186

№3380-IV від 19.01.2006, ВВР, 2006, №22, ст.188

№3475-IV від 23.02.2006, ВВР, 2006, №30, ст.258

№378-V від 28.11.2006, ВВР, 2007, №14, ст.167

№580-V від 11.01.2007, ВВР, 2007, №13, ст.132)

(Щодо визнання неконституційними окремих положень
див. Рішення Конституційного Суду №21-рп/2008 від 08.10.2008)

Цей Закон встановлює правову основу діяльності у сфері телекомунікацій.

Закон визначає повноваження держави щодо керування та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності або користуються телекомунікаційними послугами.

Г л а в а I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. **Визначення основних термінів**

1. У цьому Законі терміни вживаються в такому значенні:

абонент - споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі;

абонентна плата - фіксований платіж, який може встановлювати оператор телекомунікацій для абонента за доступ на постійній основі до своєї телекомунікаційної мережі незалежно від факту отримання послуг;

адреса мережі Інтернет - визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символний ідентифікатор доменних імен в ієрархічній системі доменних назв;

адресний простір мережі Інтернет - сукупність адрес мережі Інтернет;

безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ) - електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру;

взаємоз'єднання телекомунікаційних мереж - встановлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості

споживачам безпосередньо або опосередковано обмінюватись інформацією;

голосова телефонія - обмін інформацією голосом у реальному часі з використанням телекомунікаційних мереж;

дані - інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки;

домен - частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється;

домен.UA - домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі Інтернет;

домен другого рівня - частина адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у цій мережі;

електрозв'язок - див. "телекомунікації";

загальнодоступні (універсальні) телекомунікаційні послуги - мінімальний набір визначених цим Законом послуг нормованої якості, доступний усім споживачам на всій території України;

Інтернет - всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

інформаційна система загального доступу - сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних;

інформаційна безпека телекомунікаційних мереж - здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації;

інформація - відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

Стаття 34. Захист інформації про споживача

1. Оператори, провайдери телекомунікацій повинні забезпечувати і нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Стаття 39. Обов'язки операторів і провайдерів телекомунікацій

17) вживати заходів для недопущення несанкціонованого доступу до телекомунікаційних мереж та інформації, що передається цими мережами;

Д о д а т о к 1 0 .

ЗАКОН УКРАЇНИ

Про національну систему конфіденційного зв'язку

№2919-III, 10.01.2002, Закон, Верховна Рада України
(*Відомості Верховної Ради (ВВР), 2002, №15, ст.103*)

(*Із змінами, внесеними згідно із Законами*

№1280-IV від 18.11.2003, ВВР, 2004, №12, ст.155

№2599-IV від 31.05.2005)

Цей Закон регулює суспільні відносини, пов'язані із створенням, функціонуванням, розвитком та використанням Національної системи конфіденційного зв'язку.

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

спеціальна телекомунікаційна система (мережа) - телекомунікаційна система (мережа), призначена для обміну інформацією з обмеженим доступом;

(*Абзац другий частини першої ст. 1 із змінами, внесеними згідно із Законом №2599-IV від 31.05.2005*)

спеціальна телекомунікаційна система (мережа) подвійного призначення - спеціальна телекомунікаційна система (мережа), призначена для забезпечення телекомунікацій (електро-зв'язку) в інтересах органів державної влади та органів місцевого самоврядування, з використанням частини її ресурсу для надання послуг іншим споживачам;

(*Абзац третій частини першої ст. 1 із змінами, внесени-*

ми згідно із Законом №2599-IV від 31.05.2005)

Національна система конфіденційного зв'язку - сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/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 у разі введення надзвичайного і воєнного стану;

(Абзац четвертий частини першої ст. 1 із змінами, внесеними згідно із Законом №2599-IV від 31.05.2005)

суб'єкти Національної системи конфіденційного зв'язку - органи державної влади та органи місцевого самоврядування, юридичні та фізичні особи, що беруть участь у створенні, функціонуванні, розвитку та використанні цієї системи.

(Абзац шостий частини першої ст. 1 виключено на підставі Закону №2599-IV від 31.05.2005)

Терміни "оператор" та "мережа зв'язку" у цьому Законі вживаються відповідно у значенні термінів "оператор телекомунікацій" та "телекомунікаційна мережа", визначених у Законі України "Про телекомунікації".

