ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

ПАЛЬЧЕВСЬКА О., ДОБРОВОЛЬСЬКА С.

МАЛАНЮК М., ГУБИЧ П.

АНГЛО - УКРАЇНСЬКИЙ ГЛОСАРІЙ ТЕРМІНІВ ІТ-ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ

Львів – 2025

LVIV STATE UNIVERSITY OF LIFE SAFETY

PALCHEVSKA O., DOBROVOLSKA S.

MALANIUK M., HUBYCH P.

English-Ukrainian glossary of IT and cybersecurity terms

LVIV – 2025

УДК 004.056:81'374.3=111=161.2
ББК 32.973я2+32.817я2+81.2Англ-4+81.2Укр-4
П 14

Рецензенти: **Леся ГРЕЧУХА,** кандидат філологічних наук, доцент, доцент кафедри прикладної лінгвістики та перекладу Черкаського державного технологічного університету;
Ірина АЛЕКСАНДРУК, кандидат філологічних наук, доцент кафедри іноземних мов хіміко-фізичних факультетів Київського національного університету імені Тараса Шевченка;
Ростислав ТКАЧУК, доктор технічних наук, завідувач кафедри кібербезпеки, полковник цивільного захисту Львівського державного університету безпеки життєдіяльності.

Упорядники: **Олександра ПАЛЬЧЕВСЬКА**, кандидат філологічних наук, доцент кафедри іноземних мов та перекладознавства факультету психології та соціального захисту ЛДУ БЖД;
Світлана ДОБРОВОЛЬСЬКА, кандидат економічних наук, доцент кафедри іноземних мов та перекладознавства факультету психології та соціального захисту ЛДУ БЖД
Марія МАЛАНЮК, старший викладач кафедри іноземних мов та перекладознавства факультету психології та соціального захисту ЛДУ БЖД;
Петро ГУБИЧ, старший викладач кафедри іноземних мов та перекладознавства факультету психології та соціального захисту ЛДУ БЖД

.

English-Ukrainian glossary of IT and cybersecurity terms // Англо-український глосарій термінів ІТ-технологій та кібербезпеки / О. С. Пальчевська, С. Р. Добровольська, М. С. Маланюк, П. В. Губич. Словник – Львів: Львівський державний університет безпеки життєдіяльності, 2025. – 266 с.

У глосарії з ІТ-технологій та кібербезпеки представлено терміни і термінологічні словосполучення, що репрезентують відповідну терміносистему. До реєстру словника входять лексичні одиниці, що використовуються в науковій та навчальній літературі з програмування, системного адміністрування, захисту інформації, штучного інтелекту, блокчейн-технологій та суміжних дисциплін. Словник включає також загальнотехнічні терміни, коли вони набувають специфічного значення в контексті інформаційних технологій. Словник структуровано за алфавітним принципом з урахуванням особливостей ІТ-терміносистеми. Основні терміни (реєстрові слова) виділено напівжирним шрифтом, нижче подано розгорнуте тлумачення.

Рекомендовано до друку Вченою радою
факультету психології та соціального захисту
Протокол № 5 від 22 травня 2025 року

Рекомендовано до друку Вченою радою
Львівського державного університету безпеки життєдіяльності
Протокол № 2 від 30 вересня 2025 року

ISBN 978-617-8654-18-4

ПЕРЕДМОВА

Сфера інформаційних технологій та кібербезпеки стрімко розвивається, постійно збагачуючись новітньою термінологією переважно англійського походження. Водночас, спеціалізовані терміни та поняття цифрової безпеки розосереджено використовуються в комп'ютерних науках, інженерії, математиці, телекомунікаціях тощо, що ускладнює їх розуміння для широкого кола фахівців та студентської молоді. Зростає також потреба у швидкому опрацюванні англомовних джерел інформації та вивченні передового зарубіжного досвіду.

Пропонований словник покликаний полегшити роботу з технічною документацією та забезпечити глибше розуміння специфіки галузей, які динамічно формуються в українському ІТ-секторі. Авторський колектив узагальнив і систематизував термінологію з інформаційних технологій та кібербезпеки.

У тлумачному словнику з ІТ-технологій та кібербезпеки представлено понад 8 500 термінів і термінологічних словосполучень, що репрезентують відповідну терміносистему. До реєстру словника входять лексичні одиниці, що використовуються в науковій та навчальній літературі з програмування, системного адміністрування, захисту інформації, штучного інтелекту, блокчейн-технологій та суміжних дисциплін. Словник включає також загальнотехнічні терміни, коли вони набувають специфічного значення в контексті інформаційних технологій.

Словник структуровано за алфавітним принципом з урахуванням особливостей ІТ-терміносистеми. Основні терміни (реєстрові слова) виділено напівжирним шрифтом, нижче подано розгорнуте тлумачення.

Словник буде корисним широкому загалу ІТ-спеціалістів: розробникам програмного забезпечення, системним архітекторам, фахівцям з інформаційної безпеки, викладачам профільних дисциплін, аспірантам та студентам технічних спеціальностей, які прагнуть удосконалити свої навички роботи з англомовною технічною літературою та міжнародними стандартами в галузі інформаційних технологій.

A

Access Control Facility

Access Control Facility 2 (ACF2) is mainframe security software distributed by Computer Associates. It is used to protect a mainframe and its resources. The software prevents the deliberate or accidental modification, deletion, corruption, or viral infection of important files and data through extensive security measures like:

- Access control
- Permission requirements
- Extensive logging of activities

The system status is monitored continuously and completely, and any access attempt is logged so it helps to identify potential intruders, and allows for the identification and analysis of changes and trends in the use of the system.

Система контролю доступу (Access Control Facility)

Access Control Facility 2 (ACF2) – це програмне забезпечення для захисту мейнфреймів, яке розповсюджується компанією Computer Associates. Воно використовується для захисту мейнфреймів та їхніх ресурсів. Програмне забезпечення запобігає навмисній або випадковій модифікації, видаленню, пошкодженню або вірусному зараженню важливих файлів і даних за допомогою широких заходів безпеки, таких як:

- контроль доступу;
- вимоги до дозволів;
- велика кількість журналів активності.

Стан системи контролюється безперервно і повністю, а будь-яка спроба доступу реєструється, що допомагає виявити потенційних зловмисників, а також дозволяє виявити і проаналізувати зміни і тенденції у використанні системи.

Accessibility Testing

Accessibility testing seeks to understand how well digital content complies with established usability standards for people who have disabilities.

During the accessibility testing process, the digital product will be assessed to determine how well it meets the needs of individuals with disabilities. Types of electronic content that are

Тестування доступності

Тестування доступності має на меті зрозуміти, наскільки добре цифровий контент відповідає встановленим стандартам доступності користування для людей з обмеженими можливостями.

У процесі тестування доступності цифровий продукт оцінюється, щоб визначити, наскільки добре він відповідає потребам людей з інвалідністю. Типи електронного контенту, які

commonly tested for accessibility compliance include email, electronic documents, social media posts, web applications and websites.

Accessibility tests can be automated with software tools or conducted manually by human testers. A hybrid approach that uses both automated test tools and manual methodologies often provides the most useful assessment.

зазвичай тестуються на відповідність вимогам доступності, включають електронну пошту, електронні документи, публікації в соціальних мережах, вебдодатки та вебсайти.

Тестування доступності може бути автоматизоване за допомогою програмних засобів або проведене вручну тестувальниками. Гібридний підхід, який використовує як автоматизовані інструменти тестування, так і ручні методики, часто забезпечує найбільш корисну оцінку.

Account Hijacking

Account hijacking is a process through which an individual's email account, computer account or any other account associated with a computing device or service is stolen or hijacked by a hacker.

It is a type of identity theft in which the hacker uses the stolen account information to carry out malicious or unauthorized activity.

Techopedia Explains Account Hijacking

In account hijacking, a hacker uses a compromised email account to impersonate the account owner. Typically, account hijacking is carried out through phishing, sending spoofed emails to the user, password guessing or a number of other hacking tactics.

Захоплення облікового запису (викрадення аккаунту)

Захоплення облікового запису – це процес, за допомогою якого хакер викрадає або захоплює обліковий запис електронної пошти, комп'ютерний обліковий запис або будь-який інший обліковий запис, пов'язаний з комп'ютерним пристроєм або службою.

Це тип крадіжки особистих даних, при якому хакер використовує викрадену інформацію про аккаунт для здійснення зловмисної або несанкціонованої діяльності.

При викраденні аккаунту хакер використовує скомпрометований аккаунт електронної пошти, щоб видати себе за власника аккаунту. Зазвичай викрадення аккаунту здійснюється за допомогою фішингу, надсилання підроблених електронних листів користувачеві, підбору пароля або ряду інших хакерських тактик.

Active Directory Monitoring (AD monitoring)

Active directory monitoring (AD monitoring) is the use of manual, automated or programmatic techniques to monitor and manage the operations of the Microsoft Active Directory environment.

AD monitoring is the combination of several techniques and methodologies aimed at reducing and resolving the problems that exist within an enterprise class network directory.

AD monitoring is generally performed through purpose-built Microsoft propriety, Microsoft Operation Manager (MOM), or a third-party application. The AD monitoring software accesses the Windows Perflib library to monitor, update and manage the directory service environment. These tools also provide a monitoring dashboard for quick statistics and editing into the directory service structure or framework. Regardless of the monitoring source, all AD monitoring processes and solutions primarily help ensure optimal performance and service. Some of the process in AD monitoring includes services monitoring, critical process monitoring, domain controller roles, and diagnosis and resolution services.

Моніторинг активного середовища

Моніторинг активного середовища – це використання основних, автоматичних чи запрограмованих технік щоб контролювати та моніторити процеси в середовищі Microsoft, щодо існуючих файлів.

АС моніторинг – це поєднання декількох технік та методологій, націлених на зменшення та вирішення проблем, що існують у межах мережевого каталогу корпоративних напрямків.

Моніторинг АС зазвичай виконується за допомогою спеціального програмного забезпечення Microsoft, Microsoft Operation Manager (MOM) або сторонніх програм. Програмне забезпечення для моніторингу АС отримує доступ до бібліотеки Windows Perflib для моніторингу, оновлення та керування середовищем служби каталогів. Ці інструменти також надають інформаційну панель моніторингу для швидкого збору статистики та редагування структури служби каталогів або фреймворку.

Незалежно від джерела моніторингу, всі процеси і рішення для моніторингу АС насамперед допомагають забезпечити оптимальну продуктивність і обслуговування. Деякі процеси моніторингу AD включають моніторинг служб, моніторинг критичних процесів, ролей контролерів доменів, а також служб діагностики та усунення несправностей.

Alureon

Alureon is a Trojan primarily used for data theft and online fraud. In addition to stealing confidential data, Alureon can also corrupt and delete important files on a computer. Furthermore, it can restrict Windows Update and prevent anti-virus software from running. Alureon usually searches for usernames, passwords, credit card information and other confidential information within a network's traffic.

Alureon mainly affects Microsoft Windows-based computer systems. Typically, Alureon enters a system by being bundled and delivered with a compromised copy of Windows Security Essentials software. Once the software is installed, the Alureon Trojan first takes over the printer spooler service and then changes the master boot record to its preferred routine. Computer systems infected with Alureon were confronted with BSoD and system crashes, specifically when installing security update MS 10-015 on Windows systems.

Alureon

Alureon – це троянська програма, яка в основному використовується для крадіжки даних та онлайн-шахрайства. Окрім крадіжки конфіденційних даних, Alureon також може пошкоджувати та видаляти важливі файли на комп'ютері. Крім того, він може обмежувати роботу Windows Update і перешкоджати запуску антивірусного програмного забезпечення. Alureon зазвичай шукає імена користувачів, паролі, дані кредитних карток та іншу конфіденційну інформацію в мережевому трафіку.

Alureon переважно вражає комп'ютерні системи на базі Microsoft Windows. Зазвичай Alureon потрапляє в систему разом зі скомпрометованою копією програмного забезпечення Windows Security Essentials. Після інсталяції програмного забезпечення троянець Alureon спочатку перехоплює службу спулера принтера, а потім змінює головний завантажувальний запис на свій розсуд. Комп'ютерні системи, заражені Alureon, стикалися з BSoD та системними збоями, зокрема, при встановленні оновлення безпеки MS 10-015 в системах Windows.

Analog

Analog, in the context of technology, refers to signals derived from physical phenomena that also may be interpreted as signals representing physical measurements. Light or visual input, for example, is an analog signal, so to capture video, its analog signal must be

Аналоговий

У контексті технології аналоговим називають сигнали, отримані від фізичних явищ, які також можуть бути інтерпретовані як сигнали, що представляють фізичні виміри. Наприклад, світло або візуальний вхід є аналоговим сигналом, тому для

scanned and then translated into fluctuating electronic pulses.

Record players, VCRs and cassette players are examples of analog devices because they record information in a linear manner, and they read physical data from a media device by scanning it. An analog signal is characterized by regular sinusoidal curves or sharp, irregular spikes, while digital signals are normally constant in amplitude and characterized by flat signal waves, like plateaus.

Analog was the only mainstream device choice until quite recently, when digital device technology became cheaper and easier to manufacture.

зйомки відео його аналоговий сигнал повинен бути відсканований, а потім перетворений в електронні імпульси, що коливаються.

Магнітофони, відеомагнітофони та касетні плеєри є прикладами аналогових пристроїв, оскільки вони записують інформацію лінійно і зчитують фізичні дані з медіа-пристрою шляхом сканування. Аналоговий сигнал характеризується регулярними синусоїдальними кривими або різкими, нерегулярними стрибками, тоді як цифрові сигнали зазвичай постійні за амплітудою і характеризуються пласкими сигнальними хвилями, схожими на плато. До недавнього часу аналогові пристрої були єдиним основним вибором, доки цифрові технології не стали дешевшими і простішими у виробництві.

Analytical Engine

Analytical engine most often refers to a computing machine engineered by Charles Babbage in the early 1800s. It is considered an early and very important step toward modern computer design. This term can also be used to refer to any comprehensive internal system for analytics.

The Babbage Analytical Engine mostly used analog systems to implement some of the most basic functions of today’s digital computers. It used a series of punch cards for input, and relied on an analog printer for output. In terms of its capacity, the machine’s use of an arithmetical unit and a primitive CPU that made use of physical pegs and rotating drums enabled the machine to become, in today’s terms, "Turing-complete,"

Аналітичний двигун

Аналітичним двигуном найчастіше називають обчислювальну машину, сконструйовану Чарльзом Беббіджем на початку 1800-х років. Це вважається раннім і дуже важливим кроком до сучасного комп'ютерного дизайну. Цей термін також може використовуватися для позначення будь-якої комплексної внутрішньої системи для аналітики.

Аналітичний двигун Беббіджа здебільшого використовував аналогові системи для реалізації деяких базових функцій сучасних цифрових комп'ютерів. Він використовував серію перфокарт для введення, а для виведення покладався на аналоговий принтер. З точки зору продуктивності, використання арифметичного блоку та примітивного процесора, який

because it would have satisfied the criteria for a Turing machine, which was created in the 1900s.

використовував фізичні кілочки та барабани, що оберталися, дозволило машині стати, кажучи сучасною мовою, «повною машиною Тюрінга», оскільки вона відповідала б критеріям машини Тюрінга, яка була створена у 1900-х роках.

Android Fragmentation

Android fragmentation refers to a concern over the alarming number of different available Android operating system (OS) versions in the market. The main issue is potentially reduced interoperability between devices of applications coded using the Android Software Development Kit (Android SDK).

As Android platform updates are released, Android fragmentation has increasingly captured the attention of software developers anticipating potential interoperability issues in the Android ecosystem. This means that Android SDK applications created for specific devices do not always work with other numerous devices.

Фрагментація Android

Фрагментація Android – це занепокоєння з приводу тривожної кількості різних доступних версій операційної системи (ОС) Android на ринку. Основною проблемою є потенційно знижена сумісність між пристроями додатків, написаних за допомогою Android Software Development Kit (Android SDK).

З виходом оновлень платформи Android фрагментація Android все більше привертає увагу розробників програмного забезпечення, які очікують на потенційні проблеми сумісності в екосистемі Android. Це означає, що додатки Android SDK, створені для певних пристроїв, не завжди працюють з іншими численними пристроями.

Anomaly Detection

Anomaly detection is the identification of data points, items, observations or events that do not conform to the expected pattern of a given group. These anomalies occur very infrequently but may signify a large and significant threat such as cyber intrusions or fraud.

Anomaly detection is mainly a data-mining process and is used to determine the types of anomalies occurring in a given data set and to determine details

Виявлення аномалій

Виявлення аномалій – це ідентифікація точок даних, елементів, спостережень або подій, які не відповідають очікуваному шаблону певної групи. Ці аномалії трапляються дуже рідко, але можуть означати велику і значну загрозу, наприклад, кібервторгнення або шахрайство.

Виявлення аномалій – це переважно процес інтелектуального аналізу даних, який використовується для визначення типів аномалій, що

about their occurrences. It is applicable in domains such as fraud detection, intrusion detection, fault detection, system health monitoring and event detection systems in sensor networks. In the context of fraud and intrusion detection, the anomalies or interesting items are not necessarily the rare items but those unexpected bursts of activities. These types of anomalies do not conform to the definition of anomalies or outliers as rare occurrences, so many anomaly detection methods do not work in these instances unless they have been appropriately aggregated or trained.

виникають у певному наборі даних, та отримання детальної інформації про їх виникнення. Він застосовується в таких сферах, як виявлення шахрайства, виявлення вторгнень, виявлення несправностей, моніторинг стану системи та системи виявлення подій у сенсорних мережах. У контексті виявлення шахрайства та вторгнень, аномалії або цікаві об'єкти, це не обов'язково рідкісні об'єкти, а несподівані сплески активності. Ці типи аномалій не відповідають визначенню аномалій або викидів як рідкісних явищ, тому багато методів виявлення аномалій не працюють в цих випадках, коли вони належним чином неагреговані або ненавчені.

Anti-phishing Service

An anti-phishing service is a technological service that helps prevent unauthorized access to secure and/or sensitive information. Anti-phishing services protect various types of data in diverse ways across a varety of platforms.

An anti-phishing service addresses a specific type of attempt to obtain personal or other sensitive information. While anti-phishing services provide tools to help users recognize Web phishing, many anti-phishing service features are responses to efforts to hack a system and steal data.

Some anti-phishing tools are available via browsers, through which many phishing attempts occur. They may also include sophisticated planning designed to help clients avoid data theft.

Антифішинговий сервіс

Антифішинговий сервіс – це технологічний сервіс, що допомагає запобігти неавторизованому доступу до інформації про безпеку чи конфіденційній інформації. Антифішинговий сервіс захищає різні типи даних різними способами на різних платформах.

Антифішинговий сервіс показує певний спосіб дозволів, щоб отримати особисту чи конфіденційну інформацію. Поки антифішинговий сервіс забезпечує інструменти щоб допомогти користувачам розпізнати вебфішинг, багато функцій антифішингових сервісів є відповіддю на спроби зламати систему та викрасти дані.

Деякі антифішингові інструменти доступні через браузери, через які відбувається багато спроб фішингу. Вони також можуть включати складне планування, покликане допомогти клієнтам уникнути крадіжки даних.

Application Clustering

Application clustering typically refers to a strategy of using software to control multiple servers. Clustered servers can help to provide fault-tolerant systems and provide quicker responses and more capable data management for large networks.

