8. ТЕМАТИЧНИЙ СЛОВНИК

Аварійна ситуація — певний винятковий (граничний) стан *інформаційної системи*, який являє собою критичне сполучення *відмов* та (або) помилок функціонування її елементів і здатний призвести до порушення функціонування об'єкта управління, що пов'язано з особливо значними технічними, економічними або соціальними втратами.

Автентифікація — 1. (біометрія) процес перевірки особи (індивіда) на основі унікальних вимірюваних фізіологічних характеристик людини, див. також *ідентифікація, біометрична ідентифікація*; **2.** (криптографія) визначення походження зашифрованої *інформації* шляхом *верифікації цифрового підпису* або *публічного ключа* через його унікальні *відбитки*.

Автоматизована система (АС) **—** див. *інформаційна система*.

Автоматизована система контролю виконання документів — *інформаційна система*, призначена для обліку всієї документації установи, постановки на контроль і контролю за виконанням *документів* (нагадування про наближення строків закінчення виконання документа, повідомлення про прострочені документи тощо).

Автоматизоване робоче місце (АРМ) **—** програмно-технічний комплекс *інформаційної системи*, призначений для автоматизації діяльності певного виду. Основною характеристикою АРМ є орієнтація на людину, яка не має професійної підготовки з використання обчислювальної техніки, але фахово обізнана у конкретній предметній галузі.

Автоматизований банк даних — система інформаційних, математичних, програмних, мовних, організаційних і технічних засобів, які необхідні для інтегрованого нагромадження, зберігання, ведення, актуалізації, пошуку і видачі *даних*. Основними складовими автоматизованого банку даних є *база даних* і *система керування базою даних*.

Авторизація — надання *користувачеві* доступу до певних об'єктів і ресурсів *інформаційної системи* залежно від його повноважень, що визначаються за його *ідентифікатором* і паролем.

Агент — див. *програмний агент*.

Адаптивна надійність — властивість *інформаційної системи* виконувати свої функції, якщо вони змінюються в межах умов, зумовлених розвитком системи керування об'єкта, впродовж заданого проміжку часу.

Адміністрація реєстрації (Registration Authority) — це люди, які за допомогою відповідних засобів підтримують реєстрацію *користувачів* і виконують функції з адміністрування.

Адміністрація сертифікації (Certificate Authority) — *довірена третя сторона*, яка створює *сертифікати*, накладає на них свій *цифровий підпис* і приєднує їх до *публічних ключів* певних осіб. За допомогою *відкритого ключа* адміністрації сертифікації будь-хто може перевірити цифровий підпис, а отже, цілісність сертифіката.

Алфавіт коду — система знаків, узятих для створення *коду*.

Антивірусна програма — спеціальна програма, призначена для виявлення і знищення комп'ютерних вірусів.

Асиметричне шифрування — див. *криптографія з асиметричними ключами*.

Атака, що спричиняє відмову від обслуговування (denial of service attack, DOS-attack) — комп'ютерний злочин, зазвичай спланований, метою якого є перенавантаження Інтернет-сервера підключеннями, які не можуть бути завершені, з метою уповільнення його роботи або унеможливлення оброблення легітимних запитів.

База даних (БД) — іменована структурована сукупність взаємопов'язаних *даних*, що відображає стан об'єктів та їх відношень у визначеній *предметній галузі*. Див. також *сховище даних*.

База знань (БЗ) — упорядкована сукупність правил, фактів, механізмів виведення та програмних засобів, що описує певну *предметну галузь* і призначена для подання нагромаджених у ній *знань*.

Банк даних — система програмно-апаратних, мовних і організаційних засобів, призначених для централізованого накопичення і колективного використання даних, а також самі *дані*, які зберігаються в *базах даних*.

Безпека інформації — див. *інформаційна безпека*.

Бібліографічний пошук — *документальний пошук*, який здійснюється з метою знаходження бібліографічних описів *документів*, що відповідають *інформаційному запиту*, без видачі самих документів.

Біометрична ідентифікація — підтвердження особи шляхом зіставлення зафіксованої відцифрованої характеристики фізіології або поведінки, яка унікально ідентифікує особу (відбитки пальців, геометрія руки, почерк і т. ін.), з особистими даними людини. Див. також *автентифікація*, *ідентифікація*.

Блокування інформації — дії, наслідком яких є припинення доступу до *інформації*.

Брандмауер (firewall, «вогняна стіна») — сукупність технічних і програмних засобів (маршрутизатор, персональний комп'ютер, один або кілька *серверів*), призначена для захисту мережі або підмережі від зовнішніх мереж. Брандмауер перехоплює, аналізує і, відповідно, пропускає або блокує трафік в обидві сторони.

Броузер (іноді — браузер) — прикладна програма (клієнтська частина), яка забезпечує навігацію у *World Wide Web* та роботу з гіпертекстовими документами.

Верифікація — (криптографія) перевірка *цифрового підпису* на основі відповідного *публічного ключа* з метою визначення, що *інформацію* було справді надіслано особою, яка наклала свій підпис, і повідомлення не було змінено після цього.

Виконавча інформаційна система (Executive Information System, EIS, інформаційна система керівника) — *інформаційна система*, призначена для забезпечення необхідною актуальною *інформацією* менеджерів вищої ланки управління у процесі прийняття стратегічних рішень на базі мережних робочих станцій з графічними дисплеями і легким у використанні інтерфейсом.

Винюхування (sniffing) — сканування пакетів, які передаються у мережі, спосіб одержання *несанкціонованого доступу* до *інформації*.

Витік інформації — результат дій порушника, внаслідок яких *інформація* стає відомою (доступною) суб'єктам, що не мають права доступу до неї.

Відбитки (key fingerprint) — (криптографія) унікальна ідентифікуюча послідовність цифр і символів, що використовується для *автентифікації публічних ключів*.

Відмова у виконанні функцій — подія, яка полягає у порушенні хоча б однієї з вимог до якості виконання цієї функції, встановлених нормативно-технічною та (або) конструкторською документацією на *інформаційну систему*.

Відмовостійкість — здатність *інформаційної системи* продовжувати функціонування в разі збою її окремих частин.

Відкритий ключ — див. *публічний ключ*.

Відновлення ключа (key recovery) — спеціальна можливість схеми *управління ключами*, яка дає змогу розшифрувати повідомлення, навіть якщо початковий *ключ* було втрачено. Див. також *депонування ключів*.

Відомча мережа зв'язку — *мережа зв'язку*, що експлуатується юридичною або фізичною особою для задоволення власних потреб.

Відцифрований образ особи — зафіксоване й збережене зображення обличчя особи електронним способом за допомогою цифрової камери.

Віртуальна приватна мережа (Virtual Private Network, VPN) — група комп'ютерів у загальнодоступній мережі, наприклад в *Інтернет*, між якими здійснюється захищена передача *інформації* з використанням систем криптографічного захисту (див. *криптографія*).

Віртуальне підприємство — тимчасове об'єднання незалежних економічних суб'єктів на основі електронних комунікацій з метою досягнення певної цілі (виконання певного завдання).

Віртуальний офіс — *Web-сайт* (або його частина), призначений для забезпечення організаційної взаємодії географічно роз'єднаних співробітників компанії за допомогою єдиної системи обміну, збереження, оброблення та передавання *інформації*.

Власна макро-змінна — (ЕС) *макро-змінна*, яка містить назву *факту макро-твердження*.

Втрата інформації — дія, внаслідок якої *інформація* перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.

Географічна інформаційна система (геоінформаційна система, ГІС, Geographic Information System, GIS) — *інформаційна система*, в якій модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) поєднується з інформацією табличного типу (різноманітні статистичні дані, списки, економічні показники тощо).

Гипермедіа — розширення поняття *гіпертекст*. Термін застосовується до документів, які містять не тільки текстові елементи, а й графіку, звук, відео тощо.

