НУ “ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ”
КИЇВСЬКИЙ ІНСТИТУТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ПРАВА
Кафедра менеджменту та інформаційних технологій

Тупкало В.М., Заплотинський Б.А., Авєрічєв І.М.

ВИКОРИСТАННЯ ІНФОКОМУНІКАЦІЙИХ ТЕХНОЛОГІЙ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Навчальний посібник

Київ – 2020

УДК 378.147 : 004.34.08

Тупкало В.М., Заплотинський Б.А., Авєрічєв І.М. Використання інфокомунікаційних технологій в юридичній діяльності. Навч. посібник. Київський інститут інтелектуальної власності та права НУ “Одеська юридична академія”. К.: 2020. 164 с.

Матеріал підготовлений на основі робочих програм навчальних дисциплін “ІТ в юридичній діяльності”, “Електронне судочинство” та “Використання ІТ в судах” для студентів КІІВтаП, які навчаються за спеціальністю “081 право”. Головна увага приділена розкриттю основних понять та суті тем в стислій і доступній для сприйняття формі.

Може бути корисним для аспірантів і спеціалістів правової сфери.

Електронний ресурс. URL: http://dspace.onua.edu.ua/handle/11300/11090

Автори:

Тупкало Віталій Миколайович, д.т.н., проф., зав. кафедри МтаІТ

Заплотинський Борис Андрійович, к.т.н, доц., доцент кафедри МтаІТ

Авєрічєв Ігор Миколайович, к.е.н., доц., доцент кафедри МтаІТ

Рецензенти:

проректор з наукової роботи Державної екологічної академії післядипломної освіти та управління Мінприроди України, д.т.н., проф. Машков О.А.

професор кафедри інтелектуальної власності та права КІІВтаП, д.ю.н., проф. Шишка Р.Б.

Затверджено на засіданні кафедри МтаІТ КІІВтаП НУ “ОЮА” протокол № 9 від 30.06.2020

Розроблено на кафедрі МтаІТ КІІВіП НУ “ОЮА”, обсяг 6,83 др. арк.
02121, м. Київ, вул. Харківське шосе, 210, тел. (044) 563-80-64

ЗМІСТ

ВСТУП

Будь-яка діяльність характеризується наявністю двох складових – змісту та форми. Не є винятком і юридична сфера діяльності.

До змісту юридичної діяльності входять суб'єкти, учасники, об'єкти, юридичні дії та операції, засоби і способи їх здійснення, результати юридичних дій.

Форма юридичної діяльності може бути представлена у виді двох груп – *внутрішньої* (визначає порядок організації діяльності, яка базується на послідовності юридичних дій, процесів і процедур) *і зовнішньої* (характеризує засоби зовнішнього прояву юридичної діяльності у вигляді процесуальних документів, певних дій і усних висловлювань учасників процесу).

На підставі відомостей, наведених у нормативно-правових актах, фахових літературних джерелах і матеріалах проведених досліджень, сформулюємо визначення діяльності юриста.

Діяльність юриста – це нормативно врегульована сукупність процесуальних дій, спрямованих на одержання правової інформації стосовно певної юридичної ситуації шляхом здійснення комплексу інформаційно-правових, інформаційно-пошукових, інформаційно-комунікативних та інформаційно-аналітичних заходів з метою об'єктивного неупередженого розгляду справи, встановлення істини та документального оформлення прийнятих процесуальних рішень у вигляді, придатному для розгляду справи у суді.

Тепер дещо детальніше про судову діяльність, яка за суттю є різновидом юридичної діяльності. Їй притаманні ознаки як правоохоронної, так і правозахисної діяльності. Головним завданням у системі судової діяльності є правосуддя, що об'єднує конституційну юрисдикцію і судочинство судів загальної та спеціальної юрисдикції (як кримінальне, так і цивільне). Судам належить центральне місце у системі правового захисту конституційних та інших правових цінностей.

Демократичні перетворення в суспільстві і державі неможливі без ефективної судової діяльності. Саме вона є невід'ємним атрибутом правової держави. Через правосуддя та конституційну юрисдикцію громадяни мають можливість відстоювати свої права, причому в судах загальної та спеціальної юрисдикції – безпосередньо, а в порядку конституційного судочинства – як безпосередньо, так і за допомогою обраних ними народних депутатів.

Так, Конституційний Суд повинен гарантувати верховенство Конституції як основного закону держави. У сфері господарських відносин господарським судом захищаються права та законні інтереси учасників цих відносин, вдосконалюються законність та правове регулювання господарської діяльності. Місцеві суди як суди загального судочинства розглядають справи з усіх правовідносин (крім вищезазначених), що потребує високого професійного рівня, вміння об'єктивно й неупереджено вирішувати долю обвинуваченого або спору між позивачем і відповідачем.

Судовій діяльності притаманні такі ознаки державної влади, як юрисдикційність, публічність і субординаційність. Юрисдикційність судової діяльності полягає у сукупності правомочностей суб'єктів цієї діяльності з розгляду та вирішення спірних питань із захисту, відновлення або припинення порушеного права. Відповідно до Конституції України (ст. 124) правосуддя в Україні здійснюють виключно суди.

Публічність судової діяльності сприяє політичній або партійній незаангажованості судів та суддів. Суд виступає як державна установа, яка самостійно організує розгляд судових справ, ініціює виконання судових рішень, організує своє діловодство, а також аналізує судову статистику та узагальнює судову практику.

Субординаційність судової діяльності полягає в тому, що суди утворюють єдину систему із трьох судових інстанцій – судів першої інстанції, судів апеляційної та касаційної інстанцій.

Таким чином, судова діяльність полягає у розгляді та вирішенні спірних питань із захисту права шляхом розгляду судових справ, аналізу судової статистики та узагальнення судової практики, а також у наданні правової допомоги відповідно до міжнародних договорів.

На всіх етапах сучасної юридичної (в т.ч. судової) діяльності вирішувати питання активно допомогають інфокомунікаційні технології (ІКТ).

Пояснимо більш детально зв'язок діяльності працівників юридичної сфери (далі – просто працівників) із засобами ІКТ.

1. Робота працівника на будь-якій посаді пов'язана зі створенням, обробкою і зберіганням маси текстових документів, як-то: договори, позови, протоколи, висновки, рішення та різні додатки до них. ПК дозволяє не тільки виконати цю роботу, але в будь-який момент надрукувати документ на папері, зробити необхідні вилучення, скопіювати документ на електронний носій, передати його абоненту на електронному носії або за допомогою електронної пошти.

2. Значна частина правових документів для ефективної роботи вимагає особливої форми подання. Мова йдеться про таблиці, як основну структуру для зберігання інформації, і про спеціальні програми (наприклад, Системи управління базами даних, які дозволяють створювати інформаційні бази даних, виконувати необхідні запити і отримувати відповіді на них в зручній формі). До документів такого роду відносяться всілякі картотеки з описом справ, бібліографії, а також книги, реєстри та інші документи подібного роду.

3. З переходом до інформаційного суспільства працівників захлеснув потік актів і документів, впоратися з якими без допомоги комп'ютера важко. Це викликало цілий напрям в комп'ютерних технологіях – розробку довідково-правових, пошукових та інформаційних комп'ютерних систем, які допомагають прийняти ефективне управлінське рішення.

4. Комп'ютер – це не тільки робочий стіл працівника, а й образно кажучи офіс, який не вимагає додаткових площ, спеціальних меблів для зберігання нормативних актів, архівів, ділових папок, бюлетенів, газет і журналів. Комп'ютер значно прискорює спілкування з іншими організаціями та клієнтами без витрат на відрядження та транспортні послуги, так як може бути потужним засобом зв'язку.

5. В Україні до традиційних напрямів правової орієнтації (нерухомість, банки, фінанси та ін.) з року в рік додаються нові (наприклад, спеціалізація юристів у фармацевтиці, нафтогазовому комплексі, телекомунікаціях, агробізнесі, енергетиці, транспорті та логістиці). В цьому разі виникає необхідність готувати не просто юриста-фахівця загальної нормативної законодавчої бази, а *бізнес-юриста*, який має знання в господарських і управлінських бізнес-процесах суб'єктів підприємницької діяльності (тобто, в предметній сфері).

На базі вищенаведеного матеріалу можна сформулювати предмет і мету дисципліни "Використання ІКТ в юридичній діяльності", а також вимоги до комп'ютерно-інформаційних компетенцій випускників вищого юридичного навчального закладу.

Предметом вивчення навчальної дисципліни є інформаційні технології, які застосовуються в юридичній діяльності, а також в суміжних сферах (перш за все в судовій).

Метою викладання навчальної дисципліни є формування у майбутніх правознавців здібностей щодо ефективного використання сучасних інформаційних технологій при рішенні професійних завдань.

Студент, який пройшов підготовку з дисципліни ВІТвЮД, *повинен знати*:

 нормативну базу використання інформаційних технологій в юридичній діяльності (в органах юстиції, державної влади та управління, в судах);

 основні терміни та означення, які використовуються в ІКТ;

 принципи побудови та функціонування, характеристики персональних комп'ютерів, комп'ютерних мереж, баз даних та інформаційних систем, які діють в зазначених сферах діяльності;

 можливості сучасних інформаційних технологій для підготовки службової та процесуальної документації, виконання статистичних розрахунків;

 основні правила безпеки та експлуатації персональних комп'ютерів;

 технології роботи з програмними продуктами MS Word та Excel;

 призначення, склад та основні можливості стосовно інформаційно-пошукової системи "ЛІГА:ЗАКОН Юрист", а також "1С: Управління невеликою фірмою";

 проблеми впровадження електронного судочинства та електронного урядування у вітчизняну практику.

Студент, який пройшов підготовку з дисципліни ІТвЮД, *повинен вміти*:

 використовувати можливості сучасних офісних пакетів для підготовки службової й процесуальної документації;

 аналізувати правові та господарчо-правові питання за допомогою табличного процесору Excel;

 організувати робоче місце та діяльність у відповідності з вимогами сучасного діловодства;

 користуватися різними режимами пошуку документів в ІПС "ЛІГА: ЗАКОН Юрист" та "1С: Управління невеликою фірмою" ;

 упорядковувати створені списки документів та передавати знайдені документи або їх окремі фрагменти у текстовий процесор MS Word;

 створювати на базі знайденого матеріалу власні документи;

 здійснювати предметно-орієнтований пошук інформації в мережі Інтернет та упорядковувати його результати;

 сприяти вдосконаленню електронного судочинства та електронного урядування.

Незважаючи на доволі великий список окремих публікацій на обрану тему, за останні 10 років відсутня вітчизняна література, в якій усі представлені в посібнику розділи були б систематизовані і представлені в зручному для користування вигляді. При підготовці видання автори в певній мірі намагалися зменшити цей недолік.

Структурно матеріал представлений двома частинами:

- термінологічні поняття стосовно суті ІКТ при обробці інформації;
- основні поняття щодо електронного судочинства в світі та в Україні, а також суть електронного урядування та проблеми його впровадження в Україні.

До посібника надаються кілька додатків за темами: Принцип побудови та роботи комп'ютера; Електронний підпис; Основні відомості з організації відеоконференцзв'язку; Закон України про кіберполіцію та ін.

Опис дисципліни з орієнтовним розподілом годин наведений в табл. В1. Форма контролю знань – залік.

Таблиця В1

Форма навчання	Курс	Лекції	Практ. та сем. зан.	Всього ауд. годин	Курсові роботи	Контрольні роботи	Самостійна робота	Всього годин
Денна	2	20	20	40	–	–	50	90
Заочна	3	8	2	10	–	–	80	

Ч1. ОСНОВНІ ПОНЯТТЯ З ІНФОКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

РОЗДІЛ 1. ЗАГАЛЬНІ ВІДОМОСТІ З ІКТ

1.1. Основні термінологічні поняття

На сьогодні комп'ютер та інформаційні технології є не лише предметом вивчення цілої низки навчальних дисциплін, а й засобом здійснення навчальної, наукової і професійної діяльності працівника, який виконує свої професійні обов'язки в умовах інформаційного суспільства. В такому суспільстві інформація й технології її опрацювання перетворюються на стратегічний ресурс.

Збільшення обсягів інформації і попиту на неї обумовили появу галузі, пов'язаної з автоматизацією обробки інформації – інформатики, яка здатна значною мірою покращити ситуацію.

Інформатика – це наука про методи та засоби отримання, обробки, зберігання, передавання, подання інформації. Основне завдання інформатики полягає у визначенні загальних закономірностей, відповідно до яких відбувається створення інформації, її опрацювання, передавання повідомлень і використання інформації в різних сферах діяльності людини.

Інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів.

На основі терміну " інформаційні технології " сьогодні виникли ще два нових терміни – *інформаційне суспільство* та *інфокомунікаційні технології (послуги)*.

Згідно з визначенням, поданим 1993 року Комісією ЄС, *інформаційне суспільство – це суспільство, в якому діяльність людей здійснюється на основі використання інформаційних технологій та новітніх технологій зв'язку*.

Доступ до інформаційних ресурсів глобальної інформаційної структури реалізується за допомогою послуг зв'язку нового типу (пакетні мережі NGN), які отримали назву *інфокомунікаційних технологій (або послуг)*. Із-за складності своєї суті послуги NGN важко розділити на послуги інформаційні та послуги зв'язку, що й призвело до виникнення єдиного поняття "*інфокомунікаційні технології*". *Інфокомунікаційні технології (ІКТ) – це сукупність засобів зв'язку, що передбачають автоматизовану обробку,*

зберігання або надання відповідей на запити інформації на основі обчислювальної техніки й телекомунікаційного обладнання.

Сьогодні *інформаційний ресурс* (*організована сукупність документованої інформації, відомостей, даних і знань, яка призначена для задоволення інформаційних потреб споживача*) розглядається як одне з основних багатств кожної держави, стратегічний ресурс, цінність якого постійно зростає. Політика владних органів нашої держави в галузі інформаційної індустрії втілилася в низці важливих документів, серед яких насамперед слід назвати Закон України від 04.02.98 за №74/98-ВР "Про національну програму інформатизації", Указ Президента від 14.07.2000 за №887/2000 "Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади", Указ Президента України від 20.10.2005 № 1497/2005 "Про першочергові завдання щодо впровадження новітніх інформаційних технологій", Державна програма "Інформаційні та комунікаційні технології в освіті і науці" на 2006-2010 роки від 7.12.2005 р. № 1153 та ін.

1.2. Поняття інформації, її види і властивості

Інформація – це відомості про навколишній світ (об'єкти, явища, події, процеси тощо), які зменшують існуючу невизначеність, неповноту знань. Ці відомості можна передавати усним, письмовим або іншим способом, а також за допомогою умовних сигналів, технічних та обчислювальних засобів.

Сучасна інформація про певний об'єкт виникає тоді, коли відбувається інтерпретація даних, отриманих у вигляді повідомлення про стан об'єкту.

Дані – це сукупність кодів в пам'яті комп'ютера, що у формалізованому вигляді описують певний об'єкт.

Певним чином упорядкована сукупність даних утворює повідомлення. Наприклад, певна сукупність даних (паспортні дані) ідентифікує громадянина як фізичну особу, сукупність значень тиску, температури, об'єму і маси однозначно визначає фізичний стан тіла громадянина і т.д.

Дані, передані суб'єкту або так званій інформаційній системі, утворюють повідомлення, результатом інтерпретації якого є інформація.

Процес інтерпретації даних (сигналів, повідомлення в цілому) полягає в перетворенні повідомлення у форму, яка забезпечує виконання певних дій. Наприклад, повідомлення експерта щодо визначення групи крові, знайденої на речовому доказі, разом з даними щодо групи крові учасників певного конфлікту, може бути інтерпретоване як інформація, яка забезпечить уточнення перебігу подій. Інтерпретація штурманом повідомлення з даними

щодо курсу і швидкості судна (разом з іншими даними) дасть йому інформацію про правильність або хибність режиму руху, дозволить сформулювати команди для управління судном.

Інформація дуже різноманітна за змістом і поділяється за видами людської діяльності, що забезпечується нею: наукова, виробнича, управлінська (соціально-економічна), медична, екологічна, правова тощо.

Коли ведуть мову про інформацію, то мають на увазі її *властивості:*

 інформація достовірна, якщо вона не спотворює істинного стану явищ, процесів, фактів, подій;

 інформація повна, якщо її достатньо для розуміння і прийняття обґрунтованих рішень;

 інформація чітка й зрозуміла, якщо вона виражена мовою, якою спілкуються (яку розуміють) ті, для кого вона призначена;

 якість інформації – сукупність властивостей, що зумовлюють можливості її використання для задоволення визначених згідно з її призначенням потреб;

 цінність – комплексний показник якості інформації, її міри на прагматичному рівні, яка визначає її корисність для прийняття певного рішення;

 адекватність інформації – це певний рівень відповідності отриманої інформації образу реального об’єкта, процесу, явища.

Одним із найважливіших різновидів інформації є правова інформація. Відповідно до ст.22. Закону України “Про інформацію” *правова інформація – це сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення, боротьбу з ними та їх профілактику* тощо.

З інформацією (більш точно – з даними) виконують багато операцій, що за ознакою подібності об’єднуються в технологічний процес обробки інформації, а саме: *збір і реєстрація* даних; *передача* даних; *збереження* даних; *обробка* (наприклад, *математичні дії, коригування тексту або графіки, зміна формату*) даних; *отримання результативної інформації*.

Обробка інформації виконується відповідно до розробленого *алгоритму – набору чітко сформульованих правил, що визначають процес перетворення вхідної інформації у бажаний результат* (вихідну інформацію) *за скінченну кількість кроків*. Це дозволяє автоматично вирішувати будь-яку конкретну задачу з класу однотипних задач.

У процесі обробки інформації формуються результативні показники, що відображаються в поточних звітах і регламентованій звітності.

1.3. Форми подання інформації

Інформація може містити повідомлення, які передаються у двох формах – *аналоговій* і *дискретній*.

Аналогова, або безперервна форма подання повідомлення – це значення певної фізичної величини, що характеризує процес, який не має перерв або проміжків (наприклад, температура тіла людини).

Дискретна форма подання повідомлення – це послідовність символів, яка характеризує переривчастий ланцюг подій (наприклад, кількість працівників установи в різні періоди).

Всі різновиди довколишньої інформації можна згрупувати за такими ознаками:

- *інформація щодо процесів і явищ неживої природи* (елементарна або механічна), тваринного й рослинного світу (біологічна), людського суспільства (соціальна).

- *інформація за способом передачі і сприйняття*: інформація, передана видимими способами і символами – візуальна, звуками – аудіальна, відчуттями – тактильна, запахами і смаками – органолептична, інформація, що видається і сприймається засобами комп'ютерної техніки, – комп'ютерна.

Багатоплановість джерел і споживачів інформації призвела до існування різних *форм її подання – символьної, текстової, графічної*.

Символьна форма, заснована на використанні символів – літер, цифр, знаків тощо, є найбільш простою, але вона практично застосовується тільки для передачі нескладних сигналів про різні події. Прикладом можуть бути дорожні знаки.

Більш складною є *текстова форма* подання інформації. Тут так само, як і в попередній формі, використовуються символи – літери, цифри, математичні знаки, однак інформація закладена не тільки в цих символах, але й у їхньому сполученні, порядку проходження. Так, слова *краб* і *брак* мають однакові літери, але мають різні значення. Завдяки використанню природної мови текстові повідомлення надзвичайно зручні і широко використовуються в діяльності людини (книги, брошури, журнали, аудіозаписи і т.д).

Найбільш ємною і складною є *графічна форма* подання інформації. До цієї форми відносяться фотографії, схеми, креслення, малюнки, що мають велике значення в діяльності людини.

Властивості інформації можна розглядати в трьох аспектах: *у технічному* – це точність, надійність, швидкість передачі сигналів; *семантичному* – передача змісту тексту за допомогою кодів, *прагматичному* – наскільки ефективно інформація впливає на процеси управління об'єктами.

Величезну, незамінну роль виконує інформація в управлінській діяльності. По суті, без інформації не може бути і мови про будь-який вид управління, про цілеспрямовану діяльність взаємозалежних об'єктів і систем.

У наш час різноманітна за своїм значенням інформація, зафіксована на спеціальних носіях, стала національним багатством нового типу – *інформаційним ресурсом держави*. Будучи предметом купівлі-продажу за всіх часів, інформація має свої специфічні особливості: при обміні інформацією її кількість збільшується. Американці кажуть: "Якщо у вас є по яблуку і ви обмінюєтеся ними, у вас знову буде по яблуку, але якщо у вас є по ідеї і ми обмінюємося, то в кожного їх буде по дві". Спілкування людей, інформування один одного призводить до їхнього зближення, підвищення інтелектуального потенціалу, взаємозбагачення.

У визначенні практичної цінності інформації немає будь-яких точних кількісних параметрів. Та й визначити їх нелегко, оскільки цінність залежить від корисності інформації для множини конкретних людей.

Часто інформацію оцінюють за оптимальністю її змісту. *Оптимальний* – означає найкращий у визначеному сенсі. Наприклад, за часом – найшвидший процес, за витратою енергії – найбільш економна система, а за продуктивною дією – найбільш дохідна. Оптимальних у всіх смислах об'єктів і процесів не буває. Це пояснюється суперечливістю умов досягнення оптимальності. Найкращі в одному сенсі властивості звичайно досягаються ціною обмежень на інші властивості.

Тому коли мова йде про оптимальність повідомлення, то потрібне уточнення: в якому сенсі воно оптимальне? Дуже важливим є і друге уточнення: стосовно кого, до якого конкретно одержувача? *В ідеальному випадку повідомлення буде оптимальним, якщо воно за своєю формою, змістом, метою і часом відповідає можливостям і потребам його одержувача.* Оптимальне повідомлення відрізняється стислістю, ясністю, своєчасністю, новизною. Яскравим прикладом оптимізації повідомлення може бути упорядкування телеграми. Її відправник усе зважує: і зміст, і довжину тексту, і час відправлення. Важливо врахувати, що саме в техніці зв'язку для передачі дискретних повідомлень уперше стала використовуватися на

практиці теорія оптимального кодування повідомлень. На наш час вона широко використовується і в комп'ютерній техніці.

Оптимізація повідомлень – непросте, достатньо складне завдання, що вимагає високої інформаційної культури людини, врахування багатьох суперечливих чинників. Взяти, приміром, надмірність. Ця категорія негативна, вона збільшує довжину повідомлень. Але в ряді випадків надмірність необхідна для підвищення надійності передачі повідомлень та їхнього сприйняття. Прийоми розгорнутого (надлишкового) викладу матеріалу використовуються, наприклад, з метою оптимізації сприйняття аудиторією сутності понять високої складності.

Для визначення кількості інформації потрібно було знайти спосіб представити будь-яку її форму (символьну, текстову, графічну) в єдиному виді. Інакше кажучи, треба було зуміти ці форми інформації перетворити так, щоб вони одержали єдиний стандартний вид. Таким видом стала так звана *двійкова форма* подання інформації. Вона полягає в записі будь-якої інформації у вигляді послідовності тільки двох символів.

Ці символи можуть на папері позначатися будь-яким способом: літерами А, Б; словами ТАК, НІ. Однак заради спрощення запису взято цифри 1 і 0. У електронному апараті, що зберігає або обробляє інформацію, ці символи можуть також позначатися по-різному: в одних випадках – наявністю в розглянутій точці електричного струму або магнітного поля, в інших – їх відсутністю.

Розглянемо найпростіший випадок одержання інформації. Ви задаєте тільки одне питання: "чи йде дощ?" При цьому умовимося, що з однаковою імовірністю очікуєте відповідь: "1" або "0". Легко побачити, що будь-яка з цих відповідей несе найменшу порцію інформації. Цю порцію назвали *бітом*. Завдяки введенню поняття *біт* з'явилася можливість визначення розміру будь-якої інформації кількістю бітів (комірок пам'яті комп'ютера зі значеннями 1 або 0). Розглянутий процес одержання двійкової інформації щодо об'єктів дослідження називають *кодуванням інформації*.

В інформаційних документах широко використовуються не тільки російський чи український шрифт, але й латинські літери, цифри, математичні знаки й інші спеціальні знаки – всього близько 200-250 символів. Для кодування всіх цих символів використовується восьмирозрядна послідовність цифр 0 і 1. Наприклад, російські літери представляються восьмирозрядними послідовностями в такий спосіб: А – 11000001, И – 11001011, Я – 11011101.

Слід зазначити, що запропонований спосіб кодування використовується тоді, коли до нього не пред'являються додаткові вимоги. Але, якщо необхідно реагувати на помилку, яка виникає, виправити її, забезпечити таємність інформації, то застосовують спеціальне кодування.

Для подання графічної інформації в двійковій формі використовується так називаний *покрапковий спосіб*. На першому етапі зображення поділяють вертикальними і горизонтальними лініями. Чим більше при цьому утворилося квадратів, тим точніше буде передана інформація про картинку.

З прикладів, розглянутих вище, видно, що інформація описується багато-розрядними послідовностями двійкових чисел. Для зручності ці послідовності об'єднуються в групи по 8 біт. Така група іменується байтом: наприклад, число 11010011 – ця інформація розміром один байт. На практиці використовують похідні величини для виміру більшого обсягу інформації – 1000 байт (1 кілобайт, 1kB, 2^{10} байт), 1000000 байт (1 мегабайт, 1 Mb, 2^{20} байт), 1000000000 байт (1 гігабайт, 1 Hb, 2^{30} байт) і т.д.

1.4. Інформатика як наука про технологію обробки інформації

У сферу сучасної інформатики входить ряд питань, які можуть бути подані у вигляді таких груп:

- технічні, що пов'язані з вивченням методів і засобів надійного збору, збереження, передачі обробки та видачі інформації;
- семантичні, що визначають способи опису змісту інформації та мови її опису;
- методи кодування інформації;
- синтаксичні, що пов'язані з рішенням задач із формалізації й автоматизації деяких видів науково-інформаційної діяльності, зокрема індексування, автоматичне реферування, машинний переклад.

Величезну, по суті, революційну роль у становленні та розвитку інформатики зіграло створення електронно-обчислювальної машини (ЕОМ) і сучасної комп'ютерної техніки.

У структурі інформатики як науки виділяють алгоритмічну, програмну та апаратну галузі. Суміжними дисциплінами з інформатикою є кібернетика й обчислювальна техніка, що у багатьох випадках вирішують загальні задачі, пов'язані з переробкою інформації. Стрижневим напрямком і предметом інформатики є розробка автоматизованих інформаційних технологій на основі використання комп'ютерів.

Застосування комп’ютерів стало основою для створення нових інформаційних технологій, які дозволяють не тільки накопичувати, зберігати, переробляти інформацію, але й одержувати нову інформацію, нові знання. У цьому полягає істотна відмінність можливостей комп’ютерів від можливостей будь-якої іншої інформаційної техніки – засобів зв’язку, проекційної апаратури, телебачення. За оцінками фахівців, інформація на виходах комп’ютерних мереж відрізняється від інформації на входах приблизно так, як невирішена задача відрізняється від вирішеної. В одержанні нових відомостей, нових даних, кількісно та якісно відмінних від вхідних, і перебуває сутність тлумачення комп’ютерів як пристроїв обробки інформації та підсилювача інтелекту, а якщо врахувати її швидкодію, то прискорювача інтелекту.

Характерною рисою сучасних комп’ютерів є те, що переважна їхня частина (до 80 %) використовуються не для розв’язку обчислювальних задач, а для зручного користування інформацією (коригування текстів, виконання графічних робіт, накопичення й оперативна видача різноманітних даних, програмне пред’явлення інформації в процесі комп’ютерного навчання, автоматизований контроль знань і т.д.).

Контрольні питання до розділу

1. Яка різниця між інформатикою та інформаційними технологіями?
2. Що таке інформаційне суспільство та інформаційний ресурс?
3. Яка різниця між інформаційними та інфокомунікаційними технологіями?
4. Яка різниця між даними та інформацією?
5. Назвіть форми подання інформації.
6. В чому суть оптимізації повідомлень?
7. Які основні галузі інформатики, як науки, ви можете назвати?

РОЗДІЛ 2. ПРОГРАМНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ПК

2.1. Апаратне забезпечення персонального комп'ютера

Комп'ютер – це апаратно-програмний пристрій, призначенням якого є переробка, накопичення, аналіз, систематизація і пересилка інформації.

Основними компонентами ПК є: системний блок (рис. 2.1), монітор, клавіатура, миша, акустична система, принтер, модем, сканер.

Рис. 2.1. Зовнішній вигляд ПК у настольному варіанті

Зовні комп'ютери можуть відрізнятися один від одного, але в кожному з них є дві невід'ємні складові: *апаратна* і *програмна*.

Апаратна частина, або *hardware*, – *це електронні компоненти комп'ютера, які самі по собі є лише набором мікросхем*. Оживити їх і примусити виконувати різноманітні задачі призначене *програмне забезпечення* (*software) – операційна система і різні програми для обробки даних*.

Системний блок – основна апаратна складова комп'ютера. До нього підключається решта компонентів: пристрої введення-виведення, за допомогою яких інформація поступає в пам'ять комп'ютера і видається користувачу, а також пристрої, які, виконуючи різні функції, розширюють можливості ПК. Основним вузлом ПК є системна (материнська) плата (рис.2.2) з процесором, оперативною пам'яттю, відео- та звуковою картою, мікросхемою BIOS, PCI- та USB-роз'ємами.

Окрім того на системній платі розташовані контролери – мікросхеми, що управляють роботою всіх зовнішніх пристроїв . Окрім цієї плати в системному блоці розміщений блок живлення з вентилятором, жорсткий диск з

енергонезалежною пам’яттю, приводи для зв’язку із зовнішнією пам’яттю (наприклад, компакт-диски, флеш-пам’ять) тощо.

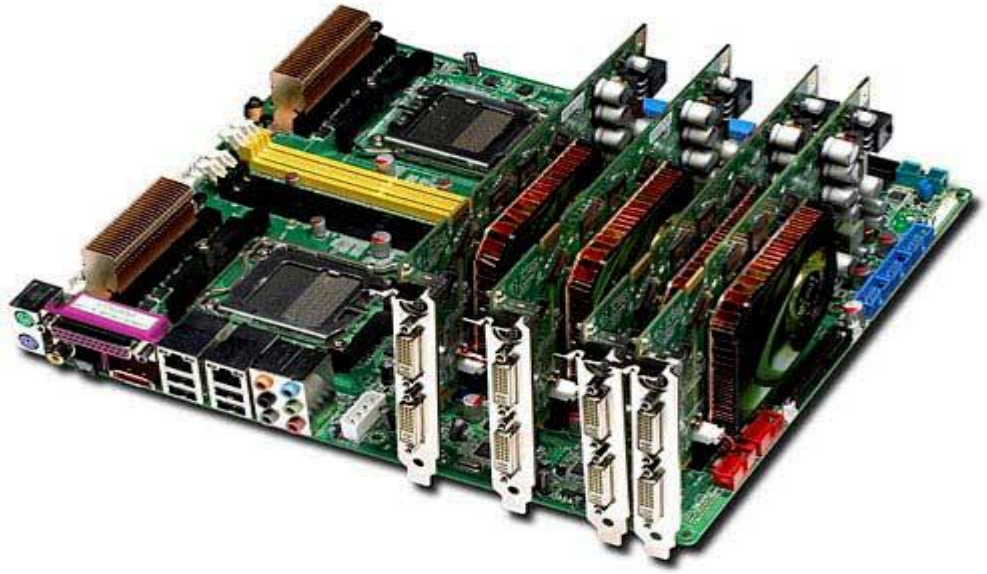


Рис.2.2. Зовнішній вигляд системної плати

Монітор – засіб відображення інформації, що поступає з ПК. Монітори можуть бути на основі електронно-променевої трубки (CRT), плоскими рідиннокристалічними (LCD) або плоскими плазменими. CRT-монітори поки ще знаходяться в експлуатації, але поступово замінюються на LCD та плазмені монітори, у яких майже повністю відсутнє шкідливе електромагнітне випромінювання.

Клавіатура і миша – пристрої, за допомогою яких можна контролювати роботу програмного забезпечення ПК, вводити алфавітно-цифрову (текстову) інформацію та параметри у діалогові вікна.

Додаткові пристрої: *акустична система* – колонки або навушники, які дозволяють відтворювати звуки і музику за допомогою звукової карти комп’ютера; *принтер* – друкуючий пристрій; *сканер* – дозволяє переводити паперові документи (книги, фотографії) в електронний вигляд; *маршрутизатор+модем*) для підключення до Інтернету, *відеокамера* та інші пристрої.

Електронним “мозком” комп’ютера є *центральний процесор*. Процесор (CPU – Central Processing Unit) – це головна мікросхема комп’ютера, яка проводить обробку всіх даних, що до неї поступають. Саме вона виконує всі команди, що містяться у програмі. Від обчислювальної потужності центрального процесора головним чином залежить продуктивність системи. Під час роботи процесор нагрівається, тому на нього встановлюють систему

охолоджування – вентилятор або кулер. Кулер – це вентилятор з радіатором, який монтується безпосередньо над процесором і охолоджує його.

Пам'ять комп'ютера можна розділити на три категорії – постійну, оперативну і зовнішню. *Постійна пам'ять* – це мікросхема BIOS на системній платі (Basic Input/Output System), в якій зберігаються програми первинного завантаження комп'ютера, тестування основних компонентів, а також набір підпрограм для управління всіма його пристроями.

Оперативна пам'ять виконана у вигляді окремих модулів – планок з мікросхемами. Вона призначена для зберігання програм і даних, з якими працює в даний момент центральний процесор. Інформація в оперативній пам'яті зберігається до того часу, поки комп'ютер включений. Для тривалого зберігання призначена внутрішня пам'ять на жорсткому диску і пристрої зовнішньої пам'яті.

У материнську плату можна встановити деякі додаткові пристрої, наприклад, плату TV-тюнера або FM-приймача, мережеву плату для підключення комп'ютера до локальної мережі, інші пристрої .

Одним із найважливіших компонентів, від якого багато в чому залежить надійність роботи комп'ютера, є *блок живлення*. Блоки живлення сучасних комп'ютерів "інтелектуальні" – вони можуть вимикатися і вмикатися за командою з материнської плати.

2.2. Загальна характеристика програмного забезпечення

Основні поняття програмного забезпечення

Можливості комп'ютера як технічної основи системи обробки даних пов'язані з використанням програмного забезпечення (програм).

Програма – це упорядкована послідовність команд комп'ютеру для вирішення задачі.

Програмне забезпечення – це сукупність комп'ютерних програм і документальних засобів для створення й експлуатації систем опрацювання даних. Програми призначені для комп'ютерної реалізації задач. Терміни *задача* і *додаток* мають широке вживання в контексті інформатики і програмного забезпечення.

Задача – це проблема, що підлягає вирішенню.

Програмний додаток (або просто додаток) – *програмна реалізація розв'язання задачі на комп'ютері у прив'язці до базового ПЗ.*

Таким чином, задача означає проблему, що підлягає реалізації з використанням засобів інформаційних технологій, а додаток – реалізоване на комп'ютері рішення задачі.

Існує багато різноманітних класифікацій задач. З позицій специфіки розробки і виду програмного забезпечення наведемо два класи задач – *технологічні* та *функціональні*.

Технологічні задачі ставляться при організації технологічного процесу обробки інформації на комп'ютері. Технологічні задачі є основою для розробки сервісних засобів програмного забезпечення у вигляді утиліт, бібліотек, процедур, які застосовуються для забезпечення працездатності комп'ютера, розробки інших програм або обробки даних функціональних задач.

Функціональні задачі вимагають рішення під час реалізації функцій управління в рамках інформаційних систем предметних областей, наприклад, управління діяльністю торгового підприємства, планування випуску продукції, управління перевезенням вантажів тощо. Функціональні задачі в сукупності утворюють *предметну область* і цілком визначають її специфіку.

Предметна область – це сукупність пов'язаних між собою функцій, задач управління, за допомогою яких досягається виконання поставлених цілей.

Процес створення програм включає таку послідовність дій: *постановка задачі*, *створення алгоритму* рішення задачі, *написання програми*.

Програмування – це теоретична і практична діяльність, пов'язана зі створенням програм. Програмування є збірним поняттям і може розглядатися і як наука, і як мистецтво, на цьому заснований науково-практичний підхід до розробки програм.

Програма являє собою результат інтелектуальної праці, для якої характерна творчість, а вона, як відомо, не має чітких границь. У будь-якій програмі присутня індивідуальність її автора, вона відбиває визначений ступінь мистецтва програміста. Разом з тим програмування припускає і рутинну працю, зв'язану з чітким регламентом виконання завдання, яке має відповідати відповідним стандартам.

Основна категорія фахівців, зайнятих розробкою програм, – *програмісти*. Вони неоднорідні за рівнем кваліфікації, а також за характером своєї діяльності. Найбільш часто програмісти поділяються на системних і прикладних.

Системний програміст займається розробкою, експлуатацією і супроводом системного програмного забезпечення, що підтримує працездатність

комп’ютера і створює середовище для виконання програм, які забезпечують реалізацію функціональних задач.

Прикладний програміст здійснює розробку і налагодження програм для вирішення функціональних задач.

В умовах створення великих за масштабами і функціями програм з’являється нова кваліфікація – *програміст-аналітик*, що аналізує і проектує комплекс взаємозалежних програм для реалізації функцій предметної області.

У процесі створення програм на початковій стадії беруть участь *постановники задач*.

Більшість інформаційних систем засновано на роботі з базами даних. Якщо база даних є інтегрованою, що забезпечує роботу з даними багатьох додатків, виникає проблема організаційної підтримки баз даних. Таку підтримку виконує *адміністратор бази даних*.

Основним споживачем програм є *кінцевий користувач*, який найчастіше відноситься до категорії користувачів-непрограмістів. Кінцевий користувач не є фахівцем у сфері програмування, але має елементарні знання і навички роботи з ПК.

Різновиди програмного забезпечення

Залежно від виконуваних функцій програмне забезпечення класифікують таким чином: системне; прикладне; інструменти (інструментарії) технології програмування.

Системне програмне забезпечення призначене для:

- створення операційного середовища функціонування інших програм;

- забезпечення надійної і ефективної роботи самого комп’ютера і обчислювальної мережі;

- проведення діагностики і профілактики комп’ютера і обчислювальних мереж;

- виконання допоміжних технологічних процесів (копіювання, архівація, відновлення файлів програм і баз даних тощо).

Прикладне програмне забезпечення призначене для вирішення конкретних завдань користувача і ділиться на кілька груп:

- *офісні програми* – Microsoft Office (Excel,Word, Access), програми для сканування зображень та розпізнавання текстів (ABBYY FineReader), засоби машинного перекладу текстів з однієї мови на іншу (Pragma, Promt), програми для роботи в Інтернеті (наприклад, браузери Opera, Google, програми електронної пошти – наприклад, mail.ua, gmail.com та ін.);

- *мультимедійні програми* – для роботи із звуком, відео, графікою (наприклад, Windows Media, Adobe Photoshop, CorelDRAW);

- *навчальні програми* (електронні посібники) та програми для розваг (програвачі музичних і відео файлів, комп'ютерні ігри тощо).

Інструментарій технології програмування забезпечує процес розробки програм і включає спеціалізовані програмні продукти (засоби) розробника (наприклад Visual Basic, Delphi, Java). Програмні продукти цього класу підтримують всі технологічні етапи процесу проектування, програмування, налагоджування і тестування створюваних програм. Користувачами інструментарію технології програмування є системні та прикладні програмісти.

2.3. Призначення і типи операційних систем

Комп'ютер виконує дії, які відповідають командам програми, описаної однією з мов програмування. Програми, що організують роботу пристроїв і не пов'язані зі специфікою розв'язуваної задачі, увійшли до складу комплексу програм, названого *операційною системою*. Функції операційної системи різноманітні, постійно розширюються за рахунок введення додаткових програм і модифікації старих.

Операційна система – це сукупність програмних засобів, що забезпечує керування апаратною частиною комп'ютера і прикладними програмами (додатками, утилітами), а також взаємодію між обчислювальною системою і користувачем.

Операційна система утворює автономне середовище, не пов'язане з жодною з мов програмування. Будь-яка ж прикладна програма пов'язана з операційною системою і може експлуатуватися тільки на тих комп'ютерах, де є відповідне системне середовище. Прикладні програмні засоби, розроблені в середовищі однієї операційної системи, не можуть бути використані для роботи в середовищі іншої операційної системи, якщо немає спеціального комплексу програм (конвертера), що дозволяє це зробити.

Найважливіші функції будь-якої операційної системи:

- управління роботою кожного блоку комп'ютера і їхньою взаємодією;
- управління виконанням програм;
- організація збереження інформації в зовнішній пам'яті;
- взаємодія користувача з комп'ютером (підтримка інтерфейсу користувача).

Зазвичай операційна система зберігається на жорсткому диску, а при його відсутності виділяється спеціальний диск, що називається системним диском. При включенні комп'ютера операційна система автоматично завантажується з диска в оперативну пам'ять і займає в ній визначене місце.

Кожна операційна система орієнтована на конкретний тип центрального процесора. Важливою характеристикою операційної системи є розрядність системи команд процесора, для якого ця система розроблена. Є 8-розрядні, 16-розрядні, 32-розрядні, 64-розрядні ОС.

Ще одна характеристика ОС – тип її користувацького інтерфейсу. Ступінь розвитку інтерфейсу характеризує ступінь її придатності для інтерактивного використання: 8-бітні ОС використовують, як правило, примітивний інтерфейс командного рядка; 16-бітні ОС постачаються спеціальною програмою-оболонкою, що реалізує інтерфейс текстових меню; 32-розрядні і 64-розрядні ОС обладнуються об'єктно-орієнтованим (як правило, віконно-графічним) інтерфейсом. У перспективі – побудова систем *інтелектуального інтерфейсу*.