In application or software clustering, some of the protocols and administrative duties that would have been handled on each individual machine are handled by the joint software program. In other words, the software application is the control unit for the cluster. This is contrasted with a system called hardware clustering, where one individual machine runs the cluster through its operating system.

One of the advantages of application clustering is the scalability of these kinds of systems. With available specialized software, companies can easily set up multiple pieces of hardware that obey the same instructions, and refer to the same sets of information. IT pros refer to a cluster-aware application as an application that can assess systems to assign failover duties or handle delegation for transaction processing. These are kinds of principles supported by application clustering.

Кластеризація додатків

Під кластеризацією додатків зазвичай розуміють стратегію використання програмного забезпечення для керування кількома серверами. Кластерні сервери можуть допомогти забезпечити відмовостійкість систем, швидке реагування та більш ефективне управління даними у великих мережах.

При кластеризації додатків або програмного забезпечення деякі протоколи та адміністративні обов'язки, які виконувалися б на кожній окремій машині, обробляються спільною програмою. Іншими словами, програмне забезпечення є блоком управління кластером. Це контрастує з системою, яка називається апаратною кластеризацією, де одна окрема машина керує кластером за допомогою своєї операційної системи.

Однією з переваг кластеризації додатків є масштабованість таких систем. За допомогою доступного спеціалізованого програмного забезпечення компанії можуть легко налаштувати кілька апаратних засобів, які підпорядковуються однаковим інструкціям і звертаються до однакових наборів інформації. ІТ-фахівці називають кластерним додатком додаток, який може оцінювати системи для призначення обов'язків обходу відмов або для делегування обробки транзакцій. Саме такі принципи підтримуються кластеризацією додатків.

Application Infrastructure Provider

An application infrastructure provider (AIP) provisions the computing and operational infrastructure for developing, deploying and managing enterprise class applications. It houses all physical resources for applications through a managed service platform. These applications include computing hardware, infrastructure operation and management software, network/Internet connectivity and power/cooling.

The required resources are leased or rented to the sourcing organization under a service level agreement (SLA).

Like a cloud Infrastructure as a Service (IaaS) provider, an AIP has purpose-built infrastructure resources for hosting high-end applications. The underlying infrastructure is accessed remotely over the Internet or within a secure virtual private network (VPN) connection.

Постачальник забезпечення додатків (AIP)

Постачальник інфраструктури додатків (AIP) надає обчислювальну та операційну інфраструктуру для розробки, розгортання та управління додатками корпоративного класу. Він надає всі фізичні ресурси для додатків через керовану сервісну платформу. Ці програми включають обчислювальне обладнання, програмне забезпечення для експлуатації та управління інфраструктурою, підключення до мережі/ Інтернету та живлення/ охолодження.

Необхідні ресурси здаються в оренду організації-постачальнику за угодою про рівень обслуговування (SLA).

Постачальник забезпечення має спеціально створені ресурси забезпечення для розміщення додатків високого класу. Доступ до базової інфраструктури здійснюється віддалено через Інтернет або через захищене з'єднання віртуальної приватної мережі (VPN). Він переважно використовується для розгортання розроблених програм, а не для розробки програм поверх інфраструктури.

Armstrong's Axiom

Armstrong's Axiom is a mathematical notation used to find the functional dependencies in a database. Conceived by William W. Armstrong, it is a list of axioms or inference rules that can be implemented on any relational database. It is denoted by the symbol F+.

Armstrong's Axiom is used to analyze, refine and maintain relational

Аксіома Армстронга

Аксіома Армстронга – це математичне твердження, яке використовується для пошуку функціональних залежностей в базі даних. Задумане Вільямом Армстронгом (William W. Armstrong), воно являє собою список аксіом або правил виведення, які можуть бути реалізовані на будь-якій реляційній

databases. It has three major modes or inferences applied on a set of data:

- axiom of Reflexivity: if user name (A) and title (B) represent a person's name, then the relationship between both (A and B) is of little importance;
- - axiom of Augmentation: if a user ID defines a person's name, then the user ID with email quota define the person's name and email quota;

- axiom of Transitivity: if a user ID determines a person's name, and a person's name defines the department, then the department can define the user ID.

базі даних. Позначається символом F+.

Аксіома Армстронга використовується для аналізу, уточнення та підтримки реляційних баз даних. Вона має три основні режими або висновки, що застосовуються до набору даних:

− аксіома рефлексивності: якщо ім'я користувача (A) і посада (B) представляють ім'я людини, то зв'язок між ними (A і B) не має великого значення;

− аксіома доповнення: якщо ідентифікатор користувача визначає ім'я особи, то ідентифікатор користувача з квотою електронної пошти визначає ім'я особи та квоту електронної пошти;

− аксіома транзитивності: якщо ідентифікатор користувача визначає ім'я особи, а ім'я особи визначає відділ, то відділ може визначити ідентифікатор користувача.

Asset Management Software

Asset management software is a dedicated application which is used to record and track an asset throughout its life cycle, from procurement to disposal. It provides an organization with information like where certain assets are located, who is using them, how they are being utilized and details about the asset. The asset management software is used for management of both software and hardware assets.

Asset management software is also known as an asset management tool.

Asset management software tracks every aspect of an asset and is very useful to an organization because, aside from keeping track of assets, it can also

Програмне забезпечення для управління активами

Програмне забезпечення для управління активами – це спеціальна програма, яка використовується для реєстрації та відстеження активу протягом усього його життєвого циклу, від закупівлі до утилізації. Воно надає організації інформацію про те, де розміщено певні активи, хто їх використовує, як їх використовувати, а також детальну інформацію про активи. Програмне забезпечення для управління активами використовується для управління як програмними, так і апаратними активами.

provide additional functions like: measuring vendor performance; optimization of supplier portfolio; vendor audit and policy compliance;

optimization of costs for licensing; streamlining of procurement processes.

Програмне забезпечення для управління активами також відоме як інструмент управління активами.

Програмне забезпечення для управління активами відстежує кожен аспект активу і є дуже корисним для організації, оскільки, окрім відстеження активів, воно також може надавати додаткові функції, як-от: вимірювання продуктивності постачальників; оптимізація портфоліо постачальників; аудит постачальників та дотримання політик; оптимізація витрат на ліцензування; оптимізація процесів закупівель.

Asset Tracking

In information technology, asset tracking is the process of keeping track of the movement of one or more IT assets throughout the organization.

It is practiced by IT administrators and managers to have administrative control and insight into the movement of the entire IT infrastructure.

- Asset tracking is generally performed through asset tracking software that scans the entire IT infrastructure network and compiles an inventory of all IT assets. Any change in the movement of devices is recorded for future reference. The change in movement can include: IP address change; physical relocation of device; device removed from network; software installation/uninstallation; software license expiration.

Відстеження активів

В інформаційних технологіях відстеження активів – це процес відстеження руху одного або декількох IT-активів по всій організації.

Це практикується IT-адміністраторами та менеджерами, щоб мати адміністративний контроль та розуміння руху всієї IT-інфраструктури.

Відстеження активів зазвичай здійснюється за допомогою програмного забезпечення для відстеження активів, яке сканує всю мережу IT-інфраструктури та складає інвентаризацію всіх IT-активів. Будь-яка зміна в русі пристроїв фіксується для подальшого використання. Зміна в русі може включати в себе: зміну IP-адреси; фізичне переміщення пристрою; видалення пристрою з мережі; встановлення/видалення програмного забезпечення; закінчення терміну дії ліцензії на програмне забезпечення.

Attribute-Based Access Control

Attribute-based access control (ABAC) is a different approach to access control in which access rights are granted through the use of policies made up of attributes working together. ABAC uses attributes as the building blocks to define access control rules and access requests. This is done through a structured language called the eXtensible Access Control Markup Language (XACML), which is as easy to read or write as a natural language.

In an attribute-based access control system, any type of attribute such as user attributes and resource attributes are used to determine access. These attributes are compared to defined static values or even to other attributes, which turns it into a relation-based access control.

Контроль доступу на основі атрибутів

Контроль доступу на основі атрибутів (ABAC) – це інший підхід до контролю доступу, в якому права доступу надаються за допомогою політик, що складаються з атрибутів, які працюють разом. ABAC використовує атрибути як будівельні блоки для визначення правил контролю доступу та запитів на доступ. Це робиться за допомогою структурованої мови, яка називається extensible Access Control Markup Language (XACML), яку так само легко читати і писати, як і природну мову.

У системі управління доступом на основі атрибутів для визначення доступу використовуються будь-які типи атрибутів, зокрема атрибути користувачів і атрибути ресурсів. Ці атрибути порівнюються з визначеними статичними значеннями або навіть з іншими атрибутами, що перетворює їх на контроль доступу на основі відношень.

Auto Scaling

Auto scaling is a cloud computing feature that allows users to automatically scale cloud services, like virtual machines (VM) and server capacities, up or down, depending on defined situations. Cloud computing providers, such as Amazon Web Services (AWS), offer this feature.

Auto scaling is an implementation of the dynamic scaling feature of cloud computing, which can be applied manually or automatically. Increasingly, cloud service providers are offering this feature due to the unpredictable demand for cloud capabilities.

Автоматичне масштабування

Автоматичне масштабування – це функція хмарних обчислень, яка дозволяє користувачам автоматично масштабувати хмарні сервіси, такі як віртуальні машини (ВМ) і потужності серверів, вгору або вниз, залежно від визначених ситуацій. Цю функцію пропонують постачальники хмарних обчислень, зокрема Amazon Web Services (AWS).

Автоматичне масштабування – це реалізація функції динамічного масштабування хмарних обчислень, яку можна застосовувати вручну або автоматично. Постачальники хмарних послуг все частіше пропонують цю функцію через непередбачуваний попит на хмарні можливості.

Automated Business Process Discovery

Automated Business Process Discovery (ABPD) is a specific kind of business process analysis that is largely automated and relies heavily on algorithmic and computational logic building.

The principle of ABPD is that similar types of business analysis tools automatically gather data from documents such as audits and event logs, and compile it into useful information that not only identifies process models, but also explores variations and gives users a much better picture of what a specific business process looks like, and how changes would affect the business as a whole.

Automated Business Process Discovery is also known as process mining.

ABPD takes existing data and looks at it in detail to identify bottlenecks, weak links and sources of liability within business processes. This can be extremely valuable to a business, where combining this kind of automated process with other kinds of business process modeling can give executives or leaders an accurate picture of not only how business processes are done, but how they are operating relative to any number of other models or simulations.

Автоматизоване виявлення бізнес-процесів

Автоматизоване виявлення бізнес-процесів (ABPD) – це специфічний вид аналізу бізнес-процесів, який значною мірою автоматизований і значною мірою покладається на побудову алгоритмів та обчислювальної логіки.

Принцип ABPD полягає в тому, що подібні типи інструментів бізнес-аналізу автоматично збирають дані з таких документів, як аудити та журнали подій, і компілюють їх у корисну інформацію, яка не лише ідентифікує моделі процесів, але й досліджує варіації та дає користувачам набагато краще уявлення про те, як виглядає конкретний бізнес-процес і як зміни вплинуть на бізнес в цілому.

Автоматизоване виявлення бізнес-процесів також відоме як інтелектуальний аналіз процесів.

ABPD бере наявні дані та детально аналізує їх, щоб виявити вузькі місця, слабкі ланки та джерела відповідальності в бізнес-процесах. Це може бути надзвичайно цінним для бізнесу, де поєднання цього виду автоматизованого процесу з іншими видами моделювання бізнес-процесів може дати керівникам або лідерам точну картину не тільки того, як виконуються бізнес-процеси, але й того, як вони функціонують порівняно з будь-якою кількістю інших моделей або симуляцій.

Automated Data Tiering

Automated data tiering is the process of copying, moving and storing data across tiered data storage devices or

Автоматизована багаторівневість обробки даних

Автоматизована багаторівневість обробки даних – це процес копіювання, переміщення та зберігання

facilities. Automated data tiering enables the automatic movement of data between different storage types as required by business or application objectives.

Automated data tiering is also known as automated tiered storage.

Automated data tiering is performed through purpose-built software and hardware appliances, and works to continuously monitor the data that's rotated within an organization's storage tiers. It works on a predefined data policy that classifies data into various levels. For example, frequently accessed and critical data is moved to the storage tiers with the fastest access rates. Similarly, less used data is moved to lower-end storage media/tiers.

даних на багаторівневих пристроях або засобах зберігання даних. Автоматизована багаторівнева обробка даних дозволяє автоматично переміщати дані між різними типами сховищ відповідно до бізнес-цілей або завдань програми.

Автоматизована багаторівневість даних також відома як автоматизоване багаторівневе сховище.

Автоматизована багаторівневість даних виконується за допомогою спеціально створеного програмного та апаратного забезпечення і працює для постійного моніторингу даних, які обертаються в межах рівнів зберігання організації. Вона працює на основі заздалегідь визначеної політики даних, яка класифікує дані за різними рівнями. Наприклад, дані, до яких часто звертаються, і критичні дані переміщуються на рівні зберігання з найбільшою швидкістю доступу. Аналогічно, дані, що використовуються рідше переміщуються на носії/рівні зберігання нижчого класу.

Automated feature engineering

Feature engineering is challenging because it relies on the engineer's patience and imagination to discover implicit relationships in data.

Automated feature engineering software tools can speed things up by analyzing large data sets and suggesting features programmatically. This approach can significantly reduce the time ML engineers have to spend researching and analyzing data relationships manually.

Automation can also be used to manage a machine learning model's

Автоматизована інженерія ознак

Інженерія ознак є складним завданням, оскільки вона залежить від терпіння та уяви інженера для виявлення неявних зв'язків у даних.

Програмне забезпечення для автоматизованої інженерії ознак може прискорити процес, аналізуючи великі набори даних і пропонуючи ознаки програмним способом. Такий підхід може значно скоротити час, який інженери ML витрачають на ручний пошук і аналіз відносин між даними.

Автоматизація також може бути використана для більш ефективного

lifecycle more efficiently. For example, feature extraction tools can be used to combine several less important features into a new, more useful feature. Automated feature selection tools can assign each feature a score programmatically and delete features with the lowest scores.

Machine learning software programs that incorporate components to automate feature engineering are commercially available. Popular vendors include:

• DataRobot – can generate hundreds of new features by analyzing the relationships between primary and secondary datasets.

• dotData – can automatically transform hundreds of columns and billions of rows into a single feature table.

• Feature Labs – provides an open-source Python framework for automatically creating new features from multiple tables of structured data.

управління життєвим циклом моделі машинного навчання. Наприклад, інструменти вилучення ознак можуть бути використані для об'єднання кількох менш важливих ознак в одну нову, більш корисну ознаку. Інструменти автоматичного вибору ознак можуть програмно призначати кожній ознаці бал і видаляти ознаки з найнижчими балами.

Програмні продукти машинного навчання, які включають компоненти для автоматизації інженерії ознак, доступні комерційно. Популярними постачальниками є:

• DataRobot – може генерувати сотні нових ознак шляхом аналізу відносин між первинними та вторинними наборами даних.

• dotData – може автоматично перетворити сотні стовпців і мільярди рядків в одну таблицю ознак.

• Feature Labs – надає відкритий фреймворк Python для автоматичного створення нових ознак з кількох таблиць структурованих даних.

Automatic Failover

Automatic failover is a resource that allows a system administrator to automatically switch data handling to a standby system in the event of system compromise. Here, automatic describes the failover process. By definition, most failover processes are programmed to operate automatically.

Automatic failover is a best practice for systems that experience damage or lose vital connectivity during various

Автоматичне перемикання на резервну систему

Автоматичне перемикання на резервну систему – це ресурс, який дозволяє системному адміністратору автоматично переключати обробку даних на підсумкову систему в разі компрометації основної системи. Тут «автоматичне» описує процес переключення. За визначенням, більшість процесів аварійного відновлення програмуються на автоматичну роботу.

Автоматичне перемикання є найкращою практикою для систем, що мають досвід пошкодження чи

scenarios, such as storms and natural disasters. Organizations may use automatic failover systems to protect against data loss in such situations, which are often referred to as disaster recovery plans or emergency planning.

An automatic failover system allows for immediate off-site handling of database and server setups, ensuring seamless operations if an original system site is under attack by a storm or other disaster.

втрати зв'язку відповідно до різних подій, таких як шторми чи природні катаклізми. Для захисту від втрати даних у таких ситуаціях організації можуть використовувати системи автоматичного перемикання на резервну систему, які часто називають планами аварійного відновлення або плануванням на випадок надзвичайних ситуацій.

Автоматична система перемикання дозволяє негайно обробляти налаштування баз даних і серверів за межами сайту, забезпечуючи безперебійну роботу, якщо основний сайт системи піддається атаці буревію або іншій катастрофічній ситуації.

B

B2 security

B2 security is a security rating for evaluating the security of computer applications and products to be used within government and military organizations and institutes. It is part of the classifications/ratings produced by the U.S. National Computer Security Center (NCSC) as part of the Trusted Computer System Evaluation Criteria (TESC), or the orange book. B2 security primarily complements B1 security by extending discretionary and mandatory access control features to all objects within the data processing or computing solution. B2 security requires that the underlying system have a formal security policy in place that addresses all object access and handling procedures. B2 security is also called structured protection, where all elements are

Безпека рівня B2

Безпека B2 — це рівень безпеки для оцінки захищеності комп'ютерних програм і продуктів, що використовуються в урядових і військових організаціях та установах. Він є частиною класифікацій/ рейтингів, розроблених Національним центром комп'ютерної безпеки США (НЦКБ) в рамках Критеріїв оцінки довірених комп'ютерних систем (КОДКС), або «помаранчевої книги». Безпека рівня B2 передусім доповнює безпеку рівня B1, розширюючи функції дискреційного та обов'язкового контролю доступу на всі об'єкти в межах системи обробки даних або обчислювального рішення. Вона вимагає наявності у базовій системі формальної політики безпеки, яка регламентує всі процедури

categorized and structured as critical and non-critical elements along with implementation of stricter security controls and authentication mechanisms throughout each access point.

доступу до об'єктів і їх обробки. B2 також називають структурованим захистом, при якому всі елементи класифікуються як критичні або некритичні, а також впроваджуються суворіші заходи безпеки та механізми автентифікації на кожній точці доступу.

B3 security

B3 security is a security rating used to evaluate the security of computer applications and products to be used within government and military organizations and institutes.

It is among the classifications/ratings produced by the U.S. National Computer Security Center (NCSC) as part of the Trusted Computer System Evaluation Criteria (TESC), or the orange book.

B3 security primarily requires that the reference monitor condition is fulfilled, access to objects is secure and all the processes are small enough that they can be easily analyzed and tested. B3 security covers the area of security domains, where the system has high-end engineered design, strict security architecture and ongoing monitoring. To achieve this, B3 security relies on comprehensive security design and engineering to reduce the complexity of the system and remove code that isn't essential to security policy and its implementation. Moreover, the system must maintain security event logs, backup and recovery procedures and be highly resistant to penetration attack from intruders.

Безпека рівня B3

Безпека B3 – це рівень безпеки, який використовується для оцінки захищеності комп'ютерних застосунків та продуктів, якими користуються в урядових, військових організаціях та інститутах.