Гіперпосилання (link) — назва *сайта*, рекламно-інформаційний рядок або графічний елемент у гіпертекстовому документі (див. *гіпертекст*), при натисканні на який мишею відбувається перехід на іншу сторінку або *Web-сайт*. Під час наведення миші на гіперпосилання курсор набуває вигляду руки з вказівним пальцем, який натискує на відповідний елемент.

Гіпертекст (гіпер- від англ. «hyper-» — «над-») — звичайний текст, який містить посилання як на власні фрагменти, так і на інші тексти (див. *гіперпосилання*). Див. також *гіпермедіа*.

Глибина класифікації — кількість ступенів класифікації.

Глобальна мережа — *комп'ютерна мережа*, яка охоплює територію регіону, держави чи декількох країн. Глобальна мережа може з'єднувати як окремі ЕОМ, так і *локальні мережі*.

Головний факт консультації — (ЕС) *факт*, з приводу якого проводиться дана консультація.

Головний факт правила — (ЕС) *факт*, який стоїть після логічної зв'язки «то» у логічній формі «Якщо… то…». Див. також *хвостовий факт правила*.

Групове забезпечення (groupware) — специфічне програмне забезпечення, призначене для підтримки колективної роботи виконавців над спільним завданням.

Дані — *інформація*, подана у формалізованому вигляді, придатному для зберігання, оброблення, пересилання й інтерпретації автоматизованими засобами за можливої участі людини.

Дейтамайнінг — добування даних — виявлення прихованих правил і закономірностей у наборах *даних*.

Декомпозиція — процес поділу системи на елементи, зручні для якихось операцій з нею, до елементів, які приймаються як неподільні об'єкти.

Депонування ключа (key escrow) — практика передачі *приватного ключа* його власником третій стороні (довіреній особі, урядовим структурам) для моніторингу зашифрованих комунікацій та можливого *відновлення ключа.*

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

Державна таємниця — вид *таємної інформації*, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою.

Дескриптор — слово або словосполучення, яке однозначно позначає поняття з теми *тезаурусу*.

Дешифрування — перетворення зашифрованої *інформації* так, щоб вона стала читабельною; операція, зворотна до *шифрування*. Звичайно виконується за допомогою *приватного ключа*. Див. також *криптографія.*

Ділова процедура — логічний етап *ділового процесу*, який необхідно реалізувати для його завершення.

Діловий процес («потік робіт» від англ. «workflow») — це логічно завершений набір операцій (*ділових процедур*), що підтримують структуру підприємства і реалізують його політику, спрямовану на досягнення поставленої мети.

Діловодство — діяльність зі створення документів та організації роботи з ними — створення умов, що забезпечують рух, пошук і збереження документів.

Довжина ключа — кількість бітів, яка визначає розмір *ключа*. Чим більше довжина ключа, тим надійнішим він є.

Довжина коду — кількість знаків у *коді* без урахування пропусків (прогалин).

Довідковий пошук — дії, методи та процедури для пошуку в *інформаційній системі* всіх видів посилань, що відповідають *інформаційному запиту*.

Довірена третя особа (Trust Third Party) — (криптографія) відповідальна сторона, на яку усі зацікавлені учасники електронних комунікацій погоджуються покласти виконання функцій *сертифікації* та запису часу створення або існування *ключів*. Довіреній особі можуть також надаватись *приватні ключі* (див. *депонування, відновлення ключа*).

Документ — передбачена законом матеріальна форма одержання, зберігання, використання і поширення *інформації* шляхом фіксації її на папері, магнітній, кіно -, відео -, фотоплівці або на іншому носієві.

Документальний пошук — дії, методи та процедури для знаходження у фонді необхідних *документів*.

Документообіг — рух *документів* з моменту їхнього одержання або створення до завершення виконання або відправлення.

Домашня сторінка — «титульна», початкова сторінка *Web-сайта*, з якої можна одержати доступ до інших *Web-сторінок*.

Доменне ім'я (domain) — назва *Web-сайта*, що являє собою набір кількох імен, розподілених точками, і замінює для зручності сприйняття людиною цифрову *IP-адресу*. Доменне ім'я обов'язково складається з домену першого рівня, який визначає географічний регіон або напрям діяльності сайта, і домену другого рівня, який позначає назву проекту або організації. У доменному імені також можуть бути присутні домени третього і нижчих рівнів, які створюються за необхідності власниками домену другого рівня.

Дорадча система — інтелектуальна *інформаційна система*, що забезпечує формування рекомендацій про послідовність і перелік можливих дій *користувача* в процесі розв'язування задачі.

Дроблення ключів (key splitting, secret sharing) — процес розділу *приватного ключа* на численні частини і розподілу їх між особами, що складають певну групу. Для того, щоб використати приватний ключ, члени групи мають скласти наявні у них компоненти цього ключа.

Економічна ефективність — результат впровадження *інформаційної системи*, який виявляється у покращанні економічних результатів функціонування об'єкта.

Експертна система (ЕС) — інтелектуальна *інформаційна система*, призначена для розв'язування *задач* у певній *предметній галузі* на основі *знань*, наданих експертами, що включає *базу знань* і яка підтримує функції обґрунтування, пояснення та виправдання. Див. також *дорадча система*, *система на основі знань*.

Електронна комерція (ЕК) — будь-яка форма бізнес-процесу, будь-який вид операцій, при виконанні яких взаємодія між суб'єктами

відбувається електронним способом замість фізичного обміну або безпосереднього фізичного контакту.

Електронна пошта (e-mail, electronic mail) — це служба поштового зв'язку, в якій повідомлення передаються в електронному вигляді з використанням комп'ютерів і каналів зв'язку.

Електронний архів — система автоматизації, призначена для фізичного збереження *електронних документів* та їхнього пошуку.

Електронний документ — *документ*, інформація в якому подана в електронній формі, що включає необхідні реквізити, в тому числі *електронний цифровий підпис*.

Електронний цифровий підпис — див. *цифровий підпис*.

Ергономічне забезпечення — сукупність засобів і методів, які створюють найсприятливіші умови праці людини в *інформаційній системі*, умови для взаємодії людини та ЕОМ.

Еталон класифікатора — врахований оригінал *класифікатора*, який ведеться відповідальною установою.

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

Ємність класифікатора — найбільша кількість *позицій*, яку може містити *класифікатор*. Див. також *резервна ємність класифікатора*.

Життєвий цикл інформаційної системи — сукупність взаємопов'язаних процесів створення і послідовної зміни стану *інформаційної системи* від формування початкових вимог до неї до закінчення експлуатації та утилізації комплексу засобів автоматизації.

Задача оброблення даних — *функція* або її частина, що являє собою формалізовану сукупність автоматичних дій, виконання яких призводить до результатів заданого виду. Див. також *правова задача*.

Закритий ключ — див. *приватний ключ*.

Засоби інформатизації — електронні обчислювальні машини, програмне, математичне, лінгвістичне та інше забезпечення, *інформаційні системи* або їх окремі елементи, інформаційні мережі й мережі зв'язку, що використовуються для реалізації *інформаційних технологій*.

Захист інформації — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника *інформації* чи *автоматизованої системи* та осіб, які користуються інформацією. Див. також *криптографія*, *стеганографія*.

Зв'язка ключів (keyring) — (криптографія) сукупність *ключів*. Кожен користувач має два типи зв'язок ключів — приватну, яка містить один або кілька *приватних ключів* цього користувача, і публічну — сукупність його *публічних ключів*.

Знання — сукупність фактів, закономірностей, відношень та евристичних правил, що відображає рівень обізнаності з проблемами деяких *предметних галузей*. Специфічними особливостями знань, які дають змогу відрізнити їх від *даних*, є внутрішня інтерпретація, наявність ситуативних зв'язків, активність і форма подання.