(Частина друга ст. 1 в редакції Закону №2599-IV від 31.05.2005)

Д о д а т о к 11.

ЗАКОН УКРАЇНИ **Про захист інформації** **в інформаційно-телекомунікаційних системах**

(Відомості Верховної Ради України (ВВР), 1994, №31, ст.286)

{Вводиться в дію Постановою ВР №81/94-ВР від 05.07.94,

ВВР, 1994, №31, ст.287}

{ Із змінами, внесеними згідно із Законом
№1703-IV від 11.05.2004, ВВР, 2004, №32, ст.394 }

{ В редакції Закону
№2594-IV від 31.05.2005, ВВР, 2005, №26, ст.347 }

{ Із змінами, внесеними згідно із Законами
№879-VI від 15.01.2009, ВВР, 2009, №24, ст.296
№1180-VI від 19.03.2009, ВВР, 2009, №32-33, ст.485 }

Стаття 1. Визначення термінів

блокування інформації в системі - дії, внаслідок яких унеможливується доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що проводяться з порушенням порядку доступу до цієї інформації, встановленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її зміст;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигнала

лів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

власники інформації;

власники системи;

користувачі;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи. {Абзац п'ятий частини першої ст. 3 в редакції Закону №879-VI від 15.01.2009 }

На підставі укладеного договору або за дорученням власник інформації може надати право розпоряджатися інформацією іншій фізичній або юридичній особі - розпоряднику інформації.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Д о д а т о к 12.

ЗАКОН УКРАЇНИ

Про захист інформації в автоматизованих системах

(Відомості Верховної Ради (ВВР), 1994, №31, ст.286)

(Вводиться в дію Постановою ВР №81/94-ВР від 05.07.94,

ВВР, 1994, №31, ст.287)

(Із змінами, внесеними згідно із Законом

№1703-IV від 11.05.2004, ВВР, 2004, №32, ст.394)

Р о з д і л І

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. **Визначення термінів**

захист інформації - сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією;

несанкціонований доступ - доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу;

порушник - фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо АС та інформації в ній;

витік інформації - результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

втрата інформації - дія, внаслідок якої інформація в АС 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 повинна оброблятися або зберігатися в АС;

блокування інформації - дії, наслідком яких є припинення доступу до інформації;

порушення роботи АС - дії або обставини, які призводять до спотворення процесу обробки інформації.

Р о з д і л ІІІ

ЗАГАЛЬНІ ВИМОГИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ

Стаття 10. Забезпечення захисту інформації в АС

Захист інформації в АС забезпечується шляхом:

дотримання суб'єктами правових відносин норм, вимог та правил організаційного і технічного характеру щодо захисту оброблюваної інформації;

використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо захисту інформації (мають відповідний сертифікат);

перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому встановленим вимогам щодо захисту інформації (сертифікація засобів обчислювальної техніки, засобів зв'язку і АС);

здійснення контролю щодо захисту інформації.

Стаття 11. Встановлення вимог і правил щодо захисту та доступу до інформації

Вимоги і правила щодо захисту та доступу до інформації, яка є власністю держави, або інформації, захист якої гарантується державою, встановлюються державним органом, уповноваженим Президентом України. Ці вимоги і правила є обов'язковими для власників АС, де така інформація обробляється, і для інших суб'єктів права власності на інформацію. *(Стаття 11 із змінами, внесеними згідно із Законом №1703-IV від 11.05.2004)*

Р о з д і л VІ

МІЖНАРОДНА ДІЯЛЬНІСТЬ В ГАЛУЗІ ЗАХИСТУ ІНФОРМАЦІЇ В АС

Стаття 20. Забезпечення інформаційних прав України

Фізичні та юридичні особи в Україні на підставі Закону України "Про інформацію" можуть встановлювати взаємозв'язки

з АС інших держав з метою обробки, обміну, продажу, купівлі відкритої інформації. Такі взаємозв'язки повинні виключати можливість несанкціонованого доступу з боку інших держав або їх представників - резидентів України чи осіб без громадянства до інформації, що є в АС України, незалежно від форм власності і підпорядкування, стосовно якої встановлено вимоги нерозповсюдження її за межі України без спеціального дозволу.