Це одна з класифікацій/рейтингів, розроблених Національним центром комп'ютерної безпеки США (НЦКБ), як частина Критеріїв оцінки довірених комп'ютерних систем (КОДКС) або «помаранчевої книги».

Безпека рівня B3 перш за все вимагає виконання умови референтного монітора, безпечного доступу до об'єктів і достатньо малих процесів для легкого аналізу та тестування.

Цей рівень охоплює сферу безпекових доменів, де система має високоякісний інженерний дизайн, строгу архітектуру безпеки та постійний моніторинг.

Для досягнення цього B3 покладається на комплексне проєктування та інженерію безпеки, щоб зменшити складність системи і усунути код, не суттєвий для політики безпеки та її реалізації.

Крім того, система повинна підтримувати журнали подій безпеки, мати процедури резервного копіювання та відновлення, а також бути дуже стійкою до атак зловмисників.

Back at keyboard

Back at keyboard (BAK) is an Internet slang phrase used to alert others that a user has returned to his or her computer. These types of acronyms are often used in online text communications to identify the user's status to other users at other locations.

Unlike some other forms of abbreviated data, acronyms like BAK are not often intended to save data storage space or transmission space. Instead, they are primarily designed to reduce the typing burden on the user. By using common shortcuts like BAK, users can quickly communicate status updates without having to type out full phrases like "back at keyboard." BAK directly corresponds to another acronym, AFK ("away from keyboard"), used to indicate that the user is temporarily not at the computer. Although today's users have access to voice communication technologies, text-based communication remains highly popular — especially on social media — which keeps acronyms like BAK and AFK relevant in digital interactions.

Користувач повернувся до свого комп'ютера

Back at keyboard (BAK) — це інтернет-сленговий вираз, який означає, що користувач повернувся до свого комп'ютера. Подібні абревіатури часто використовуються в онлайн-текстовому спілкуванні, щоб повідомити іншим про статус присутності користувача.

На відміну від деяких скорочень, абревіатури на кшталт BAK не створюються для економії пам'яті або трафіку.

Їх головна мета — зменшити навантаження на користувача під час введення тексту.

Завдяки подібним скороченням користувачі можуть швидко повідомити про свою присутність, не набираючи повну фразу «back at keyboard».

Акронім BAK є парою до популярного AFK (away from keyboard — відійшов від клавіатури).

Хоча сьогодні доступні голосові технології спілкування, текстові повідомлення залишаються дуже поширеними, особливо в соціальних мережах.

Тому скорочення на кшталт BAK та AFK досі активно використовуються в цифровій комунікації.

Back Orifice

Back Orifice is a remote administration system that enables full remote control over a computer running Microsoft Windows via a TCP/IP connection, using either a simple console or GUI.

It allows the remote user more control over the system than the person

Back Orifice

Back Orifice — це система віддаленого адміністрування, що дозволяє повний контроль над комп'ютером з ОС Microsoft Windows через TCP/IP-з'єднання за допомогою командної консолі або графічного інтерфейсу.

physically at the computer. Despite its legitimate function for system administration, BO is considered highly controversial due to its use in hacking and its ability to install covertly. Developed by hacker Sir Dystic (Josh Buchbinder) to expose the vulnerabilities of Windows 98, Back Orifice installs silently, does not appear in the task manager, and restarts automatically with the operating system. Its client is installed on another machine from which an administrator controls the infected system.

Main capabilities include:

- System control: keystroke logging, rebooting, system info access, retrieving passwords
- File system control: copy, edit, delete, lock, compress/uncompress files
- Process control: start or kill any process
- Multimedia/app control: access webcam, microphone, playback A/V, take screenshots
- Network control: packet sniffing, data logging, packet redirection

Although it has legitimate uses, BO is frequently distributed as malware, often embedded in Trojan horses, and is flagged and quarantined by antivirus software.

ВО надає віддаленому користувачу більше контролю над системою, ніж сам користувач перед комп'ютером. Попри законне застосування для адміністрування, ВО вважається вкрай суперечливим інструментом через потенційне використання у хакерських атаках. Back Orifice був створений хакером Sir Dystic (Джош Бухбіндер) для демонстрації вразливостей Windows 98. Програма встановлюється непомітно, не відображається в диспетчері задач і автоматично запускається під час старту системи. Клієнтська частина встановлюється на іншому комп'ютері, з якого здійснюється контроль.

Основні можливості:

- системний контроль: запис натискань клавіш, перезавантаження, доступ до паролів і системної інформації;
- файлова система: повний контроль над файлами: копіювання, видалення, стиснення;
- процеси: запуск і зупинка процесів;
- мультимедіа та додатки: доступ до камери, мікрофона, A/V файлів, знімки екрана;
- мережа: пакетний сніфер, логування, перенаправлення трафіку

Незважаючи на можливість легального використання, ВО часто використовується як шкідливе ПЗ, поширюється через троянські програми і блокується антивірусами.

Back quote

A back quote is a symbol or punctuation mark that is found in most standard physical and logical computer and mobile keyboards or key strings. It

Зворотний апостроф

Зворотний апостроф – це символ або розділовий знак, який можна знайти на більшості стандартних фізичних та логічних комп'ютерних і

is used in composing textual documents, sending computer commands and writing programming applications. A back quote is also known as grave accent, left quote, open quote and push. Besides a punctuation mark, a back quote is primarily a type of operator that has wide implementation in various operating systems and programming languages. For example when used in Perl language, the back quote executes a system command and stores the output or results within an array.

мобільних клавіатурах або клавішних рядках. Він використовується при складанні текстових документів, відправленні комп'ютерних команд та написанні програмних застосунків.

Зворотний апостроф також відомий як гравіс, ліва лапка, відкрита лапка або знак підкреслення. Крім того, що є розділовим знаком, зворотний апостроф є в першу чергу типом оператора, який широко використовується в різних операційних системах та мовах програмування. Наприклад, при використанні в мові Perl зворотний апостроф виконує системну команду та зберігає вивід або результати у масиві.

Backchannel

A backchannel refers to the use of networked computers and instant messaging software in a learning or team-based work environment to provide private or one-to-one communication between the student/ listener and the teacher/speaker. Backchannel technology is widely used in conferences, networked environments with supported communication and/or chatting software, as well as to deliver academic lectures.

Зворотний канал

Зворотний канал – це використання мережевих комп'ютерів і програмного забезпечення для обміну миттєвими повідомленнями в навчальному або командному робочому середовищі для забезпечення приватного або індивідуального спілкування між учнем/слухачем і викладачем/ спікером. Технологія backchannel широко використовується на конференціях, у мережевих середовищах з підтримкою комунікаційного чи чатового ПЗ, а також під час академічних лекцій.

Backend

Backend as a service (BaaS) is a strategy for developing software applications that outsource backend computing services to a cloud service provider. BaaS plays an important role in low-code/no-code (LCNC) software development, serverless computing and NoOps. The benefits of using a BaaS

Backend як послуга (BaaS)

Backend (BaaS) — це стратегія розробки програмних застосунків, яка передбачає делегування серверних обчислювальних функцій постачальнику хмарних сервісів.

BaaS відіграє ключову роль у розробці програм з низьким або нульовим кодуванням (НКНК),

provider include lower engineering costs and faster time-to-market for software applications. In the early part of this century — before cloud computing gained wide-spread acceptance — BaaS providers were usually called MBaaS providers because the services they offered met the unique needs of mobile app developers. Today, the term BaaS is sometimes used as a synonym for Platform as a Service (PaaS), but technically, they are not the same thing. Over the years BaaS has evolved to meet the needs of citizen developers and unlike PaaS, does not allow server-level access.

безсерверних обчисленнях та концепції NoOps.

Серед переваг використання BaaS – зниження витрат на інженерні ресурси та прискорення виходу продукту на ринок.

На початку XXI століття – до широкого впровадження хмарних обчислень – провайдерів BaaS зазвичай називали MBaaS, оскільки їх послуги були орієнтовані на потреби мобільних розробників.

Сьогодні термін BaaS іноді використовується як синонім PaaS (Platform as a Service), але технічно це різні поняття.

З часом BaaS еволюціонував для задоволення потреб так званих «громадських розробників» (citizen developers) і, на відміну від PaaS, не передбачає доступу до серверного рівня.

Back-end developer

A back-end developer is a type of programmer who creates the logical back-end and core computational logic of a website, software or information system. The developer creates components and features that are indirectly accessed by a user through a front-end application or system. Back-end developers primarily develop and maintain the core functional logic and operations of a software application or information system. The key job role of a back-end developer is to ensure that the data or services requested by the front-end system or software are delivered through programmatic means. Back-end developers also create and maintain the entire back-end of a system, which consists of the core application logic,

Бекенд розробник

Бекенд розробник – це тип програміста, який створює логічну внутрішню частину та основну обчислювальну логіку вебсайту, програмного забезпечення або інформаційної системи. Розробник створює компоненти та функції, до яких користувач має опосередкований доступ через інтерфейсний додаток або систему. Бекенд розробник в основному створює та підтримує основну функціональну логіку та операції програмного застосунку або інформаційної системи. Основним завданням бекенд розробника є забезпечення доставки даних або послуг, що запитуються фронтенд-системою або програмним забезпеченням, програмними засобами.

databases, data and application integration, API and other back-end processes.

Back-End розробники також створюють та підтримують весь бекенд системи, який складається з основної логіки застосунку, баз даних, інтеграції даних та застосунків, API та інших бекенд-процесів.

Backscatter

Backscatter is a type of unsolicited spam/email message that is mistakenly directed to an email inbox. They are disguised as bounce messages, so that they are not filtered as spam by the email server.

Backscatter is also known as outscatter, misdirected bounces, blowback and collateral spam.

Branch coverage testing is a methodical type of testing which requires that all program branches or conditional states be tested at least once during a testing process.

Backscatter

Backscatter – це тип небажаного спам-повідомлення, яке помилково надсилається на електронну пошту. Вони маскуються під повідомлення про повернення, щоб не фільтруватися як спам сервером електронної пошти.

Backscatter також відомий як аутскатер, неправильно спрямовані повернення, зворотний удар або колітерний спам.

Тестування розгалуження є методичним типом тестування, яке вимагає, щоб усі гілки програми або умовні стани були протестовані принаймні один раз під час процесу тестування.

Backup and Recovery Test

A backup and recovery test is a process used to make sure that a backup and recovery plan will work the way it is supposed to after a real emergency. This kind of testing can involve many different types of analysis, from basic file recovery tests to detailed scenario testing.

Businesses invest a lot of money and effort into data backup and recovery plans for simple user events, as well as emergency events like natural disasters. However, without adequate testing, it’s

Тест резервного копіювання та відновлення

Тест резервного копіювання та відновлення – це процес, який використовується для того, щоб переконатися, що план резервного копіювання та відновлення працюватиме так, як передбачається після реальної надзвичайної ситуації.

Цей вид тестування може включати багато різних типів аналізу: від базових тестів відновлення файлів до детального тестування сценаріїв.

Компанії інвестують багато грошей і зусиль у плани резервного

hard to know whether any backup and recovery plan will work. Testing, in some senses, completes the circle when it comes to preparing for natural disasters or other crises.

Ideally, companies should be able to test their actual live systems for correct backup and recovery functionality. In terms of actually testing IT systems for backup and recovery, these tests may be as diverse as simulating the loss of simple data files or an entire server; looking at backup processes for operating systems, databases and applications; or testing failback and failover processes and looking for accurate IT responses to a range of events.

копіювання та відновлення даних для простих подій користувачів, а також для надзвичайних ситуацій, таких як стихійні лиха.

Однак без належного тестування важко зрозуміти, чи працюватиме план резервного копіювання та відновлення даних.

Тестування, в певному сенсі, замикає коло, коли мова йде про підготовку до стихійних лих або інших кризових ситуацій.

В ідеалі, компанії повинні мати можливість тестувати свої реальні системи на правильність функціонування функцій резервного копіювання та відновлення.

Щодо фактичного тестування IT-систем для резервного копіювання та відновлення, ці тести можуть бути різноманітними: від імітації втрати простих файлів даних до цілого сервера;

Перевірки процесів резервного копіювання операційних систем, баз даних і додатків; або тестування процесів відновлення та переходу на резервний сайт, а також перевірки точних IT-відповідей на різноманітні події.

Backup Appliance

A backup appliance is a type of data storage device or equipment that combines backup software and hardware components within a single device. It is a turnkey solution that provides a centralized interface for backup processes, tools, and infrastructure.

A backup appliance is a hardware device that comes preinstalled with backup management software, storage drives, network interfaces/ports, and

Апаратне забезпечення для резервного копіювання

Апаратне забезпечення для резервного копіювання — це тип пристрою/обладнання для зберігання даних, що об'єднує програмне та апаратне забезпечення для резервного копіювання в одному пристрої. Це тип готового та всеосяжного рішення для резервного копіювання, яке забезпечує централізований інтерфейс для процесів, інструментів та інфраструктури резервного копіювання.

other backup administration utilities. It functions by connecting to devices or components within the local or organizational network. The appliance can also be connected to external storage or backup solutions such as SAN, NAS, or cloud backup. Additionally, it may provide data security services, such as encrypting data at rest and restricting access to the appliance to authorized users only.

Пристрій резервного копіювання — це апаратний пристрій, на якому встановлено програмне забезпечення для керування резервним копіюванням, накопичувачі, мережеві інтерфейси/порти та інші програми для адміністрування резервного копіювання. Він працює шляхом підключення до пристроїв або компонентів локальної або організаційної мережі. Пристрій також можна підключити до зовнішніх сховищ або засобів резервного копіювання, таких як SAN, NAS або хмарне сховище. Крім того, він може надавати послуги з безпеки даних, шифруючи їх у стані спокою і обмежуючи доступ до пристрою лише авторизованим користувачам.

Backup Copy

A backup copy is a duplicate instance of a data file, application, system or server that's created using backup software. It's used as a means to restore original data in case it's deleted, corrupted or lost. A data backup copy is similar to the data being backed up and is usually stored on an external backup storage facility/medium. A backup copy is also known as backup file. A backup copy is a duplicate version of any data and is the sole output of any backup process/software. Typically, the backup copy is of the same version, size and type as the original data. For a complete system or database backup, this can be a snapshot image file consisting of all the data and settings, which are essential to restoring the system to its last backed-up state. A backup copy is also used as a means to maintain data redundancy.

Резервна копія

Резервна копія — це точна копія файлу, програми, системи або сервера, створена за допомогою спеціального програмного забезпечення. Вона використовується для відновлення оригінальних даних у разі їх випадкового видалення, пошкодження або втрати. Резервна копія даних є аналогічною до даних, що резервуються, і зазвичай зберігається на зовнішньому носії або в спеціальному сховищі. Резервна копія також відома як резервний файл. Резервна копія є дублікатом будь-яких даних і є єдиним результатом будь-якого процесу або програмного забезпечення резервного копіювання. Зазвичай резервна копія має ту саму версію, розмір і тип, що й оригінальні дані. Для повного резервного копіювання системи або бази даних це може бути файл-образ (snapshot), що містить усі дані та налаштування, необхідні для відновлення системи до останнього резервного стану.

Резервна копія також використовується як засіб забезпечення надлишковості даних.

Backup Storage

Backup storage refers to a storage device, medium or facility that is used for storing copies and instances of backup data. Backup storage enables the maintenance, management, retrieval and restoration of backup data for any individual, application, computer, server or any computing device.

Backup storage is primarily an additional storage device used for keeping backup data. Typically, it is external to the system, server or device for which the backup data is created, such as a local/remote storage server. The backup storage itself can be a hard disk drive, tape drive, compact disk drive or any mass storage medium installed within a computer or storage server.

In enterprise IT environments, the backup storage medium/technology used can be RAID, a storage area network or a network-attached storage system. Backup software or a backup manager is used to create, store, manage and retrieve backup data to and from the backed up application/device and the backup storage location.

Сховище резервного копіювання

Сховище резервного копіювання – це пристрій, носій або об'єкт зберігання, який використовується для зберігання копій та екземплярів резервних даних.

Сховище резервного копіювання забезпечує підтримку, управління, вилучення та відновлення резервних даних для будь-якої особи, програми, комп'ютера, сервера або будь-якого обчислювального пристрою. Сховище резервних копій – це насамперед додатковий пристрій для зберігання резервних даних.

Як правило, воно є зовнішнім щодо системи, сервера або пристрою, для якого створюються резервні копії, наприклад, локальний або віддалений сервер зберігання.

Пристроєм для зберігання резервних копій може бути жорсткий диск, стрічковий накопичувач, компакт-диск або будь-який інший масовий носій, встановлений у комп'ютері або сервері зберігання.

У корпоративних IT-середовищах для зберігання резервних копій можуть використовуватись RAID-масиви, мережі зберігання даних (SAN) або системи мережевого зберігання (NAS).

Програмне забезпечення для резервного копіювання або менеджер резервного копіювання використовується для створення, зберігання, керування та отримання резервних копій даних між додатком/пристроєм і місцем зберігання резервних копій.

Beep Code

A beep code is a type of signal provided by a personal computer during the boot process. Most beep codes are related to a power on self test (POST), where a beep code helps show end-users

Звуковий код

Звуковий код – це тип сигналу, який видає персональний комп'ютер під час процесу завантаження. Більшість звукових кодів пов'язані з самотестуванням при увімкненні

that there is a hardware problem preventing normal operation.

(СПУ), де звуковий код допомагає кінцевому користувачеві визначити, що є проблема з апаратним забезпеченням, яка перешкоджає нормальній роботі.

Beginning Of File (BOF)

Beginning Of File (BOF) is an important designation in programming, marking the start of a file. It enables functionality that works through individual files or data sets.

BOF is a marker indicating where the file begins, allowing the use of specific operators that need to reference this point. For example, a developer may create a loop that starts at BOF and proceeds through each character until the end of the file. Improper use of BOF or EOF can cause errors when the program cannot locate a specific position. Using these markers helps developers manage files efficiently and identify errors.

Початок файлу (ПФ)

Початок файлу (ПФ) – це важливе позначення в програмуванні, яке вказує на місце початку файлу. Воно дозволяє реалізувати функціональність, що працює з окремими файлами або наборами даних.

ПФ — це маркер, що вказує на місце початку файлу, дозволяючи використовувати специфічні оператори, які мають орієнтуватися на цю точку. Наприклад, розробник може створити цикл, що починається з ПФ і проходить через кожен символ до кінця файлу. Неправильне використання ПФ або КФ може призвести до помилок, якщо програма не може знайти потрібну позицію. Використання таких маркерів допомагає розробникам ефективно працювати з файлами та виявляти помилки.

Bi-directional predictive frame

A bi-directional predictive frame (B-Frame) is part of an MPEG video compression standard. In this method, groups of sequential pictures are aggregated to form a group of pictures (GOP), which are displayed in sequence to provide video. A single bi-directional predictive frame relates to other frames directly preceding or following it. By recording just the information that differs from a preceding picture or a following picture, the data storage

Двонаправлений предиктивний кадр

Двонаправлений предиктивний кадр (B-кадр) є частиною стандарту стиснення відео MPEG. За цим методом групи послідовних зображень об'єднуються у групу кадрів (GOP), які відтворюються послідовно для формування відео. Окремий B-кадр пов'язаний із кадрами, що безпосередньо передують або слідують за ним.