2.4. Стислі характеристики основних операційних систем

Операційні системи сімейства MS-DOS. Ця система є першою і найбільш поширеною представницею 16-бітних DOS (Disk Operation Systems). Була випущена для ПК серії IBM PC у 1981 р. Її відмінні риси – однозадачність, вбудований командний інтерфейс, модульність структури, ієрархічність файлової системи, невеликий обсяг пам'яті (640 Кбайт). Як недолік слід відзначити відсутність засобів захисту від несанкціонованого доступу до ресурсів ПК і ОС. Останньою версією цієї системи була DOS 6.22. Нині однозадачні ОС на ПК не використовуються.

Операційні системи сімейства UNIX. Операційні системи сімейства UNIX – це 32-розрядні та 64-розрядні багатозадачні багатокористувацькі операційні системи. Сильний бік UNIX – це надійність роботи в мережі, а також можливість використовуватися на різних комп'ютерах – від суперкомп'ютера до ПК. Це дає змогу переносити ОС та інші програмні засоби з однієї машинної архітектури на іншу з мінімальними витратами.

UNIX забезпечує доступи до розподілених баз даних і до робочих станцій локальної мережі, до віддаленої дистанційної мережі, а також вихід в глобальні мережі. Поштова служба UNIX – один із головних її компонентів.

Більшисть сучасних UNIX-систем є комерційними версіями дистрибутивів UNIX, наприклад Solaris від Sun, HP-UX Hewlett-Packard, AIX® від IBM, які мають свої власні унікальні елементи і функціональні рішення.

Операційна система Linux. ОС Linux була задумана як бесплатна альтернатива комерційним UNIX-середовищам. Ідея була успішно реалізована Лінусом Торвальдсом, коли він був ще студентом університету в м. Хельсінкі на початку 90-х років минулого століття.

На відміну від Unix, який використовувався на серверах і великих ЕОМ (мейнфреймах), Linux в початковому вигляді був орієнтован на домашні ПК з більш простим апаратним забезпеченням.

На даний час Linux успішно працює на великій кількості платформ, більш, ніж будь-яка інша ОС. Це сервера, вбудовані системи, мікрокомп'ютери, модеми і навіть мобільні телефони. Але у цієї ОС є комерційний недолік: численні додатки до системи є платними.

Операційна система Windows. Ця багатозадачна і багатокористувацька система корпорації Microsoft, яка орієнтована на застосування зручного графічного інтерфейсу користувача при роботі з ПК. Спочатку ОС Windows була всього лише графічною надбудовою для MS-DOS, але на сьогодні під управлінням операційних систем серії Windows за даними ресурса Net Applications працює приблизно 85% всіх ПК. Основними представниками цього сімейства ОС є Windows NT, Windows 2000, Windows XP, Windows 7, Windows 10 з перспективою подальшого розвитку, а також мобільні версії Windows Mobile та Windows Phone.

Операційна система Apple. У 1984 році корпорація Apple Computer, Inc. представила новий комп'ютер Macintosh з фірменою ОС, який більш 20 років був її основним бізнесом. На даний час Apple є виробником не тільки унікальної багатозадачної ОС з графічним інтерфейсом, а й персональних і планшетних ПК, аудіоплеєрів, мобільних телефонів, програмного забезпечення (мобільна версія системи – iOS).

У січні 2007 року корпорація відмовилась від слова *Computer* у своїй назві, продемонструвавши зміну основного курсу з ринку комп'ютерної техніки на ринок побутової електроніки. Завдяки інноваційним технологіям та естетичному дизайну, корпорація створила в індустрії споживчої електроніки майже культову репутацію. Так, виробництво пристроїв iPod, iPhone и iPad сьогодні користується високим попитом у всьому світу, приносячи корпорації величезні прибутки.

Найбільше застосування ОС Apple знайшла у видавничій справі, на телебаченні, в системах відеодизайну і відеоспостереження.

Операційні системи реального часу. Термін *реальний час* у широкому розумінні застосовується до систем обробки інформації з малим гарантованим часом реакції. Як правило, цей час коливається від кількох мікросекунд до кількох часток секунди.

Операційні системи реального часу застосовуються в автоматизації таких галузей, як транспортування нафти та газу, управління технологічними процесами в металургії та машинобудуванні, в управлінні хімічними процесами, енергетиці, управлінні роботами, у банківських системах, правоохоронній діяльності та ін.

Серед найбільш популярних операційних систем реального часу для IBM PC використовуються *OS-9000, FLEX OS, QNX та інші*.

Контрольні питання до розділу

1. Назвіть та поясніть основні складові комп'ютера як засоба обробки даних.
2. Поясніть роль постійної, оперативної та зовнішньої (жорсткої) пам'яті ПК.
3. Які функції виконує системне програмне забезпечення ПК?
4. Назвіть основні групи прикладного програмного забезпечення.
5. Що таке операційна система ПК? Які основні функції вона виконує?
6. Розкажіть стисло про суть операційних систем Unix та Linux.
7. Розкажіть про переваги операційних систем Windows та Apple.
8. В чому суть операційних систем реального часу? Надайте кілька прикладів таких систем.

РОЗДІЛ 3. ОСНОВНІ ПОНЯТТЯ З ОС WINDOWS

3.1. Призначення та функції ОС Windows

Згадаємо, що *операційна система* (*ОС – operating system*) – *це комплекс взаємозв'язаних програм, призначених для управління ресурсами комп'ютера та організації взаємодії з користувачем*. Основні функції ОС Windows:

- виконання запитів програм (ввід/вивід даних, запуск і зупинка інших програм, звільнення додаткової пам'яті та ін.);
- завантаження програм в оперативну пам'ять та їх виконання;
- стандартизований доступ до периферійних пристроїв;
- управління оперативною пам'яттю (розподіл між процесами, організація віртуальної пам'яті);
- управління доступом до даних на енергонезалежних носіях (таких як жорсткий диск, оптичні диски, флеш-пам'ять та ін.), що належним чином організовані у файлах;
- забезпечення користувацького інтерфейсу;
- зберігання інформації про помилки системи.

Окрім цього, для зручності користування, ОС забезпечує ряд додаткових функцій:

- паралельне або псевдопаралельне виконання задач (багатозадачність);
- ефективний розподіл ресурсів обчислювальної системи між процесами;
- розмежування доступів різних процесів до ресурсів;
- організація надійних обчислювань (неможливості одного обчислювального процесу навмисно або помилково вплинути на обчислення в іншому процесі), які засновані на розмежуванні доступу до ресурсів;
- взаємодія у випадку обміну даними;
- захист самої системи, а також користувацьких даних і програм від дій користувачів (зловмисних або через незнання);
- багатокористувацький режим роботи з використанням аутентифікації та авторизації).

В логічній структурі типової обчислювальної машини операційна система займає місце між пристроями з їх мікроархитектурою, машинною мовою і, можливо, власними (вбудованими) мікропрограмними драйверами з одного боку і прикладними програмами з іншого.

На даний час *ОС Windows* (англ. – *Вікна*) набула значну популярність і є найбільш розповсюдженою системою серед користувачів ПК. Дійсно, всі

додатки до Windows оформлено на екрані ПК у вигляді вікон. Таким чином, робота з окремими видами програмного забезпечення означає роботу в тому чи іншому вікні системи.

Операційна система Microsoft Windows – швидкодійна мережна операційна система з графічним інтерфейсом. *У Windows реалізовано такі архітектурні рішення*: переміщуваність, багатозадачність, багатопроцесорність, масштабованість, архітектура клієнт-сервер, об'єктна архітектура, розширюваність, надійність і відмовостійкість, сумісність, багаторівнева система безпеки тощо. Розглянемо деякі з цих понять.

Під *переміщуваністю* розуміється здатність ОС працювати як на CISC-, так і на RISC-процесорах. RISC (англ. *reduced instruction set computer* – "комп'ютер зі скороченим набіром команд") – архітектура процесора, в якому швидкодія збільшувалася за рахунок спрощення інструкцій, щоб їх декодування було більш простим, а час виконання меншим. CISC (англ. *complex instruction set computer* – "комплексна інструкція мережевого комп'ютера") – тип процесорної архітектури, який характеризується такими властивостями: нефіксоване значення довжини команди; арифметичні дії кодуються в одній команді; невелика кількість регістрів, кожний з яких виконує строго визначену функцію.

Багатозадачність – використання одного процесора для роботи безлічі додатків або потоків (ниток, якщо додатки розбиваються на окремі виконувані компоненти).

Багатопроцесорна обробка припускає наявність декількох процесорів, які можуть одночасно виконувати безліч команд, по одній на кожний процесор.

Масштабованість – можливість автоматичного використання переваг доданих процесорів. Так, для прискорення роботи додатку операційна система може автоматично підключати додаткові однакові процесори.

Розширюваність забезпечена відкритою модульною архітектурою, що дозволяє додавати нові модулі на всі рівні операційної системи. Модульна архітектура забезпечує можливість з'єднання з іншими мережними продуктами. Наприклад, комп'ютери, що працюють під управлінням Windows NT, можуть взаємодіяти з серверами і клієнтами інших операційних систем.

Характеристики *надійність* і *відмовостійкість* вказують на те, що архітектура захищає операційну систему і додатки від руйнування.

Сумісність означає, що Windows продовжує підтримувати додатки MS-DOS, Windows 3.x, OS/2, а також широкий набір периферійних пристроїв.

Для захисту інформації, що передається по мережі, використовуються різні методи кодування та вбудований інтерфейс криптографування – Microsoft Cryptographic Application Program Interface (CryptoAPI).

3.2. Користувацький інтерфейс

Користувацький інтерфейс Windows включає такі основні елементи: *засоби управління*; *вікна; робочий стіл; панель задач; головне меню; контекстні меню; довідкову систему*.

Основним поняттям користувацького інтерфейсу є *вікно*. *Вікно – це прямокутна ділянка екрану, в якій відображаються папки і файли, виконувані програми і документи*.

Основну частину екрану Windows займає *Робочий стіл*. На ньому розташовуються значки *об'єктів* – папок, дисків, програм тощо. Якщо значок має в лівому нижньому куті додаткову позначку, то це значок ярлика.

Ярлик – це посилання на об'єкт, що розташований не на *Робочому столі*, а в іншому місці. Один об'єкт може мати декілька ярликів, розташованих у різних місцях.

При подвійному натисканні мишею на значок об'єкта відкривається вікно цього об'єкта. При подвійному натисканні на ярлику відкривається вікно того об'єкта, на який посилається ярлик.

Зазвичай на робочому столі представлені такі папки та рядки.

Мой компьютер – представляє відповідну універсальну програму, що забезпечує швидкий доступ до ресурсів комп'ютера.

Сетевое окружение – значок з'являється лише у випадку, якщо комп'ютер підключений до мережі і викликає програму, що забезпечує доступ до всіх доступних мережних ресурсів.

Портфель – область пам'яті для зберігання документів, з якими здійснюється робота в різних місцях: удома, на роботі тощо. В портфелі зберігається база даних, що містить декілька варіантів одного документа одночасно.

Internet – викликає програму, що призначена для перегляду даних у мережі Internet.

Корзина – місце зберігання видалених із жорсткого диска файлів. Видалені файли можуть бути відновлені. Остаточно посилання на файл зникає при очищенні *Корзины*.

Панель задач призначена для запуску застосунків і переходу між ними. За умовчанням вона міститься в нижній частині екрану. Панель задач містить

кнопку *Пуск*, кнопки з ярликами активних додатків та індикатори. Активним додатком вважається програма, яку запущено на виконання.

При натисканні на кнопку *Пуск* з'являється *Головне меню*. Якщо пункт меню позначений стрілкою ▸, то при наведенні на нього покажчика миші відкриється підменю. Головне меню забезпечує доступ майже до всіх функцій Windows і дозволяє виконати роботи, пов'язані із запуском програм, отриманням довідок, пошуком і відкриттям документів, настройкою системи.

Контекстне меню об'єкта містить основні команди з управління цим об'єктом. Для виклику контекстного меню потрібно натиснути на об'єкті правою клавішею миші. Наприклад, якщо натиснути правою клавішею миші на панелі задач, з'явиться контекстне меню панелі задач.

Інші дії з операційною системою рекомендується вивчити самостійно, користуючись довідковою системою або літературою, список якої наведено в кінці посібника.

3.3 Основні поняття роботи з редактором Word

Загальні відомості

Microsoft Word (MS Word) за своїм призначенням відноситься до текстових процесорів. За своїми можливостями він наближається до настільних видавничих систем, хоча й не належить до цих спеціалізованих програмних засобів, оскільки має певні технічні обмеження.

На наведеній нижче схемі (рис. 3.1) подано у спрощеному вигляді ієрархію об'єктів, якими оперує MS Word.

Документ → Розділ (текст, таблиці, рисунки) → Абзац → Символ

Рис. 3.1. Ієрархія об'єктів текстового процесора Microsoft Word

Основним об'єктом є *Документ*, який включає в себе всі інші об'єкти. Документ зберігається у вигляді файлу Word і характеризується назвою, місцем розташування, датою створення тощо.

Розділ є найкрупнішою складовою частиною документу. Кожний документ містить щонайменше один розділ. Саме для розділу визначаються розмір паперу, орієнтація сторінки, величина полів, нумерація сторінок, вміст колонтитулів. Якщо необхідно змінити хоча б один з цих параметрів для частини документу, слід оформити цю частину у вигляді окремого розділу.

Абзац є сукупністю розташованих підряд символів, яка закінчується символом кінця абзацу. Абзац може бути порожнім – в цьому випадку він містить лише цей спеціальний символ. Для абзацу встановлюються такі характеристики, як міжрядковий інтервал, відстань від тіла абзацу до лівого та правого полів сторінки, відступи до попереднього та наступного абзаців, формат нумерації, спосіб вирівнювання тексту в межах абзацу, відступ першого рядка тощо.

Символ (букви, цифри, розділові та інші знаки) є мінімальною одиницею інформації. Основними характеристиками символу є назва та розмір шрифту, яким виводиться цей символ, а також особливості його оформлення (жирний, курсивний, підкреслений, з тінню та ін.).

Окрім перерахованих основних об'єктів, Microsoft Word дозволяє вставляти в текст інші *об'єкти*, створені як власно Word, так й іншими програмами. Експортовані об'єкти можуть бути створені будь-якою програмою, яка підтримує можливість обміну даними між додатками Windows.

Практична частина заняття

Наберіть у редакторі Word нижченаведений текст та структурну схему.

Сьогодні найбільш поширеним методом управління організацією є метод процесно-системного управління з орієнтацією на якість кінцевої продукції, споживачів та персонал організації. За кордоном цей метод називають Total Quality Management (TQM, україномовна абревіатура – ВУЯ). Суть методу у спрощеному вигляді можна пояснити наступним чином.

В нових умовах глобалізації ринку та опанування "високих технологій" багатьма країнами і підприємствами успіх виробника почав залежити від швидкості реакцій на запит споживачів, а також від спроможності випустити високоякісну продукцію з мінімальними витратами виробництва при одержанні прийнятного прибутку.

Саме цей принцип і лежить в основі ВУЯ. Основоположники TQM японці говорять:"Все потрібно робити добре з першого разу". І ще:"Треба не виправляти брак, треба його не робити – це значно дешевше". Основні елементи методу наведені на рис.3.2.

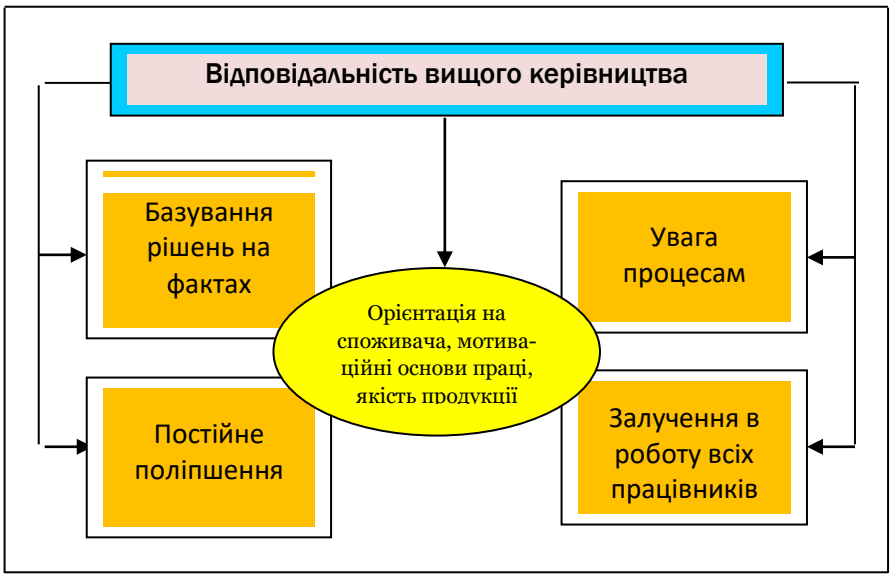


Рис. 3.2. Найважливіші елементи TQM

3.4. Загальні відомості про табличний редактор EXCEL

Microsoft Excel – програма (редактор) для роботи з електронними таблицями, яка створена корпорацією Microsoft для Windows, Mac OS, а також Android, iOS і Windows Phone. Вона *надає можливість проведення економіко-статистичних розрахунків, побудови багатьох графічних образів і користування мовою макропрограмування VBA* (Visual Basic for Application). Microsoft Excel входить до складу Microsoft Office і на сьогоднішній день є одним з найбільш популярних додатків у світі.

У порівнянні з першими табличними процесорами сучасний Excel представляє безліч нових функцій для користувача інтерфейсу, але суть залишається незмінною: *організовані в рядки і стовпці клітини можуть містити дані (числові, текстові), об'єкти або формули з відносними або абсолютними посиланнями на інші клітини*.

Запуск редактора здійснюється через головне меню: Пуск → Программы → Microsoft Excel, або з Робочого стола, якщо на ньому є цей ярлик.

Вікно редактора Excel має кілька стандартних елементів. Одні з них постійно присутні, інші можна змінювати за бажанням користувача.

Верхній рядок екрана – це рядок заголовку. Під рядком заголовку у вікні розміщено рядок меню, який містить такі меню: *Файл* – для роботи з файлами документів; *Правка* – редагування документів; *Вид* – вигляд вікна, зміна режимів перегляду документів; *Вставка* – вставка малюнків, діаграм, дати і часу, формул тощо; *Формат* – форматування документів (встановлення

шрифтів, параметрів абзацу); *Сервис* – сервісні функції (перевірка орфографії, встановлення параметрів Excel); *Данные* – робота з базами даних; *Окно* – робота з вікнами книг; ? – довідка про Excel.

Під рядком меню розміщено панелі інструментів. Для вибору необхідної панелі треба виконати команду *Вид→Панели инструментов*, після чого з'явиться вікно, у якому із списку слід вибрати необхідні панелі.

По замовчуванню виводяться панелі *Стандартная* і *Форматирование*. Деякі панелі з'являються автоматично при виконанні певних дій (наприклад, панель інструментів *Диаграмма* виводиться при побудові діаграм).

Під панелями інструментів знаходиться *рядок формул*, в лівому кутку якого висвічується ім'я поточної клітки.

Файл, створений в Excel за умовченням, називається книгою (Книга1, книга2, ...). Кожна книга складається з листів кількох типів (Лист1, лист2,...). Назва файлу в Excel має розширенням xls.

Робочі листи – це електронні таблиці, що складаються з колонок та рядків. Колонки позначаються зліва направо літерами A,B,C, . . .,AA,AB, . . . , IU,IV. Рядки зверху вниз позначаються цифрами. На перетині колонки і рядка розміщується клітинка (комірка). Позначення (адреса) клітинки складається з позначення колонки та рядка.

В Excel може існувати одночасно кілька вікон книг. Для маніпуляції з вікнами використовують *меню Окно*. Активне вікно виводиться на перший план і може перекривати інші вікна. Користувач може змінювати положення та розмір вікон.

Вікно має типові елементи. Заголовок вікна розміщується зверху і включає ім'я книги. Праворуч розміщено кнопки згортання, відновлення і закриття вікна.

Список листів розміщується ліворуч в нижньому рядку вікна. Список листів можна гортати за допомогою кнопок прокрутки, які знаходяться ліворуч від списку. Робочим листам присвоюється імена *Лист1, Лист2,* ... , а листам з діаграмами – *Диаграмма1, Диаграмма2,* ...

3.5. Основні поняття щодо роботи в Excel

Редагування даних

В клітки таблиці Microsoft Excel можна заносити дані таких типів, як *числа*, включаючи дату і час, *текст*, *формули*, *графічні образи*.

Числа використовуються у формі: цілі, дійсні, з експонентою, дробові. Для цілих чисел використовуються цифри 0, 1, ...9, знаки + та - . Дійсні числа

включають десяткову кому, що розділяє цілу і дробову частину. Мантису і порядок числа з експонентою розділяє латинська е (Е), наприклад 3Е + 8; 0,624 Е-23. При використанні дробових чисел вводиться ціла частина числа, символ пробілу, чисельник, знак / (ділення) і знаменник.

Дата вводиться у форматі – ДД/ММ/РРРР, *час* – ГГ:ХХ:СС.

Якщо дані вводяться не у форматі числа, то Microsoft Excel сприймає їх як текст. Якщо введені числа чи формули потрібно інтерпретувати як текст, то їх введення повинно починатися із апострофа (′), наприклад: ′1234.

Формула починається із символу “ = ” і являє собою сукупність операндів, з’єднаних знаками операцій і круглих дужок. Операндом може бути число, текст, логічне значення, адреса клітинки або посилання на неї, функція. В полі клітинки після введення формули може відображатися або формула, або значення, обчислене за формулою. Для цього потрібно виконати команди: *Сервис* → *Параметры* → *Вид* і включити прапорець у полі *Формулы*.

Для введення або редагування даних будь-якої комірки таблиці, слід її зробити активною. Для редагування даних активної комірки натиснути F2 або двічі клацнути мишею по ній. Натискуванням клавіші Enter закінчується введення або редагування даних в комірці.

Особливістю введення в Excel є *Автозаполнение*. Ця функція працює при встановленому прапорці *Автозаполнение* значень клітин вкладки *Правка* діалогового вікна *Параметры* команди *Сервис*. При введенні даних в цьому режимі Excel намагається угадати, що вводити і допише свій варіант до кінця. Якщо ви згодні, то натисніть Enter, інакше продовжіть введення.

Виділення діапазону клітинок: мишею; для виділення колонки або рядка – клацнути мишею по заголовку колонки або номеру рядка; для виділення несуміжного діапазону кліток утримувати натиснутою Ctrl.

Виділений фрагмент можна вилучити, очистити, вставити, перемістити, скопіювати. Для цього використовують буфер обміну.

Використання формул

Формула – це сукупність операндів, з’єднаних між собою знаками операцій і круглих дужок. У формулах розрізняють арифметичні операції і знаки відношень. При обчисленні формули спочатку виконуються операції у круглих дужках, потім арифметичні операції, за ними – операції відношень.

У Excel можливі відносні, абсолютні і змішані посилання на комірки таблиці. Посилання, яке включає назву колонки і номер рядка, *є відносним*. При копіюванні формули, а також редагуванні листа таке посилання буде

модифікуватись. *В абсолютних посиланнях* перед назвою колонки і номером рядка стоїть символ $. Такі посилання не модифікуються.

У змішаних посиланнях абсолютною є назва колонки і відносною – номер рядка або навпаки. У них модифікується тільки відносна частина посилання. У формулі можуть бути посилання на діапазон комірок.

Excel містить більше ніж 400 вбудованих функцій. Функція має ім'я і список аргументів у круглих дужках.

Ввести функції у формулу можна вручну або з використанням майстра функцій. Для роботи з майстром функцій слід натиснути кнопку *Мастер функции* панелі інстументів *Стандартная* або виконати команду *Вставка функций*. При цьому відкривається діалове вікно *Мастер функции,* в якому можна вибрати категорію функцій.

Коли встановлено автоматичний режим обчислень (цей режим встановлюється за замовчуванням), зміна змісту комірки веде до перерахунку формул, які використовують ці комірки. Для встановлення ручного режиму обчислень слід у вкладинці *Вычисления* діалогового вікна *Параметры* у блоці *Производить перерасчет* встановити режим *Вручную*. У цьому режимі Excel виводить слово *Вычислить* у рядок стану всякий раз, коли в листі з'являється не обчислена формула. Для переобчислення формул слід натиснути клавішу F9.

Якщо при обчисленні формули сталася помилка, то в комірку виводиться повідомлення про помилку, яке починається з символу "#".

Створення, відкриття та збереження файлів (книг) Excel

Для створення нового файлу можна виконати команду *Файл* → *Создать* або натиснути кнопку *Создать* на панелі інструментів *Стандартная*. При натискуванні кнопки створюється нова книга з іменем *Книга 1*.

Для відкриття створеного файлу виконати команду *Файл* → *Открыть* або натиснути кнопку *Открыть* на панелі інструментів *Стандартная*. У вікні діалогу *Открытие документа* вибрати папку, ім’я документа і натиснути кнопку *Открыть*.

Для збереження файла в меню *Файл* є кілька команд: *Сохранить*, *Сохранить как*, *Закрыть, Выход*. Кожна з цих команд має свою специфіку. Команду *Сохранить как* використовують при першому збереженні файла, а команду *Сохранить* для збереження змін у існуючому файлі. Аналогічно команді *Сохранить* діє кнопка *Сохранить* на панелі інструментів

Стандартная. При виборі команд *Закрыть* або *Выход* Excel завжди запитує про необхідність збереження змін.

Для попереднього перегляду треба виконати команди *Файл* → *Предварительный просмотр* або натиснути кнопку на панелі *Стандартная.*

Для друкування виконати команди *Файл* → *Печать*. В діалоговому вікні *Печать* задати параметри для друку, натиснути кнопку *Ok*.

Об'єкти. Побудова діаграм

Excel дозволяє вставити в робочий лист об'єкти (зокрема, діаграми), створені в інших програмах (Word, Paint...). Для цього потрібно виконати команду: *Вставка* → *Об'єкт*.

Діаграми призначені для графічного відображення числових даних у звітах, на презентаційних, рекламних сторінках тощо. Діаграми поділяються на стандартні (найбільш поширені) та нестандартні (використовуються зрідка).

Є багато типів стандартних діаграм: *гістограма, графік, кругова, точкова, з областями, кільцева, поверхнева, біржова, циліндрична, конічна* тощо. Кожний тип стандартної діаграми має декілька різновидів. З нестандартних використовують такі: блоки з областями, блакитна кругова, дерев'яна. Найчастіше будують кругові, точкові, стовпчикові стандартні діаграми різних видів. Розглянемо три основні типи діаграм.

Усі діаграми (окрім кругової) мають дві осі: горизонтальну – *вісь категорій*, вертикальну – *вісь значень*.Об'ємні діаграми мають третю вісь – *вісь рядів*.

Діаграми будують програмою, яка називається *Мастер диаграм*.

3.6. Практична частина заняття

Головна мета заняття – набути вміння проводити певну обробку даних за допомогою редактора EXCEL. Зокрема, в завданні 1 відпрацьовується вміння узагальнювати початкову інформацію, в завданні 2 – проводити трендовий аналіз, в завданні 3 – проводити нескладну статистичну обробку та прогнозування.

ЗАВДАННЯ І

1. Зайти в редактор *Microsoft Exel*.
2. За допомогою клавіатури на листі 1 набрати табл. 3.1.

Таблиця 3.1

ОБЛІК ПРОДАЖУ ПРОДУКЦІЇ ФІРМИ “АЛЕКС” за попередній місяць

Найменуваня	Ціна, $	Продаж, шт.			**Виторг,$**
		готів.	безготів.	усього	
ПК Pentium (R)	450	2	3		
Принтери LX	50	1	6		
Принтери HP	70	2	8		
Принтери LJ	230	4	2		
Адаптери NE	10	9	16		
Загальний виторг, $					

3.За допомогою меню *Вставка/Строка* доповнити таблицю новою строкою (перед “Загальний виторг”):

Сканери GENIUS 80 2 9

4. Побудувати в колонці “*усього*” формули підсумування проданих товарів готівкою та безготівкою. Спочатку це зробити в першому рядку (наприклад, =C5+D5) а потім організувати копіювання цієї формули в інші рядки (відмітити значення формули, *Копировать,* відмітити області вставки – *Вставить*).

5. Аналогічно п.4 організувати формули обчислювання в колонці “Виторг” (добуток ціни за одну одиницю на кількість проданих одиниць).

6. За допомогою функції *Автопідсумування* та виділення колонки “Виторг” визначити загальну суму продажу.

7. За допомогою меню *Формат/Ячейки* або піктограми *Внешние границы* виконати “заливку” усіх ліній таблиці.

8. Виділити частину таблиці з найменуваннями і за допомогою функції упорядкування А-Я (відповідна піктограма або меню *Таблица/Сортировка*) зробити перестановку рядків в алфавитному порядку.

9. Відмітити в табл. 4.1 колонку “Виторг” і за допомогою піктограми *Мастер диаграмм* побудувати гістограму “Виторг – складові продажу” (вид гістограми – за бажанням студента). Назва діаграми - “Виторг продукції”, назва осі X - “Тип продукції”, осі Y - “Виторг, дол.”, розміщення обох рисунків – на тому ж листі під таблицею, лінії сітки - *головні лінії X та Y.*

ЗАВДАННЯ II

1. За допомогою клавіатури на листі 2 набрати табл. 3.2.

Таблиця 3.2

ВИТОРГ ПРОДУКЦІЇ ФІРМИ “АЛЕКС”

(за жовтень, листопад і грудень поточного року в у.о.)

№	Місяці	Виторг
1	жовтень	5810
2	листопад	5690
3	грудень	5470
6	березень наступного року	?

2. Для табл. 4.2 побудувати діаграму типу *Графік* з осями “Місяць” (по горизонталі) і “Виторг” (по вертикалі).

3. За допомогою маніпулятора відмітити лінію графіка (натиснення кнопки, курсор має бути на лінії графіка) та визвати з головного меню команду *Диаграмма/Добавить линию тренда*. У вікні, що з’явилося на екрані, вибрати функцію *линейная*, потім у цьому ж вікні занести у комірку *прогноз вперед* число **3**. Після натиснення *Ok* на графіку з’явиться апроксимуюча функція, за допомогою якої візуально оцінити обсяг продажу через 3 місяці (орієнтовно 4200 у.о.).

ЗАВДАННЯ III

1. За допомогою клавіатури на листі 3 набрати табл. 3.3 з результатами зважування аркуша паперу на електронних вагах (в грамах) в різні дні одного місяця, усього 10 спроб.

Таблиця 3.3

Номер спроби	1	2	3	4	5	6	7	8	9	10
Вага, г	2,11	2,02	1,95	2,05	2,08	2,12	1,98	2,07	2,01	2,10

2. За допомогою піктограми *Fx* та статистичних функцій *срзнач* і *дисп*, а також за допомогою математичної функції *корень* визначити вагу аркуша і абсолютну помилку зважування з імовірністю 0,95 при допущенні, що помилка розподілена по нормальному закону. Для розв’язку задачі треба визначити:

- середнє арифметичне значення усіх спроб (це буде вага); (2,05)
- дисперсію відносно середнього значення; (0,003)
- середньоквадратичну помилку (СКП) як корінь з дисп; (0,05)
- помилку з імовірністю 0,95 (для цього СКП помножити на 2). (0,1)

3. Результат обчислень записати в табл. 3.4 і показати його викладачу.

Таблиця 3.4

Вага, г	2,05
Помилка, г	±0,1

Контрольні питання до розділу

1. Розкажіть про призначення та функції ОС Windows/
2. Дайте стислу характеристику редактору Excel. Які функціональні можливості він надає користувачу?
3. Які типи даних редактор Excel підтримує? Поясніть детальніше.
4. Розкажіть про роботу з формулами в Excel. Як можна побудувати діаграми?
5. Які форми діаграм можна побудувати в Excel?
6. Як в Excel можна здійснити статистичну обробку даних та провести трендовий аналіз?

РОЗДІЛ 4. ЗАГАЛЬНІ ВІДОМОСТІ З КОМП'ЮТЕРНИХ МЕРЕЖ. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ЗАХИСТ ВІД КІБЕРЗАГРОЗ

4.1. Загальні відомості

Згадаємо, що *комп'ютерною мережею називається сукупність взаємозалежних через канали передачі даних ПК, що забезпечують користувачів доступом до всіх ресурсів мережі*: апаратним, програмним, інформаційним. Частіше усього загальними ресурсами мережі є інформаційний сервер (ПК із підвищеною швидкодією, пам'яттю і надійністю), а також периферійні пристрої вводу-виводу.

У залежності від видалення ПК один від одного, а також від територіального розподілу їхніх загальних ресурсів розрізняють мережі *глобальні* (більш 1000 км), *регіональні* (від 10 до кілька сотен км) і *локальні* (не більш 10 км). Зазначені відстані носять досить умовний характер і дозволяють швидко оцінити доцільний спосіб передачі даних. Окремим класом виступають *корпоративні мережі* – будь-який із перерахованих вище видів, однак апаратура, програмне забезпечення, канали зв'язку та право доступу до них належать конкретній організації.

Більш розширена класифікація комп'ютерних мереж наведена на рис. 4.1.

Всі пристрої мережі можна розділити на три великі функціональні групи: *робочі станції* (РС); *сервери мережі* (СМ); *комунікаційні вузли* (КВ).

РС – це, як правило, звичайний комп'ютер мережі із своєю операційною системою, однак такому ПК доступні загальні ресурси системи. *СМ* – це більш потужний мережевий ПК із своєю операційною системою, який виконує загальні для певних користувачів дії: створення, зберігання, копіювання та доступ до даних (наприклад, файловий сервер, сервер баз даних, сервер прикладних програм тощо).

До *КВ* відносяться: повторювач (repeater) – пристрій для регенерації сигналу; мост або комутатор (bridge or switch) – пристрії для розв'язки сегментів мережі для можливості одночасного надійного обміну даними між кількома РС; маршрутизатор (router) – пристрій для оптимального з'єднання різних мереж, які мають один протокол обміну; шлюз (gateway) – пристрій або окремий ПК для організації обміну даними між мережами з різними протоколами обміну, концентратор (hub) – центральний з'єднувальний пристрій, до якого підключаються всі кабелі мережі. Hub отримує дані, які надсилає той чи інший комп'ютер мережі, та передає їх у мережу.

Рис. 4.1. Класифікація мереж

Для доступу користувачів до мережних ресурсів розробляється відповідне ПЗ, що частіше усього входить до складу ОС як базове. Але є й окремі мережні програми (наприклад, Novell NetWare), що доповнюють можливості ОС у вигляді відповідного додатка.

До основних показників роботи мережі відносяться *продуктивність, надійність, управляємість, можливість нарощування, прозорість*.

Продуктивність сьогодні оцінюють двома параметрами: середній час реакції (тобто час між запитом і одержанням відповіді) та кількість інформації, яка передається в мережі за одиницю часу. Найчастіше перший параметр вимірюється в секундах та хвилинах, а другий в Мбіт/сек.

Надійність оцінюють кількома параметрами: середнє число відмов для визначеного сегменту мережі за одиницю часу (як правило за годину, або за добу); час безвідмовної роботи апаратурних складових (параметр може досягати кілька десятків тисяч годин з початку експлуатації), захист інформації від збійних ситуацій (якісний параметр, який забезпечується апаратно-програмним резервуванням) та безпека (конфіденціальність) зберігаємої та передаваємої інформації. Останній параметр на сьогодні придбав таке велике значення, що забезпечується цілою низкою адміністративно-правових заходів, а також апаратно-програмних засобів.

Під управляємістю мережі розуміється наявність адміністратора (як правило, це один з користувачів мережі), який має розширені можливості

щодо доступу до будь-якого елементу мережі (в тому числі й до серверу), контролює роботу мережі та користувачів згідно з відповідними інструкціями, а також підтримує її працездатність.

Будь-яка мережа є об'єктом, що розвивається (не тільки в плані модернізації складових, а й збільшення числа користувачів), тому існують такі поняття, як *розширяємість, збільшення масштабу та апаратно-програмна сумісність*. Розширяємість визначає можливість нарощування числа користувачів без втрати працездатності мережі, збільшення масштабу визначає можливість нарощування без втрати продуктивності мережі, а апаратно-програмна сумісність означає можливість підключення обладнання та програм від різних виробників.

Під прозорістю мережі розуміється можливість звичайного користувача звертатися до загальних ресурсів так само, як до складових свого ПК (тобто приховування від користувача особливостей роботи мережі), в тому числі, можливість виконання паралельних завдань та доступу до даних, що створені в іншому форматі.

Для узгодженої роботи усіх складових мережі, а також різних мереж між собою необхідно додержуватися вимог відповідних стандартів. *Основною моделлю, яка забезпечує формування та якісну передачу даних між комп'ютерами, на сьогодні є OSI* (Open System Interconnection). Модель складається з кількох послідовних рівней перетворення інформації від зручного для оператора вигляду до сукупності дискретних сигналів "1" та "0" (прикладний, представницький, сеансовий, транспортний, мережевий, канальний та фізичний рівні).

Кожний рівень відносно незалежний, займає чітку позицію в ієрархічній структурі формування і передачі даних, а також легкозамінний. Для взаємодії між двома сусідніми рівнями встановлені відповідні правила – апаратно-програмний інтерфейс. Для взаємодії повідомлень між однаковими рівнями встановлені правила, які називаються протоколом обміну (*в загальному випадку протокол обміну – це стандарт, що визначає порядок формування, передачі та прийому повідомлень для взаємодії ПК один з одним на відповідних рівнях перетворення інформації*).

Слід додати, що на даний час всі 7 рівнів перетворення інформації зустрічаються рідко, найчастіше використовуються певні комбінації з 4-5 рівнів з різними обмовками.

Набір протоколів, достаніх для роботи в мережі, називається стеком.

4.2. Інтернет-технології та послуги в управлінні

Загальні відомості

Інтернет – це всесвітня система об'єднаних комп'ютерних мереж для зберігання і передачі інформації. Часто згадується як *Всесвітня мережа* або *Глобальна мережа* і навіть просто *Мережа*. Побудована на базі стека протоколів TCP/IP. На основі Інтернета працює Всесвітня павутина (World Wide Web, WWW) та багато інших систем передачі даних.

В середині 2018 року кількість користувачів Мережею досягло 4,5 млрд. Багато в чому це зумовлено широким розповсюдженням сотових мереж з доступом до Інтернету в стандартах 3G і 4G, развитком соціальних мереж і здешевленням вартості Інтернет-трафіка.

На даний час підключитися до Інтернету можна через супутники зв'язку, радіоканали, кабельне телебачення, телефон фіксованого зв'язку, сотовий зв'язок, спеціальні оптико-волоконні лінії або навіть провода електроживлення. Мережа стала невід'ємною частиною життя як в розвинених, так і в країнах, що розвиваються.

Інтернет складається з багатьох тисяч корпоративних, наукових, урядових і домашніх комп'ютерних мереж. Об'єднання мереж різної архітектури і топології стало можливо завдяки протоколу IP (Internet Protocol) і принципу маршрутизації пакетів даних за протоколом TCP (Transmission Control Protocol).

Протокол IP з'явився як результат внутрішніх дискусій в організації IETF (*Internet Engineering Task Force*), назву якої можна вільно перекласти як "Група розв'язку задач з проектування Інтернету". IETF та її робочі групи й досі займаються розвитком протоколів Мережі.

Послуги Інтернет

Зараз найбільш популярні *такі послуги Інтернету*: Веб-форуми, Блоги, Вікі-проекти (і, зокрема, Вікіпедія), Інтернет-магазини, Інтернет-аукціони, Соціальні мережі, Електронний підпис, Групи новин (в основному, Usenet), Електронні платіжні системи, Інтернет-радіо, Інтернет-телебачення IPTV, IP-телефонія, Месенджери, Пошукові системи, Інтернет-реклама , Віддалені термінали та управління, інші послуги.

Перегляд веб-сторінки здійснюється за допомогою спеціального редактора об'єктів – *браузера*. Браузер – це комп'ютерна програма у вигляді зручного для користування вікна. На даний час існує доволі багато браузерів, найбільш

популярні серед них в Україні Google, Opera, Mozilla Firefox, Safari. Переважною мовою Інтернету є англійська. На другому місці російська мова.

За результатами досліджень, більшість ресурсів Інтернету так чи інакше зв'язані з комерційною діяльністю. Мережа використовується для реклами і безпосереднього продажу товарів і послуг, для маркетингових досліджень, управління банківськими рахунками.

Згідно з доповіддю Oxford Economics, загальний обсяг електронної торгівлі товарами і послугами, а також ринок цифрових продуктів і послуг в сукупності оцінюється у всесвітньому масштабі більше 20 трильйонів доларів США, що становить приблизно 15% всесвітнього обсягу продажу.

За жанрами Інтернет-видання не відрізняються від офлайнових – є новинні сайти, літературні, науково-популярні, дитячі, жіночі та т.п. Однак, якщо офлайнові видання випускаються періодично (раз в день, тиждень, місяць), то Інтернет-видання оновлюються у міру появи нового матеріалу.

Завдяки розвитку Інтернет-ЗМІ, кількість людей, що віддають перевагу читати паперову пресу, з кожним роком скорочується.

Спочатку, коли Інтернет розвивався стихійно, розповсюдження інформації практично було вільне. Але на етапі перетворення його в глобальну мережу керівники держав стали проявляти інтерес до його функціонування. Оскільки в Інтернеті присутні інформаційні ресурси, які бувають незручні для деяких урядів, то останні намагаються декларувати Інтернет як засіб масової інформації з усіма обмеженнями.