Д о д а т о к 13.

КОНСТИТУЦІЯ УКРАЇНИ

Стаття 129. п. 7 . Судді при здійсненні правосуддя незалежні і підкоряються лише закону.

Судочинство провадиться суддею одноособово, колегією суддів чи судом присяжних.

Основними засадами судочинства є:

7) гласність судового процесу та його повне фіксування технічними засобами;

Д о д а т о к 14.

ЦИВІЛЬНИЙ ПРОЦЕСУАЛЬНИЙ КОДЕКС УКРАЇНИ

Стаття 6. Гласність та відкритість судового розгляду

10) Хід судового засідання фіксується технічними засобами. Порядок фіксування судового засідання технічними засобами встановлюється цим Кодексом.

11) Офіційним записом судового засідання є лише технічний запис, зроблений судом.) Наказ Державної Судової Адміністрації України від 24 вересня 2004 року № 161/04 «Про затвердження Інструкції про порядок фіксування судового процесу технічними засобами»)

Стаття 197. Фіксування судового засідання технічними засобами

1. Суд під час судового розгляду справи здійснює повне фіксування судового засідання за допомогою звукозаписувального технічного засобу.

2. Фіксування судового засідання технічним засобом здійс-

ное секретар судового засідання або за розпорядженням головуєчого інший працівник апарату суду.

3. Повне або часткове відтворення технічного запису судового засідання здійснюється на вимогу особи, яка бере участь у справі, або за ініціативою суду.

4. Носій інформації, на який здійснювався технічний запис судового засідання (касета, дискета тощо), є додатком до журналу судового засідання і після закінчення судового засідання приєднується до матеріалів справи.

5. За клопотанням особи, яка бере участь у справі, може бути за плату здійснено повне або часткове роздрукування технічного запису судового засідання за розпорядженням головуєчого. Особа, яка бере участь у справі, має право отримати копію інформації з носія, на який здійснювався технічний запис цивільного процесу.

6. Обсяг плати за роздрукування технічного запису судового засідання встановлюється Кабінетом Міністрів України.

Д о д а т о к 15.

КОДЕКС АДМІНІСТРАТИВНОГО СУДОЧИНСТВА УКРАЇНИ

Стаття. 41. Фіксування судового засідання технічними засобами

1. Суд під час судового розгляду адміністративної справи здійснює повне фіксування судового засідання за допомогою звукозаписувального технічного засобу.

2. Фіксування судового засідання технічним засобом здійснює секретар судового засідання або за розпорядженням головуєчого інший працівник апарату суду.

3. Носій інформації, на який здійснювався технічний запис судового засідання (касета, дискета, компакт-диск тощо), є додатком до журналу судового засідання і після закінчення судового засідання приєднується до матеріалів справи.

ЗАКОН УКРАЇНИ Про судоустрій в Україні

Стаття 9. Гласність судового процесу

п.4. При розгляді справ перебіг судового процесу фіксується технічними засобами в порядку, встановленому процесуальним законом.

Стаття 126. Повноваження державної судової адміністрації

п.14 організовує впровадження в судах комп'ютеризації для судочинства, діловодства та інформаційно-нормативного забезпечення судової діяльності; забезпечує суди необхідними технічними засобами фіксування судового процесу;

ГОСПОДАРСЬКИЙ ПРОЦЕСУАЛЬНИЙ КОДЕКС УКРАЇНИ

Стаття 4-4. Гласність розгляду справ

Розгляд справ у господарських судах відкритий, за винятком випадків, коли це суперечить вимогам щодо охорони державної, комерційної або банківської таємниці, або коли сторони чи одна з сторін обгрунтовано вимагають конфіденційного розгляду справи і подають відповідне клопотання до початку розгляду справи по суті.

Про розгляд справи у закритому засіданні або про відхилення клопотання з цього приводу виноситься ухвала.

Судовий процес фіксується технічними засобами та відображається у протоколі судового засідання у порядку, встановленому цим Кодексом.

Стаття 81-1. Протоколи

На вимогу хоча б одного учасника судового процесу у суді першої чи апеляційної інстанції при розгляді справи по суті або за ініціативою суду здійснюється фіксування судового про-

цесу з допомогою звукозаписувального технічного засобу.