Завдяки запису лише тієї інформації, яка відрізняється від

requirements for each individual picture become much lower than in a technique that would store each successive image completely. A bi-directional predictive frame may also be known as a bi-directional frame.

попереднього або наступного кадру, потреба у збереженні даних для кожного кадру значно зменшується порівняно з методами, які зберігають кожне зображення повністю.

В-кадр також може бути відомий як двонаправлений кадр.

Big Data Management

Big data management refers to the comprehensive processes and tools used to handle vast amounts of structured and unstructured data that organizations generate. The goal of big data management is to ensure that data is stored efficiently, analyzed properly, and utilized effectively to drive business decisions. Proper management of big data enables organizations to gain deeper insights into customer behavior, market trends, and operational efficiencies.

Big data management also requires securing data to prevent unauthorized access and ensuring that it remains available and accessible across various platforms. Techniques like data virtualization are often employed to reduce data complexity, speed up access, and allow for simultaneous use by multiple users or applications. Big data management ultimately supports the decision-making process by making data more organized, secure, and actionable.

Управління великими даними

Управління великими даними – це комплекс процесів і інструментів, що використовуються для обробки великих обсягів структурованих і неструктурованих даних, які генеруються організаціями. Метою управління великими даними є забезпечення ефективного зберігання, належного аналізу та ефективного використання даних для прийняття бізнес-рішень. Правильне управління великими даними дозволяє організаціям отримувати глибші інсайти щодо поведінки клієнтів, ринкових тенденцій і операційної ефективності.

Управління великими даними також передбачає забезпечення безпеки даних для запобігання несанкціонованому доступу та гарантування їх доступності і зручності використання на різних платформах. Для зменшення складності даних, прискорення доступу та забезпечення одночасного використання кількома користувачами або додатками часто використовуються такі методи, як віртуалізація даних. Управління великими даними зрештою підтримує процес ухвалення рішень, роблячи дані більш організованими, безпечними та придатними для використання.

Big data mining

Big data mining is referred to the collective data mining or extraction techniques that are performed on large sets/volume of data or the big data. Big data mining is primarily done to extract and retrieve desired information or pattern from humongous quantity of

A process of analyzing large volumes of unstructured data accumulated over time by an organization. It involves algorithms for data searching, refining, extracting, and comparing. Effective big data mining relies heavily on computing resources, especially memory and processor capacity, to handle complex queries and operations on vast datasets. These techniques are also applied in big data analytics and business intelligence to uncover patterns, relationships, and actionable insights.

Видобуток великих даних

Видобуток великих даних відноситься до колективних методів видобутку або екстракції даних, які виконуються на великих наборах/ обсягах даних або великих даних. Видобуток великих даних в основному здійснюється для вилучення та отримання потрібної інформації або шаблону з величезної кількості даних.

Процес аналізу великих обсягів неструктурованих даних, які накопичуються організацією з часом, включає алгоритми пошуку, уточнення, вилучення та порівняння даних. Ефективний видобуток великих даних потребує потужних обчислювальних ресурсів, зокрема процесорів і пам’яті, для обробки складних запитів та операцій. Такі методи застосовуються в аналітиці великих даних і бізнес-інтелекті для виявлення закономірностей, зв’язків і корисної інформації.

Big Data Platform

Big data platform is a type of IT solution that combines the features and capabilities of several big data application and utilities within a single solution. It is an enterprise class IT platform that enables organization in developing, deploying, operating and managing a big data infrastructure /environment.

Платформа для великих даних

Платформа для великих даних – це тип ІТ-рішення, яке об'єднує функції та можливості кількох застосунків і допоміжних програм для великих даних в рамках єдиного рішення. Це ІТ-платформа корпоративного класу, яка дозволяє організації розробляти, розгортати, експлуатувати та управляти інфраструктурою/ середовищем великих даних.

Big Data Storage

Big Data Storage – refers to infrastructure specifically designed for managing and storing large volumes of data, which includes structured, semi-structured, and unstructured data. The primary objective of such systems is to

Зберігання великих даних

Зберігання великих даних – це інфраструктура, яка спеціально розроблена для управління та зберігання великих обсягів даних, що включають структуровані, напівструктуровані та неструктуровані дані. Основною

ensure the efficient processing, searching, security, and access to data. Big data storage systems need to handle the three main characteristics of data: Volume, Variety, and Velocity. These factors are critical when developing systems for big data storage, as they require special solutions to manage vast amounts of data that are constantly changing and need to be processed quickly.

Big data storage includes several technologies such as the Hadoop Distributed File System (HDFS), which allows data to be stored on distributed nodes for redundancy. Additionally, NoSQL databases (e.g., MongoDB, Cassandra), cloud storage systems such as Amazon S3 and Google Cloud Storage, and data lakes are also employed. Data lakes allow for storing raw or unprocessed data in its original format for future processing.

Since processing large volumes of data requires significant resources, optimizing the performance of these systems through data reduction techniques is essential. For example, technologies such as data compression, deduplication, and segmentation are used to enhance query processing efficiency and reduce storage costs. Furthermore, big data storage also involves strategies for balancing cost and performance, allowing data to be moved between different storage tiers based on its usage.

метою таких систем є забезпечення ефективної обробки, пошуку, безпеки і доступу до даних. Системи зберігання великих даних повинні справлятися з трьома основними характеристиками даних: обсягом (Volume), різноманіттям (Variety) і швидкістю (Velocity). Ці фактори є основними при розробці систем для зберігання великих даних, оскільки вони вимагають спеціальних рішень для управління величезними масивами даних, що постійно змінюються та потребують швидкої обробки.

Зберігання великих даних включає в себе кілька технологій, таких як Hadoop Distributed File System (HDFS), що дозволяє зберігати дані на розподілених вузлах для забезпечення відмовостійкості. Крім того, використовуються бази даних NoSQL (наприклад, MongoDB і Cassandra), хмарні системи зберігання, як Amazon S3 і Google Cloud Storage, а також озера даних, які дозволяють зберігати необроблені або сирі дані в їхньому первісному вигляді для подальшої обробки.

Оскільки обробка великих обсягів даних потребує значних ресурсів, важливою є оптимізація роботи таких систем за допомогою методів зменшення обсягу даних. Наприклад, використовуються технології для зменшення розміру даних, видалення дублікатів та сегментації даних, щоб підвищити ефективність обробки запитів і знизити витрати на зберігання. Більш того, зберігання великих даних також включає в себе стратегії балансування вартості та продуктивності, що дозволяє переміщувати дані між різними рівнями зберігання залежно від їх використання.

Big-endian

Big-endian refers to the way that data is sequentially stored in computer memory. Just as in books or magazines, where the first word appears in the top-left-hand corner of each page, the data in a big-endian system is organized such that the most significant digits or bytes appear in the upper left corner of a memory page, while the least significant ones appear in the bottom right-hand corner. This is in contrast to little-endian systems, in which the least significant data is organized in the upper left corner, while the most important bytes appear bottom-right. Both systems refer to a computer systems' "endianness," or how bytes are arranged for that particular system.

Big-endian як спосіб зберігання даних у комп'ютерній пам'яті

Big-endian – це спосіб послідовного зберігання даних у комп'ютерній пам'яті. Як у книгах або журналах, де перше слово розміщене у верхньому лівому куті сторінки, так і в системі big-endian найбільш значущі байти зберігаються у верхньому лівому куті сторінки пам'яті, а найменш значущі — у нижньому правому.

Це протилежно little-endian системам, де найменш значущі байти розміщуються першими.

Обидва підходи відносяться до поняття «ендіанність» — способу розміщення байтів у пам'яті певної комп'ютерної системи.

Binary-Coded Decimal (BCD)

Binary-Coded Decimal (BCD) is a binary representation of decimal numbers where each digit is encoded using a fixed number of bits, typically four. Commonly used to avoid size limitations of standard binary formats.

Binary-Coded Decimal (BCD) is a method of encoding decimal numbers in binary, where each digit is represented by its own 4-bit binary sequence. This simplifies decimal conversion for display but increases circuit complexity. For example, "1001 0101 0110" equals 956 in decimal.

Двійково-десятковий код (ДДК)

Двійково-десятковий код (ДДК) – це тип двійкового представлення десяткових чисел, де кожна цифра кодується фіксованою кількістю бітів, зазвичай чотирма. Використовується для уникнення обмежень розміру, притаманних звичайному двійковому представленню.

Двійково-десятковий код (ДДК) – це спосіб кодування десяткових чисел у двійковій формі, де кожна цифра подається окремою 4-бітовою послідовністю. Полегшує перетворення для відображення, але ускладнює апаратну реалізацію. Наприклад, «1001 0101 0110» дорівнює 956 у десятковій системі.

Biohacking

Biohacking refers to the application of IT hacks to biological systems, most notably the human body, but also extending to the entire biosphere. It includes a broad range of DIY IT projects and ideas. Biohacking is often associated with positive goals, distinguishing it from malicious hacking. It can involve body modifications, such as implants and wearable computing, as well as self-medical practices like home DNA testing. It may also apply to the use of advanced IT in areas like hydroponic plant systems or other biological projects.

Біохакінг

Біохакінг відноситься до застосування IT-хаків до біологічних систем, найчастіше до людського тіла, але також і до всієї біосфери. Він охоплює широкий спектр DIY IT-проектів та ідей. Біохакінг часто асоціюється з позитивними цілями, що відрізняє його від зловмисного хакінгу. Він може включати модифікації тіла, такі як імплантати та носиму електроніку, а також самостійні медичні практики, такі як домашнє тестування ДНК. Також біохакінг може застосовуватися до використання передових IT у таких сферах, як гідропонні системи рослин або інші біологічні проекти

Biometric Authentication

Biometric authentication is a user identity verification process that involves biological input, or the scanning or analysis of some part of the body. Biometric authentication methods are used to protect many different kinds of systems – from logical systems facilitated through hardware access points to physical systems protected by physical barriers, such as secure facilities and protected research sites.

Security experts often distinguish biometric authentication from other types such as:

- Knowledge-based authentication – using passwords or secret information,
- Property-based authentication – using objects like key cards.

Biometric authentication is often seen as the most secure method because it's extremely difficult to duplicate or transfer biological features from one user to another. Although traditionally expensive and hard to implement, advances in technology are making it increasingly feasible.

Common and evolving types include:

Біометрична автентифікація

Біометрична автентифікація – це процес перевірки особи користувача, який здійснюється за допомогою біологічного вводу, сканування або аналізу частини тіла. Методи біометричної автентифікації використовуються для захисту як логічних систем (через апаратні точки доступу), так і фізичних систем (наприклад, об'єктів з обмеженим доступом).

Фахівці з безпеки розрізняють:

- автентифікацію на основі знань — паролі, PIN-коди тощо;
- автентифікацію на основі власності — ключі, картки;

Біометрична автентифікація вважається найнадійнішою, оскільки передача або підробка біологічних даних майже неможлива. Попри те, що раніше такі системи були дорогими, сучасні технології роблять їх доступнішими для різних сфер.

Найпоширеніші типи:

- сканування обличчя — контроль доступу, ідентифікація;

- Facial recognition – used for access control and surveillance,
- Fingerprint scanning – widely used in mobile devices and secure systems,
- Iris or eye-based authentication,
- Full-body scanning – for high-security environments.

Biometric Verification

Biometric verification is an identity authentication process used to confirm a claimed identity through uniquely identifiable biological traits, such as fingerprints and hand geometry. It is designed to allow a user to prove their identity by providing a biometric sample and a unique identification code to gain access to a secure environment.

Biometric verification replaces the traditional username-password authentication system, as it is nearly impossible to replicate biological signatures, unlike usernames, which can be guessed or stolen. It is one of the most secure authentication systems available. The process starts with the retrieval of a biometric sample by scanning the chosen identification attribute, such as fingerprints, hand geometry, iris patterns, facial geometry, or voice patterns. The sample is then compared to a database of authorized personnel, and when it matches, the user is asked to authenticate with a unique identification code linked to the sample. When both parameters match, access is granted. This is part of the two-step verification process, where two parameters are required for access.

- відбитки пальців — смартфони, банкомати, сейфи;
- сканування очей (райдужки або сітківки);
- комплексне сканування тіла — у зонах підвищеної безпеки.

Біометрична верифікація

Біометрична верифікація – це процес автентифікації особи, який використовується для підтвердження заявленої ідентичності за допомогою унікальних біологічних характеристик, таких як відбитки пальців та геометрія руки. Вона дозволяє користувачеві довести свою особу шляхом надання біометричного зразка та унікального ідентифікаційного коду для отримання доступу до захищеного середовища.

Біометрична верифікація замінює традиційну автентифікацію за допомогою імені користувача та пароля, оскільки відтворити біологічні характеристики людини практично неможливо, на відміну від імен користувачів, які можна вгадати або викрасти. Це одна з найбезпечніших систем автентифікації, доступних сьогодні. Процес починається з отримання біометричного зразка за допомогою сканування атрибутів, обраних для ідентифікації, таких як відбитки пальців, геометрія руки, візерунки райдужної оболонки ока, геометрія обличчя або голосу. Потім зразок порівнюється з базою даних відомого уповноваженого персоналу, і коли цей зразок виявляється позитивним, користувачеві пропонується пройти автентифікацію за допомогою унікального ідентифікаційного коду, пов'язаного зі зразком. Коли обидва параметри збігаються, доступ надається. Це стандартна процедура так званої двоетапної верифікації, коли для доступу потрібні два параметри.

BIOS

The BIOS is a program the microprocessor uses to start the computer. It runs POST to check hardware before booting. Many PC makers use beep codes to signal hardware errors – like power issues, motherboard faults, or display problems. Macintosh also has startup tones for video or logic board issues. Beep codes help with troubleshooting, and users can check manuals or online for their meaning.

BIOS

BIOS – це програма, яку мікропроцесор використовує для запуску комп'ютера. Вона виконує СПУ для перевірки обладнання перед завантаженням. Багато виробників ПК використовують звукові коди для сигналізації про помилки – наприклад, проблеми з живленням, материнською платою або дисплеєм. Macintosh теж має стартові звуки для виявлення збоїв відеоконтролера чи логічної плати. Звукові коди допомагають у діагностиці, а користувачі можуть дізнатися їх значення в посібниках або онлайн.

BITNET

BITNET was a wide-area cooperative computer network made up of networks from different universities in the US. It was established in 1981 by the City University of New York's Ira Fuchs and Greydon Freeman from Yale University, with the first network link being between these two universities. Its name was originally taken from the phrase "Because It's There Net," but later changed to "Because It's Time Net." BITNET was simply an early leader in worldwide network communications for the education and research communities. It became the groundwork for the modern Internet's introduction, especially to areas outside the US.

BITNET

BITNET – це широкомасштабна кооперативна комп'ютерна мережа, що об'єднувала мережі різних університетів США. Вона була створена у 1981 році Айрою Фуксом (Міський університет Нью-Йорка) та Грейдоном Фріменом (Єльський університет), а перший мережевий зв'язок встановили саме між цими двома вишами.

Назва спочатку походила від фрази «Because It's There Net», але згодом була змінена на «Because It's Time Net» BITNET була одним із перших лідерів у галузі глобальних мережевих комунікацій для освіти й науки.

Вона стала основою для поширення сучасного Інтернету, особливо поза межами США.

Blackphone

Blackphone is a smartphone introduced in early 2014 featuring a customized encrypted operating system. Designed to enhance user privacy by blocking unauthorized data access and alerting

Blackphone

Blackphone – смартфон, представлений на початку 2014 року. Оснащений налаштованою зашифрованою операційною системою для захисту приватності. Блокує несанк-

users about app data requests. Not entirely NSA-proof but a step toward greater privacy. Priced above average smartphones.

ціонований доступ до даних і повідомляє про запити додатків. Не є повністю захищеним від АНБ, але є кроком до більшої конфіденційності. Має вищу ціну за середній смартфон.

Blended Networking

Blended networking is a form of social interaction that combines online and offline life. This trend shifts focus from purely digital communication to real-life interests like hobbies, sports, and art. For example, social media groups around jogging or tennis often lead to in-person meetups. Unlike online interaction, which centers on personal expression through selfies or opinions, blended networking starts with shared interests and evolves into real-world socializing.

Змішане спілкування

Змішане спілкування — це форма соціальної взаємодії, яка поєднує онлайн- і офлайн-життя. Ця тенденція зміщує фокус із виключно цифрового спілкування на реальні інтереси, як-от хобі, спорт чи мистецтво. Наприклад, соціальні медіа-групи з бігу або тенісу часто переходять у зустрічі в реальному житті. На відміну від онлайн-спілкування, що зосереджується на самовираженні через селфі або думки, змішане спілкування починається зі спільних інтересів і розвивається в реальні контакти.

Blockchain

A blockchain is a tamper-resistant distributed ledger used to validate and store digital transactional records. In decentralized blockchains, no single authority is responsible for maintaining the blockchain. Instead, computers called nodes in a peer-to-peer (P2P) network each store a copy of the ledger. Specialized nodes verify transactions through a decentralized consensus mechanism to reach an agreement on the state of the network.

Transactions are stored in permanent, time-stamped units called blocks, and each block is connected (chained) to the previous block with a cryptographic hash created from the previous block’s data. These hash links make it impossible to alter data in one block without making changes to every subsequent block. Any attempt to alter or delete transactions in a block will break the cryptographic chain and immediately alert all nodes in the network.

Блокчейн

Блокчейн – це захищений від підробок розподілений реєстр, який використовується для підтвердження та зберігання цифрових записів транзакцій. У децентралізованих блокчейнах немає єдиного центру управління. Натомість комп'ютери, які називаються вузлами, в мережі типу «рівний-рівневому» (PP) зберігають копію реєстру. Спеціалізовані вузли перевіряють транзакції за допомогою децентралізованого механізму консенсусу, щоб досягти згоди щодо стану мережі.

Транзакції зберігаються в постійних, датованих одиницях, які називаються блоками. Кожен блок пов'язаний (з'єднаний ланцюжком) з попереднім блоком за допомогою криптографічного хешу, який створюється на основі даних попереднього блоку. Хеш-зв'язки роблять неможливим зміну даних в одному блоці без внесення змін до кожного

Originally created for digital currencies, blockchain is now being used across many industries and organizations. Applications range from smart contracts (computer programs that run on the blockchain) to records management for healthcare, and identity and access management (IAM). Decentralized finance (DeFi), gaming, and metaverse projects also utilize blockchain technology to ensure equal access and ownership of digital assets.

наступного блоку. Будь-яка спроба змінити або видалити транзакції в блоці порушить криптографічний ланцюжок і негайно сповістить усі вузли мережі про проблему.

Спочатку створений для цифрових валют, блокчейн тепер використовується в багатьох галузях та організаціях. Застосування включає розумні контракти, які є комп'ютерними програмами, що працюють на блокчейні, керування записами в охороні здоров'я та управління ідентифікацією та доступом (УІД). Децентралізовані фінанси (ДФ), ігри та метавсесвіт використовують технологію блокчейн для забезпечення рівного доступу та володіння цифровими активами.

Blue Noise

Blue noise is a type of noise with a gentler frequency increase than violet noise and the opposite pattern of pink noise, where intensity decreases. This change is 3 decibels per octave. It’s used in randomization and pattern projection, like dithering in digital images and audio, thanks to its logarithmic nature.

Blue noise increases in volume with increasing frequency, but at a lower rate than a similar kind of noise called violet noise.Blue noise is also known as azure noise.