Дійсно, у багатьох країнах такі обмеження існують на державному рівні (наприклад, заборона доступу до окремих ЗМІ, порнографічних сайтів, сайтів із закликами до насильних дій та ін.) або певні обмеження до всієї мережі. Одним із прикладів може служити реалізований в КНР проект "Золотий щит" – система фільтрації трафіку на Інтернет-каналі між провайдерами та міжнародними мережами передачі інформації.

Але насправді Інтернет – це тільки носій, інформаційне середовище, як телефонна мережа або просто папір. Як не дивно, на даний час можливості цензури обмежені – жодна держава в світі не наважилася повністю відключити внутрішні мережі від зовнішніх. У той же час багато інформаційних ресурсів офіційно піддаються цензурі (модерації) щодо опублікованої ними інформації в залежності від проведеної політики і власних внутрішніх правил. Це, з одного боку, не суперечить принципам свободи слова, з іншого боку, створює можливість розміщати в Інтернет фільтровану інформацію, яка не в повній мірі відображає дійсність.

За обмеженістю обсягу посібника розглянемо стисло три достатньо розповсюджених на даний час управлінських технологій на основі Internet, зокрема IP-телефонію, електронні платежі, електронний підпис.

IP-телефонія

Під IP-телефонією розуміється технологія, яка дозволяє використовувати Internet або іншу IP-мережу для ведення телефонних розмов і передачі факсів в режимі реального часу за допомогою відповідного серверу. Принцип дії серверів IP-телефонії наступний: з однієї сторони, сервер зв'язаний з телефонною мережею загального користування і, в принципі, може з'єднатися з будь-яким телефонним номером, з другої сторони, сервер зв'язаний з Internet і, в принципі, може з'єднатися з будь-яким комп'ютером. Сервер приймає повідомлення у вигляді стандартного телефонного сигналу, оцифровує його (якщо він не цифровий), стискує, розбиває на пакети (у відповідності до протоколу TCP/IP) і відправляє ці пакети через Internet до сервера одержувача повідомлення. Цей сервер здійснює усі перетворення у зворотному порядку (об'єднання пакетів – декомпресія – демодуляція) і посилає телефонний сигнал безпосередньо до одержувача.

Електронні платежі

Електронні платежі – це швидкий обмін даними щодо грошових переміщень (замовлення, рахунки, перекази і т.д.), а також власне електронний переказ грошей. Такий спосіб платежів користується у населення зростаючим попитом і на сьогодні здійснюються трьома способами:

- платежі традиційні, а підтвердження висилаються по електронній пошті (принципово, може бути навпаки);
- електронним способом передаються номера кредитних карток з наступним використанням смарт-карт (карта із мікросхемою, в яку занесені дані про користувача) для одержання грошей з банкомату;
- електронним способом передаються зашифровані серійні номера, які відповідають реальним грошам. Ці гроші тимчасово вилучаються з обігу і пересилаються до банківської установи одержувача. Сам одержувач отримує гроші відразу після надходження номерів.

Електронний підпис

Для виключення можливості підміни одного повідомлення іншим, в кінці повідомлення ставиться контрольна сума. Алгоритми розрахунку суми такі, що для кожного повідомлення утворюється своя, унікальна сума. Ця сума шифрується закритим ключем, після чого перетворюється в електронний

підпис. *Розшифрувати підпис за допомогою відкритого ключа може хто завгодно, але створити підпис може тільки власник закритого ключа*. Для виключення повторного використання цього підпису іншою особою, крім контрольної суми шифрується порядковий номер використання.

4.3. Класифікація мережевих атак

Для оцінки типів атак, які відбуваються в мережі Інтернет, необхідно знати деякі обмеження, властиві Інтернет-протоколу TPC/IP. Інтернет, в першу чергу, створювався для зв'язку між державними установами та університетами з метою надання допомоги навчальному процесу та науковим дослідженням. В результаті в специфікаціях ранніх версій Інтернет-протоколу були відсутні вимоги безпеки. Саме тому багато реалізацій IP-частини є вразливими.

Через багато років, після безлічі рекламацій, все реалізації протоколу стали доповнюватися різноманітними мережевими процедурами, послугами і продуктами, що знижують ризики безпеки. Далі коротко розглядаються типи атак, які зазвичай застосовуються проти мереж IP, а також надаються способи боротьби з ними.

1. Сніфер пакетів. Сніфер пакетів є прикладною програмою, яка використовує мережеву карту, що працює в режимі promiscuous mode (тобто, всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки). При цьому сніфер перехоплює всі мережеві пакети, які передаються через певний домен. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Однак з огляду на те, що деякі мережеві додатки передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніфера можна дізнатися про корисну, а іноді і конфіденційну інформацію.

Якщо додаток працює в режимі "клієнт-сервер", а аутентифікаційні дані передаються по мережі в текстовому форматі, який легко читається, то цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів. Хакери чудово уявляють собі, що ми користуємося одним і тим же паролем для доступу до безлічі ресурсів, і тому їм часто вдається, отримавши пароль, здійснити доступ до важливої інформації. У найгіршому випадку хакер може отримати доступ до призначеного для користувача ресурсу на системному рівні і з його допомогою створити нового користувача, якого можна в будь-який момент

використати для доступу в Мережу і до її ресурсів. Про те, як можна знизити загрозу сніфера пакетів, надано далі.

• **Аутентифікація**. Прикладом такої аутентифікації є одноразові паролі (One-Time Passwords, OTP).

OTP - це технологія двофакторної аутентифікації, при якій відбувається поєднання того, що у вас є, з тим, що ви знаєте. Типовим прикладом двофакторної аутентифікації є робота звичайного банкомату, який пізнає користувача, по-перше, по його пластиковій картці, а по-друге, по його пін-коду. Для аутентифікації в системі OTP також потрібні пін-код і особиста картка.

Під "карткою" (token) розуміється апаратний або програмний засіб, що генерує (за випадковим принципом) унікальний одномоментний одноразовий пароль. Якщо хакер дізнається про даний пароль за допомогою сніфера, то ця інформація буде марною, оскільки в цей момент пароль вже буде використаний і виведений з вжитку. Відзначимо, що такий спосіб боротьби зі сніфером ефективний тільки в випадках перехоплення паролів. Сніфери, перехоплюючі іншу інформацію (наприклад, повідомлення електронної пошти), не втрачають своєї ефективності.

• **Комутована інфраструктура**. Якщо, наприклад, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіку, що надходить на той порт, до якого вони підключені. Коммутована інфраструктура не усуває загрози сніфера, але помітно знижує її гостроту.

• **Антісніфери**. Третій спосіб боротьби зі сніфером полягає в установці апаратних або програмних засобів, які розпізнають сніфери, що працюють у вашій мережі. Ці засоби не можуть повністю ліквідувати загрозу, але, як і багато інших засобів мережевої безпеки, вони включаються в загальну систему захисту. Антісніфери вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік. Один з таких засобів, що поставляється компанією LOpht Heavy Industries, називається AntiSniff.

• **Криптографія**. Це найефективніший спосіб боротьби зі сніфером, який хоча і не запобігає перехопленню і не розпізнає роботу хакера, але робить таку роботу марною. Якщо канал зв’язку є криптографічно захищеним, то хакер перехоплює не повідомлення, а зашифрований текст (тобто незрозумілу послідовність бітів). До інших криптографічних протоколів мережевого управління відносяться протоколи SSH (Secure Shell) і SSL (Secure Socket Layer).

2. IP-спуфінг. Спуфінг відбувається в тому випадку, коли хакер, який знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача. Це можна зробити двома способами: хакер може скористатися або IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або за допомогою авторизованою зовнішньою адресою, якій дозволяється доступ до певних мережевих ресурсів. Як правило, IP-спуфинг обмежується вставкою неправдивої інформації або шкідливих команд у звичайний потік даних, переданих між клієнтським і серверним додатком, або по каналу зв'язку між однорангових пристроями. Для двостороннього зв'язку хакер повинен змінити все таблиці маршрутизації, щоб направити трафік на завідомо помилкову IP-адресу. Деякі хакери, проте, навіть не намагаються отримати відповідь від додатків, оскільки при головному завданні – отримати від системи важливий файл – відповіді додатків не мають значення. Якщо ж хакеру вдається поміняти таблиці маршрутизації і таки направити трафік на помилкову IP-адресу, він отримає все пакети і зможе відповідати на них так, як ніби є санкціонованим користувачем. Загрозу спуфінга можна послабити (але не усунути) за допомогою перерахованих нижче заходів.

• **Контроль доступу.** Найпростіший спосіб запобігання спуфінгу полягає в правильному підборі управління доступом. Щоб знизити ефективність IP-спуфінга, треба налаштуватие контроль доступу на відсікання будь-якого трафіку, що надходить із зовнішньої мережі в середину мережі, що підлягає захисту. Правда, це допомагає боротися з IP-спуфінгом, коли санкціонованими є тільки внутрішні адреси. Якщо ж санкціонованими є і деякі адреси зовнішньої мережі, даний метод стає неефективним.

• **Фільтрація RFC 2827**. В даному випадку необхідно відбракувати будь-який вихідний трафік, початкова адреса якого не є однією з IP-адрес організації, яку підлягає захисту. Даний тип фільтрації має назву RFC 2827 і може виконуватися безпосередньо провайдером організації (ISP). В результаті відбраковується весь трафік, який не має вихідної адреси, очікуваної на певному інтерфейсі. Наприклад, якщо ISP надає з'єднання з IP-адресою 15.1.1.0/24, він може налаштувати фільтр таким чином, щоб з даного інтерфейсу на маршрутизатор ISP допускався тільки трафік, що надходить з адреси 15.1.1.0/24.

Відзначимо, що до тих пір, поки всі провайдери не впровадять цей тип фільтрації, його ефективність буде набагато нижче можливої. Окрім того, чим далі від фільтрованих пристроїв, тим важче проводити точну фільтрацію.

Найбільш ефективний метод боротьби з IP-спуфінгом такий самий, що і у випадку зі сніфінгом пакетів: необхідно зробити атаку абсолютно неефективною. IP-спуфінг може функціонувати тільки за умови, що аутентифікація відбувається на базі IP-адрес. Тому впровадження додаткових методів аутентифікації робить подібні атаки марними. Кращим видом додаткової аутентифікації є криптографічний. Якщо вона неможлива, хороші результати може дати двофакторна аутентифікація з використанням одноразових паролів.

3. Відмова в обслуговуванні. Denial of Service (DoS), без сумніву, є найбільш відомою формою хакерських атак. Проти атак такого типу найважче створити стовідсотковий захист. Хоча серед хакерів атаки DoS вважаються дитячою забавою, оскільки для їх організації потрібен мінімум знань і умінь, проте саме простота реалізації і величезні масштаби завданої шкоди змушують адміністраторів мережевої безпеки приділяти цим атакам серйозну увагу.

Атаки DoS не націлені ні на отримання доступу до мережі, ні на отримання з цієї мережі будь-якої інформації. Але атака DoS робить мережу недієздатною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або прикладних програм. У разі використання деяких серверних додатків (таких як Web- або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих додатків, і тримати їх в зайнятому стані, не допускаючи обслуговування рядових користувачів.

В ході атак DoS можуть використовуватися такі звичайні Інтернет-протоколи, як TCP і ICMP (Internet Control Message Protocol). Більшість атак DoS розрахована не на програмні помилки або проломи в системі безпеки, а на загальні слабкості системної архітектури. Деякі атаки зводять до нуля продуктивність мережі, переповняючи її небажаними і непотрібними пакетами або повідомляючи помилкову інформацію про поточний стан мережевих ресурсів. Даному типу атак важко запобігти, так як для цього потрібно координація дій з провайдером. Якщо провайдер не зупинить шкідливий трафік у себе, то зробити це на вході в мережу вже неможливо, оскільки вся смуга пропускання буде зайнята.

Коли атака даного типу проводиться одночасно через безліч пристроїв, ми говоримо про розподілену атаку DoS (distributed DoS – DDoS). Загроза атак типу DoS / DDoS може бути знижена нижченаведеними способами.

• **Функції антиспуфінга**. Правильна конфигурація функцій антиспуфінга на маршрутизаторах і міжмережевих екранах доможе зменшити ризик DoS. Ці функції як мінімум мають включати фільтрацію RFC 2827. Якщо хакер не зможе замаскувати свою справжню особистість, він навряд чи наважиться провести атаку.

• **Функції анти-DoS**. Правильна конфигурація функцій анти-DoS на маршрутизаторах і межмережевих екранах здатна обмежити ефективність атак. Ці функції часто зменшують кількість напіввідкритих каналів в будь-який момент часу.

• **Обмеження обсягу трафіку** (traffic rate limiting). Організація може звернутися до провайдера (ISP) з метою обмеження обсягу трафіку. Такий тип фільтрації дозволяє обмежити обсяг некритичного трафіку, що проходить через мережу (наприклад, ICMP), який використовується тільки для діагностичних цілей. Атаки DoS/DDoS часто використовують ICMP.

4. Парольні атаки. Хакери можуть проводити парольні атаки за допомогою цілого ряду методів, таких як простий перебір (brute force attack), троянський кінь, IP-спуфінг і сніфер пакетів. Окрім того, хакери нерідко намагаються підібрати пароль і логін, використовуючи для цього спеціальні програми, які намагаються отримати доступ до ресурсу загального користування (наприклад, до сервера). Якщо в результаті хакеру надається доступ до ресурсів, то він отримує його на правах звичайного користувача і може створити собі “прохід” для майбутнього доступу, навіть якщо користувач змінить свої пароль і логін.

Ще одна проблема виникає, коли користувачі застосовують один і той же (нехай навіть дуже хороший) пароль для доступу до багатьох систем: до корпоративної, персональної і до систем Інтернету. Оскільки стійкість пароля дорівнює стійкості самого слабкого хоста, то хакер, що довідався пароль через цей хост, отримує доступ до всіх інших систем, де використовується той самий пароль.

Парольних атак можна уникнути, якщо не користуватися паролями в текстовій формі. Одноразові паролі і/або криптографічна аутентифікація можуть практично звести нанівець загрозу таких атак. На жаль, не всі програми, хости і пристрої підтримують вищезгадані методи аутентифікації. При використанні звичайних паролів треба придумати такий, який було б важко підібрати. Мінімальна довжина пароля повинна бути не менше восьми символів. Пароль повинен включати символи верхнього регістру, цифри та спеціальні символи (#, %, $ і т.д.).

5. Атаки типу Man-in-the-Middle. Для атаки типу Man-in-the-Middle хакеру потрібен доступ до пакетів, що передаються через мережу. Такий доступ можна, наприклад, отримати від співробітника цього провайдера та за допомогою сніфера пакетів. Атаки проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережевих ресурсів, для аналізу трафіку і отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії.

Ефективно боротися з атаками типу Man-in-the-Middle можна тільки за допомогою криптографії. Якщо хакер перехопить зашифровані дані, у нього на екрані з'явиться замість перехопленого повідомлення безглуздий набір символів. Відзначимо, що якщо хакер отримає інформацію про ключ сесії, то це може зробити можливою атаку Man-in-the-Middle навіть в зашифрованому середовищі.

6. Атаки на рівні додатків. Такі атаки можуть проводитися кількома способами. Найпоширеніший з них – використання добре відомих слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP). Використовуючи ці слабкості, хакери можуть отримати доступ до комп'ютера від імені користувача, що працює з додатком (зазвичай це буває не простий користувач, а привілейований адміністратор з правами системного доступу). Відомості про атаки на рівні додатків широко публікуються, щоб дати адміністраторам можливість виправити проблему за допомогою корекційних модулів (патчів). На жаль, багато хакерів також мають доступ до цих відомостей, що дозволяє їм вдосконалюватися.

Головна проблема при атаках на рівні додатків полягає в тому, що хакери часто користуються портами, яким дозволений прохід через міжмережевий екран. Наприклад, хакер, який експлуатує відому слабкість Web-сервера, часто використовує в ході атаки TCP порт 80. Оскільки web-сервер надає користувачам Web-сторінки, то міжмережевий екран повинен забезпечувати доступ до цього порту. З точки зору брандмауера атака розглядається як стандартний трафік для порту 80. Повністю виключити атаки на рівні додатків неможливо. Хакери постійно відкривають і публікують в Інтернеті нові вразливі місця прикладних програм. Найголовніше тут – якісне системне адміністрування.

7. Мережева розвідка. Мережевою розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних і додатків. При підготовці атаки проти будь-якої мережі хакер, як правило, намагається отримати про неї

якомога більше інформації. Мережева розвідка проводиться у формі запитів DNS, відлуння-тестування і сканування портів.

Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену привласнені. Відлуння-тестування адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в даному середовищі. Отримавши список хостів, хакер використовує засоби сканування портів, щоб скласти повний список послуг, що надаються цими хостами.

Далі хакер аналізує характеристики додатків, що працюють на хостах, в результаті чого він може добути інформацію, яка придатна для злому. Повністю позбавитися від мережевої розвідки неможливо. Якщо, наприклад, відключити відлуння ICMP і відлуння-відповідь на периферійних маршрутизаторах, то можна позбутися відлуння-тестування, але втратити дані, необхідні для діагностики мережевих збоїв. Окрім того, сканувати порти можна і без попереднього відлуння-тестування – просто це займе більше часу, оскільки сканувати доведеться і неіснуючі IP-адреси.

Системи IDS на рівні мережі і хостів зазвичай добре справляються з функцією повідомлення адміністратора про те, що ведеться мережева розвідка. Це дозволяє краще підготуватися до майбутньої атаки і оповістити провайдера (ISP), в мережі якого встановлена система, що проявляє надмірну цікавість.

Ця система бореться тільки з атаками проти одного хоста. У своїй роботі системи IDS користуються сигнатурами атак, які представляють собою профілі конкретних атак або типів атак. Сигнатури визначають умови, при яких трафік вважається хакерським.

Аналогами IDS в фізичному світі можна вважати систему попередження або камеру спостереження. Найбільшим недоліком IDS є їх здатність генерувати сигнали зайвої тривоги. Щоб мінімізувати кількість хибних сигналів тривоги і домогтися коректного функціонування системи IDS в мережі, необхідна ретельна настройка цієї системи.

8. Зловживання довірою. Власне кажучи, цей тип дій не є в повному розумінні слова атакою або штурмом. Він являє собою зловмисне використання відносин довіри, існуючих в мережі. Класичним прикладом такого зловживання є ситуація в периферійній частині корпоративної мережі. У цьому сегменті часто розташовуються сервери DNS, SMTP і HTTP. Оскільки всі вони належать до одного і того ж сегменту, злом будь-якого з них призводить до злому всіх інших, так як ці сервери довіряють іншим системам своєї мережі.

Іншим прикладом є встановлена з зовнішнього боку брандмауера система, що має відношення довіри з системою, встановленою з його внутрішньої сторони. У разі злому зовнішньої системи хакер може використовувати відносини довіри для проникнення в систему, захищену брандмауером.

Ризик зловживання довірою можна знизити за рахунок більш жорсткого контролю рівнів довіри в рамках своєї мережі. Системи, розташовані з зовнішньої сторони брандмауера, ні за яких умов не повинні користуватися абсолютною довірою з боку захищених екраном систем. Відносини довіри повинні обмежуватися певними протоколами і, по можливості, аутентифікуватися не тільки за IP-адресами, а й за іншими параметрами.

9. Віруси і додатки типу "троянській кінь". Робочі станції кінцевих користувачів дуже вразливі для вірусів і троянських коней. Вірусами називаються шкідливі програми, які впроваджуються в інші програми для виконання певної небажаної функції на робочій станції кінцевого користувача. Як приклад можна привести вірус, який прописується у файлі command.com (головному інтерпретаторі систем Windows) і стирає інші файли, а також заражає всі інші знайдені ним версії command.com.

Троянський кінь – це не програмна вставка, а справжня програма, яка на перший погляд здається корисним додатком, а на ділі виконує шкідливу роль. Прикладом типового троянського коня є програма, яка виглядає, як проста гра для робочої станції користувача. Однак поки користувач грає, програма відправляє свою копію електронною поштою кожному абоненту, занесеному в адресну книгу цього користувача. В результаті всі абоненти, самі того не бажаючи, отримують цю гру, викликаючи її подальше поширення.

4.4. Основи інформаційної безпеки при роботі ПК в мережі

Якщо у великих IT-компаніях (наприклад, в галузевих обчислювальних центрах, державних установах, в компаніях фінансової сфери) захистом інформації займаються окремі відділи або служби, то у випадку роботи в невеликій організації (а їх кількість значна) ступінь захищеності ПК набагато менша, оскільки робота практично контролюється самими користувачами.

Існуючі в цьому випадку загрози можна умовно поділити на фізичні, програмно-апаратні та організаційні.

Фізичні загрози включають: крадіжку даних на носіях або всієї системи; випадкове спостереження секретної інформації на дисплеї ПК; крадіжку

надрукованих документів і незаконне використання клавіатури або інших пристроїв введення для проникнення через засоби контролю безпеки і т.п.

Програмно-апаратні загрози включають: підрив операційної системи або її управління за допомогою незаконного (несанкціонованого) використання клавіатурного введення; підрив системи контролю ПК через віддалений доступ , використовуючи мережеве з'єднання; розміщення троянських коней і часових бомб, які надійшли разом з вільним або придбаним ПЗ; втрату секретності даних в результаті несанкціонованого навмисного або випадкового перегляду файлів даних, які можуть перебувати на жорсткому диску ПК або на файл-сервері ЛОМ. Крім того розроблені вірусні програми, які можуть подорожувати по мережі від одного комп'ютера до іншого, попутно руйнуючи файли, або отримуючи управління операційною системою.

Організаційні загрози включають: розкриття даних через те, що користувач, недооцінивши значення локально створеної інформації, забув провести класифікацію відповідно до стандартів підприємства і забезпечити захист; вторгнення в контрольовані файли або робочі області через легко вгадувані паролі або тривале використання старих паролів, які вже розкриті; втрату або виявлення секретної інформації через те, що мережевий принтер недостатньо захищений, або користувачі ПК не забрали або не захистили надруковані документи; відсутність плану на випадок форс-мажорних обставин, таких як пожежа, крадіжка, втрата даних внаслідок технічних помилок файлової системи та ін.

Новий рівень ризику виникає, коли співробітники працюють вдома через мережеве з'єднання зі своїм відділом або сервером баз даних. Порядок в цьому випадку майже цілком грунтується на добрій волі співробітників слідувати правильній процедурі.

Комп'ютери в звичайній комерційній фірмі знаходяться в приміщеннях, які практично відвідуються вільно. Слід відмітити цікавий факт: в більшості випадків комплекс ПК середньої фірми, з'єднаний з ЛОМ, яка зв'язана з файл-серверами, комунікаційними серверами і принтерами, є значно потужнішим, ніж комплекс середнього обчислювального центру. Однак там немає технічного штату з безпеки, немає центральної програмної системи безпеки, що має налагоджений супровід з профілями авторизованих користувачів, немає навіть закритих приміщень, куди дозволений доступ тільки авторизованому персоналу. *Замість цього вся відповідальність покладається на колектив групи користувачів. Вони самі собі керівники обчислювального центру та посадові особи з безпеки*.

Тому керівництво повинно забезпечити процес, який гарантує потрібний рівень якості інформації з урахуванням викладеного матеріалу, відповідних стандартів та наявних нормативних документів. А задача усіх співробітників таких фірм вимоги керівництва, стандартів і нормативних документів виконувати.

4.5. Кібербезпека та інформбезпека. Кіберполіція

Цифрові технології таять в собі не тільки переваги, а й загрози, причому найбільшою з них для організацій є кібератаки. Давно минули часи, коли власники компаній могли вирішити проблеми ІБ, звертаючись при необхідності до своїх ІТ-фахівців. Сьогодні це стало настільки серйозною проблемою, що компанії повинні впроваджувати техніку, ПЗ і належні протоколи безпеки інформації, запрошуючи сторонні організації і/або фахівців. Ось на цій стадії і виникли терміни "кібер-" та "інформаційна безпека".

Під кібербезпекою (КБ) розуміють практику захисту конфіденційної інформації і даних компанії від несанкціонованого доступу шляхом впровадження засобів захисту всієї комп'ютерної системи (КС) – від входу в зовнішню мережу до робочих станцій, в т.ч. всю інфраструктуру, пов'язану з прийомом/передачею та обробкою даних. Ідея полягає в тому, щоб, як мінімум, пом'якшити ці загрози не тільки для себе, а й для своїх клієнтів.

Простіше кажучи, кібербезпека – це підмножина інформційної безпеки, яка пов'язане із захистом цифрових даних від несанкціонованого цифрового доступу. А інформаційна безпека – це захист інформаційних активів організацій будь-якого типу (в тому числі компаній малого бізнесу), незалежно від форми зберігання активів.

Потенційні хакери знають, що малий бізнес більш вразливий перед кіберзагрозами, оскільки тут, на відміну від великих корпорацій, які багато інвестують в технології і стратегії безпеки, ресурсів не вистачає. Однак практика показує, що малий бізнес, який в розвинених країнах має значну питому вагу в економіці, пов'язаний і з великими корпораціями, і з державними структурами.

Звідси випливає, що захист інформації та даних сьогодні повинен бути одним з найбільш пріоритетних завдань в системі управління. Процедури і політика безпеки, що захищають цифрові мережі і комп'ютерні системи, швидко змінюються, тому ІТ-фахівцям необхідно бути весь час в курсі останніх заходів захисту інформації, щоб краще захистити свій кіберпростір.

Ілюстративно вищенаведене пояснюється на рис. 4.2.

Рис. 4.2. Спрощена структурна схема щодо місця КБ в системі ІТ-ІБ

Для боротьби з кіберзагрозами в 2017 в Україні створена кіберполіція.

Що таке кіберполіція ?

Кіберполіція – це новий підрозділ національної поліції України (*Департамент кіберполіції*), який є міжрегіональним територіальним органом Національної поліції України. Він входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень та механізмів їх підготовки, що передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних Інтернет-мереж і систем.

Згідно чинної Стратегії кібербезпеки України на Національну поліцію України покладені такі основні завдання:

1. Реалізація державної політики у сфері протидії кіберзлочинності.

2. Завчасне інформування населення про появу новітніх кіберзлочинів.

3. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.

4. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.

5. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

6. Участь у міжнародних операціях в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

7. У сфері використання платіжних систем:

❖ протидія скімінгу (шимінгу) – незаконному копіювання змісту треків магнітної смуги (чипів) банківських карток;

❖ протидія кеш-трепінгу – викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;

❖ протидія кардінгу – незаконним фінансовим операціям з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем;

❖ протидія несанкціонованному списанню коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

8. У сфері інформаційної безпеки – протидія маніпулюванню людьми шляхом соціальної інженерії. Соціальна інженерія – це технологія управління (маніпулювання) людьми в Інтернет просторі через виконання дій (“листи щастя”), або розголошення конфіденційної інформації іншим способом, ніж як через засоби технічного руйнування баз даних.

9. У сфері інформаційної безпеки:

❖ протидія створенню та розповсюдженню вірусів і шкідливого програмного забезпечення;

❖ протидія розміщенню контенту, який пропагандує

екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

10. У сфері інтелектуальної власності:

❖ протидія піратству – незаконному розповсюдженню інтелектуальної власності в Інтернеті;

❖ протидія кардшарінгу – надання незаконного доступу до перегляду супутникового та кабельного TV;

11. У сфері електронної комерції та господарської діяльності:

❖ протидія онлайн-шахрайству – заволодінню коштами громадян через інтернет-аукціони, -магазини, -сайти та телекомунікаційні засоби зв'язку.

❖ протидія фішингу – виду шахрайства побудований на надсиланні листа, ніби від банку чи іншої установи, в якому міститься запит щодо вашої конфіденційної у інформації, яка необхідна шахраю. При цьому приводи для надсилання такої інформації можуть бути різними, наприклад, відновлення бази даних після її випадкової втрати.

4.6. Хакери на кілька кроків випереджають експертів з КБ

Зловмисникам не треба активно розвиватися, оскільки старі практики НСД чудово працюють і на даний час. *Експерти з безпеки не встигають за шкідливими атаками не через брак бажання або навичок, а просто час працює проти них*. У 9-му щорічному звіті про дослідження зломів баз даних від Verizon аналізуються більш 100000 інцидентів безпеки і 3000 підтверджених витоків баз даних за минулий рік. При складанні звіту дослідники спиралися на реальні викрадення даних, з якими стикалися або Verizon, або близько 50-ти інших організацій. Серед цих організацій варто

окремо виділити Секретну службу США, Європейський центр кіберзлочинів (ЕСЗ), Британську групу реагування на кіберзагрози (UK CERT) і Ірландську Службу кібербезпеки (IRISS CERT).

Згідно зі звітом, в понад 99% атак зловмисники зламували системи за кілька днів (4 з 5 атак займали хвилини), і дві третини атак, в ході яких були викрадені дані, тривали кілька днів (кожна п'ята також тривала кілька хвилин). Це означає, що *злочинці встигають викрасти все необхідне і сховатися перш, ніж будь-хто встигне зреагувати*. Крім іншого, *злом виявляє навіть не жертва, а третя сторона* (дослідник безпеки або правоохоронні органи). Майже дві третини всіх кіберзлочинів можливі завдяки ненадійним або викраденим паролям доступу.

Як стверджують в The Register з посиланням на співробітника Verizon, хакери почали використовувати множинні точки ексфільтрації, щоб уникнути виявлення системами безпеки. *У більшості зломів найчастіше використовується фішинг*. Майже третина фішингових листів відкривається, і принаймні один з десяти одержувачів відкриває вкладення. Основними винуватцями атак є організовані кримінальні угруповання, а одна з десяти атак відбувається на замовлення держави. На частку Китаю припадає більше половини всіх атак, зв'язаних з кібершпіонажем.

Головними жертвами кібершпіонажу стають державний сектор, компанії по виробництву і надання послуг. Злочинці використовують фішингові листи і викрадені паролі для входу в корпоративну мережу. Далі шкідливе ПЗ завантажується в систему жертви. Однак, *якщо в організації для доступу до мережі використовується багатофакторна аутентифікація, корпоративну мережу складніше зламувати, навіть користуючись обліковими даними*.

4.7. Побудова системи управління ІБ/КБ: з чого почати?

В цьому розділі в спрощеному вигляді надається послідовність дій для системних адміністраторів компаній середнього і малого бізнесу, яким доводиться займатися створенням корпоративної системи управління інформаційною безпекою (СУІБ).

Аналіз ризиків

Практично усе в ІБ/КБ починається з аналізу ризиків, це основа и початок всіх процесів з безпеки. Тому згадаємо ще раз, що таке *ризик, ймовірність реалізації, вразливість*.

Ризик – це можливість понести будь-які втрати (грошові, репутаційні, конкурентоспроможні і т.д.) в зв'язку з існуючою вразливістю. *Імовірність реалізації* – це наскільки ймовірно, що дана вразливість буде успішно використана хакерами. *Уразливість* – це безпосередній пролом у системі безпеки, який з якоюсь часткою ймовірності може завдати шкоди організації.

Прийнятність ризику найкраще виражати в конкретних сумах втрат від його реалізації. Необхідно вирішити з керівництвом, яка сума втрат для них буде порогом прийнятності та зробити градацію з 3-5 рівнів. Далі зробити градацію з ймовірності, так само як за втратами, а потім оцінювати ризики за сумою цих показників.

Після проведення такої підготовчої роботи слід визначитися з реальними вразливостями організації і провести оцінку ризиків їх реаліції. У підсумку отримуємо 2 набори ризиків – прийнятних і неприйнятних. З прийнятними ризиками доведеться змиритися, а з неприйнятними є кілька варіантів розвитку подій, найпростіший – перекласти турботи про ризик на іншу особу (застрахувати організацію або передати актив, схильний до ризику в Дата-центр, де за безпеку сервера буде відповідати ця компанія.

Нормативна документація

Інформаційна безпека – це, в першу чергу, люди, яким потрібна певна нормативна документація. Основних документів для ІБ/КБ в цьому плані 3: *політика інформаційної безпеки*; *концепція інформаційної безпеки*; *положення про комерційну таємницю* (конфіденційну інформацію).

Політика інформаційної безпеки

Це основний документ, в якому описані всі процедури захисту, а також рівень безпеки, якого організація очікує. Образно кажучи це ідеальний зріз безпеки, задокументований і прийнятий за всіма правилами. Політика не повинна бути мертвим вантажем, документ має змінюватися під впливом нових загроз, віянь в ІБ або побажань. У зв'язку з цим політика повинна регулярно переглядатися на предмет актуальності не рідше 1 разу на рік.

Концепція інформаціної безпеки

Це невелика витримка з політики, де описані основи безпеки організації, немає ніяких конкретних процесів, але є принципи побудови СУІБ і принципи формування безпеки. Цей документ швидше іміджевий, він не повинен містити закриту інформацію і має бути доступним для всіх. Бажано розмістити його на сайті, вкласти в лоток на інформаційному стенді, що б клієнти організації і відвідувачі могли з ним ознайомитися або просто побачити.

Положення про комерційну таємницю (конфіденційну інформацію)

У цьому документі необхідно вказати наступне: як і де зберігаються документи, які становлять комерційну таємницю; хто відповідальний за зберігання цих документів; що буде за розголошення конфіденційної інформації (за законодавством і згідно з внутрішніми домовленостями з керівництвом). Ну і звичайно ж перелік відомостей, що становлять для організації комерційну таємницю або є конфіденційними.

Що б правильно написати зазначені вище документи, точніше, зрозуміти, що має в них бути, *потрібно провести аудит поточного стану ІБ*.

Політика доступу

Тут є дві гілки – фізичний доступ в приміщення і доступ в інформаційні системи (ІС).

Фізичний доступ. Необхідно описати систему контролю доступу (СКД). Обов'язково варто сказати про систему відеоспостереження, принципах її побудови (відсутність сліпих зон в спостережуваних приміщеннях, обов'язковий контроль входів і виходів в/з будівлі, контроль входу в серверну і т.п). Якщо немає загальної приймальні, необхідно вказати, яким чином відвідувачі потрапляють в контрольовану зону.

Для серверної повинен бути окремий перелік доступу з журналом відвідувань.

Доступ в ІС. Слід описати процедури видачі доступів і паролів (термін дії паролів, складність, кількість спроб входу, час блокування після перевищення кількості спроб) до всіх систем, в які видається доступ, і т.д.

Побудова мережі

Тут треба чітко усвідомити, де знаходяться сервера, що мають доступ зовні, як до них забезпечується доступ зсередини і зовні, чим забезпечується сегментація мережі, які сегменти захищаються за допомогою міжмережевих екранів, як захищаються робочі станції і т.п.

Віддалений доступ

Тут необхідно з'ясувати, як цей доступ організований і хто може їм користуватися. В ідеалі має бути так: тільки VPN, доступ тільки за погодженням з вищим керівництвом і з обгрунтуванням необхідності. Якщо потрібен доступ третім особам (вендори, обслуговуючий персонал і т.д.), він має бути обмеженим за часом, після якого доступ автоматично блокується.

Інциденти

В цьому випадку треба розібратися, як вони обробляються, хто відповідальний, як побудований процес інцидент-менеджменту і проблем менеджменту взагалі. Також необхідно визначитися з трендами в організації, тобто які інциденти виникають частіше, які несуть більшу шкоду. *Це допоможе у* контролі ризиків і *проведенні аналізу ризиків*.

Активи

В даному випадку під активами розуміється все, що вимагає захисту (сервера, інформація на папері або знімних носіях, жорсткі диски комп'ютерів і т.д). Якщо будь-які активи містять "службову" інформацію, то вони повинні бути відповідним чином промарковані і повинен бути перелік дозволених дій з цим активом (передача третім особам, передача по електронній пошті всередині, розміщення для публічного доступу зовні і т.д.).

Навчання

Момент, про який багато хто забуває. *Співробітникам потрібно періодично розповідати про заходи безпеки*. На практиці часто співробітники після чергового "інструктажу" просто розписуються, щоб відчепилися, не надто вникаючи в подробиці правил ІБ.

Окрім безпосереднього навчання, такі заходи корисні в плані спілкування між співробітниками і особами, відповідальними за ІБ. Можна дізнатися про якісь дрібні пригоди, побажання і навіть проблеми, про які в звичайному робочому ритмі вони б не дізналися.

Контрольні питання до розділу

1. Що таке комп'ютерна мережа?
2. Надайте класифікацію комп'ютерних мереж.
3. Що таке корпоративна мережа?
4. Що таке продуктивність та надійність мережі?
5. Що собою являє протокол обміну даними?
6. Поясніть суть моделі передачі даних OSI.
7. Поясніть суть протоколу обміну даними в Інтрнет TCP/IP.
8. Які недоліки мережі Інтернет ви можете назвати?
9. В чому різниця між інформаційною безпекою та кібербезпекою?
10. Чому на даний час хакери випереджають експертів з КБ?
11. Назвіть послідовність дій при побудові системи захисту від КБ.

РОЗДІЛ 5. ЗАГАЛЬНІ ВІДОМОСТІ З БАЗ ДАНИХ, СИСТЕМ УПРАВЛІННЯ БАЗАМИ ДАНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

5.1. Основні поняття з БД і СУБД

База даних (БД) являє собою сукупність структурованих даних, що зберігаються в пам'яті обчислювальної системи і відображають стан об'єктів та їх взаємозв'язків в предметній області.

Логічну структуру даних, які зберігаються в базі, називають моделлю даних. До основних моделей даних відносяться *ієрархічна, мережева, реляційна та ін*.

При використанні *ієрархічної моделі* зв'язки між даними можна відобразити за допомогою упорядкованого графа (рис. 5.1) або "дерева" (в IT цей термін так на практиці і закріпився: тип даних – дерево).

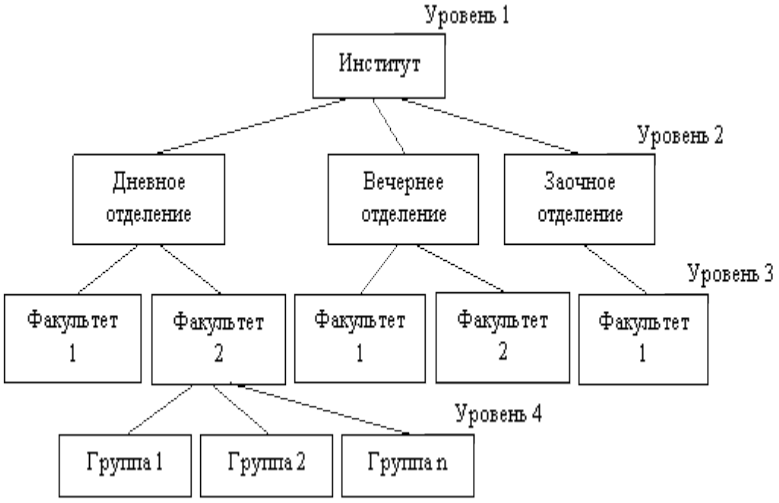


Рис. 5.1. Ієрархічна модель бази даних

Основними перевагами ієрархічної моделі даних є: ефективне використання пам'яті ЕОМ; висока швидкість виконання основнх операцій з даними; зручність роботи з ієрархічно упорядкованою інформацією.

До недоліків ієрархічної моделі даних відносять: громіздкість такої моделі для обробки інформації з достатньо складними логічними зв'язками; складність розуміння її функціонування для звичайних користувачів.

На ієрархічній моделі даних побудовано незначну кількість СУБД.

Мережева модель є подальшим розвитком і узагальненням ієрархічної моделі, яка дозволяє відобразити різноманітни зв'язки даних у вигляді певного графа. На відміну від ієрархічної моделі в мережевій присутні як вертикальні, так і горизонтальні (іноді просто довільні) зв'язки між даними.СУБД на основі мережевої моделі також не набули широкого поширення на практиці.

Реляційна модель представлення даних ґрунтується на понятті “взаємозв’язок” (relation). Найпростішим прикладом ставлення служить двовимірна таблиця (рис.5.2).

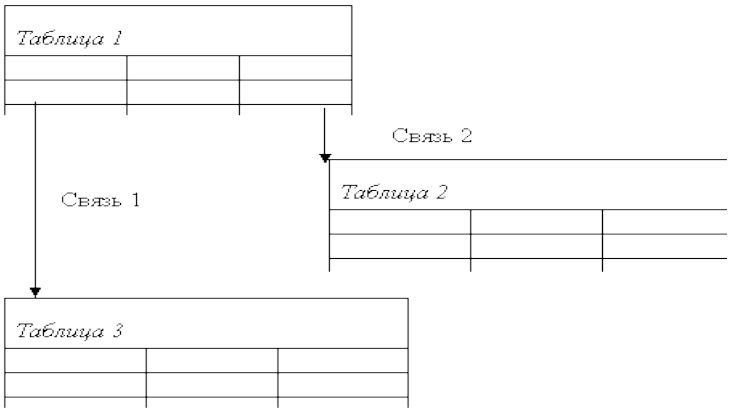


Рис. 5.2. Реляційна модель бази даних

Перевагою реляційної моделі даних (порівнянно з ієрархічною і мережевою моделями) є розуміння її побудови, простота і зручність практичної реалізації на ЕОМ.

До недоліків реляційної моделі слід віднести відсутність стандартних засобів ідентифікації окремих записів; складність опису ієрархічних і мережевих зв’язків, великий обсяг пам’яті, в якій дані зберігаються.

Система управління базами даних (СУБД) – це комплекс язикових і програмних засобів, призначений для створення, ведення і сумісного використання БД багатьма користувачами. Зазвичай СУБД розрізняють по використовуваній моделі даних. Так, якщо СУБД засноване на використанні реляційної моделі даних, то таку систему називають реляційною.

На даний час більшість СУБД побудовані саме на основі реляційної моделі (*наприклад, Visual FoxPro, Access, Oracle и др.).*

Для роботи з базою даних часто достатньо готових програмних продуктів, які знаходяться у вільному продажу. Однак якщо потрібно забезпечити зручність роботи з БД некваліфікованим користувачам або інтерфейс СУБД не влаштовує користувачів, то можуть бути розроблені додатки шляхом відповідного програмування.