Відтворення технічного запису судового процесу здійснюється в судовому засіданні при розгляді справи судом у першій інстанції, в апеляційному чи касаційному порядку, а також при розгляді зауважень на протокол судового засідання на вимогу сторін чи за ініціативою суду.

Питання про видачу копії технічного запису учаснику процесу, про його відтворення поза судовим засіданням вирішуються головуючим у кожному окремому випадку залежно від обставин.

Додаток 18.

ПОСТАНОВА КАБІНЕТУ МІНІСТРІВ УКРАЇНИ ВІД 14 СІЧНЯ

2009 р. № 14

Про затвердження Положення про Державну судову адміністрацію України

Стаття 4 ДСА відповідно до покладених на неї завдань:
28) організовує впровадження в судах комп'ютеризації для судочинства, діловодства та інформаційно-нормативного забезпечення судової діяльності; забезпечує суди необхідними технічними засобами фіксування судового процесу;

Додаток 19.

ЗАКОН УКРАЇНИ **Про бібліотеки і бібліотечну справу** **№ 32/95-ВР від 27.01.1995 із змінами**

(Відомості Верховної Ради України (ВВР), 1995, №7, ст.45)

{ Вводиться в дію Постановою ВР №33/95-ВР від 27.01.95, ВВР, 1995, №7, ст. 46 }

{ В редакції Закону №1561-III від 16.03.2000, ВВР, 2000, №23, ст.177 }

{ Із змінами, внесеними згідно із Законами №2120-III від

07.12.2000, ВВР, 2001, №2-3, ст.10 №2905-III від 20.12.2001, ВВР, 2002, №12-13, ст.92 №380-IV від 26.12.2002, ВВР, 2003, №10-11, ст.86 №594-IV від 06.03.2003, ВВР, 2003, №24, ст.159 №1344-IV від 27.11.2003, ВВР, 2004, №17-18, ст.250 №107-VI від 28.12.2007, ВВР, 2008, №5-6, №7-8, ст.78 - зміни діють по 31 грудня 2008 року }

{ Додатково див. Рішення Конституційного Суду №10-рп/2008 від 22.05.2008 }

{ Із змінами, внесеними згідно із Законом №1388-VI від 21.05.2009, ВВР, 2009, №39, ст.557 }

Цей Закон визначає статус бібліотек, правові та організаційні засади діяльності бібліотек і бібліотечної справи в Україні. Цей Закон гарантує право на вільний доступ до інформації, знань, залучення до цінностей національної та світової культури, науки та освіти, що зберігаються в бібліотеках. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» №537-V від 09.01.2007 року

Стаття 1. Визначення термінів

У цьому Законі нижченаведені терміни вживаються в такому значенні:

бібліотека - інформаційний, культурний, освітній заклад (установа, організація) або структурний підрозділ, що має упорядкований фонд документів, доступ до інших джерел інформації та головним завданням якого є забезпечення інформаційних, науково-дослідних, освітніх, культурних та інших потреб користувачів бібліотеки;

бібліотечні ресурси - упорядковані бібліотечні фонди документів на різних носіях інформації, бази даних, мережні інформаційні ресурси, довідково-пошуковий апарат, матеріально-технічні засоби опрацювання, зберігання та передачі інформації.

ЗАКОН УКРАЇНИ

Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки

№537-V від 09.01.2007 року

(Відомості Верховної Ради України (ВВР), 2007, №12, ст.102)

Верховна Рада України **п о с т а н о в л я є**:

1. Затвердити Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки, що додаються.

ОСНОВНІ ЗАСАДИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ НА 2007-2015 РОКИ

Україна має власну історію розвитку базових засад інформаційного суспільства: діяльність всесвітньо відомої школи кібернетики; формування на початку 90-х років минулого століття концепції та програми інформатизації; створення різноманітних інформаційно-комунікаційних технологій (далі - ІКТ) і загальнодержавних інформаційно-аналітичних систем різного рівня та призначення.