Ідентифікатор ключа — (криптографія) код, який унікально позначає *пару ключів*. Дві пари ключів можуть мати однаковий *ідентифікатор користувача*, але обов'язково матимуть різні ідентифікатори ключів.

Ідентифікатор користувача — **1.** код, який унікально позначає користувача; **2.** (криптографія) текстова фраза, яка ідентифікує *пару ключів*, найчастіше це — ім'я власника та адреса *електронної пошти*. Цей ідентифікатор допомагає *користувачам* (і власнику, і його кореспондентам) визначати власника ключа (пари ключів).

Ідентифікатор особи — (ЄДАПСУ) відтворений у паспорті (документі) *відцифрований образ особи*.

Ідентифікація — **1.** процедура присвоєння об'єкту ідентифікатора; **2.** встановлення тотожності особи за сукупністю її загальних та окремих даних (див. також *автентифікація, біометрична ідентифікація*); **3.** процес перевірки вірогідності *інформації*, поданої *користувачем* під час реєстрації у мережній операційній системі або багатокористувацькій *інформаційній системі* шляхом звірки імені та пароля користувача з переліком осіб, які мають право доступу до системи; якщо дані збігаються, користувач може увійти до системи і одержати доступ до ресурсів згідно зі своїми правами (див. *авторизація*).

Індекси пошукової системи — терміни, які описують зміст ресурсів *інформаційно-пошукової системи*.

Індексування — створення *індексів пошукової системи*, визначення *пошукового образу документа*.

Інтерактивний режим — режим взаємодії *користувача* з *інформаційною системою*, при якому система приймає, обробляє і видає *інформацію* у реальному масштабі часу зі швидкістю, прийнятною для сприйняття інформації людиною.

Інтернет (Internet) — *глобальна комп'ютерна мережа*, яка об'єднує мережі, що належать різним власникам і адмініструються відокремлено, з метою забезпечення уніфікованих комунікацій по всьому світу. Одним з найбільш популярних сервісів Інтернет є *World-Wide Web*.

Інтернет-провайдер (ISP, Internet Service Provider) — компанія, яка надає доступ, здебільшого платний, до *Інтернет*.

Інтерфейс користувача — комплекс апаратних і програмних засобів, призначений для забезпечення взаємодії *користувача* з комп'ютером. Інтерфейс користувача має три головні аспекти: мову дій — що може робити користувач під час взаємодії з *інформаційною системою*; мову відображення — що бачить (чує) користувач у результаті роботи системи; базу знань — що необхідно знати користувачеві для роботи з системою.

Інтранет — внутрішньокорпоративна *мережа*, побудована на основі стандартних технологій *Інтернет* (*TCP/IP*, *WWW* та ін.).

Інформатизація — сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян і суспільства на основі створення, розвитку і використання *інформаційних систем*, *мереж*, ресурсів та *інформаційних технологій*, створених на основі застосування сучасної обчислювальної та комунікаційної техніки. Див. також *правова інформатизація*.

Інформаційна база — сукупність упорядкованої *інформації*, яка використовується при функціонуванні *інформаційної системи*, має дві складові — *машинну* та *позамашинну*.

Інформаційна безпека — захищеність *інформації* від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи зруйнування *даних*. Інформаційна безпека передбачає забезпечення *цілісності* інформації, її *конфіденційності* і, водночас, доступності для всіх авторизованих *користувачів*.

Інформаційна діяльність — сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Інформаційна система — 1. людино-машинна система, яка збирає, нагромаджує, зберігає, обробляє і видає за запитом *користувача* або на замовлення *інформацію* у вигляді *даних* і *знань*, необхідних для виконання функції управління; **2**. організаційно-технічна система, яка забезпечує вироблення рішень на основі автоматизації інформаційних процесів у різних сферах людської діяльності.

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

Інформаційне забезпечення (ІЗ) — інформаційні ресурси як предмет праці, методи і засоби ведення *інформаційної бази*. Інформаційне забезпечення складають форми документів, нормативна база та реалізовані рішення щодо обсягів, розміщення та форм існування *інформації*, яка використовується в *інформаційній системі* під час її функціонування.

Інформаційний запит — текст *інформаційно-пошуковою мовою*, що відображає деяку інформаційну потребу.

Інформаційний пошук — дії, методи та процедури для знаходження у фонді необхідної *інформації*.

Інформаційно-аналітична система — автоматизована *інформаційна система*, призначена для аналізу і синтезу з деякого первісного масиву *даних*, що зберігаються в ній, нової *інформації*, яка в явному вигляді відсутня в первісному масиві.

Інформаційно-пошукова мова — спеціалізована штучна мова, призначена для опису центральних тем і формальних характеристик *документів*, а також опису *інформаційних запитів* і наступного виконання пошуку. Див. також *пошукова система Інтернет*.

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

Інформаційно-пошуковий тезаурус — структурований список *ключових слів*, призначених для однозначного подання концептуального змісту *документів* та *інформаційних запитів.*

Інформація — документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Інфраструктура публічних ключів (Public Key Infrastructures, PKI) — широкодоступна система сертифікації, призначена для надання діючих *публічних ключів* із забезпеченням їх достовірності за допомогою *сертифікатів*. Основними компонентами інфраструктури публічних ключів є *адміністрація сертифікації* та *адміністрація реєстрації*. Термін також охоплює закони, правила, стандарти і програмне забезпечення для регулювання або роботи із сертифікатами, публічними і *приватними ключами*.

Каталог — *Web-сервер*, який надає послуги з пошуку ресурсів *Інтернет* за *гіперпосиланнями*, об'єднаними в ієрархічно організовані тематичні рубрики.

Категорія класифікатора — ознака, яка вказує на належність *класифікатора* до відповідної групи і залежить від рівня його затвердження і сфери застосування (загальнодержавний, галузевий і т. ін.).

Кіберсквоттинг — реєстрація з метою наступного перепродажу потенційно цікавих для кого-небудь *доменних імен*.

Класифікатор — офіційний документ, що являє собою систематизований перелік назв і *кодів класифікаційних угруповань* або об'єктів *класифікації*. Див. також *еталон, ємність*, *категорія*, *позиція, реєстрація*, *резервна ємність класифікатора*.

Класифікаційне угруповання — частина об'єктів, виокремлена під час *класифікації.*

Класифікація — поділ множини об'єктів на частини за їх подібністю або відмінністю згідно з прийнятими методами. Див. також *ознаки класифікатора*.

Клієнт — комп'ютер, який в умовах мережі користується послугами іншого комп'ютера, який називається *сервером*.

Клієнт-серверна технологія — технологія оброблення *даних*, за якої *клієнт* формує запити до *сервера* і відображає результати їх виконання сервером.

Ключ — послідовність бітів (символів), досить велика та унікальна для того, щоб не бути підібраною, що використовується для *шифрування*, накладання *цифрових підписів*, *дешифрування* та *верифікації* електронних повідомлень. Ключі існують у відкритій (*публічний ключ*) та закритій (*приватний ключ*) формі і зберігаються у *зв'язках ключів*.

Ключова макро-змінна — (ЕС) *макро-змінна*, яка визначає *контекст* значення *факту*.

Ключові слова — слова, найбільш характерні для даного тексту або тематики.

Код — знак або сукупність знаків, що використовуються для позначення *класифікаційного угруповання* та об'єкта *класифікації*. Див. також *алфавіт, довжина, основа, розряд, структура коду, контрольне число*.

Кодування — 1. створення і присвоєння *коду класифікаційному угрупованню* та об'єкту класифікації; **2.** процес присвоєння об'єкту певного *коду*. Див. також *перекодування*.

Компонент інформаційної системи — частина *інформаційної системи*, що виокремлена за зазначеною ознакою або сукупністю ознак і розглядається як самостійне ціле. За своїм призначенням компоненти поділяються на забезпечувальні та функціональні.

Комп'ютеризація — процес розвитку та впровадження комп'ютерів, що забезпечують автоматизацію інформаційних процесів і технологій у різних сферах людської діяльності.