Словник даних являє собою підсистему БД, призначену для централізованого зберігання інформації про структуру даних, взаємозв’язки файлів БД, типи даних і форматах їх подання, приналежності даних певним користувачам, розмежування доступу до системи і т. п.

СУБД зазвичай функціонують в архітектурі клієнт-сервер. В цьому випадку сама БД розміщується на комп'ютері-сервері, а до неї з робочих місць здійснюється сумісний доступ.

Сервером певного ресурсу в комп'ютерній мережі називають комп'ютер, який здійснює управління цим ресурсом, а клієнтом – комп'ютер, що використовує цей ресурс. В якості ресурсів комп'ютерної мережі можуть виступати, наприклад, бази даних, файли, служби друку, поштові служби.

Перевагою організації СУБД за архітектурою клієнт-сервер є вдале поєднання централізованого зберігання, обслуговування і колективного доступу до загальної корпоративної інформації з індивідуальною роботою користувачів. *Зокрема, при такому підході забезпечується висока надійність захисту оброблюваної інформації, зменшується час на її обробку, а обсуговування самої СУБД потребує менших витрат*.

Згідно з основним принципом архітектури клієнт-сервер, дані обробляються тільки на сервері. Користувач або додаток формують запити, які надходять до сервера БД у вигляді інструкцій мови SQL. Сервер бази даних забезпечує пошук і витяг потрібних даних, які потім передаються на комп'ютер користувача.

Виділяють наступні два варіанти реалізації СУБД: один ПК, на якому встановлена потрібна БД (наприклад, dBaseIV, Microsoft Access, Microsoft FoxPro); мережева система управління з багатьма користувачами і кількома базами даних: сервери БД (наприклад, Microsoft SQL Server, InterBase, Oracle), засоби розробки програм роботи з БД, робочі станції, мережеве обладнання, обслуговуючий персонал роботи з системою, користувачі.

У ролі клієнтських програм можуть використовуватися СУБД, електронні таблиці, текстові процесори, програми електронної пошти та ін.

За характером використання СУБД поділяють на *багатокористувацькі* (*промислові*) і *локальні* (*персональні*).

Промислові СУБД являють собою програмну основу для розробки автоматизованих систем управління великимими економічними об'єктами.

Персональні СУБД – це програмне забезпечення, орієнтоване на розв'язок задач локального користувача або їх невеликої групи, яке призначене для використання на персональному комп'ютері. Це пояснює їхню другу назву – настільні. Визначальними характеристиками настільних систем є: відносна простота експлуатації, що дозволяє створювати на їх основі працездатні користувальницькі додатки; відносно обмежені вимоги до апаратних ресурсів.

Для роботи з даними, що зберігаються в базі, використовуються наступні типи мов:

- мова опису даних – високорівнева мова декларативного типу, призначена для опису логічної структури даних;

- *мова маніпулювання даними* – сукупність конструкцій, що забезпечує виконання основних операцій з даними: введення, модифікацію і вибірку за запитами.

Названі мови в різних СУБД можуть мати відмінності. *Найбільше поширення набули дві стандартизовані мови: QBE* – мова запитів за зразком і *SQL* – структурована мова запитів. QBE в основному має властивості мови маніпулювання даними, SQL поєднує в собі властивості мов обох типів.

СУБД реалізує наступні основні функції низького рівня:

- управління даними у зовнішній пам'яті;
- управління буферами оперативної пам'яті;
- управління транзакціями;
- ведення журналу змін до БД;
- забезпечення цілісності і безпеки БД.

Реалізація функції управління даними у зовнішній пам'яті сприяє ефективному управлінню відповідними файлами з даними.

Необхідною умовою успішного функціонування БД є забезпечення її цілісності, особливо при мережевому використанні. Цілісність БД – це властивість бази, що означає несуперечливий і адекватний стан інформації в предметній області. Цілісність стану перевіряється за допомогою певних обмежень (умов).

Безпека БД досягається шифруванням даних, забороною користування даними для осіб, які не пройшли аутентифікацію та/або ідентифікацію, а також за допомогою інженерно-технічних засобів.

5.2. Класифікація ІС. Структура та етапи її функціонування

В загальному випадку ІС являє собою автоматизовану систему обробки інформації про деякий виробничий процес (об'єкт), в якій оброблена інформація по каналах зв'язку надходить до робочого місця, з якого здійснюється управління цим процесом (об'єктом). Іншими словами, ІС – це система, що включає три структурні складові:

- автоматизоване робоче місце обробки первинної інформації;
- канал зв'язку для передачі (прийому) обробленої інформації;

- керуючий елемент (частіше усього керівник певного рангу або особа, яка приймає рішення – ОПР).

В залежності від рівня автоматизації розрізняють ручні, автоматизовані й автоматичні ІС.

У ручних ІС значну частину операцій по обробці інформації виконує людина, причому переважна частина інформація отримується традиційним способом (з службових джерел, засобів масової інформації, по телефону тощо), а комп'ютерна обробка носить вибірковий характер за певними ділянками виробництва (найчастіше бухгалтерія, відділ кадрів, плановий відділ). Хоча такі системи сьогодні достатньо розповсюдженні на підприємствах, позитивного економічного ефекту самі по собі вони надати не можуть.

В автоматичних ІС практично усі функції управління й обробки даних виконують технічні засоби (наприклад, окремі системи руху на залізничному та авіатранспорті, системи підтримки технологічних параметрів в енергетиці).

В автоматизованих ІС невелику частину обробки даних і керуючих впливів виконує людина, але самі трудомісткі і складні операції основного виробництва виконує комп'ютер. На практиці найбільше поширення на підприємствах знайшли саме автоматизовані ІС управлінського типу.

За функціональними можливостями стосовно України можна виділити наступні види ІС:

1) *сервісно-орієнтовані системи* (наприклад, системи автоматизації й обробки результатів експерименту, системи моделювання процесів, системи розробки конструкторської та технологічної документацій, довідково-експертні системи, електронні словники, системи навчання та ін.);

2) *інформаційно-управляючі системи* для об'єктів як промислового, так і непромислового виду (наприклад, системи управління підприємствами, офісні системи, системи "банк-клієнт, інформаційні системи готелей, бірж, страхових компаній та ін.);

3) *суспільні системи* (наприклад, електронна пошта, телеконференції та "всесвітня павутина" в Internet, певні електронні бази даних та знань, які знаходяться у вільному продажі, численні каталоги продукції та послуг).

Незалежно від сфери застосування та функціональних можливостей, усі ІС містять майже однаковий набір компонентів:

- *функціональні модулі* (моделі, алгоритми);
- *компоненти обробки даних* (бази даних, ПЗ, технічні засоби);

- *організаційні компоненти* (кадри, посадові інструкції та інструкції користувача, правила експлуатації тощо).

На рис.5.3 наведена типова структурна схема ІС управління нескладним технологічним процесом (ТП). *Певна сукупність ієрархічно організованих таких схем, об'єднаних у мережу за допомогою відповідних серверів, складає ІС підприємства*.

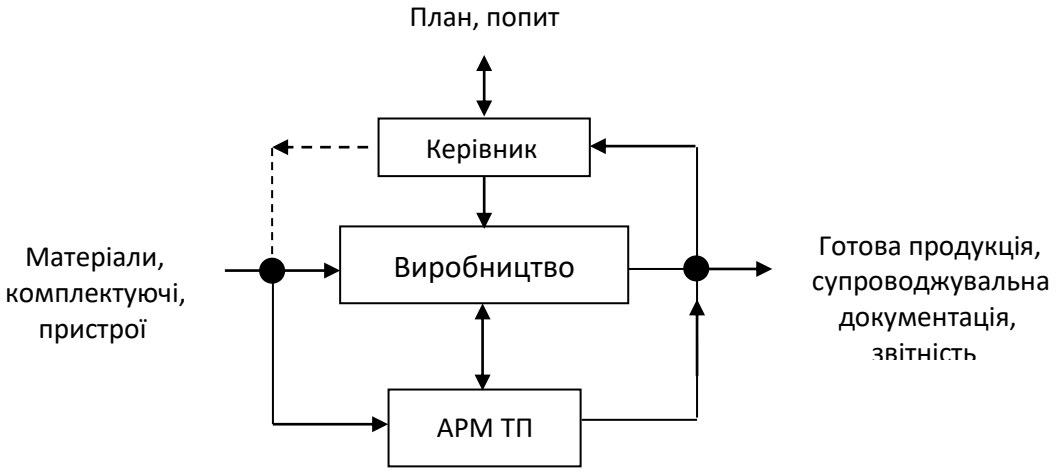


Рис.5.3. Структурна схема ІС управління технологічним процесом.

Незалежно від складності системи в її роботі можна виділити ряд однотипових етапів:

- *зародження даних*, тобто формування первинних повідомлень про об'єкт. В загальному вигляді етап проходить у два прийоми – спочатку формуються дані в звичайній формі уявлення, а потім йде формалізація даних для вводу в ПК;

- *накопичення і систематизація даних* у пам'яті ПК. По суті це ввод даних в ПК за допомогою обраного пристрою та розподіл даних за відповідними БД;

- *обробка даних* – ряд обчислювальних процесів, у результаті яких на основі раніше накопиченої інформації формуються відповідні документи і нові дані (аналітичні, рекомендаційні, прогнозні, що узагальнюють і т.д.).

- *відображення даних* - створення їх у формі, зручної для сприйняття людиною. Незважаючи на формальну сторону цього етапу, останній є дуже важливим елементом ІС, що дозволяє швидко та ефективно вести візуальний контроль;

- *виробка керуючого впливу*, тобто формалізація нових даних, що надійшли від особи, яка приймає рішення (ОПР), та введення їх в ІС;

- *прийом/передача даних*. Це чисто технічний етап, пов'язаний з передачею та прийомом даних від АРМ до керівника в цифровій формі ПК.

5.3. Етапи розвитку управлінських ІС

За час виникнення і розвитку інформаційних систем неодноразово змінювалися структура даних та їх використання, а також середовище, в якому здійснювалася взаємодія "користувач-ЕОМ" та перетворення даних. Це визначило зміну поколінь ІС. На сьогодні розрізняють *три узагальнених покоління,* стислий опис яких наведений нижче.

Перші ІС, які з'явилися на початку 60-х років XX століття, в зарубіжній літературі відомі під назвою *Data Processing System* (системи обробки даних, скорочено *DPS*), а у вітчизняній літературі відомі як *автоматизовані системи управління – позадачний підхід* (скорочено *АСУ-ПП*). В цих системах для кожної задачі дані і математична модель створювалися окремо. Такий підхід, з однієї сторони, сприяв концептуальній простоті побудови ІС, з другої сторони, зумовлював велику інформаційну надмірність системи та значний час підготовки даних. Типовими прикладами таких систем були системи управління запасами, оформлення рахунків, нарахування зарплати тощо.

ІС другого покоління в зарубіжній літературі відомі під назвою *Management Information System* (інформаційні системи в менеджменті, скорочено *MIS*), а у вітчизняній літературі відомі як *автоматизовані системи управління – концепція баз даних* (скорочено *АСУ-БД*). В таких системах почалося колективне використання даних з послідовним переходом до створення єдиної централізованої бази даних за допомогою СУБД. Цей етап почався в 70-роки, коли в колишньому СРСР був прийнятий план розвитку та створення АСУ з орієнтуванням на окремі класи та моделі ЕОМ, зокрема міні та мікрокомп'ютери. К середині 80-років був накопичений значний досвід створення управлінських ІС у вигляді АСУ технологічних процесів (*АСУ ТП*) та систем автоматизованого проектування в різних галузях науки і техніки (*САПР*).

Ефективність АСУ другого покоління була очевидною. Крім прямого економічного ефекту впровадження АСУ у виробництво мало великій вплив на зміну характеру діяльності управлінців: підвищилась оперативність, обгрунтованість та об'єктивність приймаємих рішень, стало можливим розв'язувати нові економічні задачі, збільшився час на творчу роботу працівників.

Системи третього покоління (початок етапу можна віднести до кінця 80 – початку 90-х років) в зарубіжній літературі відомі під назвою *Desision Support System* (системи підтримки рішень, скорочено *DSS*), а у вітчизняній літературі відомі як *системи підтримки прийняття рішень* (скорочено *СППР*). Ці системи призначені для підтримки різних видів діяльності в разі прийняття рішень зі слабоструктурованих або неструктурованих проблем. На відміну від попередніх видів ІС СППР повинні мати загальне математичне забезпечення у вигляді єдиної бази моделей. Ця база має таке ж ключове значення при переході до колективних обчислень, як єдина база даних в ІС другого покоління при переході до колективного використання даних. Без централізованої бази моделей ефективність СППР значно зменшується за таких причин:

- можлива взаємна несумісність окремих моделей;
- зменшується імовірність прийняття правильного рішення;
- кожний користувач повинен додатково займатися багаторазовою модифікацією моделей з метою їх адекватності змінним вимогам навколишнього середовища (краще, коли таке відслідковування ситуації будуть здійснювати централізовано відповідні фахівці).

З приводу розвитку трьох поколінь ІС слід зазначити, що кожне нове покоління не витискувало попередні розробки, а доповнювало їх, розширюючи діапазон можливого застосування. Більш того, в сучасних ІС у певній пропорції присутні елементи всіх трьох поколінь.

Серед кількох різновидів виробничих СППР у вітчизняній практиці найбільше розповсюдження знайшли автоматизовані системи управління підприємством (*АСУП*) – ієрархічно організовані комп'ютерні мережеві системи із застосуванням певних АРМ на базі ПК, централізованих баз даних та економіко-математичних моделей, а також організаційного забезпечення для рішення задач управління принаймні основною виробничо-господарською діяльністю підприємств.

Слід відмітити, що СППР знайшли застосування і в юридично-правовій діяльності, тому це питання буде розглянуто далі дещо докладніше.

5.4. Загальні відомості про ІС "1С:Підприємство. Управління невеликою фірмою"

Продукт "1С: Предприятие 8. Управление небольшой фирмой для Украины" (УНФ) є програмним рішенням (додатком), яке дозволяє автоматизувати оперативне управління невеликих підприємств. Існує

достатньо багато напрямків діяльності організацій, де таке програмне рішення можна застосувати: надання послуг і виконання робіт; логистичні та фінансові операції; операції з грошовими активами; процеси, зв'язані з позаобіговими активами; продаж і маркетингова діяльність; угоди із закупівлі та постачанню; ведення кадрової політики та ін.

Робота з додатком не потребує спеціальних знань податкового і бухгалтерського обліку. Дані з "1С: Предприятие 8. УНФ для Украины" автоматично передаються в "1С: Бухгалтерия 8 для Украины", завдяки чому немає потреби вводити одну й ту саму інформацію 2 рази.

Разібратися з програмою зможе навіть починаючий користувач, а досвідченим управлінцям ще й сподобається висока швидкість роботи додатку. Це можливо завдяки інтуїтивно зрозумілому інтерфейсу у вигляді знайомих користувачам ОС Windows так званих вікон, а також ряду інструментів для автоматизації внесення інформації. Структура програми складається зі специфічного робочого столу і панелі розділів.

Робочий стіл являє собою схему навігації по додатку і реалізує швидкий доступ до документів, звітів і задач кожного співробітника. За переміщенням між розділами програми і роботу з нею відповідає панель розділів.

Усі операції з формування документації фірми (фінансової, логістичної, торгівельної та ін.) проводяться шляхом заповнення відповідних електронних форм – аналогів паперових документів з можливістю їх виводу на друк.

Єдина інформаційна база даних ІС "1С: УНФ"

У відповідності до вищенаведеного матеріалу така база містить:

- клієнтську базу;
- касові та банківські операції, систему "клієнт-банк";
- взаєморозрахунки з персоналом і контрагентами;
- відомості стосовно продукції та замовлень;
- план розподілу навантажень між ресурсами компанії;
- ведення кадрового обліку і розрахунок заробітної плати;
- план з виконання робіт і надання послуг;
- облік виконання виробничих операцій;
- торговельні угоди, включаючи роздрібний продаж;
- калькуляцію витрат на випуск продукції та її собівартість;
- майно фірми та фінансові активи;
- фінансове планування бюджету;
- підрахунок збитків, прибутків, витрат і доходів.

Слід відмітити, що “1С: УНФ” не спеціалізована під ведення податкового і бухгалтерського обліку. Для цього використовується додаток “1С: Бухгалтерия 8”, всі необхідні дані в яку передаються з конфігурації “1С: УНФ 8” в автоматичному режимі.

Додаток “1С: УНФ” застосовується для ведення управлінського обліку однієї або кількох компаній, які можуть працювати як незалежно, так і в якості філій головної організації. Система може легко адаптуватися до змін структури бізнесу або методів організації робіт і управління.

Платформа “1С: УНФ”

Продукт “1С: Управление небольшой фирмой” працює на базі інформаційної системи (платформи) “1С: Предприятие”, що забезпечує прийнятні для практики продуктивність, гнучкість, конфігурованість, ергономічність прикладних рішень, управління за допомогою веб-браузера з використанням низькошвидкісних каналів зв’язку.

Платформа “1С: Предприятие 8” має інтуїтивно зрозумілий інтерфейс, який не визиває проблем навіть у починаючого користувача.

Дана платформа може працювати не тільки у файловому режимі, а й у взаємодії з такими популярними СУБД, як Microsoft SQL Server, Oracle Database, IBM DB2 та ін.

Сервер “1С: Предприятие 8” працює як під управлінням ОС MS Windows, так і в операційній системі Linux. Це забезпечує не тільки вільний вибір архітектури для роботи системи, а й дозволяє використовувати в роботі бази даних програмне забезпечення з відкритим початковим кодом.

5.5. Загальна характеристика правової ІПС “ЛІГА:ЗАКОН”

Для оперативного доступу до інформації, її систематизації, а також своєчасного і коректного використання все більш насущним стає застосування спеціалізованих програмно-технічних засобів. Саме цій меті служать комп’ютерні правові системи із законодавства, які знайшли широке розповсюдження в науковій, методичній і навчальній роботі провідних юридичних вищих навчальних закладів та в практичній професійній діяльності у галузі права. *Однією з найбільш розповсюджених і зручних у використанні є правова інформаційно-пошукова система (ППС) ЛІГА:ЗАКОН*.

Інформаційно-аналітичний центр “ЛІГА” успішно працює на ринку комп’ютерних інформаційних технологій з 1991 року. За цей час фахівці

Центру пройшли шлях від розробки інформаційно-довідкових пошукових систем з питань законодавства до створення сімейства систем інформаційно-правового забезпечення ЛІГА:ЗАКОН та української мережі ділової інформації “ЛІГАБізнесІнформ” (рис. 5.4).

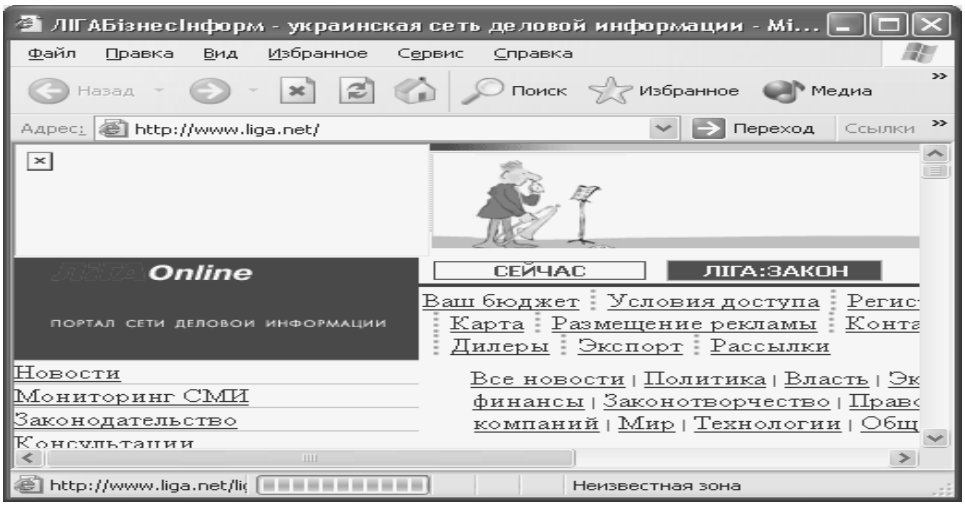


Рис. 5.4. Вигляд головної сторінки порталу ЛІГА БізнесІнформ

Метою функціонування і розвитку Центру є надання широкому колу користувачів доступу до систематизованої актуальної інформації правового і ділового характеру, яка задовольняє вимогам максимальної оперативності й надійності. Виконання зазначеної мети досягається шляхом розробки і щоденного супроводу інформаційно-програмних продуктів різного тематичного та професійного ступеня складності.

На сьогодні мережа об’єднує понад 100 тисяч користувачів, включаючи Секретаріат Президента України, Кабінет Міністрів України, різні міністерства й інші органи виконавчої державної влади та місцевого самоврядування України, банки, посольства, іноземні представництва, компанії, а також численні комерційні структури.

Програмний продукт функціонує в середовищі Windows, має віконний інтерфейс і сумісний з низкою прикладних програм, зокрема з текстовим редактором MS Word, і фактично є Windows-додатком. Тому для застосування ПІПС достатньо навичок користувача сучасного ПК, набутих в ході вивчення курсу “Інформатика”.

5.6. СППР в юридично-правовій діяльності

Уточнимо визначення СППР. *Системами підтримки прийняття рішень називають інтелектуальні системи, за допомогою яких особи, які приймають*

рішення (ОПР), мають можливість аналізувати ситуації, формулювати завдання, виробляти, контролювати й оцінювати варіанти рішень, які забезпечують досягнення поставленої мети. У загальному випадку СППР можна інтерпретувати як одну з категорій управлінських інформаційних систем. Ці системи довгий час розглядалися як системи підготовки звітів – періодичних структурованих документів. Однак на даний час СППР доцільно розглядати у вигляді інтерактивної системи, яка:

- реагує як на заплановані, так і непередбачені інформаційні запити;
- орієнтована на специфічний тип рішень або на безліч взаємопов'язаних рішень;
- застосовується там, де неможливо або небажано мати повністю автоматичну систему.

Сфера використання таких систем практично необмежена. Вони мають не тільки суто економічне застосування, але й призначаються для правоохоронних органів, судового провадження, органів виконання покарань, національної безпеки, служби охорони, військової розвідки, митниці, податкової поліції, міграційної служби та багатьох інших. Правоохоронна діяльність виділяється в цьому списку, оскільки створення СППР в цій області можливо тільки в разі взаємодії математиків, юристів, практиків та фахівців в області інформаційних технологій. При цьому готові системи повинні працювати в умовах розподілених організаційних структур, які використовують різноманітні засоби автоматизації і не завжди забезпечені якісними каналами зв'язку.

Далі стисло розглядаються основні категорії СППР.

СППР, орієнтовані на дані, – це різновид СППР, який зосереджується насамперед на доступі і маніпуляції великими базами структурованих даних. До цієї категорії відносять:

- *системи підготовки управлінських звітів*;
- *сховища даних* (Data Warehouse) – особлива форма організації бази даних, призначена для зберігання в погодженому вигляді агрегованої інформації, одержуваної з баз даних різних OLTP-систем та зовнішніх джерел;
- *системи аналізу даних* (On-line Analytical Processing, OLAP) – системи швидкого аналізу розподіленої багатовимірної інформації. Термін "OLAP" невіддільний від терміна "сховище даних". OLAP-системи забезпечують різні точки зору на дані і різні форми їх подання. Програмний продукт можна віднести до класу OLAP, якщо він має три головні особливості: багатовимірність даних, складні обчислення, швидка обробка;

- *виконавчі інформаційні системи* (Executive Information System, інформаційна система керівника) – автоматизовані системи, призначені для забезпечення необхідної актуальною інформацією менеджерів вищої ланки управління в процесі прийняття стратегічних рішень. Акцент робиться на графічні дисплеї і легкий у використанні інтерфейс, за допомогою яких подається інформація з корпоративної бази даних;

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

Другу велику категорію складають СППР, орієнтовані на доступ і маніпуляцію моделями – статистичними, фінансовими, оптимізаційними і/ або імітаційними. В основному такі системи використовують дані і параметри, які їх надають ОПР, але, як правило, не вимагають великих обсягів даних. *Приклади таких СППР*:

- *засоби аналізу рішень, які допомагають ОПР розбити проблему на складові та структурувати її* (наприклад, дерево рішень, критерій Байеса, ін.);

- *засоби лінійного програмування* – пошук оптимального розподілу ресурсів та ін.;

- *імітаційні засоби* – проведення певної кількості експериментів для перевірки результатів, що випливають з кількісної моделі системи.

Деякі OLAP-системи, які дозволяють виконувати складний аналіз даних, можуть бути класифіковані як гібридні СППР, які забезпечують і моделювання, і пошук і підсумковий аналіз даних. *Гібридним підходом до СППР вважаються також технології видобутку даних* (Data Mining). Синонімами терміна “видобутку даних” є “виявлення знань в базах даних” і “інтелектуальний аналіз даних”. Мета отримання даних полягає у виявленні прихованих правил і закономірностей в наборах даних.

Засоби видобутку даних та експертно-пошукові системи складають ще одну категорію СППР – рекомендаційні СППР (Suggestion DSS). Експертні системи як системи штучного інтелекту часто розглядають як окремий клас ІС, але останнім часом спостерігається тенденція реалізації їх модулів в складі СППР і виконавчих ІС.

СППР, орієнтовані на документи, розробляються для управління неструктурованими документами і Web-сторінками. Такі СППР інтегрують різноманітні технології зберігання і обробки гіпертекстових документів, зображень, звуків, відео і т.д.

Групові СППР (комунікаційні системи) – це інтерактивні автоматизовані системи, призначені для підтримки рішення неструктурованих і напівструктурованих проблем декількома ОПР.

5.7. Автоматизовані інформаційні системи для дактилоскопії, ідентифікації громадян за елементам зовнішності та голосу. Інші системи

Дактилоскопічні ІС

Автоматизована дактилоскопічна ІС “Папілон” (рис. 5.5) розроблена в РФ і забезпечує створення, зберігання і функціонування електронної бази даних дактилокарт слідів громадян та автоматизацію процесу дактилоскопичної ідентифікації для розв’язку широкого кола задач, а саме:

- встановлення особи за відбитками і слідах пальців рук і долонь, в тому числі шляхом проведення оперативних перевірок по відбитку пальця в режимі реального часу;
- ідентифікації невпізнаних трупів;
- встановлення причетності особи до раніше скоєних злочинів;
- об’єднання злочинів, скоєних одним і тим же особою.

АДІС “Папілон” дозволяє виконувати:

- введення і зберігання в БД електронних дактилокарт, що включають текстову інформацію, відбитки пальців і долонь, контрольні відбитки, дактилоформулу, фотозображення зовнішності і особливих прикмет, словесний опис зовнішності;
- введення і зберігання в БД слідів пальців рук і долонь, вилучених з місць злочинів;
- імпорт/експорт дактилокарт і слідів в форматах МВС Росії, Інтерпола, ФБР;
- автоматичні пошуки типу: карта-карта, карта-слід (пальця, долоні), слід (пальця, долоні)-карта та інші пошуки для кожної введеної в БД дактилокарти або сліду;
- автоматичний пошук по словесному опису зовнішності;
- автоматизоване складання дактилоформули;

- ведення автоматизованого дактилообліку: отримання вибірок з БД, сортування списків БД, видалення і редагування записів і т.д. ;

- перегляд/друк текстово-графічної інформації (фотозображення, сліди, відбитки);

- друк документів, списків, довідок, статистичної інформації;

- віддалене введення дактилоскопічної інформації, віддалений доступ до центральної БД;

- взаємодія з іншими видами автоматизованих обліків.

Рис. 5.5. АДІС “Папілон”

ІС випускається у вигляді одномашинного комплексу і мережевого. Одномашінний комплекс розрахований на обсяг БД до 25 000 дактилокарт, 10 000 слідів. Він може працювати як локальна система, а також як станція віддаленого доступу до центральної АДІС в складі багаторівневих територіально-розподілених сістем. Серверні функції і функції робочої станції суміщені на одному комп’ютері.

Мережевий комплекс АДІС «Папілон» розрахований на обсяг бази 25 ... 100 тис. дактилокарт. Складається з декількох робочих станцій, об’єднаних локальною мережею. Серверні функції забезпечуються ресурсами виділеного сервера або розподіляються між робочими станціями. Мережевий комплекс може працювати як незалежна (локальна) АДІС, а також у складі багаторівневих територіально-розподілених систем.

Ще одна розробка РФ – АДІС “Сонда”. Система призначила для створення і ведення електронної бази дактилокарт та слідів пальців і долонь, вилучених з місць злочинів, а також для проведення ідентифікацій нових дактилокарт і слідів по наявній базі даних. Система працює в середовищі Windows і Linux.

АДІС «Сонда» дозволяє:

- встановлювати особи злочинців, які залишили сліди рук на місці злочину;

- виконувати ідентифікацію невпізнаних трупів, в тому числі загиблих в результаті терактів, катастроф або стихійного лиха;

- встановлювати осіб, які перебувають в міжнародному розшуку і особистість недієздатних громадян;

- встановлювати причетність конкретної особи до вчинення злочинних дій по закордонних запитам Інтерполу, ФБР, МВС;

- виявляти причетність до скоєння злочинів особистості без певного місця проживання

- друкувати копії дактилокарт і карток слідів на принтері;

- імпорт і експорт дактилокарт і слідів для передачі в іншу АДІС на електронних носіях, в тому числі в міжнародному форматі ANSI/NIST;

- обмін дактилоскопічною інформацією, проведення пошуків та отримання результатів з віддаленої АДІС за допомогою електронної пошти або модемного з'єднання;

- аналіз цілістності та відновлення баз даних і ще багато інших дій.

Як приклад іноземних дактилоскопічних систем можна привести системи Sagem (Франція). Системами Sagem оснащені урядові установи, військові та судово-слідчі відомства, системи голосування, охорони здоров'я, страхування більш ніж в 20 країнах світу. Компанія Sagem Defense S'ecurit'e є світовим лідером у виробництві та інсталяції автоматичних систем ідентифікації за відбитками пальців (Automated Fingerprint Identification System (AFIS) і автоматичних систем ідентифікації за формою долоні і відбитку пальця (Automated Palmprint and Fingerprint Identification System (APFIS). На даний час тільки ці біометричні системи можуть працювати з базами даних користувачів будь-яких розмірів.

Автоматизовані системи обліку осіб за елементами зовнішності

Автоматизовані системи обліку осіб за елементами зовнішності поділяються на два основних типи: системи, що дозволяють створювати фотороботи (суб'єктивні портрети) підозрюваних осіб, і системи, що використовують для ідентифікації осіб готову базу даних з відео- і фотографіями.

В якості системи загального типу можна навести, наприклад, експертну автоматизовану систему портретної ідентифікації (АСПІ) "*Портрет 2005*",

розроблену фахівцями ТОВ «Барс Інтернешнл», ТОВ «Портланд» (Російська Федерація) і ТОВ “АСПІ-Софт” (Республіка Білорусь) . Система призначена для використання в експертно-криміналістичних та оперативно-розшукових підрозділах.

АСПІ “Портрет 2005” здатна здійснювати ідентифікацію людини не тільки по зіницям очей, але і по іншим антропологічним точкам. Ця специфічна особливість системи дозволяє проводити порівняння розшукуваних осіб по зображенню суб’єктивних портретів і фотографій трупів. Окрім того, програма дає можливість складати фотороботи розшукуваних осіб (за рахунок бази даних з елементами зовнішності людини) і вести бази відеозаписів на осіб, які знаходяться на обліку. АСПІ може використовуватися для створення баз криміналістичних колекцій: слідів взуття, слідів транспорту і знарядь злому, підроблених грошових купюр і т.д. .

У лютому-липні 2006 р на базі Державного експертно-криміналістичного центру МВС Республіки Білорусь було проведено тестування кількох автоматизованих біометричних ідентифікаційних систем на масиві в 110 тисяч осіб з використанням методик, розроблених в ДЕКЦ МВС Республіки Білорусь і в Національному інституті за стандартами і технологіями США.

Перевірялися можливості систем і конкретно – шанси знайти за певними зразкам з різними вихідними параметрами (вікові зміни, наявність або відсутність вусів, бороди, окулярів, повороти голови, різні умови зйомки і т.д.).

З представлених трьох систем кращою визнано саме “Портрет 2005”. Для пошуку в цій системі придатні навіть неякісні зображення, отримані за допомогою побутових фото та відеокамер, камер зовнішнього спостереження, фотокамер мобільних телефонів (рис. 5.6).

Рис. 5.6. Зображення, які придатні для пошуку в системі “Портрет 2005”

Тепер розглянемо біометричну інформаційно-пошукову систему "*Ідентифікація*". Це система оперативної ідентифікації громадян в процесі слідчих заходів правоохоронних органів, яка виконується з робочого місця шляхом віддаленого звернення до центральної бази даних. У процесі ідентифікації людини, отримані електронні фотозображення і реквізитні даних особи, яка потрапила в зону інтересу правоохоронних органів, відправляються на центральний сервер МВС. На сервері проводиться автоматична ідентифікація осіб по централізованим базам даних з інформацією про осіб: що одержали паспорти і посвідчення особи; водійські посвідчення; паспорта моряків; про осіб, які мають оперативний інтерес для правоохоронних органів; розшукуваних осіб та ін. Результат повертається в вигляді ряду фотозображень, найбільш схожих на фотографії, пред'явлені для ідентифікації, і відповідних їм анкетних даних про людину. Співробітник, отримавши відповідь, візуально ідентифікує затриманого, порівнює з представленими цією людиною даними, і, в разі розбіжності, приймає рішення про подальші дії відповідно до встановленого порядку.

Система дозволяє:

- оперативно вести пошук встановлюваних осіб по фотографіям, суб'єктивним портретам, матеріалам оперативної відеозйомки і будь-яким іншим матеріалам, що зберігаються в базі;
- виконувати ідентифікацію встановлюваної особи за пропонованими зображеннями осіб в окулярах, з бородою чи вусами, з гримасою на обличчі (посмішка і т.д.);
- здійснювати попередній відбір за словесним описом, а потім вести пошук об'єктів (персон, осіб) по попередньо відібраної базі;
- здійснювати пошук по зображеннях з великою часовою (вікової) різницею.

В останні роки правоохоронними органами країни з метою ідентифікації особистості по зображенню особи в місцях масового скупчення людей використовується автоматизована біометрична інформаційно-пошукова система відеоспостереження "*Відеопотік*". Система складається з поворотних відеокамер денного і нічного бачення, стаціонарних камер для системи розпізнавання, систем оцифровки, доставки, обробки відеозображення, серверів розпізнавання, систем моніторингу, адміністрування і управління розподіленої системою. У режимі реального часу АІПС "Відеопотік" вибирає з потоку найбільш підходящі для перевірки особи і порівнює їх зображення з наявними в базах даних фотозображеннями розшукуваних терористів і

злочинців. У разі подібності порівнюваних фотозображень програма інформує уповноважений правоохоронний орган, який приймає рішення про подальші оперативні заходи.

В якості бази даних система “Відеопотік” може використовувати комплекси “СОВА” або “Образ ++”. Система “СОВА” орієнтована на пошук і виявлення терористів, особливо небезпечних злочинців і учасників банд-формувань. За допомогою системи "СОВА" щомісяця виявляються сотні особливо небезпечних злочинців. На сьогоднішній день на базі ДІАЦ МВС РФ встановлено близько 1500 комплексів практично у всіх регіонах країни.

Система "Відеопотік" володіє хорошими точносних характеристиками ідентифікації і швидкістю роботи: швидкість обробки відеопотоку надходять зображень - 24 зображення в секунду; розрахунковий час реакції програми в разі подібності фотозображень - не більше 10 с. Однак щоб досягти режиму безпомилкового виявлення злочинця в натовпі людей, при установці системи необхідно дотримуватися деяких умов:

- стаціонарні відеокамери системи необхідно встановлювати в таких місцях проходження людей, де забезпечується найкраща якість зображення особи, наприклад, входи / виходи різних громадських місць - стадіонів, концертних залів, метро і т.п .;

- ділянку, призначений для зйомки, повинен мати рівномірний, що не дає тіні, освітлення. При необхідності освітлення повинно бути цілодобовим. Як радять розробники, на місці установки відеокамери бажано використовувати ефекти, що привертають увагу людини, наприклад, хороший ефект виходить при використанні рекламного плаката з яскравим підсвічуванням, реакція на який може привести “до повороту і (або) підйому голови в потрібному ракурсі або під потрібним кутом”.

Окрім перерахованих найпоширеніших способів ідентифікації, при необхідності використовується ідентифікація особистості за фрагментами генетичного коду, по голосу, мові, за почерком і т.п.

Фоноскопічні експертизи ґрунтуються на порівнянні голосів підозрюваних осіб з фонограмою голосу, що надійшов на експертизу, тобто з голосом, так званого диктора. На сьогоднішній день створено досить багато різних систем ідентифікації по голосу, мають різні параметри і вимоги до процесу ідентифікації в залежності від конкретних завдань. Однак, як показано в інформаційних матеріалах, не всі системи сертифіковані в якості засобів вимірювання, а також непрості для розуміння. Тому частіше вони застосовуються в якості додаткових засобів.

Програмно-апаратний комплекс дистанційного розпізнавання автомобіильних номерних знаків "Потік"

Для пошуку та ідентифікації викрадених автомобілів правоохоронні органи Росії з 2001 р використовують спеціалізований програмно-апаратний комплекс (АПК) дистанційного розпізнавання автомобільних номерних знаків "Потік" компанії "РОССИ-СП". Комплекс складається з відеокамери, що переглядає коротку ділянку траси, і пов'язаного з нею комп'ютера. Інформація, що надходить з відеокамери (номер автомобіля, час, дата його проїзду, напрямок руху, стоп-кадр з "фотографією" автомобіля), фіксується комп'ютером, швидко звіряється по базах даних викрадених автомобілів або викрадених номерів, і при виявленні ідентичного номера комп'ютер відразу подає сигнал тривоги. Обробка номера програмою, в яку входить розпізнавання номера, його запис та перевірка по базах даних виконується дуже швидко, поки автотранспорт ще тільки проїжджає зону контролю відеокамери.

Можливі відповіді комплексу на ідентифікований автотранспорт:

- звукове сповіщення, що включає інформацію про номер автотранспорту, напрямку його руху і назву бази даних, за якою транспортний засіб ідентифіковано;
- видача повної інформації про виявлений автотранспорт з його фотографією і напрямком руху, відомості про базу даних, яка "впізнала" транспорт, а також інформацію про ініціатора ідентифікації;
- регулювання дій зовнішніх пристроїв, наприклад, світлофора. У разі ідентифікації номера викраденого автотранспорту комплекс може автоматично перемкнути сигнал світлофора на червоний.

Окрім можливості ідентифікації та оповіщення в АПК "Потік" включені функції поповнення бази даних новою інформацією та реєстрації зафіксованою камерою інформації про всі автотранспорти без винятку (навіть про ті, що не мають номерного знака або знак абсолютно не читаємий) в так званому журналі проїзду. Ця можливість комплексу сприяє підвищенню ефективності розкриття злочинів, так як програма дозволяє в будь-який момент отримати інформацію про конкретний транспорт.

Заявлена ймовірність розпізнавання комплексу складає 90% від всього транспортного потоку навіть в погану погоду. При звичайних умовах АПК забезпечує в будь-який час доби вірогідність розпізнання 98% і більше. Практика підтверджує заяву розробників.

5.8. Біометричні системи в слайдах

Біометрія відноситься до категорії технологій, які вимірюють і аналізують характеристики тіла людини, такі як ДНК, відбитки пальців, сітківки очей, геометрію вен, голосові моделей і моделі осіб. Так як біометричні ідентифікатори унікальні для кожної людини, вони більш надійні в перевірці ідентичності, ніж інші методи.

Зазвичай при класифікації біометричних технологій виділяють дві групи систем за типом використовуваних біометричних параметрів:

- Перша група систем використовує статичні біометричні параметри: відбитки пальців, геометрія руки, сітківка ока і т. п.
- Друга група систем використовує для ідентифікації динамічні параметри: динаміка відтворення підпису або рукописного ключового слова, голос і т. п.

Сервіси безпеки: Біометричні ІТ технології

В даний час для захисту від несанкціонованого доступу до інформації все частіше використовуються такі біометричні системи ідентифікації:

- за відбитками пальців;
- за характеристиками мови;
- по райдужній оболонці ока;
- по зображенню особи;
- по геометрії долоні руки

Використовувані в цих системах характеристики є невід'ємними якостями особистості людини і тому не можуть бути втраченими і підробленими.

Електронна ідентифікація за відбитками пальців

Оптичні сканери зчитування відбитків пальців встановлюються на ноутбуки, миші, клавіатури, флеш-диски, а також застосовуються у вигляді окремих зовнішніх пристроїв і терміналів (наприклад, в аеропортах і банках). Якщо візерунок відбитка пальця не збігається з візерунком допущеного до інформації користувача, то доступ до інформації неможливий.