II. ЗАВДАННЯ, ЦІЛІ ТА НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ

Основним завданням розвитку інформаційного суспільства в Україні є сприяння кожній людині на засадах широкого використання сучасних ІКТ можливостей створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, повною мірою реалізуючи свій потенціал, підвищуючи якість свого життя і сприяючи сталому розвитку країни на основі цілей і принципів, проголошених Організацією Об'єднаних Націй, Декларації принципів та Плану дій, напрацьованих на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства (Женева, грудень 2003 року; Туніс, листопад 2005 року) та Постанови Верховної Ради України від 1 грудня 2005 року "Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні".

Основні засади є концептуальною основою для розробки

завдань щодо розвитку інформаційного суспільства в Україні.

Розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування визначається одним з пріоритетних напрямів державної політики.

Д о д а т о к 21.

ЗАТВЕРДЖЕНО

Наказ Державної судової
адміністрації України
03.12.2009 №129

Зареєстровано в Міністерстві
юстиції України
25 грудня 2009 р.
за №1247/17263

ПОЛОЖЕННЯ

ПРО АВТОМАТИЗОВАНУ СИСТЕМУ ДОКУМЕНТООБІГУ В АДМІНІСТРАТИВНИХ СУДАХ

1. Загальні положення

1.1. Положення про автоматизовану систему документообігу в адміністративних судах (далі - Положення), розроблене відповідно до **Кодексу адміністративного судочинства України**, Закону України "Про внесення змін до деяких законодавчих актів України щодо запровадження автоматизованої системи документообігу в адміністративних судах", визначає порядок функціонування автоматизованої системи документообігу в адміністративних судах. Дія Положення поширюється на місцеві загальні суди після запровадження в цих судах автоматизованої системи документообігу місцевих судів в частині здійснення правосуддя щодо адміністративних справ.

1.2. Автоматизована система документообігу в адміністративних судах (далі - Система) забезпечує автоматизацію процесів проходження процесуальних документів, загального діловодства і документообігу внутрішніх та зовнішніх документів,

здійснення процесуального контролю та контролю виконання документів, відстеження порядку проходження справ та документів, розподілу судових справ і матеріалів між суддями, формування звітності суду про стан здійснення правосуддя, передачу справ до електронного архіву тощо.

1.3. Порядок обігу інформації з обмеженим доступом, ведення діловодства за зверненнями громадян і діловодства з питань роботи з кадрами не є предметом регулювання цього Положення.

1.4. У цьому Положенні наведені нижче терміни вживаються у такому значенні:

держатель Системи - ДСА України, яка забезпечує здійснення матеріально-технічних та організаційно-методичних заходів функціонування Системи для адміністративних судів, окрім Вищого адміністративного суду України;

комп'ютерна програма - набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату. Комп'ютерна програма повинна забезпечити автоматизацію технологічних процесів обробки інформації, що надходить до суду:

реєстрацію та розподіл вхідної кореспонденції, реєстрацію вихідної кореспонденції та внутрішніх документів, зберігання графічних (відсканованих) копій зареєстрованих документів;

постановку на контроль та здійснення контролю виконання вхідних та внутрішніх документів, автоматичне інформування голови, керівника апарату суду та особи, відповідальної за опрацювання документа, про проблеми, пов'язані зі строками виконання документів;

фіксування порядку проходження документів з моменту їх надходження, створення, опрацювання тощо до передачі в електронний архів; автоматичну передачу виконавцям та за інстанціями залежно від поточного стану справи/документа;

автоматичне проходження по технологічній лінії виконання залежно від типу справи/документа, що виконується;

реєстрацію процесуальних дій та документів у справі з автоматичною зміною стану справи, якщо це передбачено зареє-

строваною дією та/або документом;

контроль за дотриманням процесуальних строків при розгляді судової справи та автоматичне інформування головуючого у справі суддю, суддю-доповідача, голову суду та заступника голови (голову судової палати) про наявні та потенційні проблеми дотримання процесуальних строків;

використання електронного цифрового підпису (ЕЦП) для засвідчення документа, що отримує офіційний статус;

оперативний пошук справ та документів за реквізитами;

індексацію документів та контекстний пошук за текстами документів;

видачу судових рішень (копій) та формування виконавчих листів на підставі наявних у Системі даних;

зберігання текстів судових рішень та інших документів, створених у Системі;

відправку електронних копій судових рішень до Єдиного державного реєстру судових рішень;