Комп'ютерна мережа — сукупність каналів передавання даних і/або засобів комунікації, які з'єднують окремі ЕОМ і надають можливість використовувати спільні програмні й технічні засоби.

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

Комп'ютерний злочин — 1. злочин, пов'язаний із втручанням у роботу комп'ютера або *комп'ютерної мережі*; **2.** злочин, в якому комп'ютер(-и) використовується як необхідний технічний засіб.

Консолідація — внесення до нормативного акта наступних змін і поправок та об'єднання їх в єдиному документі.

Консультація — (ЕС) процес одержання висновку експерта на задане питання на основі знань експерта та *інформації*, що надана йому

користувачем. *Користувач* надає інформацію експерту шляхом відповіді на його питання в заданому *контексті*. Користувацька інформація також може надаватись через запит до певних *баз даних*. Результат консультації — висновок експерта, що надається у вигляді звіту про консультацію. Див. *консультація «Що, якщо...»*, *консультація «А якщо...»*.

Консультація «А як...» — (ЕС) режим розмірковування, який надає *користувачеві* можливість взнати, як має змінитись ситуація, з якої проводиться *консультація* (відповіді користувача або інші висновки експерта), для одержання певної думки експерта.

Консультація «Що, якщо...» — (ЕС) режим розмірковування, який надає *користувачеві* можливість простежити зміну думки експерта у разі зміни певних відповідей користувача (моделюванні ситуації).

Контекст — (ЕС) змінна частина твердження, вже визначена експертом або *користувачем* і необхідна для коректної відповіді на задане запитання. Наприклад, у відповіді на запитання про вік підозрюваного контекстом є його ім'я.

Контрольне число — розрахункове число, яке використовується для перевірки вірогідності запису *коду*.

Конфіденційна інформація — це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Користувацький інтерфейс — див. *інтерфейс користувача*.

Користувач — особа, що бере участь у функціонуванні *інформаційної системи* або використовує результати її роботи.

Корпоративна інформаційна система (КІС) — *інформаційна система* масштабу підприємства, яку відрізняє спроможність працювати в розподіленій структурі (корпорації) з множиною територіально розкиданих філій і повнофункціональність. Головною особливістю корпоративної інформаційної системи є реалізація в ній правил визначення бізнес-результату залежно від певних умов або дій.

Криптоаналіз — мистецтво та наука перетворення зашифрованого тексту у читабельний за невідомості *ключів*, що використовувались для *шифрування* (необхідних для *дешифрування*).

Криптографічна система — сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки).

Криптографія — вид захисту *інформації*, який реалізується за допомогою її перетворень із використанням спеціальних даних (*ключів*) з метою приховування змісту, підтвердження справжності, цілісності, авторства тощо.

Криптографія з асиметричними ключами — метод криптографії, коли для *шифрування* використовується один, *публічний* (відкритий, за-

гальнодоступний) ключ, а для *дешифрування* — інший, *приватний* (секретний, закритий). Асиметричні ключі складають окремі, але інтегровані складові *пари ключів*, кожний з них має своє призначення — *ключ*, що використовується для шифрування, не може бути використаний для розшифровки. Публічний ключ не дає змоги визначити приватний ключ. Найбільш поширеними алгоритмами асиметричного шифрування є *RSA*, *Diffie-Hellman*, *DSA*. Див. також *криптографія з симетричними ключами*.

Криптографія з публічним ключем — див. *криптографія з асиметричними ключами*.

Криптографія з симетричними ключами — метод *криптографії*, згідно з яким ключ для *шифрування* і ключ для *дешифрування* збігаються (це єдиний, секретний ключ) або можуть бути обчислені один з одного. Найбільш поширеними алгоритмами симетричного шифрування є *CAST*, *DES*, *Triple-DES*, *IDEA*. Одним з новітніх алгоритмів є *Twofish*. Див. також *криптографія з асиметричними ключами*.

Криптологія — наука про проблеми захисту інформації шляхом її перетворення, розділяється на два напрями — *криптографію* та *криптоаналіз*, цілі яких прямо протилежні.

Криптосистема — див. *криптографічна система*.

Кроулер (crawler) — див. *робот*.

Логічна бомба — невелика програма, яка прихована у тексті іншої програми, спрацьовує при настанні певних умов і може призвести до часткового або повного виведення системи з ладу.

Локальна обчислювальна мережа (ЛОМ) — *комп'ютерна мережа*, що зв'язує не більше сотні вузлів в одній локальній зоні (не більше кількох кілометрів).

Люк — прихована, не задокументована точка входу у програмний модуль.

Макро-змінна — (ЕС) назва *факту* у тексті *макросу*. Див. також *власна макро-змінна*, *ключова макро-змінна*.

Макрос — (ЕС) текстовий вираз, призначений для формування тексту питання, твердження або значення *факту*.

Макро-твердження — (ЕС) *макрос*, призначений для визначення твердження *факту*.

Маскарад — використання чужого імені або пароля з метою одержання *несанкціонованого доступу*.

Машинна інформаційна база — частина *інформаційної бази*, сукупність файлів, які зберігаються у пам'яті ЕОМ та на магнітних носіях. Див. також *позамашинна інформаційна база*.

Медіа-компетентність — система навиків пошуку у середовищі *Інтернет* і застосування *інформації* з раціональним рівнем *потенціалу для вирішення задач*.

Мережа — див. *комп'ютерна мережа*.

Мережа зв'язку — сукупність засобів та споруд зв'язку, поєднаних в єдиному технологічному процесі для забезпечення інформаційного обміну.

Мережа зв'язку загального користування — *мережа зв'язку*, що експлуатується підприємствами та об'єднаннями зв'язку для забезпечення потреб у послугах зв'язку усіх споживачів.

Мережа зв'язку подвійного призначення — *мережа зв'язку*, що експлуатується юридичною або фізичною особою для задоволення власних потреб та надання на умовах ліцензування послуг усім споживачам послуг зв'язку.

Мережа спеціального зв'язку — *мережа зв'язку*, яка забезпечує обмін *інформацією* з обмеженим доступом.

Мережа технологічного зв'язку — *відомча мережа зв'язку* для обміну *інформацією* з метою забезпечення технологічних процесів у виробничій діяльності.

Мета-пошук — пошук у кількох пошукових системах одночасно за одним *пошуковим розпорядженням*.

Мета-пошукова система — *інформаційно-пошукова система*, яка здійснює пошук у кількох пошукових системах одночасно. Див. також *пошукова система Інтернет*.

Містифікація — удавання себе за іншу особу, звичайно у мережній операційній системі або багатокористувацькій прикладній системі з метою одержання *несанкціонованого доступу*.

Модель процесу — формалізований опис *ділового процесу* та *ділових процедур*, що входять до його складу, правил їхнього виконання і ролей учасників процесу.

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

Несанкціонований доступ — доступ до *інформації*, що здійснюється з порушенням встановлених в *інформаційній системі* правил розмежування доступу.

Нюкання — програмна атака на користувача *Інтернет*, у результаті якої його комп'ютер втрачає зв'язок з мережею або «зависає».

Ознака класифікації — властивість або характеристика об'єкта, за якою виконується *класифікація*.

Основа коду — кількість знаків в *алфавіті коду*.

Пара ключів — *публічний ключ* та доповнюючий його *приватний ключ*. У *криптосистемах* з публічними ключами (наприклад, PGP) кожен *користувач* має щонайменше одну пару ключів.

Пароль — секретна послідовність символів або слів, що вводиться *користувачем* у систему для *ідентифікації* або підтвердження виконання певної операції. У процесі створення *пари ключів* (криптографія) пароль у результаті певних математичних операцій перетворюється на випадкову послідовність бітів, з якої складається *ключ*.

Перекодування — присвоєння закодованому *класифікаційному угрупованню* або закодованому об'єкту нового *коду*.