Вхід в Windows за відбитками пальців

Захист банківських платіжних систем

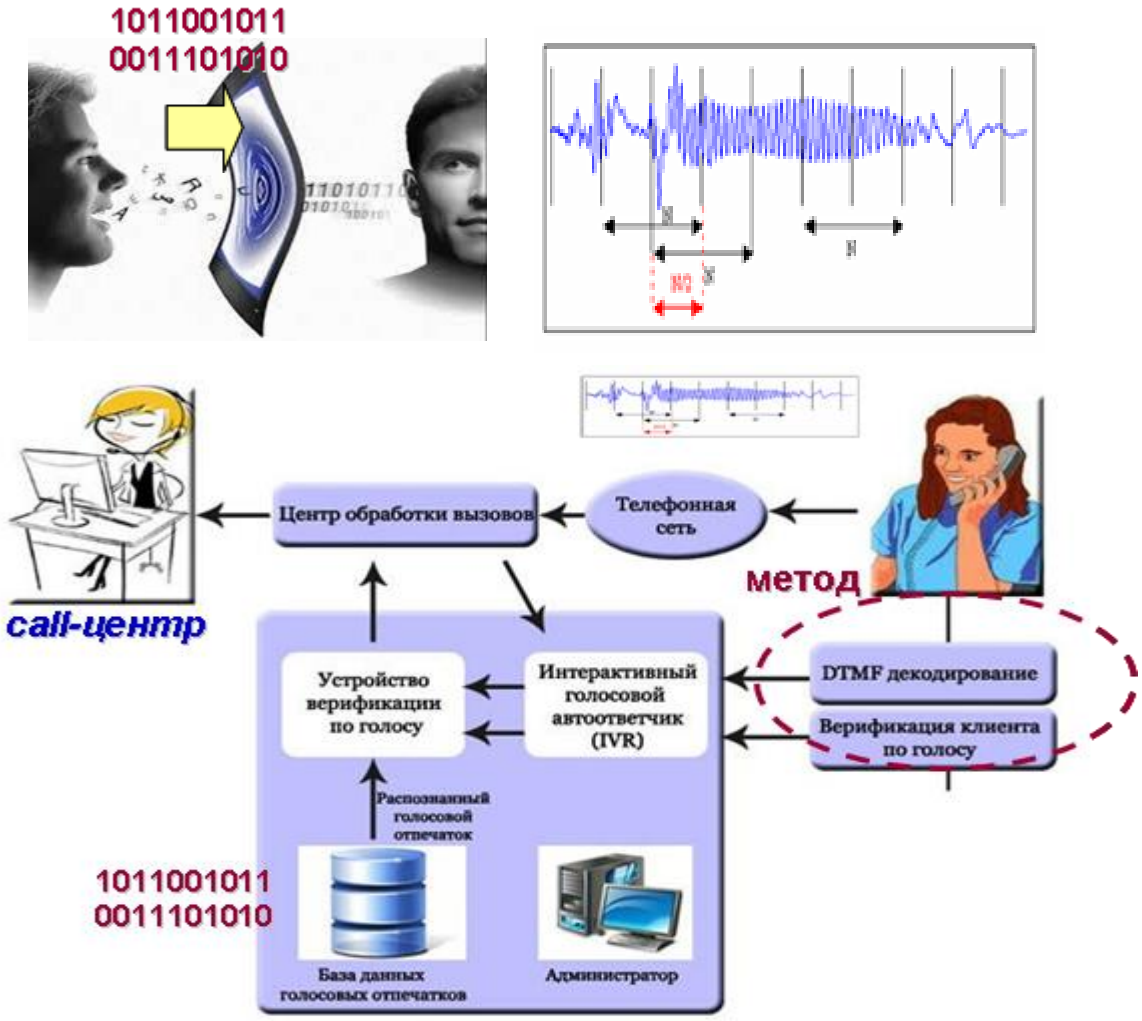
банківська картка

Окремий зовнішній індифікатор відбитків пальців

Ідентифікація за характеристиками голосу

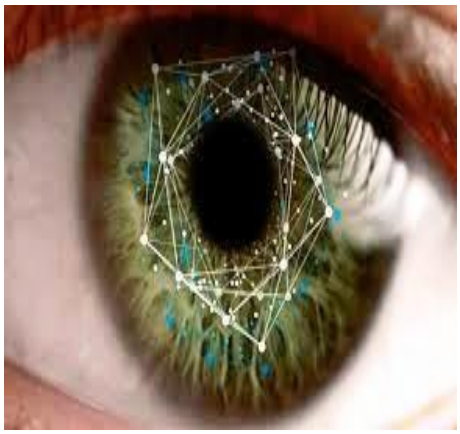
Ідентифікація людини по голосу - один з традиційних способів розпізнавання, інтерес до цього методу пов'язаний і з прогнозами впровадження голосових інтерфейсів в операційні системи. Голосова ідентифікація з використанням безконтактної технології і існують системи обмеження доступу до інформації на підставі частотного аналізу мови.

Найчастіше знаходить своє застосування в компаніях, що здійснюють свою діяльність через мережі зв'язку та зацікавлених в захисті ідентифікаційної інформації своїх клієнтів. Так, голосова біометрія ефективно використовується в сферах: *голосовий контроль доступу; контроль доступу в call-центрах; зміна пароля; безпечний конференц - зв'язок; банківське обслуговування; телекомунікація; функція «чорний список».*



Приклад застосування системи розпізнавання особистості по голосу в call-центрі

Ідентифікація по райдужній оболонці ока



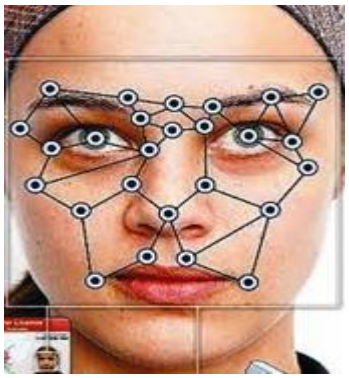
Райдужна оболонка ока є унікальною для кожної людини біометричною характеристикою. Зображення ока виділяється із зображення особи і на нього накладається спеціальна маска штрих-кодів. Результатом є матриця, індивідуальна для кожної людини.

Для ідентифікації по райдужній оболонці ока застосовуються спеціальні сканери, підключені до комп'ютера.

Біосканер

Біометричний індифікатор

Ідентифікація по зображенню обличчя



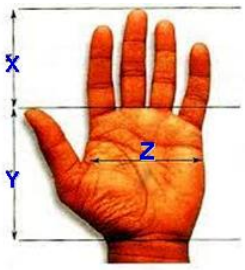
Розпізнавання людини по обличчу відбувається на відстані. Ідентифікаційні ознаки враховують форму лиця, його колір, а також колір волосся. До важливих ознак можна віднести також координати точок лиця в місцях, відповідних зміні контрасту (брови, очі, ніс, вуха, рот і овал). В даний час починається видача нових закордонних паспортів, в мікросхемі яких зберігається цифрова фотографія власника.

Вхідний контроль

Банкомат з розпізнаванням облич та відбитків пальців

Ідентифікація по долоні руки

З метою ідентифікації використовується проста геометрія руки – розміри і форма, а також деякі інформаційні знаки на тильній стороні руки (образи на згинах між фалангами пальців, візерунки розташування кровоносних судин). Сканери ідентифікації по долоні руки встановлені в деяких аеропортах, банках і на атомних електростанціях.







Японський банк Ogaki Kyoritsu запустив в експлуатацію 18 банкоматів, які дозволяють знімати готівку і керувати коштами за допомогою руки власника рахунку. Ідентифікація власника рахунку проводиться по руці з введенням пін-коду і дати народження. Ніяких пластикових карток банкомату нового типу не потрібні.

Криміналістична експертиза з ідентифікації по голосу і мовленню

Сутність криміналістичної ідентифікації особистості по голосу і усному мовенні полягає у виділенні в процесі вирішення цього завдання такого стійкого комплексу ознак, який буде достатній для встановлення індивідуально-конкретної тотожності між голосом і мовою, зафіксованими на вихідній фонограмі, та голосом і мовою на фонограмі-зразку.

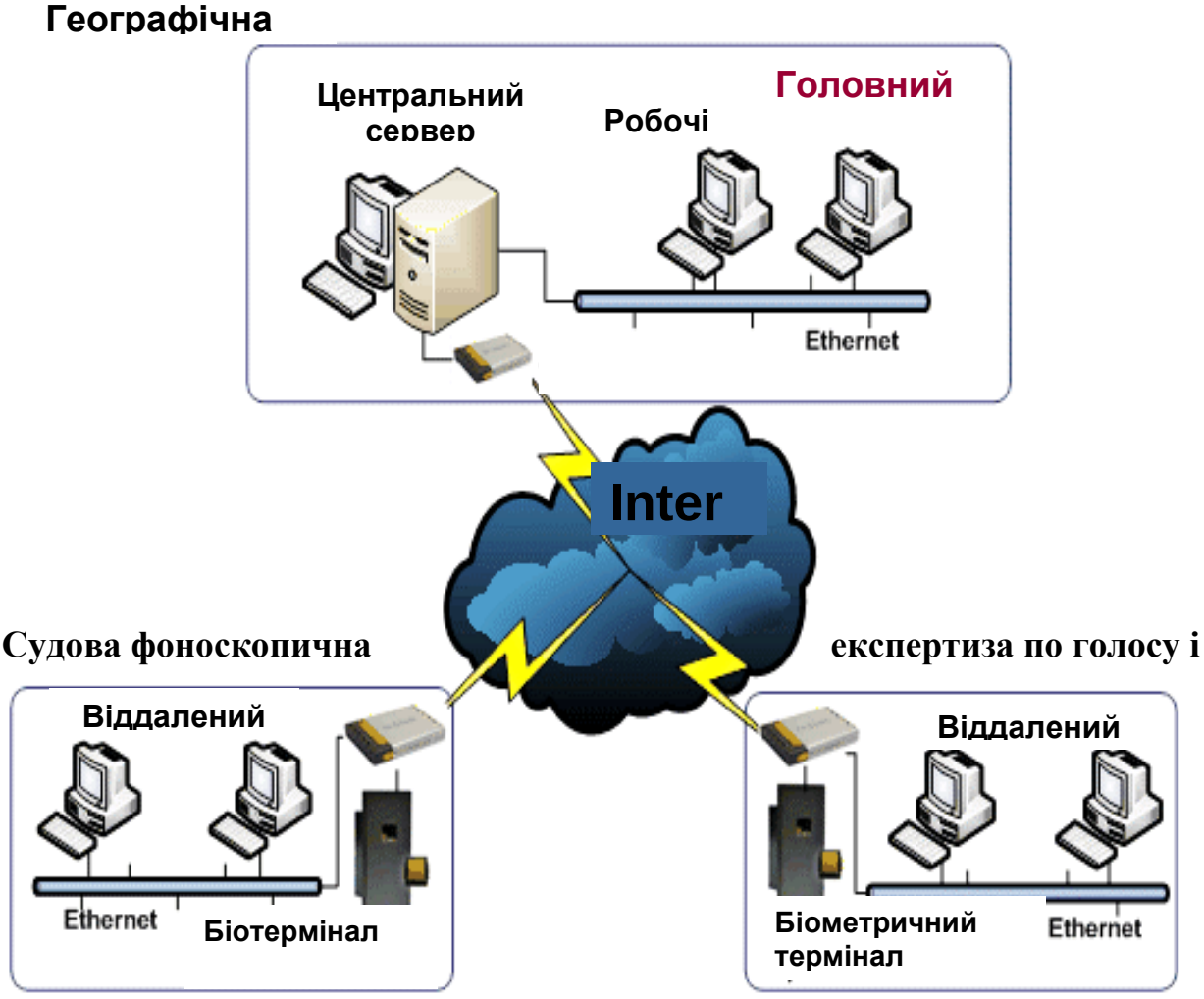
Криміналістична фоноскопія вирішує також і низку інших завдань, серед яких найчастіше трапляються наступні:

- дослідження ознак монтажу магнітної сигналограми;
- дослідження ознак копіювання фонограм;
- ідентифікація звукозаписуючого пристрою за фонограмою;
- діагностика й ідентифікація навколишнього акустичного середовища звукозапису;

- підвищення розбірливості мовного сигналу, спотвореного імпульсними перешкодами чи шумами;

- визначення особистісних параметрів диктора, як-то: стать диктора; вік диктора; регіон формування мовних навичок; регіон проживання; володіння іншими мовами; соціальне оточення диктора; професія диктора; рівень освіченості; наявність патології мовного апарату; приналежність до носіїв літературної мови, просторіччя чи діалекту; тип психологічного темпераменту; наявність психічних відхилень.

Організація системи контролю віддаленого біометричного доступу (СКВБД)



Судова фоноскопічна експертиза – це передбачена законодавством процесуальна дія по перевірці відносності та достовірності записаної на фонограмі інформації, що має значення доказу.

Найбільш розповсюдженими ідентифікаційними завданнями фоноскопічної експертизи є наступні:

- ідентифікація особи за мовленням;

- встановлення приналежності певної репліки в розмові конкретної особи;

- встановлення кількості співрозмовників, що приймають участь у комунікації;

- встановлення індивідуальних мовних особливостей (“мовний” портрет особи).

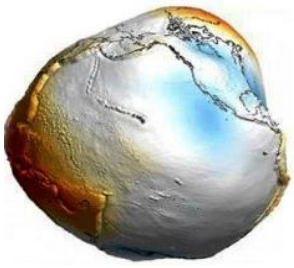
Для перевірки відносності та достовірності записаної на фонограмі голосової інформації, що має значення для доказу в суді, розроблений фоноскопичний апаратно-програмний комплекс “Ікар Лаб”.

5.9. Використання технології GPS в правоохоронній діяльності

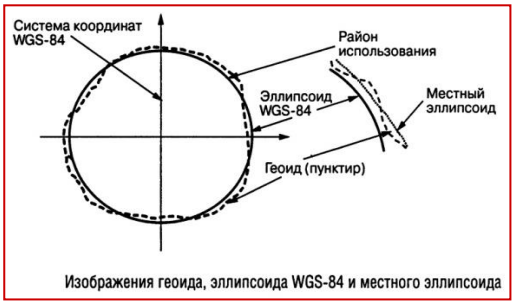
Актуальність та принцип дії системи GPS

Ефективність роботи правоохоронних органів може бути підвищена завдяки розробленню й запровадженню в їх діяльність новітніх ІТ. Однією з таких технологій є локалізація та відстеження об’єктів через глобальну систему позиціонування GPS (Global Positioning System — система глобального позиціонування). Це супутникова навігаційна система, яка забезпечує вимірювання відстані і часу та визначає місце розташування об’єктів у всесвітній трьохкоординатній системі WGS 84.

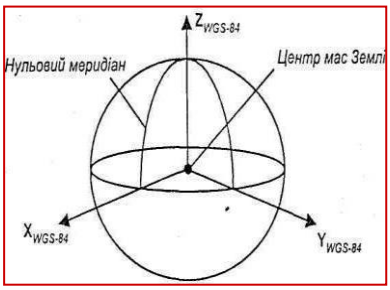
WGS 84 (англ. World Geodetic System 1984) - всесвітня система геодезичних параметрів Землі 1984 року, в число яких входить система геоцентричних координат. На відміну від локальних систем, є єдиною системою для всієї планети.



Земля - це геоід

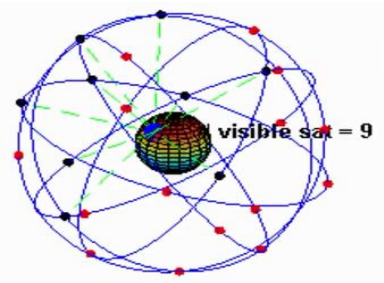


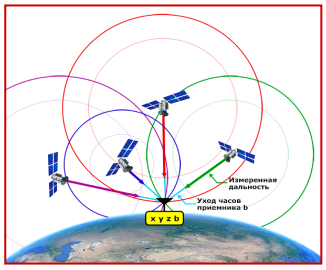
Изображения геоида, эллипсоида WGS-84 и местного эллипсоида



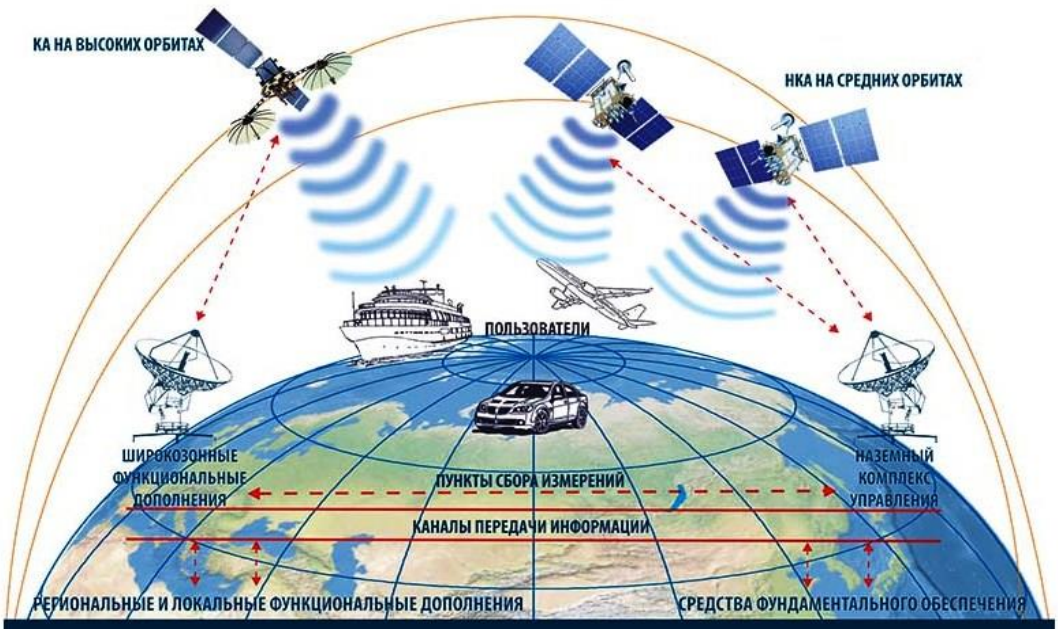
Загальна характеристика системи GPS

Система GPS складається з 32-х супутників, які рухаються по 4-6 штук в кожній з шести орбіт з різними кутами відносно Землі. Таке розміщення у просторі забезпечує прийом сигналів в будь-якій точці земної кулі одночасно як мінімум з 4-х супутників. Точність позиціонування об'єктів може досягати 2-х см.





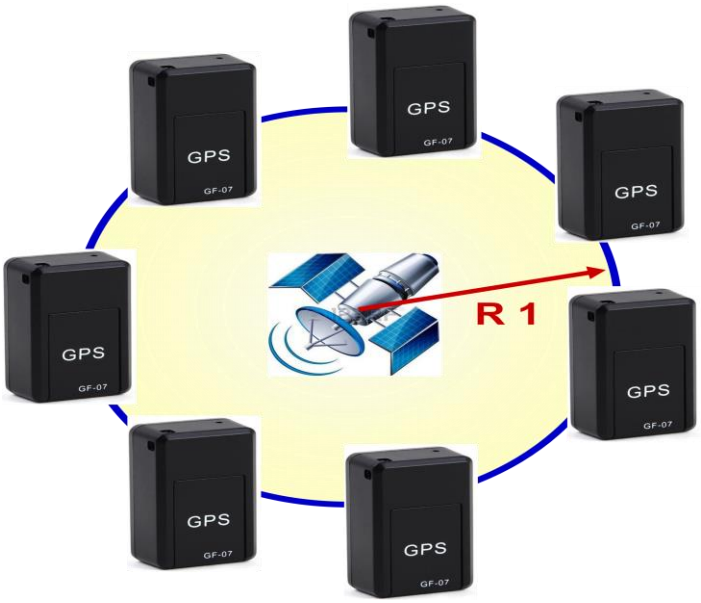
Концепція функціонування системи GPS



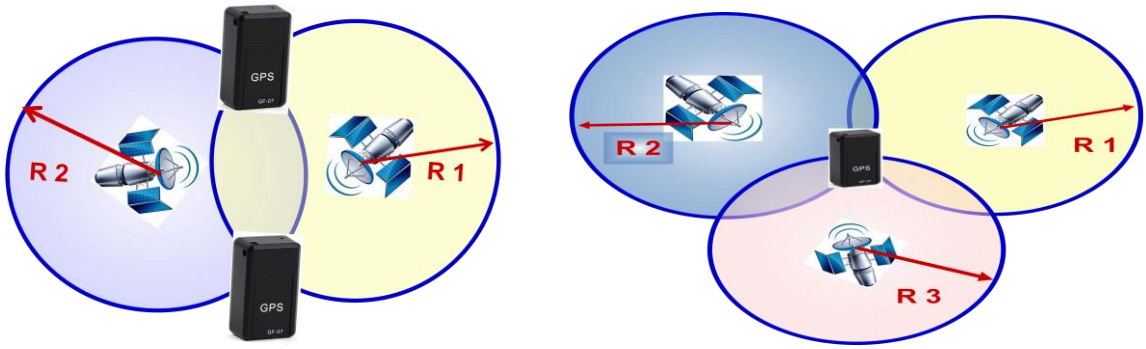
Сигнал з космосу поступає до усіх доступних приймачів GPS для обчислення свого положення в просторі по трьох координатах в реальному часі згідно всесвітній трьохкоординатній системі WGS 84.

Принцип визначення координат місця знаходження об'єкта (GPS трекера) на поверхні Землі

1. Припустимо, нам відома величина відстані від одного GPS супутника до приймача (ГПС трекера). Знаючи її, ми можемо намалювати коло навколо супутника, на краю якої і буде перебувати наш приймач.



2. Додамо дані з другого супутника. Таким чином, ми звузили сектор пошуку до перетину двох кіл. Тепер залишається додати інформацію про третій GPS супутник і ми отримуємо точні координати приймача (GPS трекера), який знаходиться на перетині трьох кіл.



Для контролю місцезнаходження наземних об'єктів застосовують різні види GPS-трекерів і маячків. Вони розрізняються не тільки призначенням, але і використовуваною системою стеження, принципом передачі даних, джерелом живлення, часом спрацьовування.

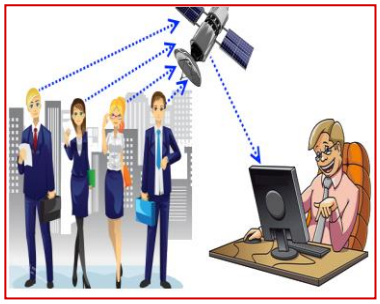
1. Маячок (закладка, маркер) відстежує місце розташування об'єкта в конкретний момент. Велику частину часу цей пристрій знаходиться в сплячому режимі, активуючи із заданою періодичністю, відсилає повідомлення з координатами. Завдяки такому режиму маячки можуть кілька років працювати без підзарядки.

2. Трекер забезпечує відстеження маршруту об'єкта. *Він включається при русі* і знаходиться в активному режимі на протязі шляху. Споживає значно більше енергії, ніж маячок.

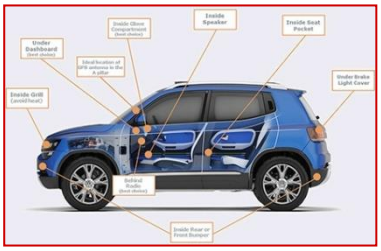
3. Навігатор - автономний прилад з можливостями трекера, який не вимагає підключення до приймаючого пристрою (комп'ютера, смартфона, кишенькового ПК). Найпростіші моделі не мають пам'яті для карт і можуть тільки запам'ятовувати шляхові точки і маршрути.

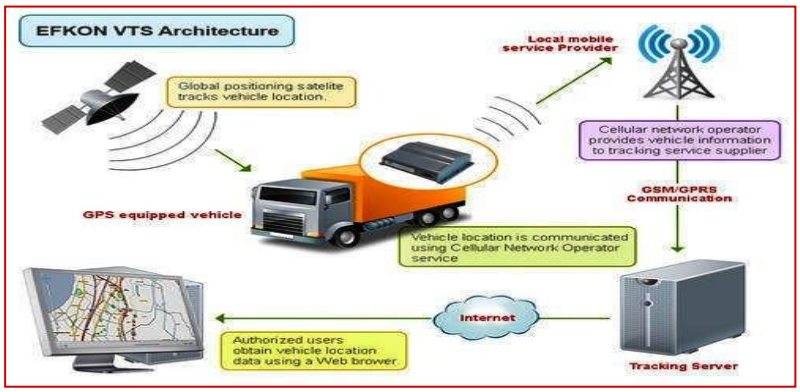
Призначення GPS-маячків

Персональні маячки призначені для прихованого спостереження за людьми або відкритого спостереження за дітьми, літніми людьми, туристами. Маячки для прихованого спостереження зовнішньо виглядають як візитки або компактні моделі;



Автомобільні маячки для стеження за транспортними засобами або їх пасивного захисту, ідеальні для прихованої установки.





Основне призначення автомобільного маячка – виявлення транспортного засобу після викрадення. Оскільки пристрій активізується на короткий проміжок часу, засікти його за допомогою сканера складно.

Портативність і автономна робота дозволяють встановити його в нестандартних місцях, що ускладнює виявлення приладу викрадачами.

Заглушити сигнал складніше, а ресурс його роботи значно перевищує час, протягом якого зловмисники зазвичай витримують викрадене авто в відстійнику з глушилками.

Тактика захисту авто від крадіжки з використанням набору GPS трекерів і маячків

Для надійного захисту від крадіжки авто у важкодоступні місця кузова автомобіля розміщуються декілька ДПС трекерів і маячків, які програмуються на спрацьовування в певні інтервали часу протягом тижневого і більшого періоду часу з метою зниження ймовірності їх виявлення злодієм при скануванні їх радіосигналу.

GPS - маячок Автозакладка: принцип роботи

Після придбання GPS маячка, потрібно через Google Play або App Store Apple завантажити додаток AvtozakladkA на свій смартфон або планшет. Потім зареєструйте в ньому свій GPS маяк і надійно сховайте пристрій в автомобілі в нестандартному місці. При з'єднанні GPS маяк відправляє дані про своє перебування за двома даними GPS і LBS на телефон власника. Власник може поглядати місцезнаходження машини з отриманими координатами.

Програма дає можливість отримувати повідомлення GPS трекера про місцезнаходження автомобіля. Крім цього програма зберігає історію переміщень, з її допомогою встановлюється період виходу GPS маячка на зв'язок і встановлюється режим «Тривоги». Натискання кнопки «Тривога» активує подачу сигналу оператору GPS і охоронній службі Венбест. Служби зв'язуються с водієм і запускають процедуру пошуку автомобіля. GPS трекер бачить режим «Тривоги» і відправляє на сервер свої координати в тривожному режимі. Мобільні екіпажі служби охорони оперативно направляються до вказаної адреси.

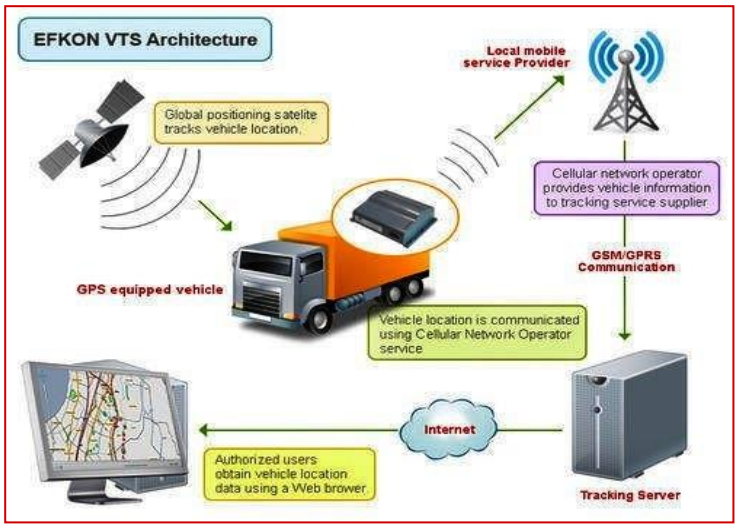
Види GPS – трекірів та варіанти їх використання

GPS-трекери необхідно мати як-що є:

Використання трекерів в правоохоронній діяльності

Використання GPS-трекерів в правоохоронній діяльності потрібне відповідно до Закону України “Про оперативно-розшукову діяльність”, ст.8 у випадках:

- оперативного моніторингу переміщення автотранспорту підозрюваних осіб (GPS закладки) ;
- оперативного відстеження руху контрабандних товарів (GPS закладки) ;
- моніторингу руху автозаків;
- контролю автопатролювання нарядами поліції (ІС “ЦУНАМІ”).

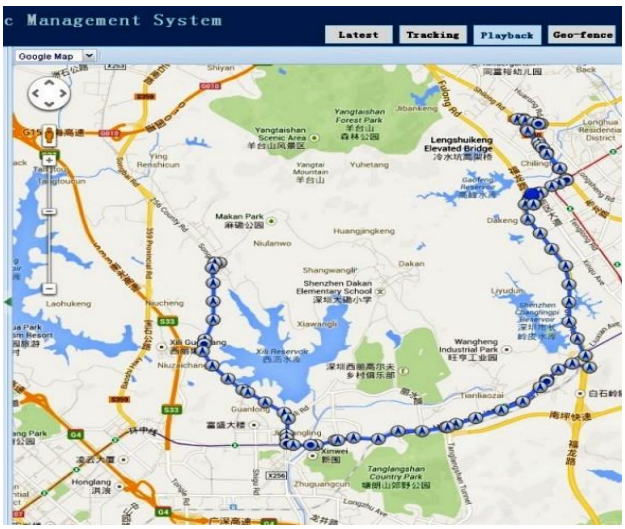


GPS трекери для контейнерів та вантажів

GPS трекер Magneto дуже легкий в експлуатації не вимагає підключення, завдяки потужним магнітів кріпиться на будь-яку металеву поверхню, має вбудовану батарею на 5 000 мАг, що дозволяє працювати GPS маяка до 90 днів в режимі очікування. Оснащений слотом під SIM карту, USB портом, індикатором стану.

Відстежувати місцезнаходження транспортного засобу можна за допомогою сайту або програми. Точність відстеження – 5 метрів.

Автономний GPS трекер "Magneto"



Відстеження за допомогою мобільного телефону - трекер скидає координати місця розташування Вам на телефон в смс-повідомленні. Крім координат в тексті смс буде посилання на карту Google, перейшовши по якій можна дізнатися точне місце на карті, яке зазначене прапорцем.

Управління GPS/GSM трекером можливо в віддаленому режимі, відправляючи текстові смс з командами на номер телефону тієї сім карти, яка встановлена в маячки.

GPS трекер iBag "Dakar"

GPS-трекер iBag "Dakar“ та автономний GPS-маяк для автомобілів або вантажів. Час автономної роботи до 3-х років, точність позиціонування 2 метра. Якісний модуль quectel, підтримка GPS та Глонасс, lbs, queccell. Може виступати як додаток для смартфонів. Магнітне кріплення.

Правові засади щодо здійснення геолокаційного відслідковування за місцем знаходження обвинувачених (підозрюваних)

Відповідно до частини 1 статті 195 КПК України, застосування електронних засобів контролю полягає в закріпленні на тілі підозрюваного, обвинуваченого пристрою, який дає змогу відстежувати та фіксувати його місцезнаходження. Такий пристрій має бути захищений від самостійного знімання, пошкодження або іншого втручання в його роботу з метою ухилення від контролю та сигналізувати про спроби особи здійснити такі дії.

У відповідності до Закону України “Про Національну поліцію”, ст.25, задачею Нацполіції є забезпечення координації органів і підрозділів поліції щодо геолокаційного відслідковування за місцезнаходженням обвинувачених, інших осіб, що підозрюються у вчинені злочину, які зобов’язані в установленому законом порядку носити електронні засоби контролю.

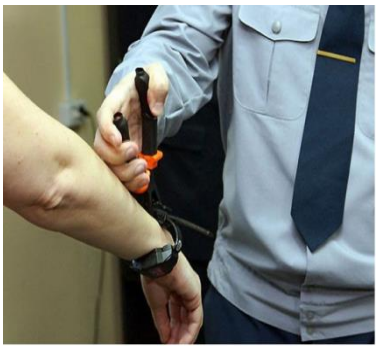
GPS-браслети для осіб, які перебувають під слідством

Мобільний контрольний пристрій – це електронний пристрій, призначений для носіння разом із електронним браслетом у разі перебування підозрюваного або обвинуваченого поза місцями, обладнаними стаціонарним контрольним пристроєм, для відстежування його місцезнаходження за допомогою глобальних навігаційних супутникових систем GPS/ГЛОНАСС.

Ретранслятор – це електронний пристрій, призначений для розширення зони прийому сигналів електронного браслета.

Електронні браслети захищені від несанкціонованого втручання. Кожен має індивідуальне кодування та пароль. У випадку спроби зняття браслета чи пошкодити його до відповідальної особи одразу надійде сигнал тривоги. Браслети протиударні, витримують значні перепади температур, перебування у воді. Він легко може бути прихований під одягом, а тому зручний у використанні.

Електронний пристрій у вигляді браслета (електронний браслет / персональний трекер) закріплюється на тілі підозрюваного, обвинуваченого (на руці чи нозі) і подаватиме сигнали на стаціонарний контрольний пристрій, що знаходиться у помешканні особи. Між контрольним пристроєм та електронним браслетом встановлено зв’язок: у випадку якщо браслет віддаляється на відстань, більшу від запрограмованої, подається сигнал тривоги, який надходить до центрального сервера, а звідти – особі, що здійснює безпосередній контроль за правопорушником.



Спосіб передачи контрольних сигналів

Функції мобільного пристрою, який заарештований завжди повинен мати при собі у разі знаходження поза місцями, обладнаними стаціонарним контрольним пристроєм

Мобільний пристрій використовують також як мобільний телефон. Тут запрограмовані мобільні номери інспектора, відповідального за підозрюваного і пульт моніторингу. Якщо у підозрюваного виникає непередбачувана обставина: проблеми зі здоров'ям, пожежа, потоп і т.д., і йому потрібно десь вийти, він набирає номер пульта, який за ним спостерігає. Розповідає про ситуацію і попереджає, що буде порушення. Пристрій подає арештанту сигнал, якщо він щось порушує. Наприклад: вийшов за дозволену зону, сідає акумулятор, пропадає сигнал GPS ... пристрій відразу «пищить» і повідомляє на екрані причину порушення.

5.10. Інтелектуальні експертні та інформаційні системи в юридичній та правоохоронній сфері

Однією з основних проблем у процесі розроблення систем штучного інтелекту є моделювання розумової діяльності людини. Історично процес моделювання розвивався у двох напрямках: відображення розумової діяльності за допомогою відповідних логічних співвідношень на великих ЕОМ з "традиційною" архітектурою та створення електронних систем (мереж) на основі нейробіонічного підходу з використанням замовлених мікросхем. В результаті досліджень та розробок по першому напрямку з'явилися так звані експертні системи (ЕС) на базі ПК, а по другому напрямку – спеціалізовані ЕОМ з принципово новою архітектурою (ЕОМ нового покоління). Зауважимо, що обидва підходи продовжують розвиватися і мають як спільні властивості, так і свої особливості.

Основні поняття щодо експертних систем в управлінні організаціями

ЕС – це комп'ютерні програми, здатні накопичувати знання і моделювати процес експертизи. Поява ЕС ознаменувала перехід від суто теоретичної сфери штучного інтелекту до прикладної. *ЕС можуть бути корисними тільки тоді, коли добре відомі способи пошуку рішення, а експерт може точно описати логіку розв'язання задачі*.

Найперпективнішими напрямами щодо створення цих систем вважають:

- *інтеграцію ЕС з традиційними пакетами* (табличними редакторами, СУБД) з метою врахувати при розв'язування кількісних задач якісні фактори;

- *створення ЕС "реального" часу* при управлінні неперервними процесами (наприклад, для підвищення надійності управління в енергетиці);

- *розробка динамічних ЕС* (тобто систем нереального часу, які враховують суттєві зміни, що відбуваються в процесі "обмірковування").

Основними сферами застосування ЕС є: *діагностика* – визначення стану об'єкта експертизи; *інтерпретація* – визначення сутності даних, що спостерігаються; *планування* – визначення програми дій за певним критерієм; *прогнозування* – визначення наслідків ситуації на основі поточного стану об'єкта експертизи; *навчання* – комплексне оцінювання результатів по багатьом факторам.

Ідеологію ЕС втілює формула СИСТЕМА = ЗНАННЯ + ВИСНОВОК. Основні компоненти такої системи надані на рис.5.7.

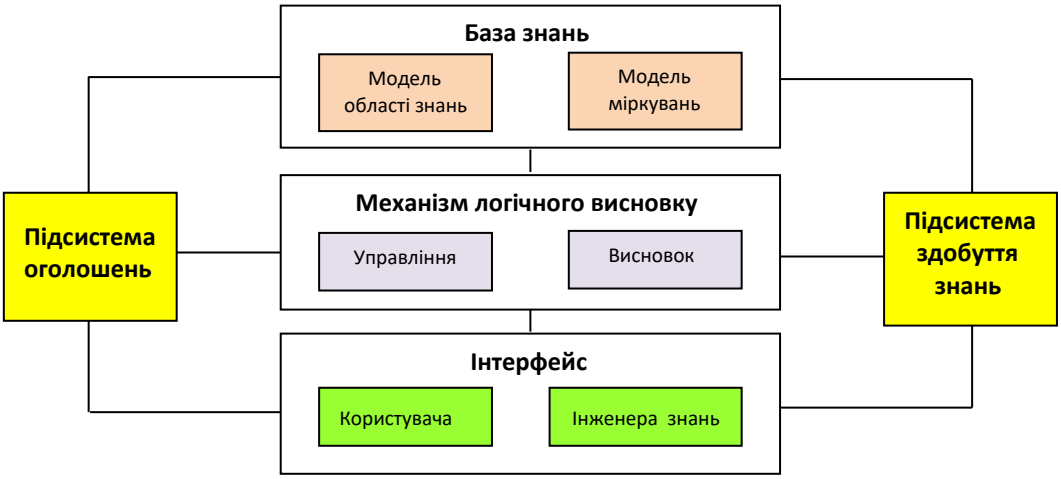


Рис. 5.7. Структурна схема експертної системи

Основні поняття щодо нейрокомп'ютерних систем

Спочатку такі системи розвивалися як системи із застосуванням традиційних методів моделювання роботи мозку людини за допомогою великих ЕОМ. Але такий підхід не давав можливості реалізувати корисні в практиці функції мозку, зокрема асоціативне мислення. Цей недолік почав усуватися з використанням нейробіонічного підходу щодо реалізації комп'ютерної системи (звідси і назва - нейрокомп'ютер, скорочено НК).

Дійсно, на звичайній ЕОМ достатньо просто моделюються формально-логічні елементи мислення, але реалізувати здатність людини адаптуватися в змінних і слабо формалізуємих умовах зовнішнього оточення на сьогодні практично неможливо. І це незважаючи на те, що рівень сучасної технології по щільності упаковки обчислювальних елементів та по економічності енергопостачання може бути зіставлений з нервовою тканиною. Тому для одержання ефективних результатів, заснованих на реалізації адаптивної здатності мозку, в дійсний момент сформувався новий науково-практичний напрямок – створення НК.

Цей напрямок знаменує появу ЕОМ нового покоління, в яких основним блоком є не системна плата з процесором, а нейронні мережі. На відміну від класичного поняття "мережа", в НК під мережею розуміється велика кількість паралельно з'єднаних та ієрархічно організованих в кожній окремій машині адаптивних елементів (нейронів у вигляді заказних мікросхем) за зразком біологічної нервової тканини. Основні відмінності НК від ПК полягають в наступному:

- *принципова інша організація обчислювань* (за допомогою нейромереж);

- *здатність к навчанню* (за допомогою адаптивної настройки нейронів);

- *висока завадо- і відмовостійкість* (за рахунок інформаційної надмірності нейромереж);

- *здатність вирішувати задачі, спираючись на неповну або суперечливу інформацію* (математичні методи та експертні системи не в змозі надати корисний результат, оскільки не мають асоціативного мислення);

- *можливість нарощувати потужність НК практично без обмежень* (за рахунок внутрішнього паралелизму нейронних мереж).

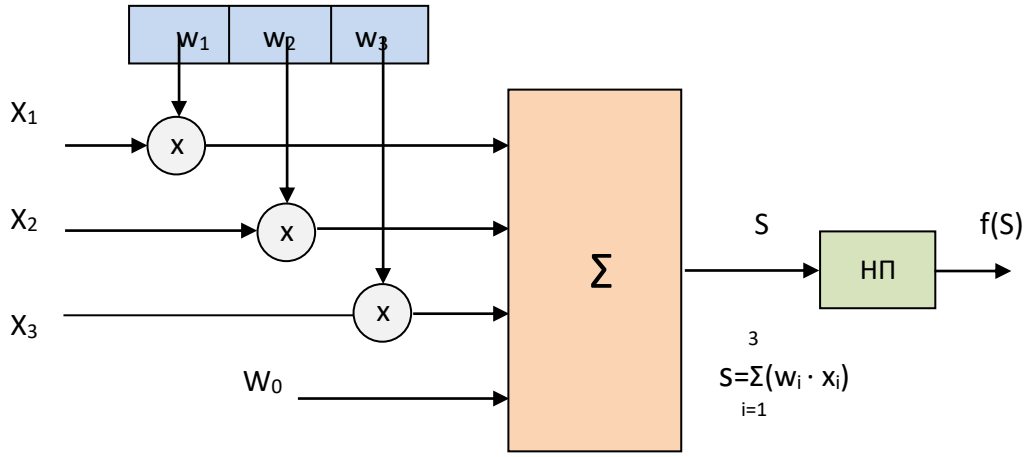


Рис. 5.8. Структурна схема нейрона в технічному виконанні

Структурна схема окремого нейрона з трьома сигнальними входами та входом зміщення на константу наведена на рис.5.8.

На даний час існує багато моделей нейромереж (наприклад, прямого розповсюдження, інша назва – багатошарові персептрони; повнозв'язані мережі Хопфілда; карти Кохонена та ін.).

Не зупиняючись на принципах організації мережі в кожному випадку, зазначимо, що усі вони використовують певний принцип підгонки вагових коефіцієнтів нейронів.