надання особам інформації про стан розгляду справ щодо них;

формування звітності суду про стан здійснення судочинства тощо;

користувач Системи - суддя, працівник апарату суду, якому відповідно до функціональних обов'язків на підставі наказу голови суду надано доступ до Системи або її окремих підсистем;

підсистема - логічно виділений за певними ознаками модуль Системи для вирішення конкретних завдань Системи, що встановлюється на кожному робочому місці залежно від функцій, повноважень та напрямів роботи користувача Системи;

Система - сукупність територіально розподілених, функціонально пов'язаних програмно-апаратних комплексів та технологічно об'єднаних підсистем, яка за допомогою використання відповідної комп'ютерної програми забезпечує реєстрацію вхідної інформації, її накопичення, зберігання, належне використання, захист на технологічних ланках від несанкціонованого доступу, формування вихідної інформації, взаємодію з користувачами тощо.

ЗМІСТ

ПЕРЕДМОВА.....	4
Глава 1. ПРАВОВА ІНФОРМАЦІЯ ТА ПРАВОВА ІНФОРМАТИКА.....	7
1.1. Інтеграція права й інформатики.....	7
1.2. Правова інформатика.....	8
1.3. Поняття правової інформації.....	9
1.4. Моделі та комп'ютерні технології в юридичній діяльності.....	11
1.5. Національна програма правової освіти населення....	14
1.6. Інформаційні системи державно-правового характеру.....	16
Контрольні питання	19
Глава 2. КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ У ПІДГОТОВЦІ ЮРИДИЧНИХ ДОКУМЕНТІВ.....	20
2.1. Сучасні підходи до автоматизації документообігу...	20
2.2. Огляд сучасних систем електронного документообігу	24
2.3. Характеристика пакета Microsoft Office.....	29
2.4. Склад пакета Microsoft Office, стисла характеристика основних додатків.....	33
Контрольні питання	40
Глава 3. ЗАСТОСУВАННЯ ПРОГРАМ ПАКЕТА MS OFFICE.....	41
3.1 Основні функціональні можливості текстового процесора MS Word при створенні юридичних документів.....	41
3.2. Робота з файлами інших форматів, що можуть містити текст.....	49
3.3. Використання можливостей Excel для статистичної обробки правових даних та побудова діаграм.....	54
3.2.1. Введення та редагування даних.....	56
3.2.2. Сортування й фільтрування даних.....	57
3.2.3. Виконання обчислень в Excel.....	58
3.2.4. Робота з майстром функцій.....	61

3.2.5. Майстер діаграм. Види діаграм та основні етапи їх побудови.....	62
3.4. Сумісне використання Word та Excel. Упровадження і зв'язування об'єктів між докумен- тами різних типів.....	64
Контрольні питання	66
Глава 4. ОСНОВИ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ.....	67
4.1. Загальне уявлення про інформаційну безпеку.....	67
4.1.1. Кримінальна відповідальність.....	67
4.1.2. Технологічні, організаційні, правові постулати захисту даних.....	68
4.2. Види загроз для комп'ютерної інформації.....	70
4.3. Засоби протидії загрозам для комп'ютерної інформації.....	77
4.4. Поняття про комп'ютерні злочини. Визначення, аналіз та фіксація слідів комп'ютерних злочинів.....	85
Контрольні питання	88
Глава 5. ТЕХНІЧНЕ ТА ЮРИДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОННОГО ПІДПISУ.....	89
5.1. Електронний бізнес та електронна комерція.....	89
5.2. Закон України “Про електронні документи та електронний документообіг”.....	90
5.3. Поняття про електронний цифровий підпис.....	93
5.4. Симетричні й несиметричні методи шифрування.....	96
5.5. Поняття про дайджест повідомлення.....	100
5.6. Поняття про криптостійкість засобів електронного цифрового підпису.....	102
5.7. Технічне та юридичне забезпечення електронного цифрового підпису.....	103
Контрольні питання	105
Глава 6. ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАКОНОТВОРЧОЇ ТА ПРАВОЗАСТОСОВНОЇ ДІЯЛЬНОСТІ....	106
6.1. Комп'ютерна мережа Верховної Ради України.....	107