Пертинентність — ступінь відповідності змісту *документа*, знайденого в результаті *інформаційного пошуку*, інформаційній потребі, вираженій в *інформаційному запиті*.

Підписати — накласти *цифровий підпис*.

Підробка інформації — навмисні дії, що призводять до перекручення *інформації*, яка обробляється та зберігається в *інформаційній системі*.

Позамашинна інформаційна база — частина *інформаційної бази*, сукупність сигналів, повідомлень і документів, призначених для безпосереднього сприйняття людиною без застосування засобів обчислювальної техніки. Див. також *машинна інформаційна база*.

Позиція класифікатора — назва і *код класифікаційного угруповання* або об'єкта *класифікації*.

Портал — *Web-сайт*, призначений для специфічної аудиторії, який об'єднує інформаційне наповнення і доставку важливої *інформації*, забезпечує сумісну роботу, надає персоналізований доступ до послуг і додатків.

Порушення роботи інформаційної системи — дії або обставини, які призводять до спотворення процесу оброблення *інформації*.

Порушник інформаційної безпеки — фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо *інформаційної системи* та *інформації* в ній.

Потенціал для вирішення задач (PSP, Problem Solving Potential) — корисність *інформації*, одержаної за допомогою *інформаційно-пошукової системи* (*Інтернет*).

Пошукова система Інтернет — *Web-сервер*, призначений для пошуку ресурсів *Інтернет* за *ключовими словами*, що їх визначає *користувач*. Пошукова система складається з трьох основних частин — *робота*, який збирає дані, бази *індексів* і безпосередньо пошукової си-

стеми, яка здійснює пошук у базі індексів. Див. також *інформаційно-пошукова система, мета-пошукова система*, *каталог*.

Пошукове розпорядження — *інформаційний запит*, викладений *інформаційно-пошуковою мовою* і доповнений допоміжною *інформацією*.

Пошуковий образ документа — короткий опис змісту документа *інформаційно-пошуковою мовою*.

Правило — встановлена залежність значення одного *факту* від значень інших *фактів*.

Правова задача — це ситуація правового характеру, яка потребує виконання певного комплексу дій, що мають на меті знайти такі кількісні та якісні характеристики початкової *інформації* про об'єкт пізнання, які, у свою чергу, дали б змогу здобути нові *знання* про нього і використовувати їх для відшукання істини у виконуваному правовому дослідженні. Див також *задача оброблення даних*.

Правова інформатизація — процес створення оптимальних умов максимально повного задоволення інформаційно-правових потреб органів суду, прокуратури, юстиції, Міністерства внутрішніх справ та інших правоохоронних органів на основі ефективної організації та використання інформаційних ресурсів, а також створення необхідних і достатніх умов для забезпечення *правовою інформацією* органів влади, організацій, суб'єктів господарської діяльності та громадян. Див. також *інформатизація*.

Правова інформація — сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Правове забезпечення — сукупність правових норм, які регламентують правові відносини під час функціонування *інформаційної системи* та юридичний статус результатів такого функціонування;

Правовий режим доступу до інформації — передбачений правовими нормами порядок одержання, використання, поширення і зберігання *інформації*.

Предметна галузь — це сукупність об'єктів, понять, зв'язків, відношень і способів перетворення та взаємодії цих об'єктів під час розв'язування задач, що відносяться до певної сфери людської діяльності (наприклад, юридичної).

Приватний домен — домен *Інтернет*, що адмініструється певною фізичною або юридичною особою у своїх власних інтересах. Див. також *публічний домен*.

Приватний ключ — складова *пари ключів*, яка має зберігатись у секреті одним або всіма учасниками комунікацій. Приватний ключ використовується для створення *цифрових підписів* та дешифрування повідомлень, зашифрованих за допомогою відповідного *публічного ключа*.

Приватність — захист *даних* від *несанкціонованого доступу*, часто шляхом їх *шифрування*.

Прикладна програма — програма, призначена для розв'язання задачі або класу задач у певній галузі застосування систем оброблення даних.

Принт-сервер — активний мережний пристрій (комп'ютер), який дає можливість підмикати кілька принтерів для створення єдиного вузла друку і сортування документів при великому документообігу. До різних портів принт-сервера можна підключати лазерні, матричні, струменеві принтери, копіри. Див. також *сервер*.

Провайдер послуг Інтернет — див. *Інтернет-провайдер*.

Програмний агент — програма, розміщена у певному середовищі і здатна до гнучкої автономної поведінки для досягнення визначеної мети.

Проксі-сервер (proxy-server) — проміжний комп'ютер — посередник між комп'ютером користувача та *Інтернет*, через який проходять всі звернення та результати їх оброблення. Проксі-сервер прискорює роботу в Інтернет, забезпечує анонімність користувачів та інші функції. Див. також *сервер*.

Протокол — сукупність правил (визначень, домовленостей), які регламентують формат і процедури комунікації двох або більшої кількості незалежних пристроїв чи процесів.

Публічний домен — домен *Інтернет*, що адмініструється в інтересах певної спільноти (див., наприклад, *українська Інтернет-спільнота*). Див. також *приватний домен*.

Публічний ключ — один із *пари ключів*, який вільно надається кореспондентам і використовується для *шифрування* і *верифікації* цифрових підписів. Знання публічного ключа не дає змоги розкрити пов'язаний із ним *приватний ключ*.

Реєстрант — особа, що бажає користуватися та розпоряджатися певним *доменним іменем* у *публічному домені*.

Реєстратор — зареєстрований в Україні суб'єкт підприємницької діяльності, який надає *реєстрантові* послуги, необхідні для технічного забезпечення делегування і функціонування *доменного імені*.

Реєстрація класифікатора — присвоєння затвердженому *класифікатору* реєстраційного номера і запис необхідних відомостей до реєстру.

Резервна ємність класифікатора — кількість вільних *позицій* у *класифікаторі*. Див. також *ємність класифікатора*.

Релевантність — ступінь відповідності змісту документа, знайденого в результаті *інформаційного пошуку*, змісту *інформаційного запиту*.

Робот — програма, яка автоматично простежує гіпертекстові сторінки, просуваючись між ними за наявними *гіперпосиланнями*.

Робот-індексувальник — див. *робот*.

Розряд коду — позиція знака в *коді*.

Сайт (site) — див. *Web-сайт*.

Своєчасність — властивість *інформаційної системи*, яка характеризує можливість отримання апаратом керівництва необхідної інформації.

Сеансовий ключ — *секретний ключ* (симетричний), що використовується під час окремої операції. Для кожної окремої сесії комунікацій використовується специфічний сеансовий ключ.

Секретний ключ — див. *приватний ключ*.

Секретний поділ ключів (secret sharing) — див. *дроблення ключів*.

Сервер — комп'ютер, що надає послуги іншим комп'ютерам у мережі, які називаються клієнтськими. Див. також *принт-сервер*, *проксі-сервер*, *сервер баз даних*, *сервер голосування*, *сервер ключів*, *файл-сервер*, *клієнт-серверна технологія, Web-сервер*.

Сервер баз даних — *сервер*, призначений для управління єдиною *базою даних*, управління доступом до неї багатьох користувачів, її захисту за допомогою засобів відновлення та створення резервних копій, контролю дотримання правил глобальної *цілісності даних*.

Сервер голосування — *сервер* на виборчій дільниці, який одержує і зберігає бюлетені, передані клієнтами через *Інтернет*, під час Інтернет-голосування.

Сервер каталогів (directory server) — див. *сервер ключів*.

Сервер ключів (key server) — сервер, який дає змогу *користувачам* вносити *публічні ключі* та *цифрові сертифікати* у відповідну базу та одержувати їх з неї. Деякі сервери ключів також надають певні адміністративні послуги із забезпечення політики безпеки. Див. також *сервер*.

Сервер сертифікатів — див. *сервер ключів*.

Сертифікат — див. *цифровий сертифікат*.