Технічно нейрон нагадує багатовходовий суматор, який виконує дві основні функції – складання добутку вхідних сигналів x_i на відповідні вагові коефіцієнти w_i та нелінійне перетворювання суми добутків S за певним критерієм (в самому простому випадку – порівняння з певним порогом, тобто $f(S)=1$ при $S>\theta$, $f(S)=0$ при $S\leq\theta$, θ - поріг спрацьовування, див. рис.7.5).

Якщо рішення задачі користувача на звичайній ЕОМ відбувається за попередньо розробленою програмою, то НК у більшості випадків повинен попередньо себе настроїти (на основі відомої відповіді тестової задачі того ж

типу). Настроюваними параметрами є вагові коефіцієнти нейронів. Можливе настроювання і без “вчителя” (самоорганізація за певним алгоритмом), але тоді клас вирішуваних задач звужується.

Слід додати, що на даний час розроблені програми-імітатори для звичайних ПК, які функціонально мало чим відрізняються від НК. До того ж такі програми (програмні комплекси) дешевші, ніж нейромережні комп’ютери. Але розв’язок задач в таких комплексах йде в режимі суттєво нереального часу.

Основне місце НК на ринку послуг – фінансові задачі, в яких нейромережі проявляють себе найбільш ефективно. Особливо це стосується задач прогнозування та передбачення в дуже ризикових інвестиційних проектах великого обсягу (від 1 млрд дол. та вище), коли традиційні методи моделювання безсилі. Крім того, НК успішно вирішують задачі медичної та промислової діагностики, надзвичайних ситуацій, в правовій діяльності.

Контрольні питання до розділу

1. Що таке база даних і система управління базами даних?
2. Охарактеризуйте стисло реляційну модель бази даних.
3. В чому суть архітектури клієнт-сервер?
4. Що таке інформаційна система? Які основні ІС ви можете назвати за функціональними можливостями?
5. Назвіть ряд однотипових етапів роботи будь-якої ІС.
6. Поясніть стисло етапи розвтку управлінських ІС.
7. Розкажіть стисло проможливості програми 1С:Підприємство. Управління малою фірмою.
8. Які можливості користувачу надає програма Ліга:Закон?
9. Що таке СППР. Чим СППР відрізняється від ІС?
10. Надайте характеристику складовим СППР, орієнтованих на дані.
11. Розкажіть стисло про складові СППР, орієнтованих на роботу з моделями.
12. В чому суть інтелектуальних експертних систем?
13. Розкажіть про можливості нейрокомп’ютерів в економіці та правоій сфері.

Ч.2. ОСНОВНІ ПОНЯТТЯ З ЕЛЕКТРОННОГО СУДОЧИНСТВА ТА ЕЛЕКТРОННОГО УРЯДУВАННЯ

РОЗДІЛ 6. ВИКОРИСТАННЯ ІТ та ІС В РОЗВИНУТИХ КРАЇНАХ

6.1. Загальні відомості

Підвищення рік від року кількості судових справ, навантаження на суддів неминуче ставить питання про підвищення продуктивності роботи судової системи в цілому. Одним з ключових напрямків підвищення ефективності роботи суддів та працівників апаратів судів, прозорості правосуддя є застосування ІТ. В ході впровадження цих технологій в судовій системі необхідно правове і нормативно-методичне забезпечення процесу впровадження автоматизованих систем судів, у тому числі процесів планування робіт, контролю і оцінки ефективності зазначених процесів. В даному питанні неоціненну допомогу може надати досвід США і окремих країн Євросоюзу, найбільш просунутих в сфері впровадження інформаційних технологій в діяльність судів.

Існує два тлумачення поняття "Електронний суд": вузька та розширена.

Вузька концепція: *ЕПК – це структурований бездокументарний обмін інформацією між сторонами і судами*. ЕПК – реальна заміна традиційного документообігу, що має таку ж правову значимість.

Ширша концепція: *ЕПК – це процес обміну інформацією з судами і надання судової інформації за допомогою електронних засобів комунікації*.

"*Електронний суд*" *включає в себе наступні компоненти*:

- звернення до суду в електронній формі та управління справою за допомогою інформаційних технологій;
- цифровий запис ходу судового розгляду;
- відеоконференції;
- безпечну електронну пошту;
- управління кадровими ресурсами суду та календар судових засідань;
- менеджмент в сфері фінансів та ІТ;
- управління рухом судових справ;
- моніторинг якості роботи та інші складові.

6.2. Електронний суд в США

Електронне забезпечення правосуддя в федеральних судах США виробляється в формах електронної публікації ("e-posting") і системи подачі судових документів у електронному вигляді ("e-filing").

Електронна публікація судових актів була розпочата в порядку експерименту в 1988 році на основі *системи Pacer*. Ініціатором створення Pacer виступав Адміністративний офіс судів США. В даний час можливий відкритий доступ всіх зацікавлених осіб до матеріалів судових справ і супутньої інформації в системі Pacer через Інтернет. Система Pacer включає в себе такі відомості: реєстр входять заяв; відомості у справі (предмет і ціна позову, номер справи, учасники засідання, в якій стадії розгляду справа перебуває); судові рішення і постанови; календар призначених до розгляду і розглянутих справ.

Для електронної подачі судових документів з 2001 року для судів США з питань банкрутства, а пізніше і для окружних та апеляційних судів було розпочато використання Системи "Управління справою / Електронне досьє справи" (Case Management / Electronic Case Files), далі – *CM/ECF*.

В даний час в разі подачі документів до федерального суду США в паперовій формі адвокати повинні обгрунтувати причини використання такої форми документів (наприклад, конфіденційність документа).

Система CM/ECF вимагає стандартного підключення до мережі Інтернет без будь-якого спеціального програмного забезпечення, подача документів здійснюється тільки в форматі Adobe Portable Document Format (pdf), яке зберігає розбивку на сторінки незалежно від типу комп'ютера.

Після подачі документів відправник отримує повідомлення про прийняті документах і система автоматично сповіщає інших учасників судової справи, зареєстрованих в системі. Правові аспекти використання електронного документообігу, захисту конфіденційності вирішуються в судах США на основі угод, що укладаються з учасниками процесу.

6.3. Електронний суд у Великій Британії

Позитивні кроки від впровадження проекту "ЕС" в Британії почали відчуватися тільки після 2010 року. Так, в 2013 р. британський уряд представив програму реформування системи кримінального правосуддя під назвою "Суд швидкий і невідворотний" (Swift and Sure Justice). Її стрижнем є максимальна діджіталізація судового процесу. Експеримент був проведений в найзавантаженішому суді країни – Бірмінгемі. Сенс експерименту полягав в тому, що використовувані технології (відеоконференції, цифрові презентації, бездротові мережі) були цілеспрямовано об'єднані в одному кримінальному процесі. Записи камер відеоспостереження, отримані протягом двох годин,

були представлені стороною обвинувачення в суді. На підставі цих доказів обвинувачений відразу визнав себе винним.

Більш того, британські судді можуть виносити вироки по Skype і Facetime, тобто приймати в онлайн-режимі рішення про взяття підсудного під варту, а також виносити вироки про позбавлення волі. Завдяки системі "живого зв'язку" судді можуть виносити рішення на попередніх слуханнях, коли обвинувачені, адвокати і прокурори зобов'язані бути присутніми в залі засідань. Зокрема, мова йде про призначення застави за звільнення. На думку представників судової системи Британії, такі нововведення дозволять заощадити час і гроші, витрачені на дорогу до суду і перевіз обвинувачених в спеціально обладнаному транспорті. На думку розробників ініціативи, такі зміни також позбавлять неповнолітніх свідків і потерпілих, які отримали психологічні травми, від знаходження в залі суду разом зі злочинцями.

Просувається ідея електронного суду і в системі цивільного правосуддя Великої Британії державною Радою з цивільного судочинства (Civil Justice Council). Так, в Лондоні триває робота над створенням єдиної системи онлайн-судів. Online dispute resolution system призначена для вирішення найпоширеніших цивільних позовів до 25 000 фунтів. З її допомогою можна отримати онлайн-роз'яснення, до якої категорії відноситься справа, а після цього система направляє відразу до судді, який вирішує спори онлайн. Розробники системи впевнені, що вона дозволить громадянам економити і вирішувати свої справи без залучення юриста.

В той же час Британська асоціація юристів, що спеціалізуються на цивільних справах (The Association of Costs Lawyers), занепокоїлася через проект Online dispute resolution system, оскільки вирішення справ без залучення юриста принесе скоріше не економію, а збільшення навантаження суддів. Адже якщо раніше громадяни залучали юриста, щоб обґрунтувати суми своєї вимоги, а судді залишалося лише прийняти рішення про стягнення, то тепер всі питання оцінки належить вирішувати самому судді.

Станом на 2016 рік за ініціативою центру Justice суди матимуть "судові декорації, що легко перевозяться, дистанційні відеоекрани, а також технології для он-лайн-доступу". Так звані суди в коробці включатимуть основні елементи, які можна легко транспортувати й зібрати на місці. Це, на думку експертів, дасть можливість створити більш цілеспрямований підхід у цифровому вигляді, тобто зробити систему правосуддя відкритішою для простих людей, з відповідними і пропорційними способами вирішення спорів, доступними для всіх.

В аналітичному центрі підкреслюють, нині утримання судових будівель у Великій Британії щорічно обходиться платникам податків у $724 млн (18,3 млрд грн. — це втричі більше, ніж цього року виділили судовій системі України на всі потреби). У зв'язку із цим в Justice пропонують відкрити мобільні суди в будівлях регіональних законодавчих рад, бібліотек, громадських центрів або навіть шкіл і університетів.

Видання відзначає, що ця пропозиція була висловлена на тлі масового закриття судів по всьому Сполученому Королівству. У лютому 2016 р. стало відомо, що Мін'юст країни вирішив закрити 86 судів на території Англії і Уельсу й продати будівлі, в яких вони розташовувалися. Таким чином уряд планує отримати кошти для "модернізації судової системи".

За результатом огляду можна зробити наступний висновок. Реалізація ідеї електронного судочинства є актуальною і перспективною, але має здійснюватися одночасно із створенням правової та матеріальної бази щодо захисту електронної інформації. Від цього залежить безпека учасників кримінально-процесуальних відносин, а також справедливість, рівність, законність та неупередженість судового процесу та рішень.

6.4. Електронний суд у Німеччині

Точкою відліку нормативного оформлення електронного судочинства в Німеччині прийнято вважати 2001 р., коли були видані два закони, що врегулювали окремі аспекти електронної комунікації з судами. Перший з них, Закон про реформу процесу в частині вручення документів при здійсненні судочинства, передбачив можливість вручення судами документів електронним способом; другий, Закон про адаптування до сучасного правового ділового обороту приватноправових вимог про дотримання форми та інших нормативних актів, ввів в законодавство поняття електронного документа та визначив умови, при яких він може використовуватися в якості рівнозначного документу в звичній письмовій формі. За більш ніж 15 років, що минули з часу прийняття названих законів, електронне судочинство в Німеччині істотно просунулася у своєму розвитку. Разом з тим говорити про те, що процес його формування завершився, поки передчасно.

До теперішнього часу вдалося створити законодавчу базу електронного судочинства. Однак практична реалізація багатьох нормативних приписів залишається справою майбутнього. Так, в липні 2017 був прийнятий закон, що встановлює обов'язок вести судові справи, в тому числі кримінальні, в електронному вигляді (Закон про введення електронних справ в сфері юстиції

та про подальше сприяння електронному правовому обігу). Цей Закон повинен бути виконаний станом на 1 січня 2026 р. До того часу Федерація і землі можуть за допомогою прийняття своїх нормативно-правових актів передбачити ведення електронних справ в певних судах або щодо певних категорій справ.

Електронне судочинство характеризується не тільки динамічністю розвитку, воно також є явищем, що охоплює велику кількість різнорідних елементів і відрізняється багатогранністю.

До складу електронного судочинства в Німеччині входять електронна комунікація між судом і учасниками процесу, електронні судові справи, різні електронні реєстри, ведення яких віднесено до компетенції судів, розміщення в мережі Інтернет інформації про судах, розміщення в банках даних судових рішень, використання відеоконференцзв'язку та ряд інших елементів.

Можливість ведення в німецьких судах електронних справ вперше була встановлена в 2005 р Законом "Про використання електронних форм комунікації в сфері юстиції". Таким чином, до існуючих з 2001 р. норм про електронну подачу позову і електронне вручення судових документів додалися норми про ведення електронних справ та прийняття судових рішень у формі електронного документа. Відповідно, з прийняттям Закону 2005 року теоретично стало можливим ведення всього судового процесу, за винятком процесу у кримінальних справах, в електронному вигляді. Для того, щоб суд міг почати вести електронні справи, федеральний або земельний уряд, кожен в межах своїх повноважень, повинні прийняти відповідне розпорядження.

Перехід до електронних справ пов'язаний з цілою низкою проблем, зокрема, із збереженням незалежності суддів і запобіганням втручання сторонніх осіб в судову діяльність, забезпеченням інформаційної безпеки і захисту персональних даних, збільшенням технологічної залежності судової влади, готовністю суддів і працівників суду до кардинальної зміни звичних робочих процесів.

Як показує досвід формування електронного судочинства в Німеччині, від прийняття політичного рішення про реформування того чи іншого аспекту судової діяльності до його практичної реалізації проходить чимало часу. Тому даний розвиток навряд чи буде стрімким. Можна вважати, що німецьке законодавство пропонує збалансоване рішення: на професійних учасників процесу (адвокатів, органи влади, нотаріусів) покладається обов'язок використовувати електронні способи комунікації з судом; громадяни ж вправі

вибирати, чи звертатися до суду по електронних каналах зв'язку або ж у звичній письмовій формі.

Також, особливого значення набуває забезпечення незалежності суддів і виключення втручання сторонніх суб'єктів в здійснення судочинства, а також забезпечення безпеки даних і їх захисту. Всім цим проблемним аспектам як в німецькій доктрині, так і на практиці приділяється серйозна увага.

Електронний суд в республіці Білорусь

У Білорусі розвивається електронне правосуддя або e-justice (electronic justice), віртуальною основою якого визнаний вебсайт Вищого господарського суду (ВГС, або court.by), що містить детальну інформацію про всі господарські суди Білорусі. У широкому сенсі під e-justice розуміють не тільки, власне, електронне судочинство, але і всі супутні судочинству процеси, включаючи організацію діяльності суду, не пов'язану з відправленням правосуддя.

Як правило, до елементів e-justice відносять такі: подача позову й іншого процесуального документа за допомогою інтернету; використання засобів доказування в електронній формі; проведення судового засідання онлайн через відеоконференції, пересилку через електронну пошту; формування електронного досьє, тобто й переклад документообігу і діловодства в електронну форму; доступ до матеріалів справи учасникам процесу та іншим особам через інтернет; використання електронних судових повісток; здійснення всього судочинства виключно за допомогою інтернету – електронний суд або cybercourt, e-court.

Підкреслюється, що ініціатором упровадження e-justice в Білорусі став Вищий Господарський Суд. На законодавчому рівні термін електронне правосуддя закріплений у Програмі діяльності Уряду Республіки Білорусь на 2011-2015 рр., згідно з якою одним із механізмів інформатизації всіх сфер діяльності є, в т. ч., сприяння формуванню електронного правосуддя.

Повномасштабне застосування елементів e-justice в господарських судах почалося 2010 р., що дозволило оптимізувати судочинство та мінімізувати час розгляду судових справ, при цьому застосовувалися такі елементи "електронного правосуддя": подача електронних копій документів, електронний розклад судових засідань, розміщення в резолютивній частині постанов касаційної інстанції в online режимі на порталі господарських судів Республіки Білорусь court.by; аудіо- та відеофіксування судових засідань, використання документкамер і таке інше.

В даний час електронне звернення можна подати з використанням веб-сайту ВГС, наприклад, за допомогою сервісу «електронні форми подачі звернень» у ВГС можна подавати: позовну заяву, відгук на позовну заяву, скаргу на дію судового виконавця, заяву про порушення наказного провадження, заяву про банкрутство та ін. Нормативно закріплені положення, що забезпечують використання в господарському судочинстві електронного документообігу та інформаційних технологій: використання електронних копій документів; розсилка повідомлень про дату і час проведення судових засідань по електронній пошті; застосування відеоконференцзв'язку для проведення судових засідань, здійснення окремих процесуальних дій онлайн.

6.6. Застосування ІТ в європейських судах у відповідності до Висновку КРЄС

При роботі над Заключенням Консультативної Ради Європейських Суддів (КРЄС) була опублікована цікава і гостра інформація стосовно використання ІТ в європейських судах. Ще одним джерелом інформації стало опитування, проведене *Комісією Ради Європи з ефективності правосуддя (СЕРЕЈ)*. До речі, таке дослідження в Європі проводиться кожні два роки. Зібрані дані публікуються у вигляді звіту двома роками пізніше. Дані за 2004 рік були опубліковані в звіті за 2006 рік. СЕРЕЈ займається вивченням використання ІТ в судах, починаючи з 2004 року, так що це дає нам огляд шести років розвитку ІТ в судах. Ці два джерела і використані в подальшому матеріалі.

Для своїх звітів СЕРЕЈ класифікує ІТ за її роллю в судовому процесі:

- пряма підтримка для судей і співробітників. Ця категорія включає в себе більшість офісних технологій, діловодство, складання списку справ, електронну пошту і бази даних з юриспруденції. Вона також включає в себе технології, що підтримують роботу в залі суда;

- підтримка взаємодії між судом і сторонами. Включає в себе комунікаційні технології для передачі інформації всередині організації та за її межі: сторонам та широкій громадськості.

Методологія СЕРЕЈ не охоплюють такі технології, як відеоконференції, обмін повідомленнями, блоги, вікі і Інтранет.

Висновок КРЄС визнає, що ІТ пропонує нові можливості для розгляду справ, а також сучасний безкоштовний доступ до правової інформації та даними за прецедентним правом. Звернення до ІТ полегшує обмін документами і доступ сторін і їх представників до інформації з розгляду

справи. Відеоконференції можуть спростити проведення слухань в умовах підвищених вимог до безпеки або заслуховування віддалених свідків.

ІТ не повинні:

- зменшувати процесуальні гарантії справедливого судового розгляду;
- створювати перешкоди для проведення обов'язкових слухань і завершення інших необхідних формальностей, передбачених законом;
- виходити за рамки заміни і спрощення процедурних кроків, які ведуть до індивідуалізованого вирішення справи по суті;
- замінювати роль судді у заслуховуванні і зважуванні фактичних доказів.

Суддя повинен зберігати за собою дану йому законом владу в будь-який час викликати сторони, надати оригінали документів та заслухати свідків. *Відеоконференції ніколи не повинні погіршувати гарантії захисту*.

Висновок КРЄС визнає, що доступ до інформації за допомогою ІТ може сприяти більшій самостійності суддів у виконанні їх завдань, і що ІТ можуть стати важливим інструментом для підвищення прозорості та об'єктивності при розподілі справ і поліпшення управління справами.

Висновок також визначає значну область ризиків, пов'язаних з впровадженням ІТ, яке може обмежити свободу прийняття судових рішень і порушити судовий процес. ІТ повинні бути використані для підвищення незалежності суддів на кожному етапі процедури і не повинні піддавати цю незалежність додатковими ризиками.

Незалежно від того, який орган відповідає за управління ІТ, існує необхідність забезпечити активну участь суддів у прийнятті рішень з використанням інформаційних технологій в широкому сенсі. Судді і співробітники суду мають не тільки право, а й обов'язок отримати початкове та поточне навчання з інформаційних технологій, щоб вони могли в повній мірі і належним чином використовувати ІТ системи.

Фінансування ІТ має будуватися на оцінці їх внеску в підвищення продуктивності суду, поліпшення якості правосуддя і рівня обслуговування громадян.

Найбільше занепокоєння у КРЄС викликає ризик того, що впровадження ІТ може загрожувати свободі суду визначати процедури і вести справи. Це занепокоєння виражено в більш ніж чверть положень Висновку.

Очевидно, що ІТ, які не впливають безпосередньо на процес судового розгляду, такі, як електронна колекція юриспруденції або, навіть, електронна подача документів, розглядаються КРЄС схвально. Крім того, ці ІТ

впроваджуються відносно легко. ІТ, які безпосередньо впливають на судовий процес, явно викликають занепокоєння і навіть опір.

Однак найбільш важливий недолік полягає у відсутності стратегічного бачення процесу здійснення правосуддя, сформованого знанням і розумінням ролі інформації в судах.

Післямова до розділу 6

Узагальнюючи міжнародний досвід впровадження ІКТ у судову діяльність, варто відзначити загальні тенденції до модернізації судової системи, а саме: централізація даних у межах країни, побудова державної мережевої інфраструктури, застосування автоматизованих систем діловодства та електронного документообігу, систем аудіо- та відеофіксації, систем захисту свідка, системи відеоконференцзв'язку, системи управління речовими доказами та ін.

Окрім вже названих країн подібні системи електронного судочинства станом на січень 2018 року впроваджені в Австралії, Канаді, Республіці Корея, Японії, а також практично в усіх західноєвропейських країнах. Швидко та ефективно йде просування ЕС в Російській Федерації та в Китаї.

Цікаво, що на даний час до електронного судочинства приєдналися вже деякі африканські країни (наприклад, Замбія, Уганда, Гана), причому одночасно з впровадженням необхідних нормативно-законодавчих документів вони реалізують й певні технічні рішення, зокрема, захищені комп'ютерні мережі, системи електронного документообігу, відеоконференції.

Контрольні питання до розділу

1. Що таке електронний суд у вузькому та широкому смислі?
2. Розкрийте суть електронного суду в США.
3. Розкрийте стисло суть електронного суду у Великій Британії та Німеччині.
4. Поясніть суть занепокоєнь КРЄС щодо застосування електронного суду в європейських судах.
5. Дайте оцінку стану розвитку ІТ в судах інших країн, зокрема в республіці Білорусь.
6. Надайте основні висновки стосовно досвіду впровадження ІКТ в судову діяльність розвинутих країн.

РОЗДІЛ 7. ВИКОРИСТАННЯ ІТ У ВІТЧИЗНЯНІЙ СУДОВІЙ СФЕРІ

В цьому розділі переважно розглядаються питання і проблеми автоматизації судів загальної юрисдикції. Незважаючи на специфіку інформатизації судової діяльності та важку формалізацію процесів судочинства, за останні роки в Україні проведена велика робота по оснащенню суддів і працівників апаратів судів засобами нових інформаційних технологій.

7.1. Про успіхи впровадження ІТ в суди України

Слід відразу зазначити, що розвинені країни, які впроваджують "електронний суд", в повній мірі його не реалізували (за винятком, може бути, Сінгапуру, де судочинство повністю здійснюється без паперових носіїв). Тому під поняттям "електронний суд" можна розглядати застосування в судочинстві певних засобів інформаційних технологій, які вже показали свою ефективність.

Так, з 2012 року Державна судова адміністрація розпочала реалізацію пілотного проекту з розвитку електронного судочинства. Згідно із затвердженим наказом ДСАУ від 07.09.2012 Тимчасового регламенту обміну електронними документами між судом і учасниками судового процесу визначена процедура подачі заявки про отримання процесуальних документів в електронному вигляді (у якості пілотних виступали 15 судів України).

В Україні застосовується дистанційна участь сторон в судовому процесі за допомогою засобів аудіо- або відеокомунікацій. Так, в кримінальному процесі України вже не тільки є можливість, а й активно застосовується проведення відеоконференції з учасником судового процесу.

Тобто, для учасників процесу створюється можливість використовувати переваги послуг "електронного суду". Проте не всі послуги ще реалізовані і не всі запущені програми широко застосовуються. Так, можлівість сторін і суду подаваті процесуальні документи в електронній формі суттєво гальмується технічним оснащенням невеликих судів, а з іншого боку – не дуже активним застосуванням електронного цифрового підпису учасниками процесу (навіть професійними адвокатами).

Найбільш активно розвивається проект "Електронний суд" в Київському районному суді м. Одеси. Там зазначають, що значним плюсом проекту є залучення інших державних органів до комунікації з судом за допомогою електронних технологій. На сьогодні налагоджено обмін інформацією з

органами юстиції, міграційної служби, прокуратури, виконавчої служби, поліції та експертними установами.

Слід зазначити, що чинне процесуальне законодавство не передбачає можливість направлення справи суду в апеляційну чи касаційну інстанцію в електронному вигляді (навіть, якщо воно все-таки існує поряд з традиційно сформованою справою). Процесуальний закон також не передбачає можливість направлення як стягувачу, так і органам виконавчої служби виконавчого листа в електронному вигляді. Це підкреслює необхідність термінової зміни законодавства, інакше всі розмови про розширення "Електронного суду" залишаться на папері, в крайньому випадку на плечах окремих ентузіастів.

7.2. АІС, АСД, ІПС та інші системи в судах загальної юрисдикції

Основними інформаційними технологіями, розробленими для судів, є програмні комплекси "Кадри", "Бухгалтерія", "Статистика", "Документообіг", ВКЗ. Однак, за твердженням фахівців, вони застосовуються лише в невеликому числі судів.

В останні роки з метою оперативного надходження до судів правової інформації деякі суди стали використовувати електронну пошту та мережу Інтернет, а також застосовувати в своїй роботі правові автоматизовані інформаційно-пошукові і довідкові системи (наприклад, "Ліга: Закон", "Юрист-експерт" та ін).

Однак використання перерахованих технологій не забезпечує єдності судової системи країни та істотного підвищення ефективності їх діяльності. Для вирішення даних проблем пропонується розробити та впровадити вітчизняну АІС "Правосуддя" на основі Державної автоматизованої системи з аналогічною назвою "Правосуддя", яка з 2007 р ефективно функціонує в усіх судах загальної юрисдикції РФ.

АІС "Правосуддя" має багаторівневу ієрархічну структуру, відповідну ієрархії судів загальної юрисдикції і складається зі спеціалізованих автоматизованих комплексів, як-то: "Адміністративне управління", "Організаційне забезпечення", "Право", "Фінанси і контроль", "Кадри", "Судове діловодство і статистика", "Банк судових рішень", "Відеоконференц-зв'язок" , "Судова експертиза", "Документообіг", "Навчання", " Громадські зв'язки", "Матеріально-технічні ресурси", "Звернення громадян", "Нерухомість", "Інформаційно-довідкова підсистема" і ряд інших підсистем.

7.3. Електронний суд запрацював у тестовому режимі у 18 судах країни

У 18 судах країни розпочато тестування підсистеми Єдиної судової інформаційно-телекомунікаційної системи "Електронний суд". Відповідно до наказу ДСАУ, з 4 червня 2018 року систему "Електронний суд" запустили у Київському апеляційному адміністративному суді, Апеляційному суді Одеської області, Київському районному суді міста Одеси, Одеському апеляційному господарському суді, господарському суді Одеської області, Вінницькому апеляційному адміністративному суді, Вінницькому окружному адміністративному суді, Донецькому апеляційному адміністративному суді, Голосіївському, Дарницькому, Деснянському, Дніпровському, Оболонському, Печерському, Подільському, Святошинському, Солом'янському, Шевченківському районних судах міста Києва.

Як пояснив заступник Голови Державної судової адміністрації України Сергій Чорнуцький, для початку роботи з сервісом необхідно зайти за веб-адресою "cabinet.court.gov.ua", де користувач має зареєструвати власний електронний кабінет (або "Офіційна електронна адреса" – відповідно до процесуальних кодексів). Реєстрація досить проста, потребує лише наявності ключа з електронним цифровим підписом. При цьому для реєстрації можуть бути використані ключі, видані будь-яким Акредитованим центром сертифікації ключів.

При реєстрації система автоматично "збирає" дані про особу з ЕЦП (прізвище, ідентифікаційний код, тощо). Недостатні (чи змінені дані, наприклад, про електронну пошту) необхідно внести чи відкоригувати самостійно. Після цього реєстрація завершена, а користувач одразу потрапляє в сервіс вже доступного на сьогодні "Електронного суду". Надалі, після розробки інших сервісів ЕС, в електронному кабінеті буде доступний перелік всіх таких сервісів та відповідне посилання для можливого їх використання.

Правові підставі та порядок використання відповідної підсистеми на перехідний період (до впровадження Єдиної системи ЕС) визначено Положенням про автоматизовану систему документообігу суду, затвердженим в редакції рішення Ради суддів України від 12.04.2018 № 16.

7.4. Проблеми функціонування ЕС в Україні від суддів

Попри усі очевидні переваги електронного судочинства проект "електронний суд" (у вузькому розумінні) не набув широкої популярності і просування його відбувається вкрай повільно. Те саме стосується деяких інших загальнодержавних електронних проектів у судочинстві (обмін електронними документами із використанням ЕЦП, проведення судових засідань у режимі відеоконференцій, використання електронно-інформаційних кіосків тощо).

Узагальнення та аналіз наявної інформації з цього приводу дозволяє назвати такі основні стримуючі чинники.

По-перше, це відсутність єдиної уніфікованої інформаційної платформи для спілкування учасників процесу з судом та з іншими державними органами.

По-друге, це відсутність єдиних стандартів щодо інформаційного контенту, котрим мають відповідати судові інформаційні ресурси та електронні сервіси, а також відсутність стимулів щодо їх покращення.

По-третє, це брак коштів. Відсутність належного фінансування судової системи взагалі і видатків на інформатизацію зокрема призводить до неспроможності задоволення потреб усіх охочих у користуванні певними сервісами внаслідок недостатності потужностей відповідних програмно-апаратних комплексів та недостатності спеціалістів для їх обслуговування.

І, *по-четверте*, це дисонанс інформаційних технологій та процесуальних правил. Зараз домінуючою є тенденція вбудовування нових інформаційних технологій до існуючої системи процесуальних норм різних гілок судових юрисдикцій. Правила судового процесу, якщо і змінюються, то лише фрагментарно, в мінімально необхідному для того чи іншого нововведення обсязі. Судовий процес у цілому, вік основних норм якого налічує десятки років, а вік основних принципів – десятки сторіч, залишається незмінним.

За таких обставин *ккд* від таких інформаційних технологічних вдосконалень є мінімальним. Це все одно, що гужовий транспорт оснастити новітніми засобами супутникової навігації, або стрілецький лук оснастити лазерним прицілом. Це незначно прискорить перший і не багато додасть ефективності другому.

Проблема інформаційно-процесуального дисонансу посідає особливе місце. Саме вона не дає можливості вітчизняному судочинству зробити перехід на якісно новий інформаційно-технологічний рівень. *Утім, усі названі*

та багато інших проблем на шляху до інформатизації судочинства є похідними від однієї стратегічної проблеми.

В Україні досі не держава існує для громадянина, а громадянин для держави. На відміну від бізнесу, який орієнтується на потреби замовників, держава в особі своїх органів орієнтується на власні потреби, тією чи іншою мірою ігноруючи потреби громадян. Відповідно, істотно розрізняються і встановлені процеси взаємодії.

За таких умов судова система внаслідок нежвавості законодавця ставиться у вкрай невигідне становище. Вона опиняється частково (а в окремих випадках повністю) непридатною для здійснення судочинства за допомогою новітніх ІТ.

Деякі з названих причин лежать на поверхні і мають відносно прості рішення. Але рішення для більшості причин, на жаль, знаходиться на даний час методом спроб і помилок, що затягує час реалізації судової реформи і призводить до відставання вітчизняного судового процесу від практики розвинутих країн.

Контрольні питання до розділу

1. Надайте стислу класифікацію сучасних ІС.
2. Назвіть компоненти та етапи функціонування ІС.
3. Розкажіть про суть існуючих АІС у судово-правовій діяльності.
4. Що таке СППР? Розкажіть про використати СППР в СД.
5. Що являє за своєю суттю ІПС “ЛІГА:ЗАКОН” та які можливості система надає своїм користувачам?
6. Розкажіть про суть правової системи IPLEX.
7. Як оцінюють перспективи впровадження “електронного” суду юристи?
8. Назвіть першочергові кроки для поліпшення стану електронного судочинства в Україні.

РОЗДІЛ 8. ПРОЕКТ “ЕУ” ЯК ОСНОВА УСПІШНОЇ РЕАЛІЗАЦІЇ ЕЛЕКТРОННОГО ПРАВОСУДДЯ

Побудова в Україні електронного правосуддя не буде достатньо ефективною без одночасної побудови ще більш масштабного системного проекту (далі, Проект) – “Електронного урядування” (ЕУ). У наступному розділі надаються основні відомості щодо суті Проекту та умовах і можливостях його впровадження в нашій країні.

8.1. Актуальність впровадження електронного урядування, його суть і напрямки його розвитку

Основні недоліки державного управління в середині минулого сторіччя в колишньому СРСР

- ❖ кризисні явища в державному управлінні – бюрократизм, централізація, тіньова економіка, корупція;
- ❖ сінонімічність управління та адміністрування;
- ❖ затратний характер державного управління.

Результат – різке падіння довіри населення до системи державного управління

Актуальність для України

У рамках реалізації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Україна має забезпечити комплексний розвиток ЕУ відповідно до європейських вимог.

Розпорядженням Кабінету Міністрів України від 3 квітня 2017 р. № 275 “Про затвердження середньострокового плану пріоритетних дій Уряду до 2020 року та плану пріоритетних дій Уряду на 2017 рік” розвиток електронного урядування визначено одним з першочергових пріоритетів реформування системи державного управління.

Суть “Концепції розвитку електронного урядування в Україні” (схвалена розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р)

Електронне урядування – форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян.

Метою електронного урядування є розвиток електронної демократії задля досягнення європейських стандартів якості надання електронних адміністративних послуг, відкритості та прозорості влади для громадянина, суспільства та бізнесу.

Електронна демократія – форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоврядування шляхом широкого застосування інфокомуніка-ційних технологій в демократичних процесах.

Електронна демократія дає змогу: поліпшити прозорість процесу прийняття рішень, а також підзвітність демократичних інститутів; поліпшити зворотну реакцію суб’єктів владних повноважень на звернення громадян; сприяти публічним дискусіям та привертати увагу громадян до процесу прийняття рішень.

ПРОБЛЕМА: Як свідчить вітчизняна практика, будь-яка інформація від державних органів завжди є значною мірою дозованою. При цьому влада, у випадку коли якась інформація є їй певним чином “незручною”, а її розповсюдження є невигідним, у більшості випадків тяжіє до банального приховування від суспільства під егідою її конфеденційності.

Першочергові проблеми розвитку електронного урядування в Україні (з Концепції)

1. Низька якість управління розробленням, впровадженням, підтримкою функціонування та розвитком інформаційно-телекомунікаційних систем (бази даних, реєстри тощо) та ресурсів (центри обробки даних, телекомунікаційні мережі тощо) органів влади.
2. Несформованість базової інформаційно-телекомунікаційної інфраструктури електронного урядування як техніко-технологічної основи для реалізації всіх проектів і завдань у зазначеній сфері.
3. Відсутність автоматизованого обміну даними та інтероперабельності між інформаційно-телекомунікаційними системами органів влади.
4. Недостатній рівень інформаційної безпеки та захисту інформації в інформаційно-телекомунікаційних системах органів влади.
5. Низькі темпи запровадження електронних форм взаємодії між органами влади і фізичними та юридичними особами, зокрема надання електронних послуг та доступу до відкритих даних.
6. Неврегульованість питання електронної ідентифікації та аутентифікації фізичних та юридичних осіб під час взаємодії з органами влади.
7. Низькі темпи розвитку внутрішніх систем електронного документообігу та сучасних інформаційно-аналітичних інструментів підтримки прийняття управлінських рішень.
8. Недостатній рівень готовності державних службовців та працівників органів місцевого самоврядування, фізичних та юридичних осіб до запровадження і використання інструментів електронного урядування.
9. Цифрова нерівність у використанні інформаційно-комунікаційних технологій між органами влади на центральному та місцевому рівні.
10. Недостатній рівень участі громадян та контролю у зазначеній сфері.

Шляхи вирішення проблеми розвитку електронного урядування в Україні

У затвердженій Концепції електронного урядування вказано, що вирішення проблеми розвитку електронного урядування в Україні необхідно здійснювати шляхом застосування сучасних інноваційних підходів, методологій та технологій (у тому числі Інтернету речей, хмарної інфраструктури, Blockchain, Mobile ID, shareding economy, просування

методики опрацювання даних великих обсягів (Big Data). Пояснемо детальніше суть цих технологій.

Інтернет речей (англ. Internet of Things, IoT) – це об'єднання будь-яких об’єктів (речей) в мережу для покращення їхньої функціональності.

Хмарна інфраструктура -– це чітко спроектоване і надане в комерційне користування віртуальне програмне середовище (сервери, комп’ютери, окремі сервіси), розгорнуте на базі дата-центрів.

Blockchain – новітня блокова технологія створення баз даних в Internet.

Mobile ID – це цифровий підпис, згенерований на мобільному телефоні або на SIM-карті мобільного телефона.

Shareding economy - спільне споживання. Ця концепція має на увазі здачу в оренду невикористовувані автомобілі, будинки, велосипеди, техніку та інші об'єкти.

Big Data - технології пошуку, обробки та застосування неструктурованої інформації у великих обсягах.

Інтернет Речей або Internet of Things (IoT) – це мережа речей, які підключені до мережі Інтернет. Речі включають IoT-пристрої і фізичні об’єкти, які оснащені IoT. Цей термін включає в себе широкий спектр застосувань, від споживчих пристроїв (наприклад, розумний холодильник, трекери для домашніх вихованців, сенсори для худоби, машини, роботи, нафтогазові комплекси або навіть працівники). Етапи розвитку технології наведені на рис. 8.1.

Рис. 8.1. Етапи технологічного розвитку “Інтернет Речей” у часі

8.2. Основні складові Концепції електронного урядування

Далі надана деталізація усіх чотирьох складових Концепції електронного урядування.

Електронна взаємодія органів влади

Електронний доступ до публічної інформації та відкритих даних в інформаційному просторі:

- забезпечення суспільства інформацією про діяльність органів влади;
- забезпечення суспільства важливими даними з усіх сфер діяльності.

ЕЛЕКТРОННА УЧАСТЬ ГРОМАДЯН В УРЯДУВАННІ (Е-ДЕМОКРАТІЯ)

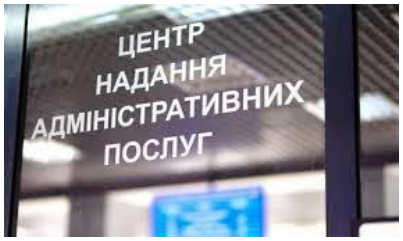
ЕЛЕКТРОННЕ
підключення

ЕЛЕКТРОННА
on-line участь

ЕЛЕКТРОННЕ
партнерство

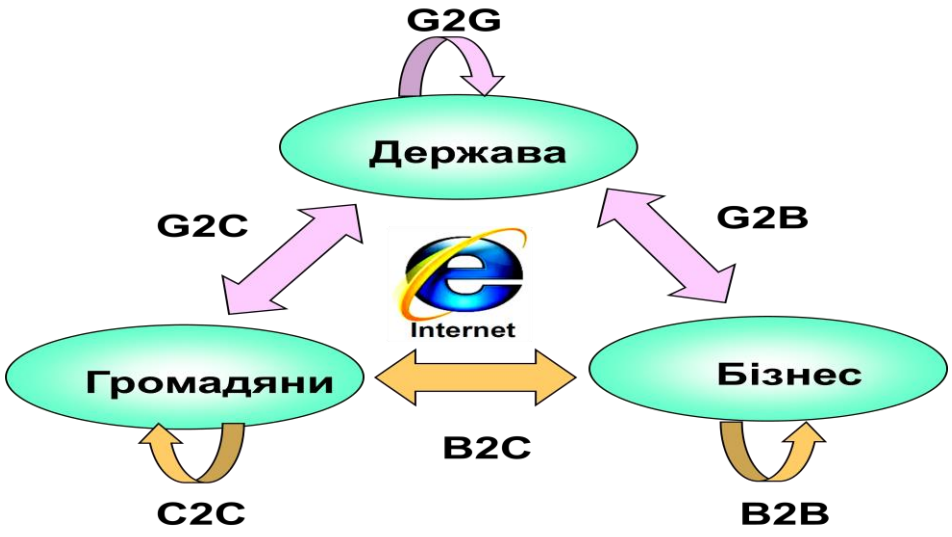
ЕЛЕКТРОННІ ПОСЛУГИ (СЕРВІСИ)

Адміністративні послуги з електронним оформленням

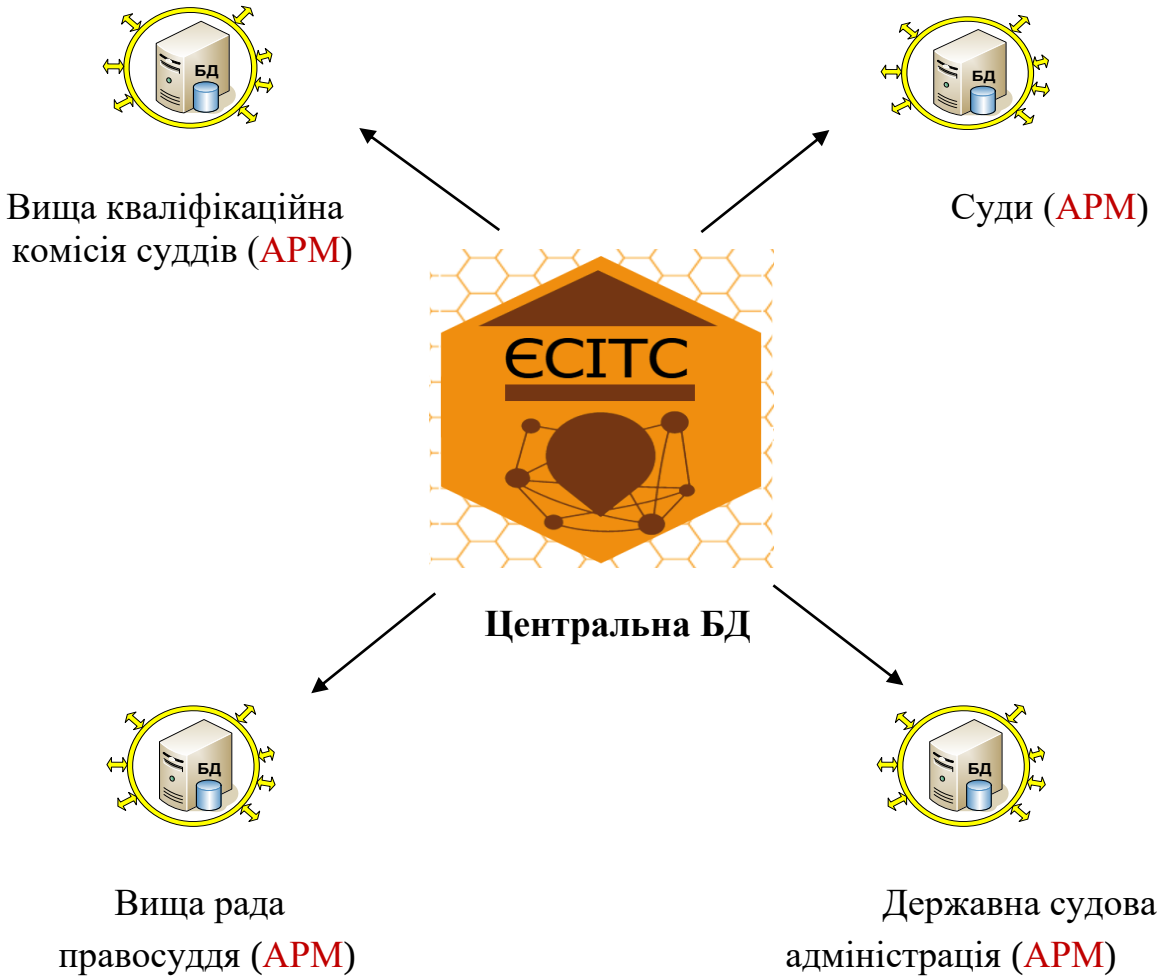


Електронні консультації та інші електронні сервісні послуги

РІВНЕВА МОДЕЛЬ ПРОЦЕСІВ ВІДНОСИН В СЕРЕДИНІ ЕЛЕКТРОННОГО УРЯДУВАННЯ



Приклад взаємодії G2G – G2G на основі АІС “Єдина судова інформаційно-телекомунікаційна система органів судової влади України”



Сервіси ЄСІТС

Приклад взаємодії B2B – B2B

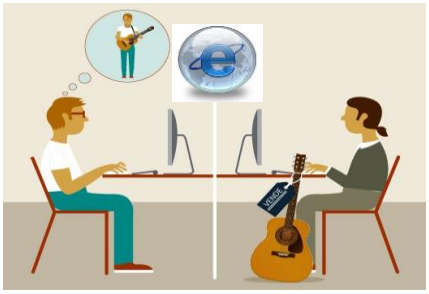
Основні складові такої взаємодії – це бізнес-посередництво, виробничий та збутовий бізнес, Інтернет-торгівля. Для спрощення подальшого матеріалу зупинимося на Інтернет-торгівлі.