Синій шум

Синій шум — це тип шуму з менш різким підвищенням частоти, ніж у фіолетового, і протилежним ефектом до рожевого, де інтенсивність зменшується. Ця зміна становить 3 децибели на октаву. Його використовують для рандомізації та проєктування шаблонів, зокрема у дизерингу зображень та аудіо, завдяки логарифмічним властивостям.

Синій шум збільшується в гучності зі збільшенням частоти, але з меншою швидкістю, ніж подібний різновид шуму, який називається фіолетовим шумом. Синій шум також відомий як блакитний.

Blue Wire

Blue wire generally refers to a type of wire or cable that is added to a hardware product at a factory in order to resolve design problems.Blue wires are also known as bodge wires in British.

Синій дріт

Синій дріт зазвичай відноситься до типу дроту або кабелю, який додається до апаратного продукту на заводі, щоб вирішити проблеми з дизайном. У британській англійській

A temporary fix used in hardware production to correct design errors before product shipment. Despite the name, the wire's insulation may be any color. It is often 30 AWG wire, thin and flexible, ideal for quick adjustments or rerouting connections. The term refers to the function, not the color, similar to "purple wire" used in debugging.nglish.

мові сині дроти також відомі як "bodge wires".

Тимчасове рішення, яке застосовується у виробництві для виправлення помилок у дизайні перед відправкою продукції. Назва не означає обов'язково синій колір ізоляції. Часто використовується дріт калібру 30 AWG — тонкий і гнучкий. Термін описує призначення дроту, подібно до «фіолетового дроту», що використовується для налагодження.

Blue-Box

Blue-Box is an electronic device used in the 1960s and 1970s to imitate the tones of a telephone operator's console, typically around 2600 Hz, to control the switching of long-distance calls. It allowed users to enter operator mode and reroute calls without being charged. The device became popular among phone hackers ("phreakers") after key technical details were published in the Bell System Technical Journal. Due to its ability to bypass billing and the difficulty in tracing such calls, it was widely used for illegal purposes.

Синя коробка

Синя коробка – це електронний пристрій, який використовувався у 1960–1970-х роках для імітації тонів телефонного комутатора, зазвичай у діапазоні 2600 Гц, з метою керування комутацією міжміських дзвінків. Дозволяв користувачам переходити в режим оператора і безкоштовно перенаправляти дзвінки. Пристрій став популярним серед телефонних хакерів («фрікерів») після публікації технічної інформації в журналі Bell System Technical Journal. Через можливість обходити оплату та складність відстеження дзвінків активно використовувався з незаконною метою.

BlueJ

BlueJ is an Integrated Development Environment (IDE) for the Java programming language. This software application helps to provide a more precise interface for creating projects and coding in Java. BlueJ was primarily built to assist with user education on object-oriented programming. The interface supports visual views of classes and

BlueJ

BlueJ – це інтегроване середовище розробки (IDE) для мови програмування Java.

Ця програма забезпечує зручний інтерфейс для створення проєктів та написання коду на Java. BlueJ був створений насамперед як навчальний інструмент для вивчення об'єктно-орієнтованого програмування.

coded objects. The idea is that by organizing and presenting visual representations of Java code, tools like BlueJ can make programming more intuitive. Similar to object-oriented studios like MS Visual Basic, BlueJ uses a multi-view approach to show both graphical objects and underlying source code. Users can create new projects, add classes from external files, and work with Java code through a layered, icon-based interface. BlueJ also allows users to compile code within the program. Additional features include a code pad for testing small snippets of Java code, built-in regression testing tools, and multilingual support for international users.

Інтерфейс підтримує візуальне відображення класів і об'єктів коду, що дає змогу краще розуміти структуру програми.

Ідея полягає в тому, що впорядковане візуальне представлення коду Java робить процес програмування доступнішим, особливо для новачків.

Як і в середовищах типу MS Visual Basic, BlueJ використовує багатовидовий підхід — показує як графічні об'єкти, так і вихідний код. Користувачі можуть створювати нові проєкти, імпортувати класи з інших файлів і працювати з кодом через багаторівневий інтерфейс з піктограмами.

BlueJ також дозволяє компілювати код прямо в середовищі розробки.

Серед додаткових функцій: code pad (блокнот коду) для тестування фрагментів Java-коду, інструменти для регресійного тестування та підтримка багатьох мов для користувачів з різних країн.

Body Area Network (BAN)

A body area network (BAN) is a network that includes a collection of wearable devices. It is a specific type of wireless network with a very particular use and scope.

Мережа локального тіла (МЛТ)

Мережа локального тіла (МЛТ) – це мережа, яка включає набір пристроїв, що носяться на тілі. Це специфічний тип бездротової мережі з дуже конкретним застосуванням та охопленням.

Bogon Filtering

Bogon Filtering is the process of dismissing bogus IP address components. A bogon refers to a URL that is typical in denial of service attacks but atypical in legitimate network traffic.

Фільтрація богонів

Фільтрація богонів – це процес відсіювання фіктивних компонентів IP-адрес. Богон – це URL-адреса, яка є типовою для атак на відмову в обслуговуванні, але нетиповою для легітимного мережевого трафіку.

Bogon Filtering is a method to filter out potentially illegitimate or harmful traffic by targeting bogus Internet address prefixes or components. Firewalls and other tools use bogon filtering to eliminate these harmful addresses, and ISPs may offer this service. The term "bogon" comes from "bogus" and "bogosity" and is widely used in IT slang.

Фільтрація богонів – це метод фільтрації потенційно неправомірного або шкідливого трафіку шляхом обробки фіктивних префіксів або компонентів інтернет-адрес. Брандмауери та інші інструменти використовують фільтрацію богонів для усунення таких шкідливих адрес, а інтернет-провайдери можуть пропонувати цей тип послуги користувачам. Термін «богон» походить від слів «богусний» та «богусність» і є загальноприйнятою частиною ІТ-сленгу.

Bohr Bug

A Bohr bug is an error, flaw, or failure that appears under consistent and quantifiable conditions. The Bohr bug is named after the atomic model developed by Danish physicist Niels Bohr. There is a rough similarity, in that like the atomic model, the Bohr bug conforms to certain kinds of logic, in this case, programming logic.

The opposite of a Bohr bug is a Heisenberg bug, one that cannot be easily replicated under commonly defined conditions. Programmers or IT professionals refer to a Bohr bug as a ‘good solid bug’ or an ‘easy bug’ because identifying and fixing it is simply a matter of running the identifiable conditions and checking for errors. By contrast, a Heisenberg bug, as an indeterminate kind of bug, is much more difficult to fix, illustrated, for example, in Ellen Ullman’s groundbreaking IT novel of the 1980s simply titled “The Bug.”

Bohr Bug

Bohr bug – це помилка, недолік або збій, який з'являється за послідовних і кількісно вимірюваних умов. Bohr bug названа на честь атомної моделі, розробленої данським фізиком Нільсом Бором. Існує приблизна схожість у тому, що, як і атомна модель, Bohr bug відповідає певним видам логіки, в даному випадку логіці програмування.

Протилежністю Bohr bug є Heisenberg bug, який важко відтворити за стандартних умов. Програмісти або ІТ-фахівці називають Bohr bug «хорошим стабільним багом» або «легким багом», оскільки його виявлення та виправлення зводиться до відтворення певних умов та перевірки на помилки. На відміну від Bohr bug, Heisenberg bug є невизначеним типом помилки, який значно складніше виправити. Це добре ілюструє, наприклад, новаторський ІТ-роман Елен Ульман 1980-х років, просто названий “The Bug”.

Bonephones

Bonephones are a type of audio device that transmits sound through the bones of the skull, bypassing the eardrum. This technology works on the principle of bone conduction, unlike traditional headphones that deliver sound directly to the ear. While some models of bonephones date back to the 2000s, the idea of sound conduction through bones has a rich history, with innovators, including classical musicians, experimenting with similar concepts for centuries. Bonephones are considered by some to be a safer way to deliver sound, though the audio quality may differ from traditional headphones. They also represent an early step toward technologies like cochlear implants, which provide alternatives to traditional audio input.

Бонефони

Бонефони – це тип аудіообладнання, яке передає звук через кістки черепа, обминаючи барабанну перетинку. Ця технологія працює на принципі кісткової провідності, на відміну від традиційних навушників, які передають звук безпосередньо у вухо. Хоча деякі моделі кісткових навушників з'явилися ще в 2000-х роках, ідея передавання звуку через кістки має багатий історичний досвід, включаючи новаторів, серед яких класичні музиканти, що експериментували з подібними концепціями століттями. Кісткові навушники деякі експерти вважають більш безпечним способом доставки звуку, хоча якість звуку може відрізнятися від традиційних навушників. Вони також є першим кроком до таких технологій, як кохлеарні імпланти, які пропонують альтернативу звичному введенню звуку через зовнішнє вухо.

Boolean Expression

A Boolean expression is one that results in one of two Boolean outcomes, typically true or false. These expressions and operators are key elements in computer science and programming languages.

Boolean expressions are used in many algorithms and code modules. For example, loops or functions can operate based on a Boolean value, or variables can be set using a Boolean expression. While Boolean expressions follow a binary structure (true/false, on/off), they don’t directly relate to the binary structure of machine code, which is a sequence of ones and zeros. Boolean values are logical operators, making them distinct from binary values. This

Булевий вираз

Булевий вираз – це вираз, який має один з двох можливих булевих результатів, зазвичай істину або хибність. Ці вирази та оператори є основною частиною інформатики та мов програмування.

Булеві вирази використовуються в багатьох алгоритмах та модулях коду. Наприклад, цикл або функція може працювати на основі булевого значення, або змінна може бути встановлена відповідно до булевого виразу. Хоча булеві вирази відповідають бінарній структурі (істина/хибність, увімкнено/вимкнено), вони не мають прямого зв'язку з бінарною структурою машинного коду, яка є послідовністю одиниць та нулів. Булеві значення є

difference is a fundamental point that students learn in computer science when studying programming syntax.

логічними операторами, що робить їх відмінними від двійкових значень. Ця різниця є фундаментальною в комп'ютерних науках, коли студенти вивчають синтаксис програмування.

Botnet Attack

A botnet attack is a cyberattack where a network of infected computers (botnet) is used to flood a target—like a website, server, or device—with traffic, aiming to slow it down or disable it. The goal is to disrupt normal operations or degrade service. This often involves a botnet army sending massive amounts of requests, such as pings or emails. A common example is a Distributed Denial of Service (DDoS) attack, which overwhelms a system by bombarding it with simultaneous requests.

Ботнет-атака

Ботнет-атака — це кібератака, у якій мережа заражених комп’ютерів (ботнет) використовується для навантаження цілі — сайту, сервера чи пристрою — великою кількістю трафіку з метою уповільнення або виведення з ладу. Мета — порушити нормальну роботу або знизити якість обслуговування. Зазвичай армія ботів надсилає масові запити, наприклад, ping або електронні листи. Поширений приклад — атака типу DDoS, що перевантажує систему одночасними запитами.

Bottom-up Testing

Bottom-up testing is an integration testing method that starts with testing the lowest components of the code. It refers to a phase where integrated code units are tested together before testing the entire system. IT professionals refer to design assemblies or code module groups tested for functionality in integrated testing environments.

Bottom-up testing contrasts with top-down testing, where higher-level components are tested first. It can create smaller, independent test bases but lacks the skeletal program design of top-down testing. Developers must choose the appropriate testing method based on the project's needs.

Тестування знизу вгору

Тестування знизу вгору – це метод інтеграційного тестування, при якому спочатку тестуються найнижчі компоненти коду. Це етап, коли інтегровані блоки коду тестуються разом перед тестуванням усієї системи. ІТ-фахівці називають дизайнерські збірки або групи модулів коду, які тестуються на функціональність в інтеграційних середовищах.

Тестування знизу вгору протиставляється тестуванню зверху вниз, де спочатку тестуються вищі компоненти. Воно може створювати менші, незалежні тестові бази, але не забезпечує такої ж демонстрації програми, як тестування зверху вниз. Розробники повинні вибрати відповідний метод тестування залежно від потреб проекту.

Bounced email

A bounced email refers to an email message that is not delivered to the recipient and is returned to the sender. This can happen for various reasons such as typographical errors, technical issues, or security concerns. The original email is sent back as an attachment in a new email from either the sender's or the recipient's email server. Common reasons for bounced emails include incorrect email addresses, full inboxes, or security blocks, such as when the sender's email is not on the recipient's allowed list.

Відхилений лист

Відхилений лист – це електронне повідомлення, яке не було доставлено одержувачу і повернулося назад до відправника. Це може статися з різних причин, таких як друкарські помилки, технічні проблеми чи проблеми з безпекою. Оригінальний лист повертається як вкладення в новому електронному листі, надісланому з поштового сервера відправника або одержувача. Найпоширенішими причинами відхилених листів є неправильні адреси електронної пошти, переповнені поштові скриньки або блокування через безпеку, коли електронна пошта відправника не є в дозволеному списку одержувача.

Brain Dump

A brain dump is the act of capturing electronically or memorizing the questions and things in an IT certification examination and then recreating almost an exact replica of the same, for illegal distribution. A brain dump violates most of the non-disclosure agreements provided before an IT certification exam. It can result in loss or ban of any IT certifications as it is considered an illicit tool designed to pass an exam. Most brain dumps are used in IT certification exams or in other exams, where questions rarely change and the certification expense is high. A brain dump is not commonly used in exams where the questions are randomly selected. It is not considered legitimate training or a method for preparing resources for a knowledge test. There is no scientific approach involved, rather just memorizing the entire set of questions and answers. Memorizing content does not demonstrate the much-needed competency in the selected

Brain Dump

Brain Dump – це дія електронного запису або запам'ятовування питань та інформації з іспиту на IT-сертифікацію з подальшим відтворенням майже точної копії для незаконного розповсюдження. Brain Dump порушує більшість угод про нерозголошення інформації, які надаються перед іспитом на IT-сертифікацію. Це може призвести до втрати або заборони будь-яких IT-сертифікатів, оскільки це вважається незаконним інструментом для складання іспиту. Більшість brain dumps використовуються на іспитах з IT-сертифікації або на інших іспитах, де питання рідко змінюються, а витрати на сертифікацію високі. Brain dump зазвичай не використовується на іспитах, де питання обираються випадковим чином. Це не вважається законним навчанням чи методом підготовки ресурсів для тестування знань. Тут немає наукового підходу, а лише зазубрювання всього набору запитань і відповідей. Заучування

domain. It is not a legitimate exam aid for helping candidates succeed in the exam. There is no quality control in brain dumps, and no reasoning is involved in memorizing the answers. There is no scope for real learning in a brain dump. There is no real understanding involved, which is essential for mastering the subject.

матеріалу не демонструє необхідної компетентності у вибраній галузі. Це не є законним засобом підготовки до іспиту для допомоги кандидатам у досягненні успіху при врахуванні специфічних умов іспиту. Контроль якості в brain dump відсутній. Процес заучування відповідей не передбачає логічного мислення. Brain Dump не передбачає справжнього навчання. Відсутнє реальне розуміння предмета, яке необхідне для його вивчення.

Browser Caching

Browser caching is a technique where parts or most of recently used web pages and data are temporarily stored in a web browser. This method helps increase the speed of a user's browsing experience by locally storing web page components in the browser cache. The browser does not store the entire page but focuses on elements that are less likely to change frequently, such as images, logos, banners, and stylesheets (CSS) or scripts (JavaScript). When the user revisits the web page, the browser loads these cached elements instead of downloading them again, resulting in faster load times.

Кешування браузера

Кешування браузера – це техніка, при якій частина або більшість нещодавно використаних веб-сторінок та даних тимчасово зберігаються у веб-браузері. Це використовується для підвищення швидкості перегляду користувачем шляхом локального завантаження компонентів веб-сторінок у кеш браузера. Браузер не зберігає всю веб-сторінку, а фокусується на елементах, які рідко змінюються, таких як зображення, логотипи, банери та стилі CSS чи скрипти JavaScript. Коли користувач повторно відвідує веб-сторінку, браузер завантажує ці кешовані елементи замість того, щоб знову завантажувати їх, що призводить до швидшого завантаження сторінки.

Browser Security Test

A browser security test is an operation performed to determine the security level of a Web browser and its settings and extensions. Various tools and test suites are used to evaluate a browser’s security features, including:

- The type of data broadcast by the browser
- Allowed levels of tracking

Тестування безпеки браузера

Тестування безпеки браузера – це процедура, яка проводиться для визначення рівня захищеності веб-браузера, його налаштувань і розширень. Зазвичай застосовуються спеціальні інструменти й тестові набори, що перевіряють:

- який тип даних передає браузер;

- Presence or absence of software vulnerabilities (exploits)

The goal of a browser security test is to evaluate how well a browser protects user data and systems from malware, tracking, and cyberattacks. Tests typically focus on vulnerabilities in browser code or configuration. When flaws are found, tools may recommend or apply patches. Modern testing often uses off-the-shelf tools, but manual testing (e.g., by ethical hackers) is still common for targeted assessments.

Key browser elements that may be tested include:

- Internet Protocol (IP) address exposure
- JavaScript and Java applet handling
- Flash player
- WebGL (Web Graphics Library)
- Content filtering mechanisms
- Geolocation API

- дозволені рівні стеження за користувачем;
- чи є уразливості (експлойти) в програмному забезпеченні браузера.

Мета тесту – оцінити здатність браузера захищати дані користувача та систему від шкідливих програм і атак. Зазвичай перевіряються вразливості, притаманні коду або налаштуванням браузера. У разі виявлення проблем, інструмент рекомендує або встановлює відповідні патчі.

У сучасній практиці часто використовуються готові рішення, але також поширене ручне тестування – наприклад, коли організація залучає етичного хакера для перевірки безпеки.

Серед перевірених елементів браузера:

- відкритість IP-адреси;
- підтримка JavaScript та Java-аплетів;
- flash-плеєр;
- WebGL (графічна бібліотека);
- фільтри вмісту;
- API геолокації.

BSD daemon

The BSD daemon is a conceptual mascot for the Berkeley Software Distribution (BSD) variations of the open-source UNIX operating system. It symbolizes the BSD programs and is depicted as a red creature with horns and a pitchfork, embodying a playful, open-source spirit. The term "daemon" in IT refers to a background program that operates without user control. Over the years, Beastie has been used in BSD operating system manuals and as a logo. Its creation blends artistic and technical expertise, reflecting the collaborative spirit of the BSD development community.

BSD daemon

BSD daemon є концептуальним талісманом для варіацій операційної системи Berkeley Software Distribution (BSD) з відкритим вихідним кодом UNIX. Він символізує програми BSD і зображений як червона істота з рогами та вилами, уособлюючи грайливий дух відкритого програмного забезпечення. Термін «демон» в IT означає програму, що працює у фоновому режимі без контролю користувача. Протягом років «звірятко» використовувалося в посібниках операційних систем BSD та як логотип. Його створення поєднує художні та технічні навички, відображаючи колективний дух спільноти розробників BSD.

BTS

A BTS is essential in cellular networks and is responsible for creating the individual «cells» in mobile networks such as GSM, CDMA, WiMAX, or LTE. Although the term "BTS" is sometimes used incorrectly to refer to the whole tower, it specifically means the radio equipment responsible for communication.