Сертифікат авторизації — електронний *документ*, який доводить права доступу або привілеї *користувача*, а також те, що він (вона) є особою, якою себе називає. Див. також *цифровий сертифікат*.

Сертифікація — (криптографія) створення *цифрового сертифіката*, накладання *цифрового підпису* на чийсь *публічний ключ*.

Симетричне шифрування — див. *криптографія з симетричними ключами.*

Система автоматизації ділових процесів (САДП, система автоматизації управління потоками робіт, workflow-система, Workflow Management System) — *інформаційна система*, призначена для опису та забезпечення виконання багатокрокових процесів управління (*ділових процесів*).

Система керування базою даних — комплекс програмних і мовних засобів загального і спеціального призначення, необхідних для створення *бази даних*, підтримки її в актуальному стані, маніпулювання *даними* й організації доступу до них різних *користувачів* чи прикладних програм в умовах чинної технології оброблення *інформації*.

Система керування (електронними) документами (Electronic/Enterprise Document Management System) — *інформаційна система*, призначена для автоматизації *діловодства* (включаючи *документообіг*) та інших функцій з управління документами.

Система класифікації — сукупність методів і правил *класифікації* та її результат.

Система на основі знань — інтелектуальна *інформаційна система*, в якій *знання* про *предметну галузь* подані в явному вигляді і відокремлені від інших знань системи. Див. також *дорадча система*, *експертна система*.

Система оперативного аналізу даних — див. *OLAP-система*.

Система організації групової роботи — див. *групове забезпечення*.

Система підтримки прийняття рішень (СППР, Decision Support System) — інтерактивна комп'ютерна система, призначена для підтримки різних видів діяльності в разі прийняття рішень зі слабкоструктурованих або неструктурованих проблем.

Сліпий підпис — *цифровий підпис*, що накладається особою («цифровим нотаріусом»), якій невідомий зміст повідомлення.

Словникова атака — атака з метою розкриття *пароля* шляхом перебору очевидних і логічних комбінацій слів.

Спайдер (spider) — див. *робот*.

Спам — масова розсилка повідомлень за допомогою *електронної пошти* та інших засобів персонального обміну *інформацією* (включаючи служби миттєвої доставки повідомлень типу SMS, IRC і т. п.), що здійснюється без явно та недвозначно вираженої ініціативи одержувачів.

Спаммер — особа, яка здійснює відправлення *спаму*, незалежно від того, чи робить вона це у власних інтересах або в інтересах інших осіб.

Спеціальна мережа зв'язку — див. *мережа спеціального зв'язку*.

Спеціальна мережа зв'язку подвійного призначення — *спеціальна мережа зв'язку*, призначена для забезпечення зв'язку в інтересах органів державної влади та органів місцевого самоврядування, з використанням частини її ресурсу для надання послуг іншим споживачам.

Список розсилки — варіант організації *електронної пошти* «одне джерело — багато одержувачів», коли повідомлення розсилаються всім зацікавленим особам за заздалегідь визначеним списком.

Спонсор домену Інтернет — організація, яка представляє спільноту, найбільш зацікавлену у цьому домені, і якій делеговано повноваження з формулювання політики функціонування домену.

Стеганографія — метод захисту *інформації*, який полягає у приховуванні повідомлень в аудіо- та відеофайлах, а також файлах з оцифрованими зображеннями.

Структура коду — умовне позначення складу та послідовності розміщення знаків у *коді*.

Ступінь класифікації — 1. етап *класифікації* при ієрархічному методі, у результаті якого формується сукупність *класифікаційних угруповань*; **2.** результат чергового поділу об'єктів одного *класифікаційного угруповання*.

Суб-ключ (sub key) — *ключ*, створений за алгоритмом Diffie-Hellman, який додається як підмножина до головного ключа. Для суб-ключа можна встановлювати строк використання, анулювати його незалежно від головного ключа або підписів, зібраних на нього.

Сховище даних (Data Warehouse) — особлива форма організації *бази даних*, призначена для зберігання у погодженому вигляді агрегованої *інформації*, що одержується з баз даних різних *OLTP-систем* та зовнішніх джерел. Характеристиками сховища даних є предметна орієнтація, інтегрованість, підтримка хронології, незмінність, мінімальна надмірність, захищеність.

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

Тезаурус — див. *інформаційно-пошуковий тезаурус*.

Теледемократія (teledemocracy) — використання телекомунікаційних технологій для більшого залучення громадян у політичні процеси на основі поліпшення передачі політичної інформації та думок між громадянами, політиками і виконавчою владою.

Телекомунікації (від грец. «tele» — «далеко» та «communico» — «спілкуюся») — здатність передавати текст, голос, зображення і навіть нематеріальні активи (грошові кошти) через *мережі* разом із функціональною інформацією, призначеною для управління комп'ютерними системами.

Термінальний факт — (ЕС) *дані*, які невідомі експерту (він не може вивести їх самостійно) і можуть бути повідомлені тільки *користувачем* або одержані із зовнішньої *бази даних*. Див. також *факт, що виводиться*.

Топологія мережі — конфігурація з'єднання елементів *комп'ютерної мережі*.

Транслітерація — система запису літер однієї писемності за допомогою літер іншої писемності.

Трафік — інтенсивність потоку повідомлень у мережі передачі даних.

Троянськй кінь — програма з небажаною поведінкою, яка функціонує секретно, без зовнішніх проявів, або частина більшої, корисної програми, яка при збереженні працездатності останньої виконує додаткові, не задокументовані функції.

Українська Інтернет-спільнота — спільнота всіх громадян та/або резидентів України, фізичних та юридичних осіб, органів державної влади та управління України, органів місцевого самоврядування, які використовують мережу *Інтернет* та Інтернет-технології незалежно від мети та способів такого використання.

Управління ключами — (криптографія) процес і процедури генерування, безпечного зберігання, встановлення справжності та надання правильних *ключів* авторизованим користувачам.

Файл-сервер — центральний вузол *мережі*, на якому зберігаються файли *даних*, доступні всім *користувачам*. Див також *сервер*.

Факт — (ЕС) інформаційна сутність про певну частину світу, яка має назву, множину можливих значень або значення, що обчислюється, і контекст. У контексті створення і використання ЕС важливою властивістю фактів є можливість поставити щодо них питання або висловити твердження. Див. також *термінальний факт, факт, що виводиться, головний факт консультації, головний факт правила, хвостовий факт правила.*

Факт, що виводиться — (ЕС) *факт*, значення якого залежить від значень інших фактів (*термінальних фактів* або *фактів, що виводяться*) і виводиться шляхом застосування *правил* даної ЕС.

Функціональна надійність — властивість *інформаційної системи* зберігати у часі в установлених межах значення усіх параметрів, які характеризують здатність системи виконувати потрібні *функції* у заданому режимі та умовах експлуатації. Цей показник якості функціонування інформаційної системи пов'язаний з такими її властивостями, як *відмовостійкість*, ремонтопридатність, довговічність.

Функціональна повнота — властивість *інформаційної системи*, яка характеризує рівень автоматизації управлінських робіт.

Функція — сукупність дій *інформаційної системи*, спрямованих на досягнення зазначеної мети. Перелік функцій конкретної інформаційної системи залежить від сфери її діяльності, об'єкта управління, призначення та ін.

Хвостовий факт правила — (ЕС) *факт*(-и), які стоять після логічної зв'язки «якщо» у логічній формі «Якщо… то…». Див. також *головний факт правила*.

Хостинг — послуги з розміщення сайта у *World-Wide Web*.

Цифровий водяний знак — псевдовипадкова послідовність шумових сигналів, згенерованих на основі секретних ключів, що заноситься за допомогою спеціального програмного забезпечення у певні файли з метою забезпечення автентичності або недоторканності *документа*, *ідентифікації* автора або власника, перевірки прав дистриб'ютора або *користувача*. Створення цифрових водяних знаків є одним із застосувань комп'ютерної *стеганографії*.