Інтернет-магазин (*online shop или e-shop)* дозволяє користувачам онлайн в своєму браузері або через мобільний додаток сформувати замовлення на покупку, вибрати спосіб оплати і доставки замовлення, оплатити замовлення. При цьому продаж товарів здійснюється дистанційним способом і він накладає обмеження на товари, що продаються. Так, в деяких країнах є заборона на інтернет-торгівлю алкоголем, зброєю, ювелірними виробами.

Процес оформлення замовлення в інтернет-магазині автоматизовано на 100%, тому величезні портали з багатотисячним асортиментом товарів можуть з легкістю обслуговувати меньша чилельність менеджерів, ніж у звичайній (традиційній) торговельній компанії.

Обираємо товар | Кладемо твар у віртуальний кошик | оформляємо онлайн заказ | оплачуємо | отримуємо товар

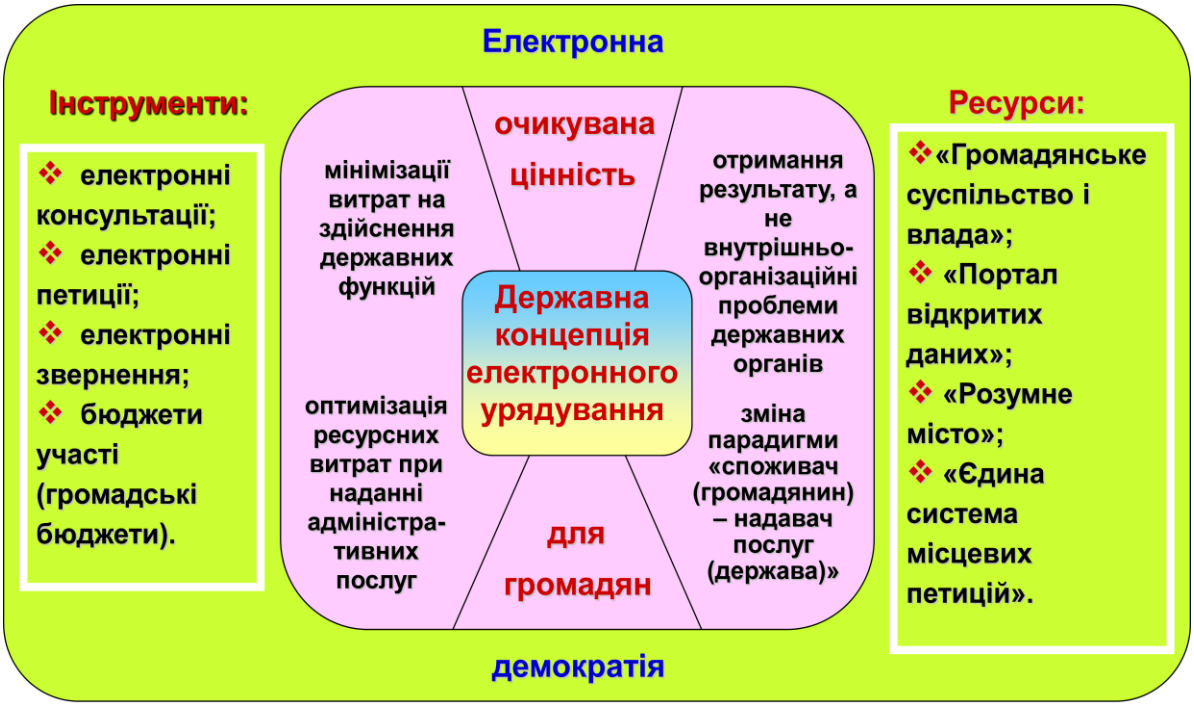
Приклад взаємодії C2C (споживач-споживачу)



Такий спосіб здійснення електронної комерції передбачає укладення угод між двома споживачами (найчастіше в Україні – усних), жоден з яких не є підприємцем в юридичному сенсі слова. Інтернет-майданчики для подібної торгівлі є чим-то середнім між ринком-товкучкою і колонкою оголошень в газеті. Для клієнтів таких систем основна зручність полягає в більш низькій ціні товару, у порівнянні з його вартістю в магазинах.

На даний час комерція C2C стає все більш популярною на сайтах Інтернет-аукціонів.

Модель комплексу сталого розвитку України «Електронне урядування - Електронна демократія»



Проблеми Е-урядування в Україні на даний час

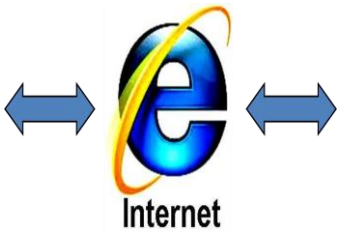
Можна відзначити наступні основні недоліки щодо реалізації в країні електронного урядування:

- відсутність інтегрованої системи інформаційних ресурсів та взаємодії між органами державної влади та місцевого самоврядування;
- обмежений (або відсутній) доступ до державних інформаційних ресурсів;
- недосконаліть діючих веб-сайтів органів влади, що не забезпечують інтерактивний режим їх функціонування;
- недостатній рівень підготовки держслужбовців та громадян.

Для подолання цих недоліків треба буде в найближчому майбутньому вирішити наступні основні задачі:

- створити офіційні сайти в Internet та наповнити їх актуальною офіційною інформацією. До офіційної інформації відноситься загальна справочна та контактна інформація державних установ, статистика, повідомлення про події в державі, закони й нормативні акти, урядові звіти, зміст державних архівів.

- провести тотальну інформатизацію суспільства (інформатизація – це політика і процеси, які направлені на розвиток телекомунікаційної інфраструктури та об'єднання територіально розподілених інформаційних ресурсів.



Школи, ВНЗ, безкоштовні курси
для широких верств населення

8.3. Інструменти та ресурси електронної демократії

Найбільш поширеними інструментами електронної демократії, що застосовуються сьогодні в Україні як на загальнодержавному, так і на місцевому рівні, є:

- ❖ електронні консультації;
- ❖ електронні петиції;
- ❖ електронні звернення;
- ❖ бюджети участі (громадські бюджети).

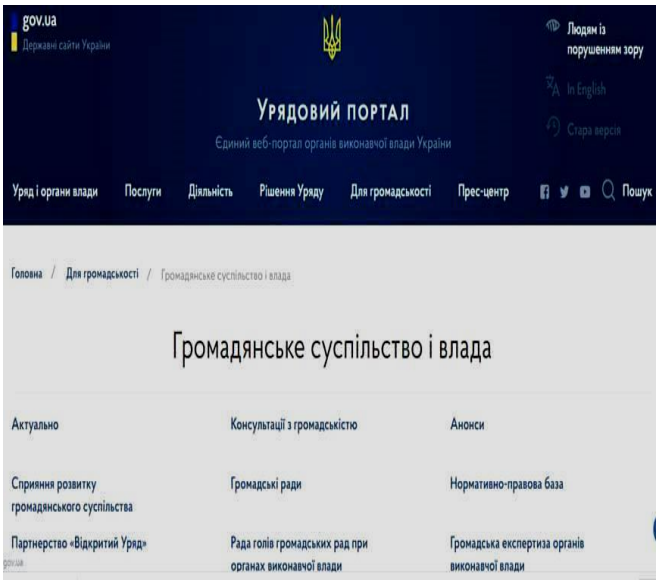
Найефективнішим інструментом демократії на даний час є бюджет участі.

Подай свої пропозиції
до місцевого бюджету
(наприклад, в Київську Міську Раду)

Ефективними ресурсами для оприлюднення наборів відкритих даних з використанням електронних платформ, які поєднують у собі кілька електронних інструментів участі, на даний час в Україні є:

- “Громадянське суспільство і влада”;
- “Портал відкритих даних”;
- “Розумне місто”;
- “Єдина система місцевих петицій”.

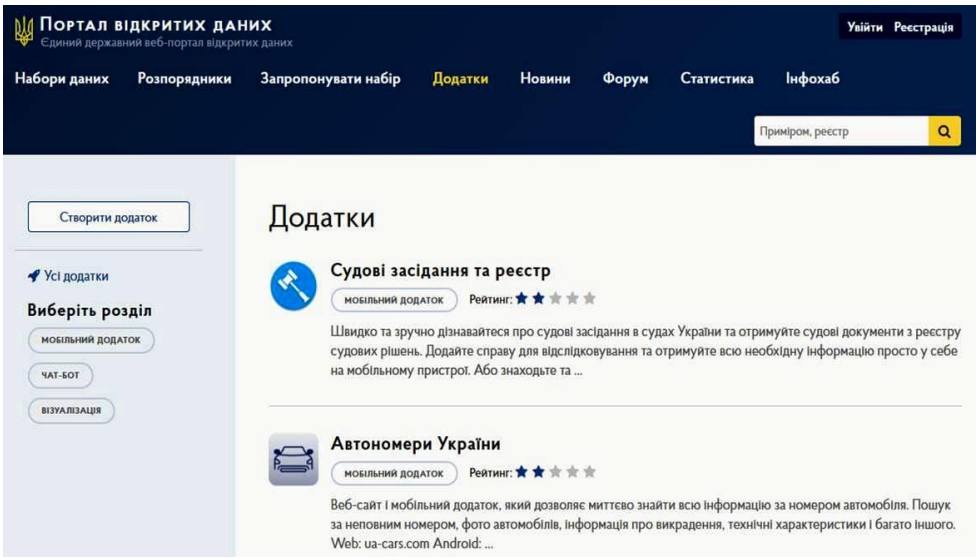
“Громадянське суспільство і влада” — це інтерактивна урядова інформаційно-аналітична система, що підтримується Управлінням у зв'язках з громадськістю Секретаріату Кабміну України



Також на сайті розміщено реєстри всеукраїнських, місцевих, а також міжнародних об’єднань громадян, що діють в Україні:

- політичних партій;
- громадських організацій;
- благодійних організацій;
- релігійних організацій;
- професійних спілок;
- творчих спілок.

Електронна платформа «Портал відкритих даних»



Єдина система місцевих петицій

Пети́ція (лат. petitio) — індивідуальна або колективна вимога, звернення, пропозиція, скарга, прохання, клопотання, яка подається в органи державної влади у письмовій формі.

колективна електронна петиція

до Президента України

до Верховної Ради

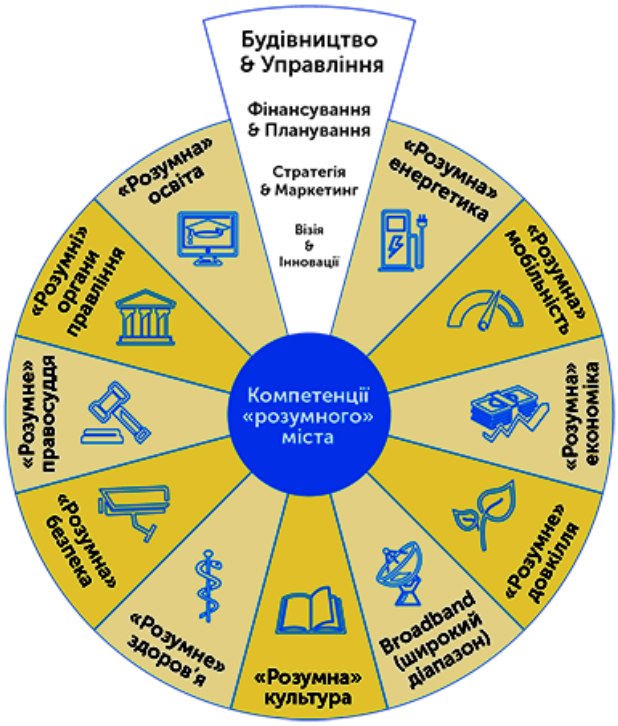
до Кабміну України

до органів місцевого самоврядування

“Розумне місто”

Принципи розумного міста

1. **Інформаційно-орієнтоване**
   Збір, інтеграція, доповнення, зберігання і поширення даних для вдосконалення процесу прийняття рішень
2. **Взаємопов’язане**
   Ефективне використання Інтернету речей (IoT) для покращення можливостей міста сприймати та реагувати на нагальні потреби мешканців
3. **Інтелектуальне**
   Використання аналітики і когнітивних інструментів для стимуляції поведінкових змін
4. **Об’єднане**
   Об’єднання міських службовців і мешканців для співпраці. Ключовими є прозорість та відкритість даних
5. **Чітко організоване**
   Надання мешканцям міста доступних, зручних та ефективних послуг



Основні заходи розвитку е-демократії передбачають:

1) удосконалення нормативно-правової бази електронної взаємодії громадян, організацій та органів влади;

2) активне використання інформаційно-комунікаційних технологій (ІКТ) для забезпечення участі громадян та організацій у формуванні та реалізації державної політики;

3) створення та впровадження інтегрованої інформаційно-аналітичної системи “Електронний парламент України”, яка забезпечить доступ громадян до інформації про парламентську діяльність та документів;

4) приведення у відповідність із європейським законодавством Закону України “Про звернення громадян”;

5) створення інтерактивної системи “Оцінка електронної готовності України”.

Сектори електронного урядування

Назва сектору	Пояснення
Е-Верховна Рада України	використання інформаційно-комунікаційних технологій (ІКТ) для оприлюднення результатів зібрань народних депутатів, а також висловлювань політичних та публічних діячів з метою активізації залучення громадян до законотворчої діяльності.
Е-законодавство	використання ІКТ для коментування, обговорення, складання, структурування, виправлення, голосування та видання законів і нормативно-правових актів, прийнятих представницькими органами.
Е-правосуддя	використання ІКТ в реалізації правосуддя всіма зацікавленими сторонами в юридичній сфері з метою підвищення ефективності та якості роботи державних служб.

8.4. Державні електронні послуги

До впровадження **е**-урядування громадянам України доводилось звертатися до 24 структур (зокрема, до Мінюсту, Міносвіти і науки, Мінсоцполітики, Державної міграційної служби, Державного земельного кадастру, Пенсійного фонду, Держбудінспекції, Державної фіскальної служби, ЄДР юридичних і фізичних осіб, Держреєстру прав на нерухоме майно, Держреєстру осіб з правами на пільги, Держреєстру загальнообов'язкового страхування, Держреєстру цивільного стану громадян та ін.).

Після впровадження **е**-урядування передбачається користування громадянами усього вісімью унікальними зверненнями до: Державного реєстру громадян, які народилися, отримали паспорт, дипломи та інші офіційні документи; Єдиного державного реєстру юридичних та фізичних осіб, підприємців та громадських формувань; Державного реєстру фізичних осіб – платників податків; Єдиний державний реєстр стосовно зареєстрованих транспортних засобів та їх власників;

Єдиний державний портал адміністративних послуг

ЄДПАП забезпечує:

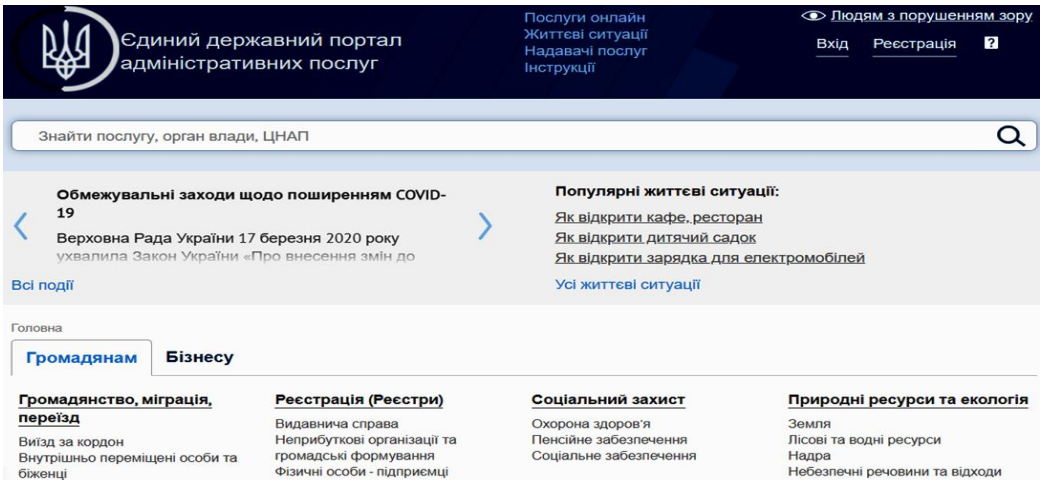
1) доступ суб'єктів звернення до інформації про адміністративні послуги,

2) доступність для завантаження і заповнення в електронній формі заяв та інших документів, необхідних для отримання адміністративних послуг;

3) можливість отримання суб'єктами звернення інформації про хід розгляду їх заяв;

4) можливість отримання суб'єктами звернення за допомогою засобів телекомунікаційного зв'язку результатів надання адміністративних послуг;

5) можливість здійснення суб'єктами звернення щодо оплати за надання адміністративної послуги дистанційно, в електронній формі.

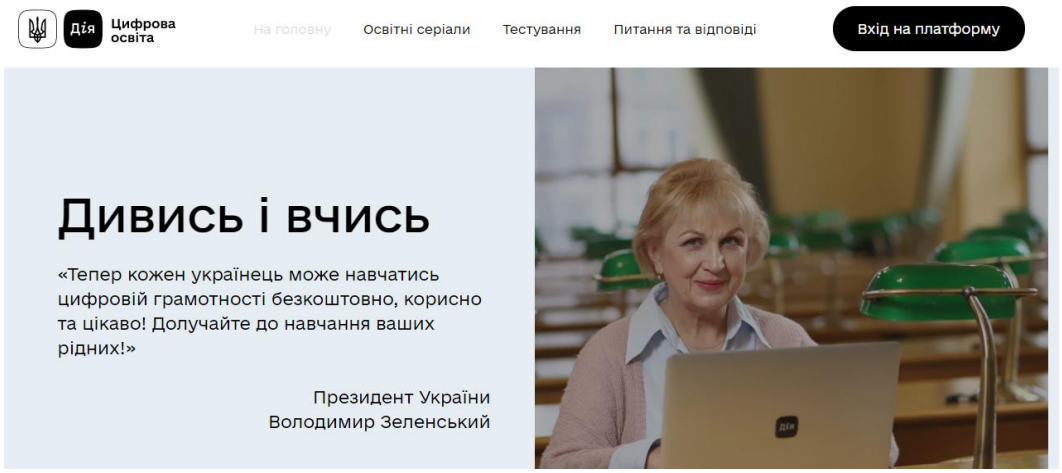


Портал “ДІЯ”

(затверджено постановою КМУ від 4 грудня 2019 р. № 1137)

Портал “Дія” – це ІКТ-система, яка організаційно та функціонально складається з реєстру адміністративних послуг, електронного кабінету, мобільного додатка Порталу “Дія”, інших підсистем та програмних модулів.

Портал призначений для реалізації права кожного на доступ до електронних послуг та інформації про адміністративні та інші публічні послуги, звернення до органів виконавчої влади, інших державних органів, органів місцевого самоврядування, підприємств, установ і організацій (у т. ч. відповідно до Закону України “Про звернення громадян”), отримання інформації з національних електронних інформаційних ресурсів, яка необхідна для надання послуг, а також для проведення моніторингу та оцінки якості послуг у випадках, визначених цим Положенням.



Види електронних послуг в Україні

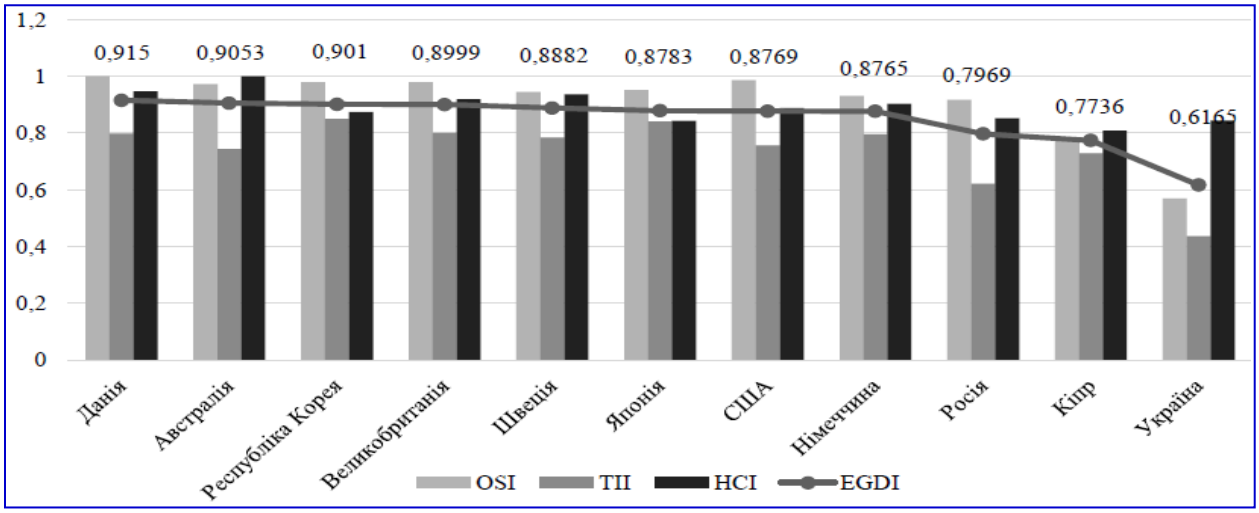
Приклад суспільно важливих послуг

Оцінки рівня розвитку електронного урядування в Україні

Для оцінки рівня розвитку електронного урядування в Україні виділено сім категорій (індикаторів) електронного урядування:

- доступ до інформації;
- зворотний зв'язок з громадкістю;
- адміністративні послуги;
- доступ до публічної інформації;
- зручність користування веб-сайтом;
- оцінка системи електронного документообігу в органі місцевого самоврядування;
- оцінка діяльності центрів надання адміністративних послуг.
-

Індекс розвитку електронного урядування EGDI країн-лідерів та України за 2018 р.



В математичному плані EGDI – це середнє арифметичне трьох нормалізовованних основних показників, які оцінюють найбільш важливі аспекти електронного уряду: широта і якість онлайн-послуг (Online Service Index, OSI), рівень розвитку телекомунікаційної інфраструктури (Telecommunication Infrastructure Index, TII) і обсяг людського капіталу (Human Capital Index, HCI).

До чого нам треба прагнути при реалізації ЕУ ?

США:

- ❖ **офіційна довідка on-line - не довше 30 хвилин ;**
- ❖ **отримання ліцензії - 1 доба.**

Канада;

- ➢ **41% громадян - постійно отримують адміністративні послуги через Інтернет;**
- ➢ **81% з них задоволені якістю їх надання.**

Великобританія:

- ✓**реєстрація підприємства - не більше 30 хвилин;**
- ✓**подання податкової декларації – до 5 хвилин.**

8.5. Трансформаційний сценарій розвитку ЕУ

З урахуванням економічної ситуації, що склалася на даний час в Україні, единим можливим напрямком розвитку електронного урядування є реалізація так званого трансформаційного сценарію (ТС). Цей сценарій, з одного боку, дозволяє запустити необхідні модернізаційні процеси, а з іншого – не потребує надлишкових витрат як з боку держави, так і з боку громадян і організацій.

ТС пропонує перехід до електронного самоврядування від орієнтації на відомчі процеси до орієнтації на користувача, а в області управління розвитком ЕУ – впровадження сучасних управлінських підходів, включаючи архітектурний. В умовах скорочення бюджету реалізація даного підходу дозволить скоротити державні витрати на адміністрування апарату управлінських органів. Для реалізації ТС пропонуються наступні дії:

- комплексний розвиток законодавчої бази, що зачіпає широкий спектр питань, в тому числі: уніфікацію застосування ІКТ на всіх рівнях і гілках влади при реалізації Проекту, сниження бар'єрів для громадсько-правових відносин в електронному вигляді.
- застосування сучасних методів управління: загальну координацію інформатизації в рамках розвитку ЕУ, включаючи методи управління якістю, моніторинг ключових показників ефективності, активну громадянську участь в державному управлінні.
- розвиток сервисів електронного урядування.

Реалізація ТС може супроводжуватися наступними ризиками:

- високий рівень міжвідомчих бар'єрів в державних органах влади, територіальна специфіка учасників, конфлікти інтересів, неузгодженість понятійного апарату;
- неготовність ІКТ-інфраструктури певних регіонів до підключення к загальним комп'ютерним мережам та інформаційним системам надання електронних послуг. Це може призвести до розрізненості та багатократному дублюванню інформаційних ресурсів державних органів;
- повільний розвиток організаційної культури в органах державної влади і місцевого самоврядування може призвести до гальмування процесів створення ЕУ співробітниками цих органів та ін.

Усі відмічені ризики в рамках трансформаційного сценарію можна суттєво зменшити за рахунок використання сучасних методів менеджменту якості в рамках розвитку ЕУ.

В результаті реалізації ТС цілком реально, що в найближчі п'ять років з урахуванням вже зроблених в нашій країні перших кроків (якщо коротко – Кабмін України прийняв дві Постанови про роботу з відкритими даними і затвердив Концепцію розвитку електронного урядування в Україні) ЕУ може вийти на новий рівень розвитку.

8.6. Більш детально щодо розв'язку певних проблем ЕУ

1. Для збільшення частки громадян, які вже сьогодні отримують послуги в електронній формі, потрібно сформувати відповідний рівень обізнаності про таку можливість, а також створити єдиний портал держуправління (ЄПДУ). Особливу увагу слід приділити послугам, для отримання яких громадяни віддають перевагу особистому візиту, ніж електронним каналам.

Для можливості отримання достовірної інформації щодо надаваних електронних послуг і формування сталого попиту на них необхідно забезпечити регулярне проведення кампаній в ЗМІ і рекламних каналах (телебачення, Інтернет, зовнішня реклама, друковані видання, радіо і т.д.). В тому числі треба постійно аналізувати пошукові запити громадян в мережі Інтернет і задовольняти їх потреби шляхом розміщення об'яв у вигляді контекстної реклами.

Поруч із засобами масової інформації і рекламним каналам доцільно використати власні комунікаційні канали органів влади: центри підтримки користувачів, сайти відомств, громадські приймальні громадян, інформаційні електронні розсилки. Важливо зазначити, що популярізація електронних послуг в місцях прийому громадян має здійснюватися консультантами в активному режимі.

Як показує практика, невміння використовувати ІКТ часто стає головною причиною відмов громадян від комунікацій з державою за допомогою електронних каналів. Розробка і затвердження стандарту комп'ютерної грамотності і створення навчальних онлайн курсів дозволить уніфікувати і росширити систему підготовки населення до використання ІКТ, зробити її більш доступною.

2. Відомості, які містяться в інформаційних системах (ІС) одних державних органів, часто недоступні іншим органам державної влади для оперативного використання, а в деяких випадках ці відомості вже неактуальні із-за їх несвоєчасного оновлення. На практиці це призводить до дублювання частково неактуальних відомостей в різних інформаційних системах учасників міжвідомчої взаємодії, що тягне за собою додаткові часові і вартісні витрати, необхідні для усунення виявлених помилок і актуалізації інформації.

Для забезпечення сталої актуальності відомостей ІС необхідно створити єдиний каталог типів і атрибутів даних – джерел майстер-даних (тобто початкове місце виникнення даних про суб'єкт інформаційного обміну), які приймають участь в міжвідомчої взаємодії, механізм його ведення і оновлення. Окрім джерел майстер-даних, каталог типів даних і атрибутів має містити атрибутний склад інформаційного ресурсу відомств, а також взаємозв'язки джерел майстер-даних.

На основі вищеназваного каталогу необхідно забезпечити можливість автоматичного розповсюдження оновлень баз даних учасників міжвідомчої взаємодії з урахуванням оновлення тільки необхідної частки.

Окрім того на учасників міжвідомчої електронної взаємодії необхідно покласти зобов'язання щодо публікації і актуалізації довідників, за які вони відповідають.

Використання такої моделі обміну відомостями зменшує витрати на експлуатацію інформаційних систем та інфраструктури електронного урядування в цілому.

Для спрощення проектування і організації системи міжвідомчої електронної взаємодії (СМЕВ) необхідно організувати публікацію всіх доступних видів відомостей, які державні органи влади, а також інші учасники взаємодії можуть використовувати. Також в цілях виключення дублювання витрат учасників МЕВ необхідно законодавчо закріпити можливість формування електронного платежу громадянами виключно за допомогою державних ІС, в тому числі, якщо цей платіжний документ направляється громадянину на паперовому носії.

З метою моніторингу термінів відповідей учасників МЕВ на запити, а також для контролю мети відправки відомствами цих запитів потрібно ввести маркіровку кожного запиту/відповіді в СМЕВ, котра буде відповідати певному ідентифікатору.

3. Основним способом он-лайн ідентифікації та аутентифікації є застосування користувачем простого електронного підпису, ключом якого виступає пара логін-пароль від облікового запису в Єдиній системі ідентифікації та аутентифікації (ЄСІА). ЄСІА також застосовується для забезпечення доступу посадових осіб до інформаційних систем органів державної і муніципальної влади.

Для можливості доступу користувачів до послуг без необхідності ручного введення логіна и пароля, для виключення ймовірності втрати, крадіжки, підробки і передачі пароля третім особам необхідно реалізувати доступ в ЄСІА із застосуванням технічних засобів ідентифікації та аутентифікації. Найбільш часто використовуються такі типи голосової та/або біометричної ідентифікации, як голос, відбитки пальців, форма обличчя, райдужна оболонка ока, підпис, геометрія руки.

Для застосування вказаних типів ідентифікації в інфраструктурі електронного урядування (ІЕУ) необхідно забезпечити в ЄСІА розвиток відповідних інтерфейсів і сервісів окремиxx ІС, а також закріпити порядок використання і передачі ідентифікаційних даних в профільних нормативних правових актах.

Для розв'язку вказаної задачі має бути реалізовано автоматичне, проактивне оновлення даних про користувачів в ЄСІА за допомогою адресних оповіщень з базових державних інформаційних ресурсів (БДІР) із збереженням отриманих даних після змін, які надійшли з БДІР. При цьому необхідно забезпечити однозначу відповідність даних про користувачів ЄСІА з даними в БДІР.

Слід відмітити, що існує реальна проблема несанкціонованої реєстрації та протиправного використання персональних даних громадян для отримання доступу до результатів надання державних і муніципальних послуг в електронній формі, причому такі дії частіше здійснюються не хакерами або злочинними групами, а органами і організаціями, законно підключеними до ІЕУ.

В зв'язку з цим необхідно провести роботи по вдосконаленню відповідних нормативних правових актів щодо визначення закритого переліку органів і організацій, які мають право здійснювати створення і видачу електронного підпису.

4. Одна з головних задач ЕУ – можливість використання інформаційних систем і сервісів для підтримки діяльності громадянського суспільства і бізнесу, залучення громадян в процеси державного і муніципального управління.

ЕУ як одна з точок взаємодії з державою, дозволить громадянам більш активно приймати участь в громадському житті, отримувати доступ до публічної інформації, офіційним документам і протоколам адміністративних органів в режимі он-лайн. Особливе значення набуває можливість використання сервісів ЕУ некомерційними організаціями (НКО), соціальними співтоваристами і бізнесом в рамках громадянсько-правових відношень, в тому числі сервісів ідентифікації та аутентифікації, сервісів довіреної третьої сторони, сервісів інформаційної підтримки. Це буде сприяти підвищенню якості надаваних послуг та зменшенню фінансових і часових витрат.

Необхідно відзначити, що органи влади також зацікавлені в інтерактивному партнерстві між державою і суспільством. Багато державних органів відчувають нестачу ресурсів для спеціалізованих експертиз в рамках законотворчої діяльності або потребують механізми довіреного електронного зворотного зв'язку при здійсненні великих економічних і соціальних ініціатив.

З урахуванням викладеного розвиток електронного уряду доцільно проводити в рамках розширення механізмів та практик загальної взаємодії громадян, організацій та державних (муніципальних) органів. Це відкриває можливості для безпечного персоніфікованого режиму он-лайн комунікацій. У таких комунікаціях зацікавлені всі учасники процесу.

В рамках інфраструктури електронного урядування необхідно реалізувати механізм, за допомогою якого громадяни зможуть подати звернення або скаргу в будь-який орган влади будь-якого рівня з будь-якого питання. В рамках цього механізму повинна бути розроблена форма подачі звернень, яка розміщується на Єдиному порталі, а також може бути розміщена на офіційному сайті органу влади або органу місцевого самоврядування.

Одночасно, в рамках формування сервісів електронного урядування, буде вдосконалюватися інститут електронного голосування і проведення офіційних опитувань (референдуми, вибори, перепис населення).

Контрольні питання до розділу

1. Що таке електронне урядування? Поясніть його актуальність.
2. Розкрийте суть Концепції електронного урядування.
3. Назвіть та поясніть основні складові Концепції ЕУ.
4. Назвіть проблеми реалізації ЕУ в Україні. Поясніть шляхи їх розв’язку.
5. Що таке електронна демократія? Розкажіть про інструменти її розвитку.
6. Поясніть суть трансформаційного сценарію розвитку ЕУ.
7. Розкажіть про розвиток взаємодії між електронним урядом і суспільством.
8. Розкажіть про розвиток Єдиної системи ідентифікації та аутентифікації.
9. Для чого потрібна підтримка діяльності громадських організацій і бізнесу в умовах ЕУ?
10. Як можна ефективно організувати надання електронних послуг на комерційній основі?
11. Поясніть суть зв’язку між ЕУ та проектом “Електронне судочинство”.

Література

Основна

1. Бринцев О. В. Електронний суд в Україні. Досвід і перспективи. Монографія. Х.: Право. 2016. 72 с.

2. Бурцева Е. В., Рак И. П., Селезнев А. В., Терехов А. В., Чернышов В. Н. Информационные системы: Уч. пособие. Тамбовский Государственный технический университет. 2009. 120 с.

3. Тимохова Н.А. ИТ в юридической деятельности: Конспект лекций. Пермский институт экономики и финансов. 2013. 112 с.

4. Емельянов С. Л., Якутко В.Ф., Логинова Н.И. Информационные технологии в юриспруденции: Уч. пособие. Одеса: Фенікс. 2007. 266 с.

5. Литвинов В. Информационные технологии в юридической деятельности: Уч. пособие. Стандарт третьего поколения. СПб: Питер. 2013. 320 с.

6. Співаковський О. В., Шерман М. І., Стратонов В.М., Лапінський В.В. Інформаційні технології в юридичній діяльності: базовий курс: Навч. посібник. Херсон: ХДУ. 2012. 220 с.

7. Экономическая информатика: Уч. пособие / Под ред. П. В. Конюховского, Д. Н. Колесова. СПб.: Питер. 2001. 560 с.

Допоміжна

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

2. Косинський В. І., Швець О. Ф. Сучасні інформаційні технології: Навч. посіб. К.: Знання. 2012. 318 с.

3. Вдовіна О. О. Порівняльний аналіз систем електронного діловодства судової влади в Україні та зарубіжних країн. Зб. матеріалів VII Міжнародної наук.-практ. конференції "Інформаційна освіта та професійно-комунікативні технології XXI ст. Одеський національний політехнічний ун-т. 2014 (вересень). С. 92-97.

4. Вивчарук К. Г. Электронное судопроизводство: отечественный опыт – достоинства и недостатки. Бизнес. Общество. Власть (онлайн-издание). 2013. № 14. С. 15-19.

5. Зозуля Д. Д. Проблеми впровадження електронного документообігу в судовій системі України. Зб. матеріалів всеукраїнської наук.-теорет. конф. молодих учених "Культура та інформаційне суспільство". Харків. ДАК. 2014 (квітень). С. 239-240.

6. Проскурякова Мария. Электронное правосудие в Германии: актуальное состояние и перспективы развития. Вестник Санкт-Петербургского университета. Право. 2018. №3. С. 433-447.

7. Решетняк В. И. Электронное правосудие и судебное представительство в гражданском и арбитражном процессах. 2011. № 5. С. 16–23.

8. Фишер Н. Электронное правосудие в Германии. Российский ежегодник гражданского и арбитражного процесса / под ред. В. В. Яркова. С.-Пб. : Юридическая книга. 2008. С. 630-643.

Інтернет-джерела

1. Український ІТ-портал. URL: http://www.ua-admin.com
2. Ліга: Закон. URL: http://www.ligazakon.ua/
3. Офіційний сайт Верховної Ради України. URL: http://www.rada.gov.ua
4. Науково-дослідний центр правової інформатики. URL: http://ippi.org.ua
5. Юридична бібліотека (Україна). URL: http://law.biz.ua
6. Брувеліс А. А. LURSOFT в розробці ІТ-рішень. URL: http://www.pravo.by/ conf2010/reports/Bruvelis.doc
7. Електронне судочинство: сучасний стан та перспективи розвитку. URL: http://yurincom.com/ua/ yuridichnyi_visnyk_ukrainy/overview/?id=5533
8. Ермак А., Якимец Т. Как обустроить открытый суд. URL: http://racurs.ua/628-elektronnyy-sudpublichnyi-sudebnyi-prosess
9. Їжак О. Створення ефективної судової системи: досвід. URL: http://jurliga. ligazakon.ua/news/2013/8/6/95832.htm.
10. Федотов О. Электронное правосудие в Республике Беларусь. URL: http://e-gov.by/ekspert/elektronnoe-pravosudie-v-respublike-belarus
11. Білоус В. В. Інноваційні напрямки інформатизації судочинства. URL: http://www.nbuv.gov.ua/ old_jrn/Soc_ Gum/Tpsek/ 2011_11/Bilous.pdf
12. Каланча І. А. Міжнародний досвід використання електронного сегмета в кримінальній процесуальній діяльності суду. URL: http://www.jurnaluljuridic. in.ua/archive/2015/6/50.pdf

ДОДАТОК 1

Принцип побудови і роботи комп'ютера

Принцип побудови універсальної обчислювальної машини в сучасному вигляді був сформований ще в першій половині XIX століття англійським математиком Беббіджом, але реалізувати цей принцип вдалося тільки у XX столітті наприкінці 40-х років з появою відповідної електронної техніки та математичних основ функціонування комп'ютерів за Нейманом.

На рис. Д1.1 наведена логічна схема ЕОМ Неймана, яка, як не дивно, й досі є актуальною. З моменту появи першої лампової машини в 1949 році суттєво змінилися елементна база ЕОМ, організація пам'яті, дії з даними, адресами, командами і, в певній мірі, процесс обчислювання. Але принцип роботи ЕОМ широкого застосування поки незмінний.