A BTS performs various tasks, including:

- Encrypting and decrypting communication
- Filtering radio signals (spectrum filtering)
- Managing multiple frequencies and sectors using several transceivers

BTS units are managed by a Base Station Controller (BSC) through a Base Station Control Function (BCF), which connects to the Network Management System (NMS).

Whether integrated or standalone, the BTS's core role remains the same across all wireless technologies.

БТС (BTS)

BTS має важливе значення в стільникових мережах і відповідає за створення окремих «комірок» в мобільних мережах, таких як GSM, CDMA, WiMAX або LTE.

Нерідко термін «БТС» помилково застосовується до всієї вежі мобільного зв'язку, хоча він позначає саме радіообладнання для комунікації.

Основні функції БТС:

- шифрування та дешифрування даних;
- фільтрація радіосигналів;
- робота з кількома частотами та секторами через кілька трансиверів

Керування БТС здійснює Базовий контролер станції (БКС) через Функцію керування базовою станцією (ФКБС), яка підключається до Системи управління мережею (СУМ). Незалежно від типу бездротової технології, призначення БТС залишається незмінним.

Bunny Suit

A bunny suit is a slang term for a protective suit designed to prevent human skin, hair, or other materials from contaminating the environment. These suits, often referred to as «clean suits,» are commonly used in industrial or commercial settings where it is necessary to maintain a controlled atmosphere. For example, they may be used in nanotechnology research or data storage facilities. Some bunny suits are equipped with anti-static features to protect sensitive hardware from static electricity. The suit helps minimize the

Костюм кролика

Костюм кролика — це сленговий термін для захисного костюма, який запобігає потраплянню людської шкіри, волосся або інших матеріалів в контрольоване середовище. Ці костюми часто називають «чистими костюмами», використовуються в промислових або комерційних сферах, де необхідно підтримувати контрольовану атмосферу. Наприклад, їх можуть носити в дослідженнях нанотехнологій або в сховищах даних. Деякі костюми кролика мають антистатичні властивості, щоб захис-

amount of debris that enters the workspace, ensuring a cleaner, safer environment. Specific protocols regarding the use of bunny suits may vary depending on the project and its requirements.

тити чутливе обладнання від статичної електрики. Такі костюми допомагають зменшити кількість дрібного сміття, що потрапляє в робочу зону, забезпечуючи чистіше і безпечніше середовище. Конкретні протоколи носіння костюмів кролика можуть змінюватися залежно від вимог проекту.

Business continuity and disaster recovery

Business continuity and disaster recovery (BCDR or BC/DR) is a set of processes and techniques used to help an organization recover from a disaster and continue or resume routine business operations. It is a broad term that combines the roles and functions of IT and business in the aftermath of a disaster.

BCDR is divided into two different phases/components:

Business Continuity (BC) deals with the business operations side of BCDR. It involves designing and creating policies and procedures that ensure that essential business functions/processes are available during and after a disaster.

BC can include the replacement of staff, service availability issues, business impact analysis and change management.

Disaster Recovery (DR) is primarily focused on the IT side of BCDR. It defines how an organization's IT department will recover from a natural or artificial disaster.

The processes within this phase can include server and network restoration, copying backup data and provisioning backup systems.

Typically, most medium and large enterprises have an integrated BCDR

Безперервність бізнесу та аварійне відновлення

Безперервність бізнесу та аварійне відновлення (ББАВ) – це набір процесів і методів, які допомагають організації відновитися після катастрофи й продовжити або відновити регулярні бізнес-операції.

Це широкий термін, який об'єднує ролі та функції ІТ і бізнесу після катастрофи.

ББАВ поділяється на дві ключові фази/компоненти:

- безперервність бізнесу (ББ) охоплює бізнесову складову ББАВ. Вона включає розробку політик і процедур, які гарантують доступність основних бізнес-функцій під час і після катастрофи.

До таких заходів можуть належати заміна персоналу, забезпечення доступності послуг, аналіз впливу на бізнес і управління змінами.

- аварійне відновлення (АВ) зосереджене на ІТ-аспектах ББАВ. Воно визначає, як ІТ-відділ організації має діяти у відповідь на природні або техногенні катастрофи.

Процеси на цьому етапі можуть включати відновлення серверів і мереж, копіювання резервних даних та активацію резервних систем.

plan or separate BC and DR plans for dealing with unforeseen natural or man-made disasters.

Зазвичай більшість середніх і великих підприємств мають інтегрований план ББАВ або окремі плани ББ і АВ для реагування на непередбачувані ситуації.

Business Intelligence Reporting

Business Intelligence Reporting is a process of collecting, analyzing, and delivering data-driven reports to end users, organizations, or applications through business intelligence (BI) software. BI reporting is typically a built-in feature of BI solutions, which, based on set parameters, automatically generates structured reports in the form of charts, statistics, or text. These reports help in tactical, strategic, and operational decision-making and can be integrated with other systems for further processing.

Звітність бізнес-аналітики

Звітність бізнес-аналітики – це процес збору, аналізу та надання звітів на основі даних кінцевим користувачам, організаціям або застосункам за допомогою програмного забезпечення бізнес-аналітики. Звітність зазвичай є вбудованою функцією BI-рішень, яка, згідно з заданими параметрами, автоматично формує структуровані звіти у вигляді діаграм, статистичних даних або тексту. Такі звіти сприяють тактичному, стратегічному та операційному прийняттю рішень і можуть бути інтегровані з іншими системами для подальшої обробки.

Business process

Business process as a service (BpaaS) is a term for a specific kind of web-delivered or cloud hosting service that benefits an enterprise by assisting with business objectives. In general, a business process is simply a task that must be completed to support business operations. Using the term BpaaS implies that the business process is automated through a remote delivery model.

Бізнес-процес

Бізнес-процес як сервіс (BpaaS) – це термін, що позначає певний тип веб-сервісу або хмарного хостингу, який допомагає підприємству досягати бізнес-цілей.

У загальному розумінні бізнес-процес – це завдання, яке необхідно виконати задля підтримки бізнес-операцій.

Використання терміна BpaaS означає, що цей процес автоматизується та надається дистанційно.

C

Camper

A camper is a video gamer who finds a strategic spot within a level and waits there for players, game-controlled enemies or choice items to appear. This strategy is known as camping.

Camping is most popular in first-person shooter (FPS) games, but depending on the game being played, it is usually considered a form of cheating, or at least a degenerative strategy. This is because if every single player follows a camping strategy, then there won't be any possibilities for players to confront each other, leaving no game to play. Some FPS games can be customized to employ a camping strategy where entire groups are dedicated to sniper-only challenges.

Кемпер

Кемпер – це відеогеймер, який знаходить стратегічне місце на рівні і чекає там на гравців, ворогів, керованих грою, або предметів на вибір. Ця стратегія відома як кемпінг.

Кемпінг найпопулярніший у шутерах від першої особи (FPS), але залежно від гри, в яку грають, він зазвичай вважається формою шахрайства або, принаймні, виродженою стратегією. Це пояснюється тим, що якщо кожен гравець дотримується стратегії кемпінгу, то у гравців не буде жодних можливостей протистояти один одному, і не залишиться жодної гри. Деякі FPS-ігри можна налаштувати так, щоб використовувати стратегію таборування, коли цілі групи займаються виключно снайперськими завданнями.

Capacitive Touch Screen

A capacitive touch screen is a device display screen that relies on finger pressure for interaction. Capacitive touch screen devices are typically handheld, and connect to networks or computers via an architecture that supports various components, including satellite navigation devices, personal digital assistants and mobile phones.

Ємнісний сенсорний екран

Ємнісний сенсорний екран – це екран пристрою, який реагує на натискання пальцем для взаємодії. Пристрої з ємнісним сенсорним екраном зазвичай є портативними і підключаються до мереж або комп'ютерів за допомогою архітектури, яка підтримує різні компоненти, включаючи пристрої супутникової навігації, персональні цифрові асистенти та мобільні телефони.

Chipset

A chipset is a group of interdependent motherboard chips or integrated circuits that control the flow of data and instructions between the central processing unit (CPU) or microprocessor and external devices. A chipset controls external buses, memory cache and some peripherals. A CPU is unable to function without impeccable chipset timing.

A chipset includes the circuit board layout/functionality and circuit mechanisms. Varieties include microprocessors and modem card chipsets. In addition, a CPU has several different chipsets that vary according to architecture.

A chipset is specifically designed for a motherboard. The chipset and motherboard must be compatible with the CPU to prevent system failover. Most chipset drivers are manually updated and installed.

Чіпсет

Чіпсет – це група взаємозалежних мікросхем або інтегральних схем материнської плати, які керують потоком даних та інструкцій між центральним процесором (ЦП) або мікропроцесором і зовнішніми пристроями. Чіпсет контролює зовнішні шини, кеш-пам'ять і деякі периферійні пристрої. Процесор не може функціонувати без бездоганної синхронізації чіпсета.

Набір мікросхем включає в себе макет/функціональність друкованої плати та механізми схеми. Різновиди включають мікропроцесори та набори мікросхем для модемів. Крім того, процесор має кілька різних наборів мікросхем, які відрізняються за архітектурою.

Чіпсет спеціально розроблений для материнської плати. Чіпсет і материнська плата повинні бути сумісними з процесором, щоб запобігти аварійному завершенню роботи системи. Більшість драйверів чіпсета оновлюються та встановлюються вручну.

Cisco EnergyWise

Cisco EnergyWise is a green computing technology that uses a network-based procedure to communicate messages, which helps to calculate and regulate energy between network devices and endpoints. The Cisco EnergyWise technology helps the network to discover Cisco EnergyWise-controllable devices, keep track of their power use, and carry out necessary actions according to business rules in order to cut down their power consumption.

Cisco EnergyWise

Cisco EnergyWise – це технологія «зелених» обчислень, яка використовує мережеву процедуру обміну повідомленнями, що допомагає розраховувати і регулювати енергоспоживання між мережевими пристроями і кінцевими точками. Технологія Cisco EnergyWise допомагає мережі виявляти пристрої, керовані Cisco EnergyWise, відстежувати їх енергоспоживання і виконувати необхідні дії відповідно до бізнес-правил, щоб знизити їх енергоспоживання.

Class C Network

A class C network is the most common of the five computer network classes, designated as A through E, in classful network network addressing architecture. The class designations were based on the split of 32 bits required for an IP address, the first four of which indicated the address classe in binary code.

Although the classful network and the class C network designation were discontinued, network administrators and IT personnel still occasionally make reference to them. Some hardware and software components may also reference them.

Мережа класу

Мережа класу С – це найпоширеніший з п'яти класів комп'ютерних мереж, позначених від А до Е, в архітектурі класової мережевої адресації. Позначення класів ґрунтується на поділі 32 бітів, необхідних для IP-адреси, перші чотири з яких вказують на клас адреси у двійковому коді.

Хоча позначення мережі класу С та мережа класу С більше не використовуються, мережеві адміністратори та IT-персонал все ще іноді згадують про них. Деякі апаратні та програмні компоненти також можуть посилатися на них.

Clean Computing

Clean computing, a subset of green computing, is a concept that refers to the environmentally responsible use, manufacture and disposal of computers, computer peripherals, equipment and other technology products. While green computing refers to the environmental impact of computing as a whole, clean computing is specifically focused on the production of environmental waste.

Чисті комп'ютери

Чисті комп'ютерні технології (англ. Clean computing) – це концепція екологічно відповідального використання, виробництва та утилізації комп'ютерів, комп'ютерних периферійних пристроїв, обладнання та інших технологічних продуктів. У той час як зелені обчислення стосуються впливу обчислювальної техніки на навколишнє середовище в цілому, чисті обчислення зосереджені на виробництві екологічно чистих відходів.

Collaboration Data Objects

Collaboration Data Objects (CDO) is an application programming interface (API) built into Microsoft Server products. CDO provides access to the global address list, mailbox content, public folders and other server objects

Об'єкти даних для спільної роботи

Об'єкти даних для спільної роботи (Collaboration Data Objects, CDO) – це інтерфейс прикладного програмування (API), вбудований у продукти Microsoft Server. CDO надає доступ до глобального списку адрес,

related to messaging and Microsoft Outlook. CDO cannot be used to directly program added functionality to MS Outlook.

The function library of CDO gives developers a convenient way to create, manipulate and send internet messages, which is not possible with applications such as Microsoft Outlook.

Collaboration Data Objects was previously known as OLE Messaging or Active Messaging.

вмісту поштових скриньок, загальних папок та інших серверних об'єктів, пов'язаних з обміном повідомленнями та Microsoft Outlook. CDO не можна використовувати для безпосереднього програмування додаткової функціональності MS Outlook.

Бібліотека функцій CDO надає розробникам зручний спосіб створення, маніпулювання та надсилання інтернет-повідомлень, що є неможливим у таких програмах, як Microsoft Outlook.

Collaboration Data Objects раніше була відома як OLE Messaging або Active Messaging.

Commerce Server

A commerce server is a server that provides the basic components and functions of an online storefront, such as a shopping cart, credit card processing and product displays. Commerce servers also manage and maintain accounting and inventory data, also called back-end data.

A commerce server is a product intended for e-commerce websites or e-commerce applications.

Microsoft is one of the providers of commerce servers. Microsoft Commerce Server was first released in 2000 and was used to creatie e-commerce systems. It uses Microsoft's .NET technology. The latest release was in January 2009 and includes a comprehensive solution for many business scenarios.

Комерційний сервер

Комерційний сервер – це сервер, який забезпечує основні компоненти і функції вітрини інтернет-магазину, такі як кошик для покупок, обробка кредитних карток і відображення товарів. Комерційні сервери також керують і підтримують дані бухгалтерського обліку та інвентаризації, які також називаються внутрішніми даними.

Комерційний сервер – це продукт, призначений для веб-сайтів електронної комерції або додатків електронної комерції.

Microsoft є одним з постачальників комерційних серверів. Microsoft Commerce Server був вперше випущений у 2000 році і використовувався для створення систем електронної комерції. Він використовує технологію NET від Microsoft. Останній реліз відбувся в січні 2009 року і включає в себе комплексне рішення для багатьох бізнес-сценаріїв.

CompactFlash

CompactFlash (CF) is a removable storage device used for mass storage in portable electronic machines, such as PCs. Based on non-volatile technology (flash memory), CF does not require a battery. CF competes with other memory cards and chips, such as SD/MMC and PC card type-I.

CF was launched in 1994 by SanDisk. Memory chips and cards are key electronic device components manufactured according to memory size, physical size, volatile/non-volatile features, compatibility and other specifications. CF technology is also strong in the camera memory market.

CompactFlash

CompactFlash (CF) – це знімний запам'ятовуючий пристрій, який використовується для масового зберігання даних у портативних електронних пристроях, таких як ПК. Заснований на енергонезалежній технології (флеш-пам'яті), CF не потребує батареї. CF конкурує з іншими картами пам'яті та мікросхемами, такими як SD/MMC та PC card type-I.

Технологія CF була запущена в 1994 році компанією SanDisk.

Мікросхеми пам'яті та карти пам'яті – це ключові компоненти електронних пристроїв, які виготовляються відповідно до обсягу пам'яті, фізичного розміру, енергонезалежних/ енергонезалежних характеристик, сумісності та інших специфікацій. Технологія CF також добре зарекомендувала себе на ринку пам'яті для фотоапаратів.

Computational Origami

Computational origami is the set of tools and techniques used to model different materials and paper-folding designs on a computer. Computational origami explains the way a three-dimensional origami structure can be created from two-dimensional paper with the help of several algorithms.

Комп'ютерне орігамі

Комп'ютерне орігамі – це набір інструментів і технік, що використовуються для моделювання різних матеріалів і конструкцій з паперу на комп'ютері. Комп'ютерне орігамі пояснює, як за допомогою декількох алгоритмів можна створити тривимірну структуру орігамі з двовимірного паперу.

Concerns about Facial Recognition

Facial recognition software has come under great scrutiny in the past several years because some companies have leveraged the technology in ways that many people believe violate their privacy rights. These companies

Проблеми з розпізнаванням обличчя

Програмне забезпечення для розпізнавання обличчя піддалося великій критиці за останні кілька років, оскільки деякі компанії використовували цю технологію

surreptitiously collected biometric data from users that were, in some cases, unaware that the data was being collected. The data was then compiled into large databases that were shared, or even sold to third-party entities.

Other concerns around using facial recognition to support a zero trust architecture include:

• The potential for race, gender or age-related biases.

• Compliance concerns about how to collect, retain, and secure images reference templates.

• Privacy concerns about whether or not people who have not opted into a facial recognition system should be notified when their image has been captured.

• Establishing standards and passing legislation to govern law enforcement agencies' use of the technology.

способами, які, на думку багатьох людей, порушують їхні права на приватність. Ці компанії таємно збирали біометричні дані користувачів, які в деяких випадках не знали про збір даних. Потім дані були зібрані у великі бази даних, які були передані або навіть продані стороннім організаціям.

Інші проблеми, пов'язані з використанням розпізнавання обличчя для підтримки архітектури нульової довіри, включають:

• Потенційні упередження щодо раси, статі чи віку.

• Проблеми відповідності щодо збору, зберігання та захисту шаблонів еталонних зображень.

• Проблеми конфіденційності щодо того, чи слід повідомляти людей, які не погодилися на систему розпізнавання обличчя, про те, що їхнє зображення було захоплено.

• Встановлення стандартів та прийняття законодавства для регулювання використання технології правоохоронними органами.

Criticality Level

Criticality level is directly proportional to certain factors and criteria, including required total cost of ownership (TCO), overall operations and enterprise and system downtime and behavior. Numbered systems may be developed for criticality level rating.

Рівень критичності

Рівень критичності прямо пропорційний певним факторам і критеріям, включаючи необхідну сукупну вартість володіння (TCO), загальну операційну діяльність, а також час простою і поведінку підприємства і системи. Для оцінки рівня критичності можуть бути розроблені нумеровані системи.

Cyberbullying

Cyberbullying is a practice where an individual or group uses the Internet to ridicule, harass or harm another person. The social and emotional harm inflicted by cyberbullies grows out of – or leads

Кібербулінг

Кібербулінг – це практика, коли окрема особа або група осіб використовує Інтернет для висміювання, переслідування або заподіяння шкоди іншій людині. Соціальна та

to – physical bullying in the offline world.

Cyberbullying is a prosecutable offense in some jurisdictions, but a globally uniform legal approach has not yet been established.

Cyberbullies use social media and smartphones to harass victims from remote or local areas. Traditional bullying usually stops when a victim returns to the safety of his home, but cyberbullying is a continuous process maintained through email, texting, forum/blog posts and other communication vehicles. Even if cyberbullying victims change profile settings and avoid certain websites, cyberbullies may easily continue public bullying activities.

емоційна шкода, яку завдають кібербулери, виростає з фізичного цькування в офлайн-світі або призводить до нього.

У деяких юрисдикціях кібербулінг карається згідно з законом, але єдиного глобального правового підходу ще не вироблено.

Кібербулери використовують соціальні мережі та смартфони, щоб переслідувати жертв з віддалених або місцевих районів. Традиційний булінг зазвичай припиняється, коли жертва повертається в безпечне місце, але кібербулінг – це безперервний процес, який підтримується за допомогою електронної пошти, текстових повідомлень, повідомлень на форумах/блогах та інших засобів комунікації. Навіть якщо жертви кібербулінгу змінюють налаштування профілю та уникають певних вебсайтів, кібербулери можуть легко продовжувати публічні знущання.