6.2. Призначення та основні принципи побудови інтегрованої системи інформаційно-аналітичного забезпечення (СІАЗ) законотворчої діяльності Верховної Ради України.....	107
6.3. Загальноправові бази даних.....	111
6.4. Автоматизована інформаційно-пошукова система “Нормативні акти України”.....	112
6.4.1. ДПС як інструмент отримання інформації.....	112
6.4.2. Особливості АІПС “Нормативні акти України”	113
6.4.3. Функціональні можливості ІПС.	116
6.4.4. Робота зі знайденою інформацією.....	118
6.4.5. Створення власної бази.	118
6.4.6. Елементи інтелектуального пошуку: підсистема “Експерт”.....	118
6.5. Всесвітня електронна мережа правових документів	119
Контрольні питання	120
Глава 7. КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ У ЮРИДИЧНІЙ ДІЯЛЬНОСТІ.....	121
7.1. Комп’ютерні технології фіксування судового процесу	121
7.2. Основні програми фіксування судового процесу	124
7.3. Правові засади фіксування судового процесу технічними засобами.....	126
7.4. Електронне (віртуальне) судочинство.....	130
7.5. Комп’ютерні технології забезпечення розгляду судових справ.....	135
7.6. Відеоконференцз’язок у судовій системі	145
7.7. Голосові портали в судовій діяльності	147
7.8. Реєстр судових рішень.....	149
7.9. Єдиний державний реєстр виконавчих проваджень..	150
7.10. Нотаріальні реєстри.....	153
7.11. Автоматизована система ведення Державного земельного кадастру.....	155
7.12. Інформаційно-аналітичні системи криміналістичних обліків.....	156

7.13. Системи “Фоторобот і портретна ідентифікація”, “АР” (автоматичні пістолети).....	158
7.14. Автоматизація судово-експертних досліджень. Система “Автоекс”.....	159
7.15. Експертиза фонограм усного мовлення, дактилоскопічна експертиза, ідентифікація почерку оператора ЕОМ.....	161
Контрольні питання	162
Глава 8. МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ.....	164
8.1. Поняття про глобальну комп’ютерну мережу Інтернет.....	164
8.2. Технологічні та соціальні аспекти Інтернету.....	165
8.3. Правова характеристика базових понять.....	168
8.4. Пошук інформації у мережі.....	169
8.5. Основні пошукові портали.....	170
8.6. Новітні пошукові технології.....	172
8.7. Автоматизований бібліотечний комплекс Академії.....	172
8.8. Локальні комп’ютерні мережі юридичних установ та організацій. Інформаційні сервіси в локальній мережі Національної юридичної академії України.....	174
Контрольні питання	175
СЛОВНИК ТЕРМІНІВ.....	177
СПИСОК ЛІТЕРАТУРИ.....	195
ДОДАТКИ.....	197

Навчальне видання

ПРАВОВА ІНФОРМАЦІЯ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Навчальний посібник

*За загальною редакцією
професора В.Г. Іванова*

Автори: ІВАНОВ Володимир Георгійович,
ІВАНОВ Станіслав Миколайович,
КАРАСЮК Володимир Васильович,
КОМАРОВ Вячеслав Васильович,
КОШЕВА Наталія Анатоліївна,
ЛОМОНОСОВ Юрій В'ячеславович,
ЛЮБАРСЬКИЙ Михайло Григорович,
ГВОЗДЕНКО Марина Владиславівна,
МАЗНИЧЕНКО Наталя Іванівна

Відповідальний за випуск *В.Г. Іванов*

Редактор *О.І. Борисенко*

Коректор *Л.М. Рибалко*

Комп'ютерна верстка *Л.П.Лавриненко*

Підписано до друку 05.08.2010. Формат 60×84 ¹/₁₆. Папір офсетний.
Гарнітура Times. Умови, друк. арк. 11,5. Об'єм літ.-вид. арк. 5,6.
Вид. № 525. Тираж 500 прим.

Видавництво «Право» Національної академії правових наук України
Україна, 61002, Харків, вул. Чернишевська, 80

Свідectво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників і розповсюджувачів
видавничої продукції — серія ДК № 559 від 09.08.2001 р.

Надруковано в друкарні СПДФО Білетченко
тел. 8(057) 758-35-98