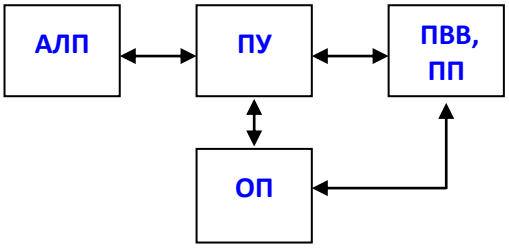


Рис. Д1.1. Логічна схема ПК

У відповідності з принципами Неймана комп'ютер можна розглядати як систему, що складається з 4-х основних складових з певними логічними функціями: *запам'ятовуючого* пристрою, котрий поділяється на *оперативну* і *постійну* пам'ять (ОП, ПП), *арифметично-логічного* пристрою (АЛП), пристрою *управління* (ПУ) та пристрою *вводу-виводу* (ПВВ).

Запам'ятовуючий пристрій призначений для зберігання інформації та команд програми в ЕОМ. Інформація, яка зберігається в пам'яті, являє собою закодовані числа у вигляді 0 та 1.

Під записом числа в пам'ять розуміють розміщення цього числа в комірці за вказаною адресою і зберігання його там до відповідної команди програми. Попередняя інформація, що знаходилася в цій комірці, перезаписується.

Під зчитуванням числа з пам'яті розуміють вибірку числа з комірки за вказаною адресою. При цьому копія числа передається з пам'яті в потрібний пристрій, а саме число залишається в комірці.

Пересилання інформації означає, що інформація з однієї комірки записується в іншу.

Числа, символи, команди зберігаються в пам'яті на рівноправних засадах і мають один і той же формат. Ні для пам'яті, ні для самого комп'ютера не має значення тип даних. Типи розрізняються тільки при обробці даних програмою.

Для характеристики пам'яті використовуються наступні параметри: обсяг пам'яті – максимальна кількість інформації, що зберігається в байтах; швидкодія

пам’яті – час звернення до пам’яті, яке визначається часом зчитування або часом запису інформації (біт/сек).

Арифметично-логічний пристрій (АЛП). Цей пристрій здійснює арифметичні і логічні дії. Слід зазначити, що будь-яку арифметичну операцію можна реалізувати з використанням операції додавання. Складна логічна задача розкладається на більш прості завдання, де досить аналізувати тільки два рівня: ТАК аб НІ.

Пристрій управління керує всім ходом обчислювального і логічного процесу в комп’ютері, тобто виконує функції “регулювальника руху” інформації. ПУ читає команду, розшифровує її і підключає необхідні ланцюги для її виконання. Зчитування наступної команди відбувається автоматично. Фактично ПУ виконує наступні дії: формування адреси чергової команди; читання команди з пам’яті та її розшифровку; виконання команди.

У сучасних комп’ютерах функції ПУ та АЛП виконує один пристрій – *центральний процесор* (ЦП), англ. скор. – CPU.

При включенні ПК з постійної пам’яті за участю мікросхеми BIOS в ОП завантажується операційна система, за допомогою якої при підтримці центрального процесора і драйверів периферійних вузлів можна виконати програму користувача. По завершенню роботи комп’ютера всі коди з оперативної пам’яті вилучаються.

Нагадаємо, що BIOS (від англ. basic input/output system – базова система вводу-виводу) являє собою набір мікропрограм, за допомогою яких здійснюється самотестування основних вузлів ПК та підготовка їх до роботи, а також реалізується інтерфейс взаємодії між комп’ютером та підключеними до нього пристроями. Згадаємо, що інтерфейс – це спільна межа між двома функціональними об’єктами, вимоги до якої визначаються стандартом.

Основними параметрами ПК є параметри системного блоку, а саме: тактова частота, розрядність даних і обсяг інформації на жорсткому диску.

Тактова частота показує, скільки елементарних операцій процесор виконує за 1 сек, розрядність – скільки бітів інформації передається за 1 такт, обсяг – скільки байтів інформації може одночасно зберігатися в довгостроковій пам'яті.

Найбільш поширеними на сьогодні є такі параметри ПК: тактові частоти – одиниці гігагерц; розрядність даних – 32 або 64 біт; обсяг довгострокової пам’яті – від десятків до сотен гігабайт.

Принцип роботи ЕОМ спрощенно можна пояснити так. Спочатку за допомогою одного з зовнішніх пристроїв в оперативну пам’ять комп’ютера вводиться потрібна програма, яка складається з пронумерованих за порядком команд-інструкцій. ПУ зчитує зміст комірки, в якій знаходиться перша команда (адреса цієї комірки фіксована) та організує її виконання. Після повного виконання першої команди за допомогою ПУ слідує виконання другої, третьої команд і так далі аж до останньої (адреси команд змінюються у відповідності з їх номером). Такий порядок виконання програми в принципі може бути змінений з використанням умовних переходів, але суть роботи ЕОМ від цього не змінюється. Таким чином, ПУ виконує інструкції програми автоматично, без втручання людини. Після виконання останньої команди ЕОМ переходить в режим очікування команди оператора.

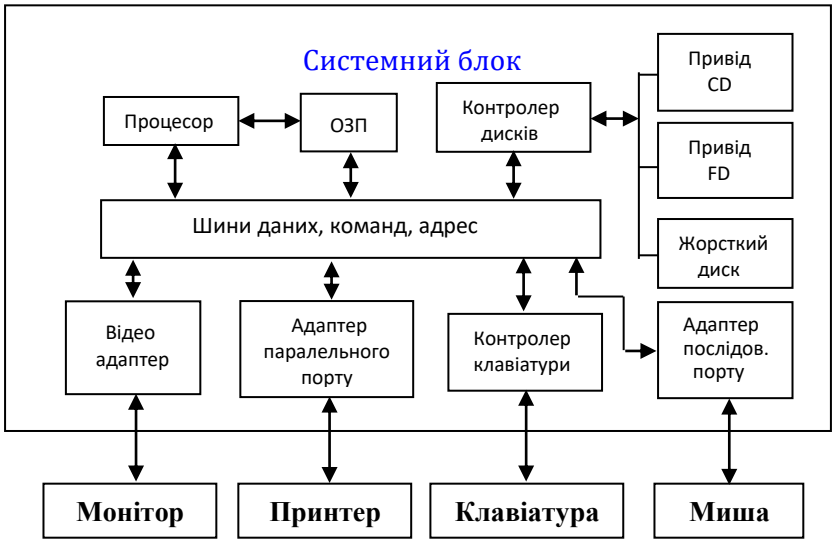


Рис. Д1.2. Спрощена функціональна схема персонального ком'ютера.

Функціональна схема сучасного ПК відрізняється від логічної і в спрощеному вигляді без блоків живлення та BIOS наведена на рис. Д1.2.

ДОДАТОК 2

Електронний підпис

Електронний підпис (ЕП), Електронний цифровий підпис (ЕЦП), Цифровий подпис (ЦП) – на сьогодні це практично синоніми реквізиту електронного документа, отриманого в результаті певного криптографічного перетворення інформации. Реквізит створюється з використанням закритого ключа підпису і дозволяє перевірити відсутність спотворення інформації з моменту формування підпису (тобто перевірка на цілістність), належність підпису саме власнику ключа (перевірка на авторство), а в разі успішної перевірки підтвердити факт підписання електронного документа (перевірка на неспростовність).

Електронний підпис застосовується при здійсненні цивільно-правових угод, надання державних та муніципальних функцій і послуг, при здійсненні інших юридично значимих дій. При використанні ЕП передбачається реалізація наступних важливих напрямків в електронній економіці:

• *повний контроль цілісності переданого електронного платіжного документа*. У разі будь-якої випадкової або навмисної зміни документа цифровий підпис стане недійсним, оскільки обчислюється за спеціальним алгоритмом на підставі початкового стану документа і відповідає лише йому;

• *ефективний захист від змін (підроблення) документа*. ЕП дає гарантію, що при здійсненні контролю цілісності будуть виявлені будь-якого роду підробки. Як наслідок, підроблення документів стає в більшості випадків недоцільним;

• *неможливість відмови від авторства даного документа*. Це аспект випливає з того, що знову створити правильний електронний підпис можна лише в разі володіння так званим закритим ключем, який, в свою чергу, повинен бути відомий тільки власнику цього ключа (автору документа). У цьому випадку власник не зможе сформувати відмову від свого підпису, а значить – від документа.

• *підтвердження авторства документа*: виходячи з того, що створити коректний електронний підпис можна лише знаючи закритий ключ, а він за визначенням має бути відомий тільки власнику (автору) документа, власник ключа може однозначно довести своє авторство підпису під документом.

Перераховані вище властивості електронного цифрового підпису дозволяють використовувати його в багатьох випадках, в т.ч. в електронних системах звернення громадян до органів влади.

Існує кілька схем побудови цифрового підпису, однак на даний момент найбільш поширені і знаходять широке застосування алгоритми *асиметричного шифрування*.

Оскільки документи, що підписуються, змінного (і як правило досить великого) обсягу, ЕП часто ставиться не на сам документ, а на його хеш (код). Для обчислення хеша використовуються криптографічні хеш-функції, які гарантують виявлення змін документа при перевірці підпису. Хеш-функції не є частиною алгоритму ЕП, тому в схемі може бути використана будь-яка надійна хеш-функція.

Використання хеш-функцій дає наступні переваги:

- *швидкість обчислення*. Зазвичай хеш цифрового документа займає набагато менший обсяг пам'яті, ніж обсяг самого документа, тому й алгоритм обчислення хеша більш швидкий (тобто сформувати хеш документа і підписати його можна набагато швидше, ніж підписувати сам документ);
- *сумісність*. Хеш-функцію можна використовувати для перетворення довільного вхідного тексту в потрібний формат.

Суть асиметричного шифрування зображена на рис. Д2.1.

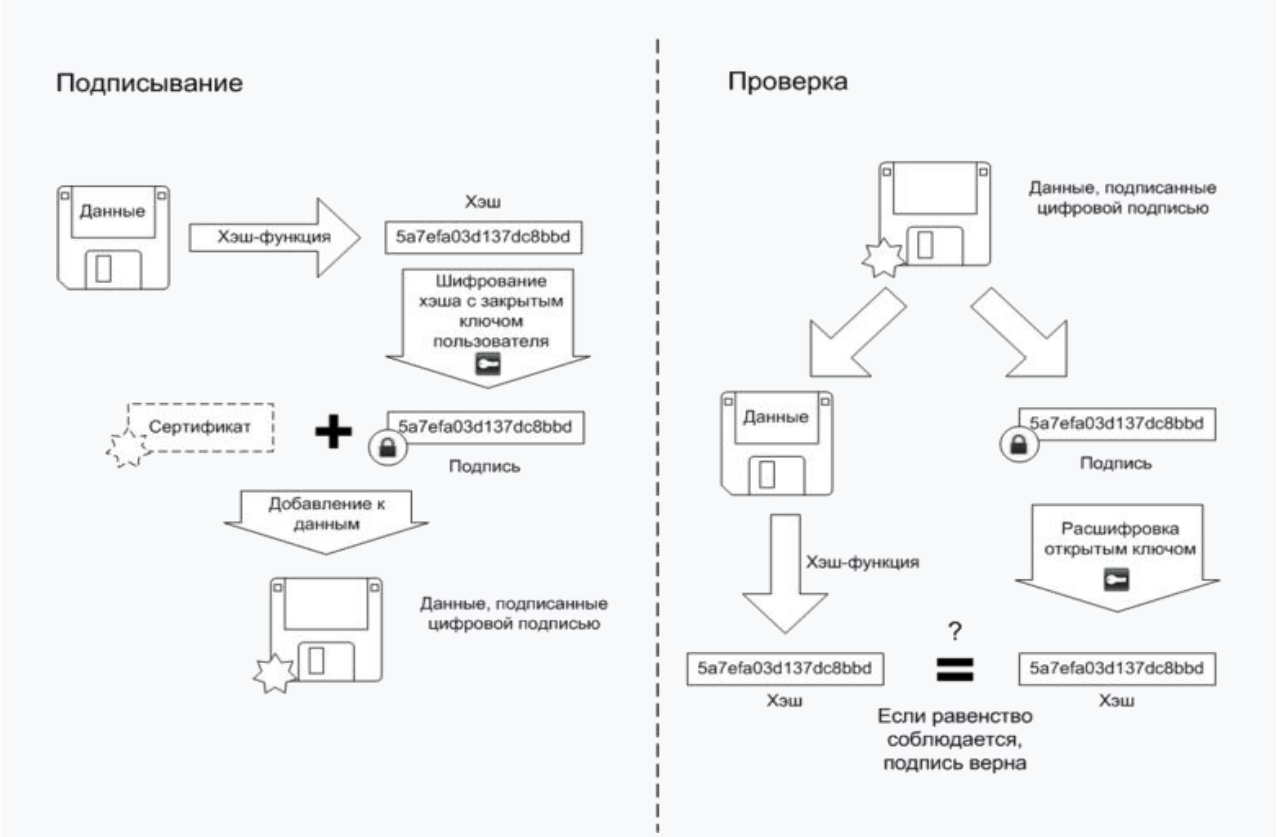


Рис. Д2.1. Схема, яка пояснює алгоритм підпису при асимметричному шифруванні підпису закритим ключем, а перевірку підпису – відритим ключем

Закритий ключ є найбільш уразливим компонентом всієї криптосистеми цифрового підпису. Зловмисник, який вкрав закритий ключ користувача, може створити дійсний цифровий підпис будь-якого електронного документа від імені цього користувача. Тому особливу увагу потрібно приділяти способу зберігання закритого ключа.

В даний час існують наступні пристрої порівняно надійного зберігання закритого ключа: дискети, смарт-карти, USB-брелоки, "таблетки" Touch-Memory, реєстр в захищеній пам'яті комп'ютера. Крадіжка або втрата одного з таких пристроїв зберігання може бути легко помічена користувачем, після чого відповідний сертифікат на користування ключем повинен/може бути негайно відкликаний.

Найбільш захищений спосіб зберігання закритого ключа – зберігання на смарт-карті. Для того, щоб використати смарт-карту, користувачеві необхідно не тільки її мати, але і ввести свій PIN (тобто, здійснюється двофакторна аутентифікація). Крім

того, зробити копіювання інформації зі смарт-карти складніше, ніж з інших пристроїв зберігання.

Відповідно до закону "Про електронний підпис", відповідальність за зберігання закритого ключа несе сам власник.

В Україні використання ЕЦП регулюється законом, виданим в 2003 році. Він координує відносини, що з'являються внаслідок застосування ЕЦП. Система функціонування ЕЦП складається з центрального засвідчувального органу, який видає дозволи центрам сертифікації ключів (ЦСК) та забезпечує доступ до електронних каталогів, контролюючого органу і центрів сертифікації ключів, які видають ЕЦП кінцевому споживачу.

У квітні 2007 року було прийнято Постанову "Про затвердження порядку подання звітів до Пенсійного фонду України в електронній формі". А в квітні 2008 року вийшов наказ № 233 Податкової Служби України "Щодо подання електронної цифрової звітності". В результаті активної роз'яснювальної діяльності податкових служб в 2008 році кількість суб'єктів, які подають звітність з ПДВ в електронному вигляді, зросла з 43% до 71%.

16 червня 2015 року на Україні запрацював сайт електронних державних послуг ***iGov.org.ua***. Тут можна замовити довідку про несудимість для пред'явлення в МРЕВ, оформити заявку на отримання субсидії, довідки про доходи, а також заповнити документи на закордонний паспорт.

ДОДАТОК З

Загальні відомості про організацію відеоконференцій

Груповий термінал відеоконференцзв'язку (HD)

Відеоконференція – це ділянка IT, яка забезпечує одночасно двосторонню передачу, обробку, перетворення і подання інтерактивної інформації на відстань в режимі реального часу за допомогою апаратно-програмних засобів обчислювальної техніки. Інша назва такої взаємодії – сеанс зв'язку.

Групова відеоконференція (стандартна роздільна здатність)

Відеоконференцзв'язок (ВКЗ) – це телекомунікаційна технологія інтерактивної взаємодії трьох і більше віддалених абонентів, за якої між ними можливий обмін аудіо- и відеоінформацією в реальному часі, з урахуванням передачі управляючих даних.

Відеотелефон для участі у відеоконференціях

Відеоконференція застосовується як засіб оперативного прийняття рішення в певній ситуації, при надзвичайних ситуаціях, для скорочення витрат на відрядження, підвищення ефективності проведения судових процесів з дистанційною участю засуджених, як один з елементів телемедицини та ін.

У багатьох державних і комерційних організаціях відеоконференція приносить великі результати і максимальну ефективність, а саме:

- *знижує час на переїзди і пов'язані з ними витрати*;
- *прискорює процеси прийняття рішень* в надзвичайних ситуаціях;
- *скорочує час розгляду справ у судах* загальної юрисдикції;
- *збільшує продуктивність праці*;
- *допомагає вирішити кадрові питання* і соціально-економічні ситуації;
- *дає можливість приймати більш обґрунтовані рішення* за рахунок залучення при необхідності додаткових експертів;
- швидко і *ефективно розподіляє ресурси* і так далі.

Для спілкування в режимі відеоконференції абонент повинен мати термінальний пристрій (кодек) ВКЗ, відеотелефон або інший засіб обчислювальної техніки. Як правило, в комплекс пристроїв для ВКЗ входить: центральний пристрій (кодек) з відеокамерою і мікрофоном, забезпечує кодування/декодування аудіо- та відеоінформації, захоплення і відображення контенту; пристрій відображення інформації

та відтворення звуку. У якості кодека може використовуватися персональний комп'ютер з програмним забезпеченням для відеоконференцій.

Велику роль у відеоконференції грають канали зв'язку, тобто транспортна мережа передачі даних. Для підключення до каналів зв'язку використовуються мережеві протоколи IP або ISDN.

Існує два режими роботи ВКЗ, які дозволяють проводити сеанси зв'язку: двосторонні (режим "точка-точка") і багатосторонні (режим "многоточка").

Для впровадження ВКЗ керівнику (особі, що приймає рішення) організації необхідно визначити головну мету застосування, тобто: проведення нарад, підбір персоналу, оперативність при прийнятті рішень, здійснення контролю, дистанційне навчання, консультація лікарів, проведення судових засідань, допит свідків і так далі.

Категорії відеоконференцзв'язку

Персональні системи. Забезпечують можливість індивідуального відео-спілкування користувача в режимі реального часу, не покидаючи свого робочого місця. Конструктивно персональні системи зазвичай виконуються у вигляді настільних терміналів або у вигляді програмних рішень.

Групові системи. Призначені для проведення групових сеансів відео-конференц-зв'язку в переговорних кімнатах. Групова система здатна перетворити приміщення будь-якого розміру в відео-конференц-студію для проведення інтерактивних нарад. В групових системах ставляться приставки відео-конференц-зв'язку (set-top) стандартного дозволу і з підтримкою високої чіткості (High Definition). До цієї ж категорії відносяться і системи класу TelePresence (телеприсутність), які представляють собою комплекс засобів, що забезпечує максимальний ефект присутності віддалених співрозмовників в одній кімнаті.

Галузеві системи. Це системи, які застосовуються безпосередньо в певній галузі. Наприклад, у медичній галузі дуже часто застосовують системи для проведення операцій (телемедицина), в судовій системі – для проведення дистанційних касаційних і наглядових судових процесів, в нафтогазовій, енергетичній, будівельній галузі для оперативності подання інформації.

Мобільні системи. Це компактні переносні системи ВКЗ для використання у віддалених районах і екстремальних умовах. Мобільні системи дозволяють за короткий час організувати сеанс зв'язку в нестандартних умовах. Дані системи зазвичай використовуються державними органами, які приймають оперативні рішення (військові, рятувальники, лікарі, служби екстреного реагування).

Інфраструктура мережі відеоконференцзв'язку

До інфраструктурі мережі ВКЗ відноситься сукупність апаратно-програмних засобів адміністрування/управління з використанням різного кінцевого обладнання та програмного забезпечення – *сервера* багатоточкового відеоконференцзв'язку (Multipoint Control Unit), інтеграція з уніфікованими комунікаціями, *системи управління відеоконференціями* (облік, управління конфігурацією, безпекою, продуктивністю і помилками вузлів, ліній і кінцевого обладнання ВКЗ), системи

розподілу навантаження розподілених серверів, *шлюзи для проходження трафіку через міжмережеві екрани, шлюзи з мобільними мережами та абонентами*.

Основну роль у відеоконференції грають канали зв'язку між абонентами. Розглянемо кілька методів організації каналів зв'язку для відеоконференцій.

Інтернет. Це найпростіший і дешевий метод організації відеоконференцзв'язку. Однак якість сеансу зв'язку в даному випадку може бути низькою, оскільки Інтернет не є гарантованим каналом передачі аудіо- та відеоданих. До цього додається проблема безпеки відеоконференції, тобто вона може стати "суспільним надбанням". Для організації відеоконференцзв'язку через Інтернет потрібно мати статичні IP-адреси і канали зв'язку з пропускною здатністю не менше 384 кбіт / с в обидва боки (для вихідного та вхідного трафіку).

За протоколом ISDN. Аббревіатура ISDN (англ. *Integrated Services Digital Network*) розшифровується як цифрова мережа з інтеграцією послуг. Цифрові мережі з інтегральними послугами відносяться до мереж, в яких основним режимом зв'язку є режим комутації каналів, а дані обраблюються в цифровій формі. ISDN имеет ряд переваг у порівнянні з традиційними аналоговими мережами, однак, у порівнянні з новими телекомунікаційними технологіями передачі даних має ряд серйозних недоліків:

• важко відстежити, на якій ділянці стався збій зв'язку;

• низька оперативність відновлення каналів зв'язку;

• дану технологію підтримують не так вже й багато операторів зв'язку;

• порівняно висока вартість застосування послуги зв'язку при міжрегіональному сполученні.

За технологією IP VPN MPLS. В даний час є однією з найбільш надійних і дешевих для організації відеоконференцій. Цьому сприяє:

• VPN (англ. Virtual Private Network) - віртуальна приватна мережа, тобто узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережевих захищених з'єднань (логічну мережу) поверх іншої мережі.

• MPLS (англ. Multiprotocol Label Switching) – мультипротокольна комутація по мітках, тобто, механізм передачі даних, який емулює різні властивості мереж з комутацією каналів поверх мереж з комутацією пакетів.

ДОДАТОК 4

Засади використання автоматизованої системи документообігу господарського суду Запорізької області (скорочено, як приклад)

ЗАТВЕРДЖЕНО
рішенням зборів суддів господарського суду
Запорізької області "15" березня 2016 р. № 3

Засади використання АСД господарського суду Запорізької області

1. У зв'язку з прийняттям Закону України "Про забезпечення права на справедливий суд" відповідно до "Положення про автоматизовану систему документообігу суду", затвердженого рішенням Ради суддів України № 25 від 02 квітня 2015 року та наказом Державної судової адміністрації України № 45 від 02 квітня 2015 року (далі – "Положення"), із змінами внесеними рішенням Ради суддів України від 05.06.2015 № 55 та наказом ДСА України від 05.06.2015 № 76, рішенням Ради суддів України від 03.03.2016 № 21 та наказом ДСА України від 03.03.2016 № 41, у господарському суді Запорізької області запроваджується використання автоматизованої системи документообігу суду шляхом використання комп'ютерної програми "Діловодство спеціалізованого суду" (далі - програма "Діловодство"), яка розроблена адміністратором автоматизованої системи для судів господарської юрисдикції.

2. Використання автоматизованої системи документообігу суду та порядок її функціонування визначається вказаним вище "Положенням" з особливостями, визначеними цими Засадами.

3. Збори суддів господарського суду Запорізької області (далі - "Збори суддів") мають визначені вказаним Положенням та цими Засадами повноваження щодо розгляду питань стосовно порядку функціонування автоматизованої системи.

4. Затверджені рішенням зборів суддів Засади використання автоматизованої системи документообігу суду вносяться до автоматизованої системи не пізніше робочого дня, що настає після проведення цих зборів.

5. Засади використання автоматизованої системи документообігу суду (зі змінами та доповненнями) вносяться до автоматизованої системи та оприлюднюються на веб-порталі судової влади України не пізніше робочого дня, що настає після проведення цих зборів.

Розподіл судових справ між суддями

6. Розподіл судових справ здійснюється в суді в день їх реєстрації, на підставі інформації, внесеної до автоматизованої системи, уповноваженою особою апарату суду, відповідальною за здійснення автоматизованого розподілу судових справ.

7. Визначення судді або колегії суддів для розгляду конкретної справи у господарському суді Запорізької області здійснюється автоматизованою системою шляхом:

автоматизованого розподілу судових справ під час реєстрації відповідної судової справи; пакетного автоматизованого розподілу судових справ після реєстрації певної кількості судових справ; розподілу судових справ шляхом передачі судової справи раніше визначеному у судовій справі судді; визначення складу суду з метою заміни судді (суддів); повторного автоматизованого розподілу судових справ.

Збори суддів господарського суду Запорізької області суду мають право визначати особливості автоматизованого розподілу судових справ у випадках, прямо передбачених Положенням.

8. Не розподіляються щодо конкретного судді судові справи, що надійшли: за два місяці до закінчення повноважень судді; за три робочих дні до початку відпустки, якщо її тривалість становить менше чотирнадцяти календарних днів; за чотирнадцять днів до початку відпустки (якщо її тривалість становить від 14 до 25 календарних днів, включно); за 30 днів до початку відпустки (якщо її тривалість становить 26 та більше календарних днів у період відпустки судді та інші умови;

Дні, у які не розподіляються щодо конкретного судді судові справи, враховуються при розрахунку коефіцієнту навантаження судді на момент автоматизованого розподілу судової справи.

Правила здійснення автоматизованого розподілу судових справ між суддями

9. Автоматизований розподіл судових справ здійснюється в автоматизованій системі за такими правилами: із загального списку суддів визначаються судді, які мають повноваження щодо розгляду судової справи на момент автоматизованого розподілу; для суддів, які мають повноваження щодо розгляду судової справи на момент автоматизованого розподілу, здійснюється розрахунок коефіцієнтів навантаження; із числа суддів, які мають повноваження щодо розгляду судової справи на момент автоматизованого розподілу з урахуванням визначених автоматизованою системою коефіцієнтів навантаження здійснюється визначення судді для розгляду конкретної судової справи за принципом випадковості.

10. Визначення суддів, які мають повноваження щодо розгляду судової справи на момент автоматизованого розподілу, здійснюється згідно з вимогами пункту 8 цих Засад, а також з урахуванням дотримання правил поєднання судових справ.

11. Коефіцієнт навантаження судді на момент автоматизованого розподілу судової справи розраховується за формулою, визначеною пунктом 2.3.6 Положення.

12. Обрання судді за випадковим числом здійснюється відповідно до коефіцієнту навантаження судді на момент автоматизованого розподілу судової справи.

13. Копія табеля обліку використання робочого часу щодо суддів відповідного суду, що складається для виплати заробітної плати, вноситься відповідальною особою суду до автоматизованої системи не пізніше наступного робочого дня після підписання цього табеля.

14. Здійснення автоматизованого розподілу судових справ без урахування правил, зазначених у пункті 9 цих Засад (підпункті 2.3.4 пункту 2.3 Положення) , не допускається.

Повноваження зборів суддів щодо здійснення автоматизованого розподілу судових справ між суддями

15. Збори суддів господарського суду Запорізької області мають право запроваджувати спеціалізацію суддів з розгляду конкретних категорій судових справ. Спеціалізація суддів визначається із розрахунку розподілу не менше двох суддів на одну спеціалізацію.

16. Спеціалізація та склад судових колегій у господарському суді Запорізької області визначено рішенням зборів суддів № 7 від 19.05.2015р.

17. Якщо розгляд справи здійснюється колегіально, склад колегії суддів визначається автоматизованою системою. Збори суддів можуть визначити склади постійно-діючих колегій суддів.

18. Збори суддів господарського суду Запорізької області мають право визначати особливості здійснення автоматизованого розподілу судових справ: у випадках виконання суддями іншої роботи, не пов’язаної із здійсненням правосуддя; у випадках виявлення значної різниці в навантаженні на суддів; у разі повторного надходження до суду позовних заяв, апеляційних і касаційних скарг, з передбачених процесуальним законом підстав.

19. Збори суддів мають право визначати: коефіцієнт складності категорій судових справ (визначено рішенням зборів суддів господарського суду Запорізької області № 21 від 09.12.2014 р.); особливості розподілу судових справ при виконанні суддею інших повноважень, не пов’язаних із здійсненням правосуддя; коефіцієнт адміністративних посад (рішенням зборів суддів господарського суду Запорізької області № 7 від 19.05.2015 р. визначено коефіцієнт навантаження голови суду на рівні 40%, заступника голови суду - 80% від коефіцієнту навантаження інших суддів), тощо;

20. Збори суддів мають право зменшити навантаження щодо розгляду справ на суддів, які обіймають адміністративні посади в суді або виконують інші обов'язки, не пов'язані із здійсненням правосуддя (є членами Ради суддів України або здійснюють науково-викладацьку діяльність в Національній школі суддів України) але не більше ніж на шістдесят відсотків порівняно з навантаженням інших суддів.

21. Збори суддів мають право розглядати питання щодо настання обставин, які унеможливлюють участь судді у розгляді судових справ, що може мати наслідком порушення строку розгляду судових справ, передбаченого відповідним процесуальним законом.

22. Рішенням зборів суддів господарського суду Запорізької області № 7 від 19.05.2015р. визначено, що у разі настання вказаних у п. 21 обставин на підставі подання такого судді, а за його відсутності - на підставі доповідної записки його помічника, або особи, що його замінює, керівником апарату суду приймається вмотивоване розпорядження про здійснення повторного автоматичного розподілу справи.

23. Зміни до налаштувань автоматизованої системи згідно з пунктами 15 - 22 цих Засад (підпунктами 2.3.10–2.3.18 пункту 2.3 Положення) , вносяться не пізніше

одного робочого дня, що передує даті їх застосування, визначеній зборами суддів відповідного суду.

Автоматизований розподіл судових справ між суддями

24. Автоматизований розподіл судових справ між суддями (колегіями суддів) здійснюється з урахуванням спеціалізації суддів.

25. Відмова судді від отримання розподіленої в установленому порядку судової справи не допускається.

26. Судові справи підлягають автоматизованому розподілу між суддями, які мають на момент автоматизованого розподілу судових справ повноваження для здійснення процесуальних дій.

27. При об'єднанні судових справ автоматизованою системою автоматично перераховується коефіцієнт навантаження на суддю (суддів), якому передано для розгляду ці судові справи.

Засади формування колегій суддів у випадку необхідності здійснення колегіального розгляду справ

28. Якщо судова справа підлягає розгляду колегією суддів, при автоматизованому розподілі судових справ автоматизованою системою в суді визначається головуючий суддя із числа всіх суддів відповідного суду з урахуванням їх спеціалізації (за її наявності).

29. Після визначення головуючого судді автоматизованою системою визначається склад колегії суддів із числа всіх суддів відповідного суду з урахуванням їх спеціалізації (за її наявності) .

30. Результатом автоматичного визначення складу колегії суддів є протокол автоматичного визначення складу колегії суддів (додаток 2), що автоматично створюється автоматизованою системою.

31. Якщо збори суддів визначили склади постійно діючих колегій, то автоматизована система визначає склад колегії з числа суддів основного складу. У разі неможливості визначити необхідну кількість суддів з числа суддів основного складу, автоматизована система визначає суддів, яких не вистачає, з числа резервних суддів даної колегії.

32. У разі необхідності розгляду судової справи колегією суддів після проведення автоматизованого розподілу судової справи між суддями здійснюється повторний автоматизований розподіл судової справи з метою збільшення складу суду у порядку, зазначеному в підпункті 2.3.23 пункту 2.3 Положення.

33. У випадку неможливості з підстав, визначених законодавством, Положенням та цими Засадами, формування повного складу колегії суддів (окрім головуючого судді) для розгляду конкретної справи з числа суддів відповідної спеціалізації допускається формування колегії з числа суддів іншої спеціалізації.

34. Рішенням зборів суддів господарського суду Запорізької області від 15 березня 2016р. № 3 визначено, що у разі необхідності розгляду судової справи колегією суддів та визначення відповідно до п. 28 цих Засад (п. 2.3.23 Положення)

головуючого судді автоматизована система визначає суддів, яких не вистачає, з числа всіх суддів господарського суду Запорізької області з урахуванням їх спеціалізації.

35. Відповідно до визначеного процесуальним законодавством принципу незмінності складу суду, розгляд справи, як правило, проводиться визначеною автоматизованою системою колегією суддів. Тимчасова відсутність судді-члена колегії, як правило, не може бути підставою для зміни складу колегії суддів.

36. У разі неможливості продовження розгляду справи одним із суддів-членів колегії (призов на військову службу, відпустка у зв'язку з вагітністю та пологами, довготривале перебування на лікарняному або у відпустці тощо) заміна судді-члена колегії здійснюється автоматизованою системою на підставі мотивованого розпорядження керівника апарату суду.

37. У разі задоволення відводу заміна судді здійснюється автоматизованою системою на підставі рішення про відвід (самовідвід) у порядку, зазначеному в підпункті 2.3.23 пункту 2.3 Положення.".

38. У разі розгляду судової справи колегією суддів до протоколу та звіту автоматично включаються прізвища суддів, які входять до складу колегії із зазначенням прізвища головуючого судді.

Розподіл судових справ шляхом передачі судової справи раніше визначеному у судовій справі судді

39. Судові справи, що надійшли із судів апеляційної або касаційної інстанцій після скасування ухвал, які перешкоджають подальшому розгляду судової справи (крім ухвал про закриття, припинення провадження), а також ухвал, які не перешкоджають подальшому розгляду судової справи, передаються раніше визначеному у судовій справі головуючому судді (судді-доповідачу), ухвалу яких скасовано чи у провадженні яких перебувала або перебуває судова справа.

40. Раніше визначеному в судовій справі головуючому судді (судді-доповідачу) передаються також: судові справи, що надійшли для вирішення питання про прийняття додаткового судового рішення, виправлення описок та помилок, роз'яснення судового рішення, повернення судового збору; судові справи, за якими надійшли заяви (клопотання), пов'язані із виконанням судових рішень, передбачені статтями 117, 119–121, 121-2, 122 Господарського процесуального кодексу України; зустрічні позови та позови третіх осіб, які заявляють самостійні вимоги щодо предмета спору у судовій справі, у якій відкрито провадження, що надійшли до суду тощо.

41. У разі відсутності раніше визначеного в судовій справі головуючого судді у випадках, передбачених підпунктами 2.3.44-2.3.46 пункту 2.3 Положення, такі судові справи та матеріали підлягають автоматизованому розподілу за правилами, визначеними Засадами використання автоматизованої системи документообігу суду.

Повторний автоматизований розподіл судових справ між суддями

42. Повторний автоматизований розподіл судових справ між суддями застосовується у випадках визначених законом, а також з метою заміни одного,

декількох суддів, всього складу суду, збільшення складу суду в порядку, визначеному підпунктами 2.3.4, 2.3.23 Положення".

43. Винятково у разі, коли суддя у передбачених законом випадках не може продовжувати розгляд справи, невирішені судові справи передаються для повторного автоматизованого розподілу за вмотивованим розпорядженням керівника апарату суду.

44. За вмотивованим розпорядженням керівника апарату суду здійснюється повторний автоматизований розподіл судових справ у разі виявлення очевидних помилок в налаштуваннях автоматизованої системи діловодства суду.

45. З 01 серпня 2016 року результатом повторного автоматизованого розподілу судової справи є протокол повторного автоматизованого розподілу судової справи між суддями відповідного суду (додаток 13), що автоматично створюється автоматизованою системою.

Неможливість автоматизованого розподілу судових справ між суддями

46. У разі визначення автоматизованою системою неможливості здійснення розподілу судових справ створюється протокол щодо неможливості такого розподілу судових справ між суддями відповідного суду (додаток 10).

47. У разі усунення обставин, що унеможливлюють здійснення автоматизованого (повторного автоматизованого) розподілу судових справ, такий розподіл відбувається відповідно до вимог Положення та цих засад.

Передача судових справ для подальшого розгляду суддею (колегією суддів)

48. Після автоматизованого розподілу судових справ автоматизованою системою відповідальна особа суду не пізніше наступного робочого дня передає судові справи визначеному автоматизованою системою головуючому судді.

49. Інформація щодо процесуальних дій та судових рішень вноситься до автоматизованої системи відповідним користувачем автоматизованої системи.

Прикінцеві положення

50. Збори суддів господарського суду Запорізької області за необхідності, але не рідше одного разу на рік, заслуховують керівника апарату суду з питань функціонування автоматизованої системи, стану розподілу судових справ з метою дотримання збалансованого навантаження суддів.

51. Інформація щодо стану навантаження на кожного суддю відповідного суду є відкритою для суддів цього суду та не може бути обмежена.

52. Заміна суддів у складі колегії суддів у справах, що надійшли до суду до набрання чинності Положенням та затвердження цих Засад, відбувається в порядку визначеному цими Засадами.

53. Робота щодо наповнення та використання інформації в автоматизованій системі здійснюється після створення правових умов (видання керівником апарату суду наказів про визначення прав користувачів автоматизованої системи) та впровадження і налагодження програмно-технічних засобів для забезпечення функціонування підсистем на кожному автоматизованому робочому місці.

ДОДАТОК 5

СИСТЕМА ДИСТАНЦІЙНОГО НАВЧАННЯ Д-3

Комп'ютерна програма документообігу загальних судів "Д-3" призначена для:

- забезпечення автоматизації процесів проходження процесуальних документів, загального діловодства;
- здійснення процесуального контролю та контролю виконання завдань по документам;
- відстеження порядку проходження справ та документів;
- формування звітності суду про стан здійснення правосуддя;
- передачі справ (документів) до електронного архіву;
- значного підвищення ефективності роботи судів у зв'язку зі зменшен-ням часу, який працівники суду витрачають на обробку справи, а саме її реєстрацію, пошук, виготовлення процесуальних документів тощо.
- фактичне місцезнаходження паперових документів.
- автоматичного контролю виконання робіт з документообігу, що суттєво підвищує якість роботи виконавців, робить терміни підготовки документів більш прогнозованими і керованими.
- значного зменшення обігу документів у паперовому варіанті;
- організації доступу громадян до необхідної інформації, що робить суд більш відкритим та доступним для громадян.
- автоматичного розподілу справ між суддями.
- автоматичного направлення судових рішень до Єдиного Державного Реєстру Судових Рішень України.

МОДУЛІ "Д-3" ДЛЯ САМОСТІЙНОГО ІНТЕРНЕТ-НАВЧАННЯ

Реєстрація та ведення вхідної та вихідної кореспонденції (загальна канцелярія)

Пройшовши дистанційний курс "Реєстрація та ведення вхідної та вихідної кореспонденції (загальна канцелярія)" користувач отримує такі навики роботи:

- реєстрація вхідної і вихідної документації – створення завдань по документу, перевірка своєчасного доведення їх до виконавця, узагальнення результатів виконання завдань.;
- друк реєстру вхідної (вихідної) кореспонденці;
- відбір у будь-якому реєстрі потрібних записів і роздруковка реквізитів за допомогою засобів фільтрації;
- групування та сортування даних;
- створення фільтрів.

Реєстрація справ та ведення статкарток (канцелярія по справах)

Пройшовши дистанційний курс "Реєстрація справ та ведення статкарток (канцелярія по справах)" користувач отримує такі навики роботи:

- роботу з обліково-статистичними картками;
- обмін з Єдиним реєстром досудових розслідувань;
- реєстрації справ;
- судовий збір;
- поєднувати справи;
- встановлення дати набрання судовими рішеннями законної сили;
- відправлення документів електронною поштою;
- розсилка повісток за допомогою SMS-повідомлень ...

Виготовлення документів судочинства та фіксування судового процесу (секретарі судових засідань)

Пройшовши дистанційний курс “Виготовлення документів судочинства (судді та їх помічники)”, користувач отримує такі навики роботи:

- загальні відомості про кримінальне впровадження (КП);
- створення оперативно-статистичної картки (ОСК);
- додавання учасників процесів;
- реєстрація судового збору;
- робота в редакторі шаблонів;
- встановлення ДНЗС;
- створення підписки на отримання процесуальних документів та отримання sms-повісток;
- реєстрація завдань (доручень) по документу, справі
- переміщення документів, справ;
- створення деталізації;
- фіксування судового процесу...

Виготовлення документів судочинства (судді та їх помічники)

Пройшовши дистанційний курс “Виготовлення документів судочинства (судді та їх помічники)”, користувач отримує такі навики роботи:

- загальні відомості про КП "Д-3";
- створення ОСК;
- додавання учасників процесу;
- встановлення ДНЗС;
- реєстрація судового збору;
- робота в редакторі шаблонів;
- створення нових шаблонів документів;
- відправлення процесуальних документів до ЄДРСР;
- створення підписки на отримання процесуальних документів на електронну пошту та sms-повістки;
- робота з довідниками, налаштування автоматичного розподілу справ;
- налаштування персональних і загальних параметрів призначення.

ДОДАТОК 6

ЗАКОН УКРАЇНИ
“Про основні засади забезпечення кібербезпеки України”

(Відомості Верховної Ради, 2017, № 45, ст.403)

{Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241}

(**надається в скороченому вигляді**)

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз – показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки – відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4) кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

5) кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

8) кіберзлочин (комп'ютерний злочин) – суспільно небезпечне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність – сукупність кіберзлочинів;

10) кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

12) кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури;

16) критично важливі об'єкти інфраструктури (далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки

і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

17) Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

18) національні електронні інформаційні ресурси (далі – національні інформаційні ресурси) – систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

19) об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

20) система управління технологічними процесами (далі – технологічна система) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

21) системи електронних комунікацій (далі – комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Стаття 8. Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

2. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту

якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

4) Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

5) залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

8) розвитку мережі команд реагування на комп'ютерні надзвичайні події;

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

12) обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем та ін.

Тупкало Віталій Миколайович,
Заплотинський Борис Андрійович,
Авєрічєв Ігор Миколайович

Використання інфокомунікаційних технологій в юридичній діяльності

Навчальний посібник на 164 стор.