D

Data Access

Data access refers to a user's ability to access or retrieve data stored within a database or other repository. Users who have data access can store, retrieve, move or manipulate stored data, which can be stored on a wide range of hard drives and external devices.

There are two ways to access stored data: random access and sequential access.

Доступ до даних

Доступ до даних – це можливість користувача отримати доступ до даних, що зберігаються в базі даних або іншому сховищі. Користувачі, які мають доступ до даних, можуть зберігати, отримувати, переміщувати або маніпулювати збереженими даними, які можуть зберігатися на різних жорстких дисках і зовнішніх пристроях.

Існує два способи доступу до збережених даних: довільний доступ і послідовний доступ.

Data Administration

Data administration is the process by which data is monitored, maintained and managed by a data administrator and/or an organization. Data administration allows an organization to control its data assets, as well as their processing and interactions with different applications and business processes. Data administration ensures that the entire life cycle of data use and processing is on par with the enterprise's objective.

Адміністрування даних

Адміністрування даних – це процес, за допомогою якого адміністратор даних та/або організація здійснює моніторинг, підтримку та управління даними. Адміністрування даних дозволяє організації контролювати свої активи даних, а також їх обробку та взаємодію з різними додатками та бізнес-процесами. Адміністрування даних гарантує, що весь життєвий цикл використання та обробки даних відповідає цілям підприємства.

Data Breach (Data Spill)

A data breach, also known as a data spill or data leak, refers to an incident that involves the unauthorized or illegal viewing, access, or retrieval of data by a threat actor – a term used to describe an entity capable of potentially attacking an organization's digital infrastructure or network. It is a type of security breach including hacking, malware, phi shing attacks, or even physical theft of devices, specifically aimed at stealing or publishing data to an unsecured or illegal location.

By definition, data breach refers to gaining access to an entity's information *without authorization*. Therefore, not all data breaches are intentional. In some cases, an accidental data breach may occur when protected data is inadvertently exposed. For example, an employee accessing confidential data they are not authorized to view is considered a data breach, regardless of whether the act was intentional or not.

Порушення даних (витік даних)

Порушення даних, також відоме як витік даних, стосується інциденту, пов'язаного з несанкціонованим або незаконним переглядом, доступом або отриманням даних суб'єктом загрози – термін, що використовується для опису суб'єкта, здатного потенційно атакувати цифрову інфраструктуру або мережу організації. Це тип порушення безпеки, що включає хакерство, шкідливе програмне забезпечення, фішингові атаки або навіть фізичну крадіжку пристроїв, спеціально спрямовану на крадіжку або публікацію даних у незахищеному або незаконному місці.

За визначенням, витік даних означає отримання доступу до інформації організації без дозволу. Тому не всі витоки даних є навмисними. У деяких випадках витік даних може статися випадково, коли захищені дані ненавмисно стають доступними. Наприклад, доступ працівника до конфіденційних даних, які він не має права переглядати, вважається порушенням даних, незалежно від того, чи була ця дія навмисною, чи ні.

Data Deduplication

Data deduplication is a data compression technique in which redundant or repeated copies of data are removed from a system. It is implemented in data backup and network data mechanisms and enables the storage of one unique instance of data within a database or information system (IS).

Data deduplication is also known as intelligent compression, single instance storage, commonality factoring or data reduction.

Дедуплікація даних

Дедуплікація даних – це техніка стиснення даних, при якій надлишкові або повторні копії даних видаляються з системи. Він реалізований в механізмах резервного копіювання даних і мережевих даних і дозволяє зберігати один унікальний екземпляр даних в базі даних або інформаційній системі (ІС).

Дедуплікація даних також відома як інтелектуальне стиснення, зберігання одного екземпляра, факторинг спільності або скорочення даних.

Data Transfer Rate

A data transfer rate (DTR) refers to the speed at which a device or network component can send and receive data. This can also be referred to as throughput, although data transfer rate applies specifically to digital data streams. Data transfer is often measured in megabytes per second, although other measurements can also be used.

DTR is important in assessing various devices and technologies. In general, the data transfer rate reflects changes and improvements in digital technologies, where newer systems like solid-state electronics have resulted in much higher data transfer rates within only a few decades.

Швидкість передачі даних

Швидкість передачі даних (DTR) – це швидкість, з якою пристрій або компонент мережі може надсилати та отримувати дані. Її також можна назвати пропускною здатністю, хоча швидкість передачі даних стосується саме цифрових потоків даних. Швидкість передачі даних часто вимірюється в мегабайтах на секунду, хоча можуть використовуватися й інші одиниці виміру.

DTR важлива для оцінки різних пристроїв і технологій. Загалом, швидкість передачі даних відображає зміни та вдосконалення цифрових технологій, де новіші системи, такі як твердотільна електроніка, призвели до значно вищих швидкостей передачі даних всього за кілька десятиліть.

Decision Table

A decision table is used to represent conditional logic by creating a list of tasks depicting business level rules.

Таблиця рішень

Таблиця рішень використовується для представлення умовної логіки шляхом створення списку завдань, що

Decision tables can be used when there is a consistent number of conditions that must be evaluated and assigned a specific set of actions to be used when the conditions are finally met.

Decision tables are fairly similar to decision trees except for the fact that decision tables will always have the same number of conditions that need to be evaluated and actions that must be performed even if the set of branches being analyzed is resolved to true. A decision tree, on the other hand, can have one branch with more conditions that need to be evaluated than other branches on the tree.

відображають правила бізнес-рівня. Таблиці рішень можна використовувати, коли є послідовна кількість умов, які необхідно оцінити і призначити певний набір дій, які будуть використані, коли умови нарешті будуть виконані.

Таблиці рішень досить схожі на систему рішень, за винятком того, що таблиці рішень завжди мають однакову кількість умов, які необхідно оцінити, і дій, які необхідно виконати, навіть якщо набір функцій, що аналізуються, вирішується як істинні. З іншого боку, основа рішень може мати одну варіацію з більшою кількістю умов, які потрібно оцінити, ніж інші приклади розгалужень в системі рішень.

Decryption

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

Дешифрування

Дешифрування – це процес перетворення даних, які стали нечитабельними внаслідок шифрування, назад у незашифровану форму. Під час дешифрування система витягує і перетворює спотворені дані та перетворює їх на тексти і зображення, які легко зрозумілі не тільки читачеві, але й системі. Розшифрування може здійснюватися вручну або автоматично. Також вона може виконуватися за допомогою набору ключів або паролів.

Dedicated IP Address

A dedicated IP address is the permanent assignment of a single and unchanging Internet Protocol (IP) address for a website or network's TCP/IP node. It is provided by a network administrator (NA) or Internet service provider (ISP).

Виділена IP-адреса

Виділена IP-адреса – це постійне призначення єдиної та незмінної адреси інтернет-протоколу (IP) для вебсайту або вузла TCP/IP мережі. Вона надається адміністратором мережі (NA) або інтернет-провайдером (ISP).

To reduce the number of IP addresses, most Internet sites and nodes share IP addresses because they are a finite resource. Generally, a dedicated IP address is only used by a website that requires Secure Sockets Layer (SSL) verification.

Щоб зменшити кількість IP-адрес, більшість інтернет-сайтів і вузлів поділяють IP-адреси, оскільки вони є кінцевим ресурсом. Як правило, виділена IP-адреса використовується лише вебсайтом, який вимагає перевірки рівня безпечних сокетів (SSL).

Desktop Environment (DE)

Desktop environment (DE) is a graphical users interface (GUI) that enables a user to access and manage the important and frequently accessed features and services of an operating system.

A desktop environment is a default interface provided by virtually all modern operating systems, including Windows, Linux, Mac and more. This type of interface was developed to replace the command-line interface, which was used in legacy operating systems such as DOS and Unix. However, a user may still have command-line access for some system-level services that aren't accessible through a desktop environment.

The primary desktop environment is often called simply a desktop.

Середовище робочого столу

Середовище робочого столу – це інтерфейс за замовчуванням, що надається практично всіма сучасними операційними системами, включаючи Windows, Linux, Mac та інші. Цей тип інтерфейсу було розроблено на заміну інтерфейсу командного рядка, який використовувався у старих операційних системах, таких як DOS та Unix. Однак користувач все ще може мати доступ до командного рядка для деяких служб системного рівня, які недоступні через середовище робочого столу.

Основне середовище робочого столу часто називають просто робочим столом.

Digital

Digital means using electronic technology to generate, store, and process data in a format that uses discrete values, typically represented by zero and one. Data is transmitted and stored as strings of zeros and ones, each of which is referred to as bit. These bits are grouped together into bytes to represent data such as numbers, letters, images, or sounds.

Цифровий

Цифровий означає використання електронної технології для створення, зберігання та обробки даних у форматі, що використовує дискретні значення, зазвичай представлені нулем та одиницею. Дані передаються та зберігаються у вигляді рядків нулів та одиниць, кожен з яких називається бітом. Ці біти групуються разом у байти для представлення

This method of computation is known as the binary system (0s and 1s), and although it seems simple, it can be used to represent huge amounts of complex data, such as a song from iTunes or a downloaded movie.

Prior to digital technology, electronic transmission was limited to analog, which conveys data as a continuous stream of electronic signals with varying frequency or amplitude.

таких даних, як числа, літери, зображення або звуки.

Цей метод обчислень відомий як двійкова система (0 і 1), і хоча він здається простим, його можна використовувати для представлення величезних обсягів складних даних, таких як пісня з iTunes або завантажений фільм.

До появи цифрових технологій електронна передача обмежувалася аналоговою, яка передавала дані у вигляді безперервного потоку електронних сигналів зі змінною часто звуку та амплітуди.

DNS Cache Poisoning

DNS cache poisoning is a process by which DNS server records are illegitimately modified to replace a website address with a different address. DNS cache poisoning is used by hackers and crackers to redirect visitors of a particular website to their defined/ desired website.

DNS cache poisoning is also known as DNS spoofing.

Отруєння кешу DNS

Отруєння кешу DNS – це процес, за допомогою якого записи DNS-сервера незаконно змінюються з метою заміни адреси вебсайту на іншу адресу. Отруєння кешу DNS використовується хакерами та зловмисниками для перенаправлення відвідувачів певного вебсайту на визначений/бажаний ними вебсайт.

Domain Name System (DNS)

The Domain Name System (DNS) is called the phonebook of the Internet. When a user types a domain name or website address into the address bar of the browser, the DNS server is responsible for translating the domain name to a specific IP address, driving it to the correct website.

A DNS server is a server that manages the domain name system or DNS protocols, matching Internet domain names and IP addresses. The DNS server

Систему доменних імен (DNS)

Систему доменних імен (DNS) називають телефонною книгою Інтернету. Коли користувач вводить доменне ім’я або адресу вебсайту в адресний рядок браузера, DNS-сервер відповідає за перетворення доменного імені на певну IP-адресу, перенаправляючи його на потрібний вебсайт.

DNS-сервер – це сервер, який керує системою доменних імен або DNS-протоколами, узгоджуючи доменні імена та IP-адреси в Інтернеті. DNS-

may also manage domain resolution services.

In the traditional client/server Internet model, DNS servers are built on specific hardware, and run specialized DNS software to accomplish these goals. In the DNS server, there is a database of domain names, host information, DNS records and network data. The DNS server will search records to return a result. This process allows DNS clients to access the DNS server through a web browser. A process of DNS caching can make this type of work more effective through removing the load of repetitive queries: A DNS cache system will keep a local copy of a DNS lookup so that an operating system (OS) or browser can retrieve it more quickly, and a website's URL can be resolved to a proper IP address more efficiently.

As DNS server designs have evolved, not all DNS servers are still run on individual on-premises hardware pieces. DNS servers can be run through the use of virtual machines in a logically partitioned network.

The versatility of virtualization has ushered in new models for how to achieve the DNS processes that have always been part of Internet data transfer protocols. In a general sense, virtualization and logical partitioning are making the requirement of isolated server function practically obsolete, and allowing stakeholders to consolidate these and other kinds of processes through large mainframe computers in modern data centers.

сервер може також керувати службами дозволу доменів.

У традиційній моделі Інтернету клієнт/сервер DNS-сервери побудовані на спеціальному обладнанні і працюють зі спеціалізованим програмним забезпеченням DNS для досягнення цих цілей. На DNS-сервері є база даних доменних імен, інформація про хост, записи DNS і мережеві дані. DNS-сервер здійснює пошук записів і повертає результат. Цей процес дозволяє клієнтам DNS отримати доступ до DNS-сервера через веббраузер. Процес кешування DNS може зробити цей тип роботи більш ефективним завдяки усуненню навантаження від повторюваних запитів: Система кешування DNS зберігає локальну копію DNS-запиту, щоб операційна система (ОС) або браузер могли отримати її швидше, а URL-адреса вебсайту могла бути ефективніше перетворена у відповідну IP-адресу.

З розвитком дизайну DNS-серверів, не всі DNS-сервери все ще працюють на окремих локальних апаратних засобах. Сервери DNS можна запускати за допомогою віртуальних машин у логічно розділеній мережі.

Універсальність віртуалізації відкрила нові моделі для реалізації процесів DNS, які завжди були частиною протоколів передачі даних в Інтернеті. У загальному сенсі, віртуалізація і логічне розділення роблять вимогу ізольованої роботи сервера практично застарілою і дозволяють зацікавленим сторонам консолідувати ці та інші види процесів на великих мейнфреймах у сучасних центрах обробки даних.

E

Electronic Discovery Reference Model (EDRM)

The Electronic Discovery Reference Model (EDRM) is a highly detailed reference model that is used as a standard for the discovery and recovery of digital data. EDRM's data collection scheme ensures that electronic data is handled in a cost-effective and efficient manner.

Електронна довідкова модель відкриття

Електронна довідкова модель відкриття (англ. Electronic Discovery Reference Model, EDRM) – це деталізована еталонна модель, яка використовується як стандарт для виявлення та відновлення цифрових даних. Схема збору даних EDRM забезпечує економічну та ефективну обробку електронних даних.

Electronic Textile (E-textile)

An electronic textile (E-textile) is a type of fabric that contains electronic elements. In general, the development of electronic textiles supports the idea of wearable computing, or electronic devices worked into garment designs. However, there are other applications of electronic textiles, such as interior design technologies, that also rely on integrating electronic components into fabrics or fibers.

An electronic textile may also be known as a smart textile.

Електронний текстиль

Електронний текстиль – це тип тканини, який містить електронні елементи. Загалом, розробка електронного текстилю підтримує ідею переносних обчислень або електронних пристроїв, що працюють на дизайні одягу. Однак існують і інші застосування електронного текстилю, такі як технології дизайну інтер'єру, які також покладаються на інтеграцію електронних компонентів у тканини або волокна.

Електронний текстиль також може бути відомий як розумний текстиль.

Electronics disposal efficiency (EDE)

Electronics disposal efficiency (EDE) is a performance metric used to evaluate the percentage of electronic disposals that have been completed in an environmentally responsible way. It is used to measure how well organizations dispose of their electronic equipment and waste once it is no longer in use or is depleted.

Ефективність утилізації електроніки (EDE)

Ефективність утилізації електроніки (EDE) – це показник продуктивності, який використовується для оцінки відсотка електронних диспозицій, які були завершені екологічно відповідальним способом. Він використовується для вимірювання того, наскільки добре організації утилізують своє електронне обладнання та відходи, коли воно більше не використовується або виснажується.

Email Server Mean

An email server, or simply mail server, is an application or computer in a network whose sole purpose is to act as a virtual post office. The server stores incoming mail for distribution to local users and sends out outgoing messages. This uses a client-server application model to send and receive messages using Simple Mail Transfer Protocol (SMTP).

An email server may also be known as a mail or message transer agent.

Сервер електронної пошти

Поштовий сервер або просто поштовий сервер – це додаток або комп'ютер у мережі, єдиною метою якого є діяти як віртуальне поштове відділення. Сервер зберігає вхідну пошту для розсилки локальним користувачам і розсилає вихідні повідомлення. Це використовує модель клієнт-серверної програми для надсилання та отримання повідомлень за допомогою простого протоколу передачі пошти (SMTP).

Сервер електронної пошти також може бути відомий як агент передачі пошти або повідомлень.

Email Thread

An email thread is an email message that includes a running list of all the succeeding replies starting with the original email. The replies are arranged visually near the original message, usually in chronological order from the first reply to the most recent. This order is useful for the readers following the conversation because it is arranged in some hierarchical structure and may be arranged from top to bottom or vice versa depending on the email client or email provider used. Usually, the topmost email is the latest one.

Ланцюжок імейлів

Ланцюжок імейлів – це повідомлення електронної пошти, яке містить послідовний список усіх наступних відповідей, починаючи з початкового листа. Відповіді розташовуються візуально поруч з оригінальним повідомленням, зазвичай у хронологічному порядку від першої відповіді до останньої. Такий порядок корисний для читачів, які стежать за перепискою, тому що він має певну ієрархічну структуру і може розташовуватися згори вниз або навпаки, залежно від використовуваного поштового клієнта або постачальника послуг електронної пошти. Зазвичай, верхній лист є найновішим.

Engineer-to-Order Enterprise Resource Planning (ETO ERP)

Engineer-to-Order Enterprise Resource Planning (ETO ERP) is a class of Enterprise Resource Planning (ERP) systems designed to support manufacturer requirements for the

Планування ресурсів підприємства на замовлення

Планування ресурсів підприємства на замовлення – це клас систем планування ресурсів підприємства (ERP), призначених для підтримки вимог виробника до унікальних

unique engineering designs of their customer products. Specific processes are involved in each phase of product manufacturing, including estimates, materials, engineering changes, cost allocation, tracking, communication and customer interaction. Most manufacturing organizations have unique processes, size variations, resources and end products. Thus, not all manufacturing processes are suited to a standard ERP.

інженерних конструкцій їх продукції замовника. Конкретні процеси беруть участь у кожному етапі виробництва продукції, включаючи оцінки, матеріали, інженерні зміни, розподіл витрат, відстеження, спілкування та взаємодію з клієнтами. Більшість виробничих організацій мають унікальні процеси, варіації розмірів, ресурси та кінцеві продукти. Таким чином, не всі виробничі процеси підходять для стандартної ERP.

Enterprise data quality

Enterprise data quality refers to class of software that is designed to organize and maintain stored information so that it can be used effectively by all the different applications in an organization. Enterprise data quality is meant to ensure that all data is accurate, complete, consistent and as up-to-date as possible.

Якість даних підприємства

Якість даних підприємства відноситься до класу програмного забезпечення, призначеного для організації та підтримки збереженої інформації, щоб вона могла ефективно використовуватися всіма різними додатками в організації. Якість даних підприємства призначена для забезпечення того, щоб всі дані були точними, повними, послідовними і якомога актуальнішими.

Enterprise Information System (EIS) Tier

The enterprise information system (EIS) tier, in J2EE architecture, handles enterprise information system software, which provides an enterprise’s critical business information infrastructure. Enterprise information systems include enterprise resource planning systems (ERPs), relational databases and mainframe transaction processing systems.

