

Лекція 1 Основні терміни та визначення

Слово «інформація» походить від латинського слова *informatio*, що в перекладі означає зведення, роз'яснення, ознайомлення. Поняття інформації розглядалося ще античними філософами. До початку промислової революції, визначення суті інформації залишалося прерогативою переважно філософів. Далі розглядати питання теорії інформації стала нова на той час наука кібернетика.

Визначення інформації. Інформація – це поняття, пов'язане з об'єктивною властивістю матеріальних об'єктів і явищ (процесів) породжувати різноманітні стани, які за допомогою взаємодій (фундаментальні взаємодії) передаються іншим об'єктам та відображаються в їх структурі. В повсякденній діяльності інформація – це відомості про навколишній світ, що сприймаються людиною або спеціальним пристроєм. На даний час не існує єдиного визначення терміна інформація. В різних галузях знання дане поняття описується своїм специфічним набором ознак.

Загальне поняття інформації подано у філософії, де під нею розуміють відображення реального світу. Як філософську категорію її розглядають як один з атрибутів матерії, що відбиває її структуру.

Погляд на інформацію з точки зору її споживачів окреслює таке поняття: Інформація — це нові відомості, які прийняті, зрозумілі і оцінені її користувачем як корисні. Іншими словами, інформація — це нові знання, які отримує споживач (суб'єкт) у результаті сприйняття і переробки певних відомостей. Інформація – це відомості, повідомлення, знання, дані, які є об'єктом збирання, зберігання, переробки та передачі з метою зменшення невизначеності в тій галузі, до якої вони відносяться, і вирішення поставлених задач.

Цінність інформації визначається корисністю та здатністю її забезпечити суб'єкта необхідними умовами для досягнення ним поставленої мети.

Достовірність — здатність інформації об'єктивно відображати процеси та явища, що відбуваються в навколишньому світі. Як правило достовірною вважається насамперед інформація, яка несе у собі безпомилкові та істинні дані. Під безпомилковістю слід розуміти дані які не мають, прихованих або випадкових помилок. Випадкові помилки в даних обумовлені, як правило, неумисними спотвореннями змісту людиною чи збоями технічних засобів при переробці даних в інформаційній системі. Тоді як під істинними слід розуміти дані зміст яких неможливо оскаржити або заперечити.

Актуальність — здатність інформації відповідати вимогам сьогодення (поточного часу або певного часового періоду).

Часові властивості

Часові властивості визначають здатність даних передавати динаміку зміни ситуації (динамічність). При цьому можна розглядати або час запізнення появи в даних відповідних ознак об'єктів, або розходження реальних ознак об'єкта і тих же ознак, що передаються даними. Відповідно можна виділити:

Актуальність — властивість даних, що характеризує поточну ситуацію;

Оперативність — властивість даних, яка полягає в тому, що час їхнього збору та переробки відповідає динаміці зміни ситуації;

Ідентичність — властивість даних відповідати стану об'єкта.

Властивість недоступності

При розгляді захищеності даних можна виділити технічні аспекти захисту даних від несанкціонованого доступу та соціально-психологічні аспекти класифікації даних за мірою їхньої конфіденційності та секретності (властивість конфіденційності).

Інші властивості інформації

Суспільна природа — джерелом інформації є пізнавальна діяльність людей, суспільства.

Мовна природа — інформація виражається за допомогою мови — знакової системи будь-якої природи, яка служить засобом спілкування, мислення, висловлювання думки. Мова може бути природною, що використовується у повсякденному житті та служить формою висловлення думок і засобом спілкування між людьми, а також штучною, створеною людьми з певною метою (наприклад, мова математичної символіки, інформаційно-пошукова, алгоритмічна та ін. мови).

Невідривність від мови носія

Дискретність — одиницями інформації як засобами висловлювання є слова, речення, уривки тексту, а у плані змісту — поняття, висловлювання, описання фактів, гіпотези, теорії, закони тощо.

Незалежність від творців

Старіння — головною причиною старіння інформації є не сам час, а поява нової інформації, з надходженням якої попередня інформація виявляється невірною, перестає адекватно передавати явища та закономірності матеріального світу, людського спілкування та мислення.

Розсіювання — існування у багатьох джерелах.