Цифровий підпис (ЦП) — унікальна сукупність *даних*, що створюється на основі *секретного ключа*, додається до *електронного документа* і дає змогу підтвердити його *цілісність* та ідентифікувати особу, що його підписала, під час *автентифікації*.

Цифровий сертифікат — (криптографія) *електронний документ*, який додається до *публічного ключа довіреною третьою особою* і доводить, що публічний ключ належить легітимному власнику і не скомпрометований. Сертифікат складається із сертифікуючої інформації (*ідентифікатор* і ім'я *користувача* тощо) та одного або кількох *цифрових підписів*. Див. також *сертифікат авторизації*.

Цілісність даних — характеристика *даних*, яка означає, що дані зберігаються для використання згідно з призначенням, захищені від прихованої модифікації неавторизованими персонами (невідомими засобами), передаються та приймаються без змін і купюр. Цілісність даних звичайно забезпечується *шифруванням* та/або накладанням *цифрового підпису*.

Часова бомба — різновид *логічної бомби*, який спрацьовує у певний момент часу.

Шифрування — перетворення за допомогою математичних операцій відкритого тексту на нечитабельний (зашифрований), який можна прочитати тільки за допомогою *приватного ключа*. Див. також *криптографія*, *криптографія з симетричними ключами*, *криптографія з асиметричними ключами*.

Шифрування з єдиним (секретним) ключем — див. *криптографія з симетричними ключами*.

Шифрування з публічним ключем — див. *криптографія з асиметричними ключами*.

CAST — алгоритм *симетричного шифрування*, розроблений у Канаді Карлайлом Адамсом і Саффордом Таваресом (Carlisle Adams, Stafford Tavares). Оперує 64-бітовими блоками тексту (шифру) з використанням 128-бітових ключів.

Data Mining — див. *дейтамайнінг*.

DEA (Data Encryption Algorithm, алгоритм шифрування даних) — див. *DES*.

DES (Data Encryption Standard, стандарт шифрування даних) — алгоритм *симетричного шифрування*, розроблений фірмою IBM і прийнятий у 1976 році як *FIPS 46*, також відомий як стандарт ANSI DEA та стандарт ISO DEA-1. Оперує 64-бітовими блоками тексту (шифру) з використанням 56-бітових ключів.

Diffie-Hellman — перший алгоритм *асиметричного шифрування* з використанням дискретних алгоритмів у скінченному полі, розроблений у 1976 році і названий за прізвищами авторів — Уітфілда Діффі та Мартіна Хеллмана (Whitfield Diffie, Martin Hellman).

DSA (Digital Signature Algorithm, алгоритм цифрового підпису) — алгоритм *асиметричного шифрування*, запропонований NIST для використання в *DSS*.

DSS (Digital Signature Standard, стандарт цифрового підпису) — стандарт, запропонований NIST для створення *цифрових підписів* на основі алгоритму *DSA*.

FIPS (Federal Information Processing Standard, федеральний стандарт оброблення інформації) — урядовий стандарт США, опублікований NIST.

FTP (File Transfer Protocol, протокол передачі файлів) — протокол, який визначає правила передачі файлів (а також цілих каталогів із вкладеними каталогами і файлами) з одного комп'ютера на інший; назва програми з відповідним призначенням.

HTML (Hypertext Markup Language, мова розмітки *гіпертексту*) — нотація, що використовується для форматування тексту і мультимедійного наповнення *Web-сторінок*.

HTTP (HyperText Transfer Protocol) — базовий протокол пересилання *гіпертекстів* (пересилання *Web-сторінок* між Web-*броузером* і *Web-сервером* в *Інтернет*).

IDEA (International Data Encryption Standard, міжнародний стандарт шифрування даних) — алгоритм *симетричного шифрування* з 128-бітовими ключами та опрацюванням 64-бітових блоків тексту (шифру) на основі змішаних операцій різних алгебраїчних груп. Вважається одним з найпотужніших алгоритмів. Розроблений у Цюріху Джеймсом Мессі (James L. Massey) та Ксуейя Лей (Xuejia Lai). Опублікований у 1990 році Початкова назва — IPEA (Improved Proposed Encryption Standard).

IP (Internet Protocol, протокол Інтернет) — базовий протокол обміну пакетами в *Інтернет*, який лежить в основі інших протоколів Інтернет, зокрема, *HTTP*.

IP-адреса — унікальна числова послідовність, що присвоюється кожному комп'ютеру *Інтернет*, включаючи домашні комп'ютери з тимчасовим підімкненням.

OLAP-система (On-line Analytical Processing, оперативне аналітичне оброблення) — система швидкого аналізу розподіленої багатовимірної *інформації*. OLAP-системи розглядають як різновид *систем підтримки прийняття рішень*.

OLTP-система (On-line Transaction Processing, оперативне оброблення транзакцій) — звичайна управлінська *інформаційна система*, яка не має характеристик *OLAP-систем*.

RSA — алгоритм *асиметричного шифрування*, оснований на факті, що легко перемножити два великі прості числа, але важко розкласти результат на множники. Назва алгоритму походить від прізвищ його авторів — Рона Рівеста, Аді Шаміра та Лена Ейдлмана (Ron Rivest, Adi Shamir, Len Adleman), засновників RSA Data Security, Inc. (нині — RSA Security).

TCP (Transport Control Protocol) — *протокол* управління передаванням *даних* у *мережі* у вигляді пакетів, працює поверх протоколу IP.

TCP/IP — сімейство *протоколів* передавання *даних*, основними з яких є *TCP* та *IP*.

Telnet — *протокол* і програма одержання послуг віддаленого доступу.

Triple DES (потрійний DES) — метод *симетричного шифрування*, під час якого алгоритм *DES* застосовується тричі з трьома різними *ключами* розміром 168 бітів.

Twofish — новітній алгоритм *симетричного шифрування* з опрацюванням 256-бітових блоків тексту (шифру), створений Брюсом Шнейєром (Bruce Schneier). Є одним з п'яти кінцевих алгоритмів проекту AES (Удосконаленого стандарту шифрування) NIST.

URL (Uniform Resource Locator, універсальний покажчик ресурсів) — стандартний формат задання адрес і ресурсів мережі *Інтернет*, що належать до *World-Wide Web*.

Web-сайт — комплекс пов'язаних за темою *Web-сторінок*, як правило, розміщених на одному *Web-сервері* і доступних з однієї, *домашньої сторінки*.

Web-сервер — комп'ютер, який підімкнений до *Інтернет*, має *IP-адресу*, зберігає *Web-сторінки* та інші файли і надає їх *користувачам* у відповідь на запити.

Web-сторінка — одиниця зберігання *гіпертексту* у *World Wide Web*, електронний документ, який підготовлено за допомогою мови розмітки гіпертексту *HTML* і містить текст, службову *інформацію*, графічні блоки, *гіперпосилання* на інші Web-сторінки або *Web-сайти*, можливо, елементи програмного коду, зокрема, мовою Java.

World-Wide Web (WWW, Web, W3) — всесвітня система організації мультимедіа та гіпертекстової інформації, один із найпопулярніших сервісів *Інтернет*.

9. СПИСОК ВИКОРИСТОВУВАНИХ СКОРОЧЕНЬ

АБД — автоматизований банк даних
АРМ — автоматизоване робоче місце
АС — автоматизована система
АСУ — автоматизована система управління
АСУ ТП — автоматизована система управління технологічними процесами
БД — база даних
БЗ — база знань
ГІС — географічна інформаційна (геоінформаційна) система
ЕК — електронна комерція
ЕОМ — електронна обчислювальна машина
ЕЦП — електронний цифровий підпис
ЕС — експертна система
ЄДАПСУ — Єдина державна автоматизована паспортна система України
ІЗ — інформаційне забезпечення
ІПС — інформаційно-пошукова система
ІС — інформаційна система
ІТ — інформаційна технологія
КІС — корпоративна інформаційна система
ЛОМ — локальна обчислювальна мережа
МВСУ — Міністерство внутрішніх справ України
НІТ — нова інформаційна технологія
ОС — операційна система
ПЗ — програмне забезпечення
ППП — пакет прикладних програм
РКК — реєстраційно-контрольна картка
САПР — система автоматизації проектування
СКБД — система керування базою даних

СППР — система підтримки прийняття рішень
ЦП — цифровий підпис
ANSI — American National Standards Institute — Американський інститут національних стандартів
ARPAnet — Advanced Research Projects Agency Network — мережа Агентства перспективних досліджень
CENTR — Council of European National Top level domain Registries — Рада європейських національних регістрів верхнього рівня
CORE — Council of Registrars — Рада Інтернет-регістраторів
DEA — Data Encryption Algorithm — алгоритм шифрування даних
DES — Data Encryption Standard — стандарт шифрування даних
DNS — Domain Name System — служба доменних імен
DSA — Digital Signature Algorithm — алгоритм цифрового підпису
DSS — 1. Decision Support System — система підтримки прийняття рішень
2. Digital Signature Standard — стандарт цифрового підпису.
EARN — European Academic and Research Network — Європейська академічна та дослідницька мережа
ECLAC — European Commission Libraries Catalogue — Каталог бібліотек Європейської Комісії
ECMA — European Computer Manufactures Association — Європейська асоціація виробників комп'ютерів
e-mail — electronic mail — електронна пошта
FAQ — Frequently Asked Questions — питання, що часто задаються
FIPS — Federal Information Processing Standard — федеральний стандарт оброблення інформації
FTP — File Transfer Protocol — протокол передачі файлів
GIS — Geographic Information System — географічна інформаційна (геоінформаційна) система
GLIN — Global Legal Information Network — Глобальна мережа правової інформації
Groupware — групове забезпечення
gTLD-MoU — The Generic Top Level Domain Memorandum of Understanding — Меморандум розуміння щодо gTLD
gTLDs — generic Top Level Domains — описові імена родових доменів

HTML — Hypertext Markup Language — мова розмітки гіпертексту
HTTP — HyperText Transfer Protocol — протокол пересилки гіпертексту
IAB — Internet Architecture Board — Рада з архітектури Інтернет
IAHC — International Ad Hoc Committee — Міжнародний спеціальний комітет
IANA — Internet Assigned Numbers Authority — Адміністрація адресного простору Інтернет
ICANN — The Internet Corporation for Assigned Names and Numbers — Інтернет-корпорація з присвоєння імен і номерів
IDEA — International Data Encryption Standard — міжнародний стандарт шифрування даних
IEEE — Institute of Electronic and Electrical Engineers — Інститут інженерів з електроніки і радіоелектроніки
IETF — Internet Engineering Task Force — Цільова група з інжинірингу в Інтернет
INTA — International Trademark Association — Міжнародна організація з торгових марок
IP — Internet Protocol — протокол Інтернет
ISO — International Organization for Standardization — Міжнародна організація зі стандартизації
ISOC — Internet SOCiety — Всесвітнє Співтовариство Інтернет
ISP — Internet Service Provider — Інтернет-провайдер
ITU — International Telecommunication Union — Міжнародний союз з телекомунікацій
NIST — National Institute of Standards and Technology — Національний інститут стандартів і технології США
OLAP — On-line Analytical Processing — оперативне аналітичне оброблення
OLTP — On-line Transaction Processing — оперативне оброблення транзакцій
OSI — Open System Interconnection — модель взаємодії відкритих систем
PKI — Public Key Infrastructure — інфраструктура публічних ключів
RARE — Reseaux Associees pour la Recherche Europeene — Європейське об’єднання дослідників
RFC — Request for Comments — запит коментарів
RIPE NCC — The RIPE Network Coordination Centre — Мережний Координаційний Центр RIPE

TCP — Transmission Control Protocol — протокол управління передаванням даних

TERENA — Trans-European Research and Education Networking Association — Транс-європейська мережна асоціація в галузі досліджень та освіти

TLDs — Top Level Domains — домени верхнього рівня

URL — Uniform Resource Locator — універсальний покажчик ресурсів

VPN — Virtual Private Network — віртуальна приватна мережа

WIPO — World Intellectual Property Organization — Всесвітня організація з охорони інтелектуальної власності

WWW — World-Wide Web — Всесвітня павутина

ЛІТЕРАТУРА

Основна

1. *Денісова О. О*. Інформаційні системи і технології в юридичній діяльності. — К.: КНЕУ, 2003. — 315 с.
2. *Ситник В. Ф*. та ін. Основи інформаційних систем. — К.: КНЕУ, 2001. — 420 с.

Додаткова

1. *Береза А. М*. Основи створення інформаційних систем. — К.: КНЕУ, 2001. — 214 с.
2. *Гаврилов О. А*. Основы правовой информатики. — М.: Академ. правовой ун-т при Ин-те государства и права РАН, 1998. — 42 с.
3. *Горьовий Л. Є*. та ін. Комп'ютеризована система інформаційно-аналітичного забезпечення законотворчої та правозастосовної діяльності. — К.: Парлам. вид-во, 1998. — 149 с.
4. ДСТУ 2394-94. Інформація та документація. Базові поняття. Терміни та визначення. — К.: Держстандарт України, 1994. — 53 с.
5. ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення. — К.: Держстандарт України, 1994. — 55 с.
6. ДСТУ 2429-94. Система «людина — машина». Ергономічні та техніко-естетичні вимоги. Терміни та визначення. — К.: Держстандарт України, 1994. — 35 с.
7. ДСТУ 2481-94. Системи оброблення інформації. Інтелектуальні інформаційні технології. Терміни та визначення. — К.: Держстандарт України, 1994. — 72 с.
8. ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни і визначення. — К.: Держстандарт України, 1994. — 55 с.
9. *Єрьоміна Н. В*. Проектування баз даних. — К.: КНЕУ, 1999. — 214 с.
10. Информационно-поисковый тезаурус. Русская версия тезауруса EUROVOC. Т. 1: Тематическое представление / Федер. собр. — Парламент РФ. Гос. Дума; [Науч. ред. и сост. Т. А. Москаленко]. — М.: Изд. Гос. Думы, 2001. — 500 с.

11. Информационно-поисковый тезаурус. Русская версия тезауруса EUROVOC. Т. 2: Тематическое представление / Федер. собр. — Парламент РФ. Гос. Дума; Парлам. б-ка; [Науч. ред. и сост. Т. А. Москаленко]. — М.: Изд. Гос. Думы, 2001. — 180 с.

12. Информационно-поисковый тезаурус. Русская версия тезауруса EUROVOC. Т. 3: Многоязычное представление / Федер. собр. — Парламент РФ. Гос. Дума; Парлам. б-ка; [Науч. ред. и сост. Т. А. Москаленко]. — М.: Изд. Гос. Думы, 2001. — 126 с.

13. *Кісельов М.* Про створення єдиної інформаційної системи органів юстиції України // Право України. — 1997. — № 3.

14. Компьютерные технологии в юридической деятельности: Учеб. и практ. пособ.: Под. ред. проф. Н. Полевого, канд. юрид. наук В. Крылова. — М.: БЕК, 1994. — 304 с.

15. Компьютерные юридические системы: принципы реализации, технология использования, направления развития. — К.: КИТ, 1992. — 55 с.

16. *Саницький В. А., Карацюба А. М., Святобог В. В.* та ін. Система інформаційного забезпечення ОВС України: Навч.-практ. посіб. — К.: Ред.-вид. відділ МВС України: ТОВ АНТЕКС, 2000. — 144 с.

17. *Ситник В. Ф.* Системи підтримки прийняття рішень. — К.: КНЕУ, 2004.