Види інформації:

За суспільним значенням: наукова, виробнича, управлінська, технічна, масового подання, повсякденна, суспільно-політична;

За способами сприйняття: візуальна, аудіальна, тактильна, нюхова, смакова.

За формами подання: текстова, числова, графічна, комбінована, естетична.

Властивості інформації, що захищається:

- конфіденційність (доступ до інформації обмежено за бажанням відповідної особи, крім суб'єктів владних повноважень);
- цілісність (відсутність зловмисних модифікувань інформації);
- доступність (спроможність доступу до інформації в межах відповідних повноважень).

Становлення мережі інтернет

У 1969 році Міністерство оборони США започаткувало розробку проекту, котрий мав на меті створення надійної системи передачі інформації на випадок війни. Агентство передових досліджень США (англ. ARPA) запропонувало розробити для цього комп'ютерну мережу. Її розробка була доручена Каліфорнійському університетові Лос-Анджелеса, Стенфордському дослідному центрові, Університету штату Юта та Університету штату Каліфорнія в Санта-Барбарі.

Ця мережа була названа ARPANET (англ. Advanced ResearchProjectsAgency Network — Мережа Агентства передових досліджень). В рамках проекту мережа об'єднала названі заклади; всі роботи по її створенню фінансувались за рахунок Міністерства оборони США. Потім мережа ARPANET почала активно рости й розвиватись; її дедалі ширше почали використовувати вчені із різних галузей науки.

Перший сервер ARPANET було встановлено 1 вересня 1969 року у Каліфорнійському університеті в Лос-Анджелесі. Комп'ютер «Honeywell 516» мав 12 кілобайт оперативної пам'яті.

До 1971 року була розроблена перша програма для відправки електронної пошти по мережі, котра відразу стала дуже популярною.

У 1973 році до мережі через трансатлантичний кабель були підключені перші іноземні організації з Великобританії та Норвегії; мережа стала міжнародною.

У 1970-х роках мережа в основному використовувалась для пересилки електронної пошти, тоді ж появились перші списки поштових розсилок, групи новин та дошки оголошень. Але в ті часи мережа ще не могла легко взаємодіяти з іншими мережами, котрі були побудовані на інших технічних стандартах. До кінця 1970-х років почали активно розвиватись протоколи передачі даних, що були стандартизовані у 1982—1983 роках.

1 січня 1983 року мережа ARPANET перейшла з протоколу NCP на протокол TCP/IP, який досі успішно використовується для об'єднання мереж.

Розвиток

Саме у 1983 році за мережею ARPANET закріпився термін «Інтернет».

У 1984 році була розроблена система доменних назв (англ. DomainNameSystem, DNS). Тоді ж у мережі ARPANET появився серйозний суперник — Національний науковий фонд США (NSF) заснував міжуніверситетську мережу NSFNet (англ. NationalScienceFoundationNetwork), котра була сформована з дрібніших мереж, включаючи відомі на той час Usenet та Bitnet і мала значно більшу пропускну здатність, аніж ARPANET. До цієї мережі за рік під'єдналось близько 10 тисяч комп'ютерів; звання «Інтернет» почало плавно переходити до NSFNet.

У 1988 році було винайдено протокол Internet RelayChat (IRC), завдяки якому в Інтернеті стало можливим спілкування в реальному часі (чат).

У 1989 році в Європі, в стінах Європейського центру ядерних досліджень (франц. ConseilEuropéenpourlaRechercheNucléaire, CERN) народилась концепція тенет. Її запропонував знаменитий британський вчений Тім Бернерс-Лі, він же протягом двох років розробляв протокол HTTP, мову гіпертекстової розмітки HTML та ідентифікатори URI.

У 1990 році мережа ARPANET припинила своє існування, програвши конкуренцію NSFNet. Тоді ж було зафіксовано перше підключення до Інтернету по телефонній лінії (т. зв. «дозвонювання» англ. Dial-up access).

У 1991 році тенета стали доступні в Інтернеті, а в 1993 році появився знаменитий Веб-браузер (англ. web-browser) NCSA Mosaic. Всесвітня павутина ставала дедалі популярнішою.

Розповсюдження

У 1995 році NSFNet повернулась до ролі дослідницької мережі; маршрутизацією всього трафіку Інтернету тепер займались мережеві провайдери(постачальники послуг), а не суперкомп'ютери Національного наукового фонду.

В тому ж році тенета стали основним постачальником інформації в Інтернеті, обігнавши по об'єму трафіку протокол передачі файлів FTP; було сформовано Консорціум всесвітньої павутини (англ. WWW Consorcium, W3C). Можна сказати, що тенета перетворили Інтернет і створили його сучасний вигляд. З 1996 року Всесвітнє павутиння майже повністю підмінило собою поняття «Інтернет».

Протягом 1990-х років Інтернет об'єднав у собі більшість існуючих на той час мереж (хоча деякі, як, наприклад, Фідонет, залишились відособленими). Завдяки відсутності єдиного керуючого центру, а також

завдяки відкритості технічних стандартів Інтернету, що автоматично робило мережі незалежними від бізнесу чи уряду, об'єднання виглядало неймовірно привабливим. До 1997 року в Інтернеті нараховувалось близько 10 мільйонів комп'ютерів і було зареєстровано більше мільйона доменних назв. Інтернет став дуже популярним засобом обміну інформацією.

Виділяються чотири основних сервіса Інтернету.

Електронна пошта — найбільш простий, корисний і доступний для багатьох користувачів сервіс Інтернету.

Передача файлів з одного комп'ютера до іншого — одне з найбільших комфортних нововведень, що були надані революцією в мережі. Воно ґрунтується на протоколі передачі файлів FTP (FileTransferProtocol).

Віддалений доступ надає можливість підключитися до віддаленого комп'ютера і працювати з ним в інтерактивному режимі. За допомогою протоколу TELNET, що забезпечує такий доступ, можна користуватися бібліотеками, каталогами різних університетів або організацій і т. п. Віддалений комп'ютер буде виконувати команди, а особистий — працювати як простий термінал.

WWW (WORLD WIDE WEB або всесвітня павутина) — сервіс Інтернету, що ґрунтується на гіпертекстовій технології², розроблений в Європейському центрі ядерних досліджень (CERN).

Зараз спостерігається швидкий розвиток і розширення спектру послуг Інтернету. З'являються і швидко поширюються нові інформаційні джерела — електронні газети, електронні мультимедійні журнали, що розмовляють, щотижневі радіопередачі, що транслюються через Інтернет, відео-конференції та інші.

В Інтернеті базовим протоколом є протокол TCP/IP (Transmission Control Protocol/Internet Protocol). IP відповідає за доставку повідомлень за необхідною адресою. Ці протоколи були запропоновані в 1974 році Робертом Кеном, одним з основних розроблювачів ARPANET, і вченим-комп'ютерщиком Віктором Серфом. Необхідно мати на увазі, що TCP/IP не являється єдиним протоколом, що дозволяє з'єднувати різні мережі. Інтернет є багатопроTOCOLною мережею, що інтегрує й інші стандарти. Основні серед них — стандарти взаємодії відкритих систем (OSI). Запропоновані Міжнародною організацією стандартизації (ISO) протоколи OSI одержали широке поширення в Європі, де не так сильно, як у США, відчувався вплив TCP/IP. Системи, що засновані на інших протоколах, також підключаються

до Інтернет через шлюзи. Наприклад, BITNET — це мережа, що для передачі даних використовує особливі стандарти, але частково, вона доступна через шлюзи Інтернет.

Іншими словами, визначити Інтернет можна як взаємозв'язок мереж, що базується на єдиному комунікаційному протоколі — TCP/IP.

Модель OSI — абстрактна мережева модель для комунікацій і розробки мережевих протоколів. Представляє рівневий підхід до мережі. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережевого обладнання й програмного забезпечення стає набагато простішою, прозорішою й зрозумілішою.

На даний час основним використовуваним стеком протоколів є TCP/IP, розробка якого не була пов'язана з моделлю OSI і до того ж була здійснена до її прийняття. За увесь час існування моделі OSI вона не була реалізована, і, очевидно, не буде реалізована ніколи. Сьогодні використовується тільки деяка підмножина моделі OSI. Вважається, що модель занадто складна, а її реалізація займе занадто багато часу.

Таблиця 1 – Рівні моделі OSI

Модель OSI				
Уровень (layer)		Тип данных (PDU ^[1])	Функции	Примеры
Host layers	7. Прикладной (application)	Данные	Доступ к сетевым службам	HTTP, FTP, SMTP, RDP, SNMP, DHCP
	6. Представительский (представления) (presentation)		Представление и шифрование данных	ASCII, EBCDIC
	5. Сеансовый (session)		Управление сеансом связи	RPC, PAP
	4. Транспортный (transport)	Сегменты ^[en] (segment)	Прямая связь между конечными пунктами и надёжность	TCP, UDP, SCTP, PORTS
Media ^[2] layers	3. Сетевой (network)	Пакеты (packet)/ Дейтаграммы (datagram)	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk
	2. Канальный (data link)	Биты (bit)/ Кадры (frame)	Физическая адресация	PPP, IEEE 802.22, Ethernet, DSL, ARP, L2TP, сетевая карта.
	1. Физический (physical)	Биты (bit)	Работа со средой передачи, сигналами и двоичными данными	USB, кабель ("витая пара", коаксиальный, оптоволоконный), радиоканал

Електронний документ

Електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

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

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Зміст електронного документа - це текстові та графічні частини, що складають документ. Контекст електронного документа - інформація про зв'язки задокументованої інформації з фізичними або юридичними особами та іншими документами.

Структура електронного документа: внутрішня структура - це структура змістовної частини документа; зовнішня структура - це структура середовища, в якому існує електронний документ (носій інформації, формат файла тощо).

Електронний документ визначається своїми метаданими. Метадані - це дані, що пов'язані та стосуються електронного документа, містять інформацію про його соціальну визначеність та розуміння змісту, контексту, структури. Метадані електронного документа мають елементи юридичних, ділових, організаційних, процедурних доказів цілісності електронного документа та його автентичності для авторів, користувачів та дослідників.

Цілісність електронного документа визначається як доказ того, що документ повний за складом та не підлягав неавторизованим змінам.

Загроза втрати автентичності/цілісності електронного документа зумовлена здатністю редагування програмними засобами, а також необхідністю у конвертуванні та міграції документів - переміщення електронного документа в інше середовище, наприклад, в наступне покоління програмно-технічних засобів.

Для забезпечення автентичності/цілісності електронного документа згідно із Законом України "Про електронний цифровий підпис" використовується електронний цифровий підпис (ЕЦП), який є обов'язковим реквізитом електронного документа, створюється і перевіряється за допомогою системи закритого та відкритого ключів з відповідними повноваженнями з їх створення та розповсюдження.

Електронний документообіг (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно із законодавством. Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ. Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

Інформаційні загрози

- **Інформаційна загроза** - це сукупність факторів, які створюють небезпеку для конституційних прав і свобод особистості, державної таємниці, зберігання цінної для суспільства інформації, від несанкціонованого доступу і розповсюдження.

Інформаційна безпека в різних сферах має свою **специфіку**:

- **політична** – ІБ стосується інформаційно-аналітичної діяльності дипломатичних представників і зовнішньо - економічних відомств;
- **економічна** – захист інформації у банківських системах та мережах зв'язку, конфіденційної інформації від несанкціонованого доступу.

Об'єктами захисту інформації є документи, програми ЕВМ, ноу-хау, бази даних, тексти та інші матеріальні носії інформації, захист яких передбачений державними нормативними актами, внутрішньовідомчими постановами, розпорядженнями та спеціальними документами.

Найбільш важливі види інформації, яких стосується ІБ є *стратегічна* інформація, *соціально-економічна* інформація, *військова*, *наукова*. Надання інформації на державному рівні повинно включати

проблему ІБ. Кожна країна включає питання ІБ в компетенцію Національної безпеки.

Інформаційні загрози та їх різновиди

Розглядаються *зовнішні* і *внутрішні* загрози ІБ, а також заходи і засоби протистояння і боротьба проти несанкціонованого доступу до інформації.

Зовнішні загрози

- інформаційному простору;
- інформаційному суверенітету;
- внутрішній стабільності;
- діяльності державного або недержавного органів і фірм.

Внутрішні загрози

- національній безпеці;
- для впливу на свідомість суспільства;
- доступу до інформаційних ресурсів країни;