Інформаційна система підприємства (EIS)

Інформаційна система підприємства (EIS), в J2EE архітектурі, обробляє програмне забезпечення інформаційної системи підприємства, що забезпечує критичну інформаційну інфраструктуру підприємства. Корпоративні інформаційні системи включають системи планування ресурсів підприємства (ERP), реляційні бази даних та системи обробки транзакцій мейнфреймів.

ERP Software

An ERP system is a type of software designed to encompass all aspects of your business. ERP software typically offers a series of connected modules for business processes, such as: Project management; Supply chain management; Risk management and compliance; Customer relationship management; Accounting; Human resources.

ERP software also collects data across all these modules and offers analysis tools to help you gain insights into your business.

Importantly, by providing these modules, ERP software enables all your departments to use the same software platform rather than relying on individual, department-specific solutions. This ensures that information can easily be shared across your company.

Програмне забезпечення ERP

ERP система – це тип програмного забезпечення, призначеного для охоплення всіх аспектів вашого бізнесу. ERP програмне забезпечення зазвичай пропонує ряд підключених модулів для бізнес-процесів, таких як: управління проектами; управління ланцюгами поставок; управління ризиками та комплаєнс; управління відносинами з клієнтами; бухгалтерський облік; людські ресурси.

ERP програмне забезпечення також збирає дані в усіх цих модулях і пропонує інструменти аналізу, які допоможуть вам отримати уявлення про свій бізнес.

Важливо відзначити, що, надаючи ці модулі, програмне забезпечення ERP дозволяє всім вашим відділам використовувати ту саму програмну платформу, а не покладатися на індивідуальні, специфічні для відділу рішення. Це гарантує, що інформація може бути легко передана у вашій компанії.

Event Queue

An event queue is a repository where events from an application are held prior to being processed by a receiving program or system. Event queues are often used in the context of an enterprise messaging system.

Черга подій

Черга подій – це сховище, де події з програми зберігаються до обробки приймаючою програмою або системою. Черги подій часто використовуються в контексті корпоративної системи обміну повідомленнями.

Events Per Second

EPS is primarily part of event logging and management software, which monitors and records every instance of external or internal events a system generates. Typically, the use of EPS varies depending on the underlying

Події в секунду

EPS – це насамперед частина програмного забезпечення для реєстрації та управління подіями, яке відстежує і реєструє кожен випадок зовнішніх або внутрішніх подій, які генерує система. Як правило, використання EPS залежить від

system, application or operational environment.

EPS is also used in network security to help security administrators identify the number of incident or penetration attempts on a system.

базової системи, програми або операційного середовища.

EPS також використовується в мережевій безпеці, щоб допомогти адміністраторам безпеки визначити кількість інцидентів або спроб проникнення в систему.

Exbibyte

An exbibyte (EiB) is a unit of digital information storage used to denote the size of data. It is equivalent to 260, or 1,152,921,504,606,846,976, bytes and equal to 1,024 pebibytes.

Ексбібайт (EiB)

Ексбібайт (EiB) – це одиниця зберігання цифрової інформації, яка використовується для позначення розміру даних. Це еквівалентно 260, або 1,152,921,504,606,846,976, байт і дорівнює 1,024 пебібайт.

Exception

An exception is an abnormal or unprecedented event that occurs after the execution of a software program or application. It is a runtime error of an undesired result or event affecting normal program flow.

An exception is also known also a fault.

Виняток

Виняток становить ненормальна або безпрецедентна подія, яка відбувається після виконання програмного забезпечення або програми. Це помилка виконання небажаного результату або події, що впливає на нормальний потік програми.

Виняток також називають помилкою.

Exchangeable image file format (EXIF)

Exchangeable image file format (EXIF) is a specification that defines data pertaining to images, sounds and tags used in digital still cameras.

EXIF was conceived by the Japan Electronics Industries Development Association (JEIDA) to support and standardize the type of information stored by a digital camera.

Змінний формат файлу зображення (EXIF)

Змінний формат файлу зображення (EXIF) – це специфікація, яка визначає дані, що стосуються зображень, звуків та тегів, які використовуються в цифрових фотоапаратах.

EXIF була задумана Японською асоціацією розвитку електронної промисловості (JEIDA) для підтримки та стандартизації типу інформації, що зберігається цифровою камерою.

Explicit Enhancement Point

An explicit enhancement point is an ABAP source code plug-in provided by SAP beginning in its Enterprise Core component version onwards. Prior to the release of the enterprise Core Component version, objects could be modified by either user-exits, business add-ins or by modifying the standard code of the SAP objects. Explicit enhancement points are part of the enhancement framework provided by SAP for reducing the complexity involved in the customer system landscape. They provide another source code enhancement technique that is flexible and provides upward compatibility.

Явна точка розширення (явне покращення)

Явна точка розширення – це плагін вихідного коду ABAP, що надається SAP починаючи з версії компонента Enterprise Core. До випуску корпоративної версії Core Component об'єкти могли бути змінені або користувачами-виходами, бізнес-надбудовами або зміною стандартного коду об'єктів SAP. Явні точки підвищення є частиною структури вдосконалення, наданої SAP для зменшення складності, пов'язаної з ландшафтом системи клієнтів. Вони забезпечують ще одну гнучку техніку покращення вихідного коду та забезпечують висхідну сумісність.

External Cloud

An external cloud is a cloud solution that exists outside of an organization's physical boundaries. It can be private, public or community-based, as long as it is not located on an organization's property.

An external cloud is similar to a public cloud, but they differ in implementation.

Зовнішня хмара

Зовнішня хмара – це хмарне рішення, яке існує поза фізичними межами організації. Він може бути приватним або громадським, якщо він не перебуває у власності організації.

Зовнішня хмара схожа на публічну хмару, але вони відрізняються реалізацією.

Extremely Large Database (XLDB)

An extremely large database (XLDB) is a database that stores and processes enormous amounts of data and associated records and entries. As the largest database form factor, XLDB is created and managed by very few organizations around the world, typically scientific research institutes that have massive data sets at their disposal.

Надзвичайно велика база даних (XLDB)

Надзвичайно велика база даних (XLDB) – це база даних, яка зберігає та обробляє величезну кількість даних та пов'язаних записів та записів. Як найбільший форм-фактор бази даних, XLDB створюється і управляється дуже небагатьма організаціями по всьому світу, як правило, науково-дослідними інститутами, які мають у своєму розпорядженні масивні набори даних.

F

Fabric-Based Infrastructure

Fabric-based infrastructure (FBI) is an approach that aims to deliver an automated data center solution by integration of hardware and software infrastructures. It calls for delivering a real-time data center infrastructure that is dynamically provisioned, controlled and automated.

FBI primarily combines and unifies hardware and software infrastructure, controlled and managed by an automation solution at the top. It is mainly a vendor-side infrastructure provisioning approach, where the vendor automates the provisioning of servers, storage, software, networking and/or IT, cloud and virtualization environments.

Інфраструктура на основі тканин

Інфраструктура на основі тканин (IOT) – це підхід, спрямований на створення автоматизованого рішення для центру обробки даних шляхом інтеграції апаратної та програмної інфраструктур. Він передбачає створення інфраструктури центру обробки даних в режимі реального часу, яка динамічно надається, контролюється та автоматизується.

IOT в першу чергу об'єднує та уніфікує апаратну та програмну інфраструктуру, яка контролюється та управляється рішенням для автоматизації на верхньому рівні. В основному це підхід до надання інфраструктури на стороні постачальника, коли постачальник автоматизує надання серверів, сховищ, програмного забезпечення, мереж та/або інформаційних технологій, хмарних і віртуалізованих середовищ.

Facebook Like-Gating

Facebook «Like-gating» refers to the practice of forcing Facebook users to like a profiler page in order to see additional content.

Previously, some marketers and other promoters resorted to the practice of setting up Facebook profiles that required users to first «like» the business or organization on Facebook before proceeding. To encourage users to do so, incentives were provided including Facebook Like-gating contests, coupons or other opportunities.

«Накрутка вподобань» у Facebook

Facebook «накрутка вподобань» – це практика примусу користувачів Facebook до вподобання сторінки профайлера для того, щоб побачити додатковий контент.

Раніше деякі маркетологи та інші рекламодавці вдавалися до практики створення профілів у Facebook, які вимагали від користувачів спочатку «вподобати» бізнес або організацію у Facebook, перш ніж продовжити. Щоб заохотити користувачів робити це, були надані стимули, включаючи конкурси, купони та інші можливості для отримання «вподобань» у Facebook.

Facebook Official

"Facebook official" means that a Facebook user has made changes to a page or profile to illustrate some point of information about themselves, thereby making it "official" to a Facebook audience. This term has been coined to describe the effect that Facebook profile information has in the real world.

Experts such as psychologists, counselors, family services providers and others have weighed in on the extent to which Facebook can influence social mores, outlooks, and interactions with others.

«Офіційний представник Facebook»

«Офіційний Facebook» означає, що користувач Facebook вніс зміни до сторінки або профілю, щоб проілюструвати певну інформацію про себе, тим самим зробивши її «офіційною» для аудиторії Facebook. Цей термін був вигаданий, щоб описати ефект, який інформація з профілю Facebook має в реальному світі.

Експерти, такі як психологи, консультанти, працівники сімейних служб та інші, обговорюють те, наскільки Facebook може впливати на соціальні норми, погляди та взаємодію з іншими людьми.

Facsimile

A facsimile, more commonly referred to as a fax, is the transmission of a document or image from one place to another electronically. The document to be sent is scanned and sent over a telephone or Internet connection. A combined scanner and transmitter is usually known as a fax machine. Modern-day Internet connections have greatly reduced the use of fax machines.

A facsimile is also known as a telefax or telecopy.

A fax transmits data electronically over a network connection. Originally this network connection was an analog telephone line, but now the Internet is also being used for this purpose. A document to be sent is treated as an image, scanned and converted into bits and transmitted over the line by the facsimile machine. The facsimile machine on the receiving end takes the whole message in terms of bits and then converts it into image. This image is

Факсиміле

Факсиміле – це передача документа або зображення з одного місця в інше електронним способом. Документ для відправки сканується та відправляється по телефонному або інтернет-з'єднанню. Комбінований сканер і передавач зазвичай називається факсимільним апаратом. Сучасні інтернет-з'єднання значно скоротили використання факсимільних апаратів.

Факсиміле також відомий як телефакс або телекопія.

Факсиміле передає дані електронним способом через мережеве з'єднання. Спочатку таким мережевим з'єднанням була аналогова телефонна лінія, але зараз для цього також використовується Інтернет. Документ для відправки обробляється як зображення, сканується та перетворюється на біти, які передаються по лінії факсимільним апаратом. Факсимільний апарат на приймаючому кінці приймає все повідомлення

either displayed onscreen or printed for the user on receiving end to read. Facsimile technology is still in use, but has largely been replaced by email

у вигляді бітів і потім перетворює його на зображення. Це зображення або відображається на екрані, або друкується для користувача на приймальному кінці для читання. Технологія факсу все ще використовується, але в основному замінена електронною поштою.

Factory Reset

Factory reset is the term used to describe the removal of user data from an electronic device and restore it back to factory settings. It is a software restore and aims at resetting the software found in the device to original manufacturer settings. A factory reset can be used to resolve some software issues associated with the device or simply to wipe all user data from a device.

A factory reset is also known as a hard reset, hardware reset or master reset.

A factory reset effectively removes all the user data, third-party applications, associated application data and settings found on the device. It is similar to hard drive reformatting in a computer. However, data present on other media, such as a secure digital card, is not affected by a factory reset.

Скидання до заводських налаштувань

Скидання до заводських налаштувань – це термін, який використовується для опису видалення користувацьких даних з електронного пристрою та відновлення його до заводських налаштувань. Це програмне відновлення, яке спрямоване на скидання програмного забезпечення, що міститься в пристрої, до оригінальних налаштувань виробника. Скидання до заводських налаштувань можна використовувати для вирішення деяких програмних проблем, пов’язаних із пристроєм, або просто для видалення всіх користувацьких даних з пристрою.

Скидання до заводських налаштувань також відоме як жорстке скидання, апаратне скидання або головне скидання.

Скидання до заводських налаштувань ефективно видаляє всі користувацькі дані, сторонні програми, пов’язані дані та налаштування програм, що містяться на пристрої. Це схоже на форматування жорсткого диска на комп’ютері. Однак дані, що зберігаються на інших носіях, таких як карта SD, не впливають на скидання до заводських налаштувань.

Failure Mode and Effects Analysis

Failure mode and effects analysis (FMEA) is a method for failure analysis. It developed in the middle of the 20th century to examine issues with military IT.

In general, IT professionals can use failure mode and effects analysis (FMEA) as part of a greater reliability study for an IT architecture. Here, the various parts of the system are put together and reviewed to show how they work together.

Аналіз режимів і наслідків відмов

Аналіз режимів і наслідків відмов (АРНВ) – це метод аналізу відмов. Він був розроблений в середині 20-го століття для вивчення проблем з військовими інформаційними технологіями.

Як правило, фахівці з інформаційних технологій можуть використовувати аналіз режимів і наслідків відмов (АРНВ) як частину більш глибокого дослідження надійності інформаційної архітектури. Тут різні частини системи збираються разом і розглядаються, щоб показати, як вони працюють разом.

Failure-Directed Testing

Failure-directed testing, also sometimes called heuristics testing, is a type of software testing that focuses on the most likely errors for a piece of software or a program. This type of testing tries to work more intelligently than blanket or standard testing in order to seek out bugs or glitches and fix them.

Some types of failure-directed testing consist of black box testing, where instead of looking at the source code of a program, programmers run the program and see what happens.

Тестування на відмовостійкість

Тестування, спрямоване на відмову, яке також іноді називають евристичним тестуванням, – це тип тестування програмного забезпечення, який фокусується на найбільш ймовірних помилках у програмному забезпеченні або програмі. Цей тип тестування намагається працювати більш розумно, ніж суцільне або стандартне тестування, щоб знайти помилки або збої та виправити їх.

Деякі типи тестування, спрямованого на відмову, складаються з тестування чорного ящика, де замість того, щоб дивитися на вихідний код програми, програмісти запускають програму і дивляться, що відбувається.

Fax Server

A fax server is a system capable of receiving incoming faxes, sending faxes and distributing faxes over a computer network. Software applications for most operating systems are also available to

Факс-сервер

Факс-сервер – це система, здатна приймати вхідні факси, відправляти факси та розподіляти їх через комп’ютерну мережу. Існують програмні додатки для більшості

make a computer in a network act as a fax server. The incoming fax messages can be stored in any printable file format such as graphics or word processing. A fax server helps in reducing the number of dedicated fax lines needed in an environment or organization.

A fax server consists of four components, namely:

- Fax service manager
- Fax application
- Fax modem
- Network connection and connection to users

операційних систем, які дозволяють перетворити комп'ютер у мережі на факс-сервер. Вхідні факс-повідомлення можуть зберігатися у будь-якому друкованому файловому форматі, наприклад, графічному або текстовому. Факс-сервер допомагає зменшити кількість виділених факс-ліній, необхідних у середовищі чи організації.

Факс-сервер складається з чотирьох компонентів:

- менеджер факс-служби
- факс-додаток
- факс-модем
- мережеве підключення та підключення до користувачів.

Federal Communications Commission

The Federal Communications Commission (FCC) is an independent US government agency regulating interstate and international communication by means of radio, television, satellite and cable. The Federal Communications Commission has the right to issue warnings, impose monetary fines and even revoke licenses for airing inappropriate content.

The mission of the Federal Communications Commission is to ensure availability of national and worldwide communication services to Americans at reasonable cost and without any prejudice or discrimination.

Федеральна комісія зв'язку

Федеральна комісія зі зв'язку (ФКЗ) – це незалежний урядовий орган США, який регулює міждержавний та міжнародний зв'язок за допомогою радіо, телебачення, супутникового та кабельного зв'язку. Федеральна комісія має право виносити попередження, накладати грошові штрафи і навіть відкликати ліцензії за трансляцію неприйнятного контенту.

Місія Федеральної комісії зі зв'язку полягає в забезпеченні доступності національних і міжнародних комунікаційних послуг для американців за розумною ціною і без будь-якої упередженості чи дискримінації.

Federated Application Life Cycle Management

Federated application life cycle management (FALM) is a type of federated architecture approach that deals with multiple stages or phases of an application life cycle, from early

Федеративне управління життєвим циклом додатків

Федеративне управління життєвим циклом додатків (ФУЖЦД) – це тип підходу до федеративної архітектури, який охоплює кілька етапів або фаз життєвого циклу додатка, від ранньої

development to final release. IT professionals may use FALM strategies to promote a multimodal, streamlined or agile process for working across segments of application life cycles.

FLAM is also known as federated ALM.

In general, federated architecture relies on the ability to integrate decentralized or autonomous processes and systems into what is, in some ways, a unified whole. Many federated architecture strategies support information sharing and a controlled exchange of information within a greater IT system. Many federated architecture efforts attempt to arrive at what is called a «federated architecture foundation,» where components still operate autonomously but have a certain degree of integration. Federated architecture strategies can also help break down information silos, where isolated information becomes useless.

розробки до фінального випуску. Фахівці з інформаційних технологій можуть використовувати стратегії ФУЖЦД для просування мультимодального, впорядкованого або гнучкого процесу для роботи в різних сегментах життєвого циклу додатків.

ФУЖЦД також відоме як федеративне УЖЦД.

Загалом, федеративна архітектура ґрунтується на здатності інтегрувати децентралізовані або автономні процеси та системи в те, що певним чином є єдиним цілим. Багато стратегій федеративної архітектури підтримують обмін інформацією та контрольований обмін інформацією в рамках більшої IT-системи. Багато зусиль у сфері федеративної архітектури спрямовані на створення так званого «фундаменту федеративної архітектури», де компоненти все ще працюють автономно, але мають певний ступінь інтеграції. Стратегії федеративної архітектури також можуть допомогти зруйнувати інформаційні силоси, де ізольована інформація стає марною.

Feed Aggregator

A feed aggregator is a type of software that brings together various types of Web content and provides it in an easily accessible list. Feed aggregators collect things like online articles from newspapers or digital publications, blog postings, videos, podcasts, etc.

A feed aggregator is also known as a news aggregator, feed reader, content aggregator or an RSS reader.

Feed aggregators can be built into websites, email technologies or other applications. They are generally easy for

Агрегатор стрічки

Агрегатор стрічки – це тип програмного забезпечення, який об’єднує різні типи вебвмісту і надає його у вигляді легкодоступного списку. Агрегатори стрічок збирають такі речі, як онлайн-статті з газет або цифрових видань, публікації в блогах, відео, подкасти тощо.

Агрегатор стрічок також відомий як агрегатор новин, програма для читання стрічок, агрегатор контенту або програма для читання стрічок.

Агрегатори новин можна вбудовувати в веб-сайти, технології елек-

users to either use or ignore, or unsubscribe from if they are placed in a particular area of an end-user application.

тронної пошти або інші програми. Користувачі можуть легко використовувати їх або ігнорувати, або відписатися від них, якщо вони розміщені в певній області програми кінцевого користувача.

Female Connector

A female connector is a type of connector that consists of a jack into which a male connector can be inserted. It is usually present at the end of a cable or other hardware such that a secure physical and electrical connection between two or more devices is made possible. A male connector can be converted into a female connector and vice versa by a tool called a gender changer.

A female connector is a connector used for electrical, physical or data transfer. A female connector has one or more holes into which a male connector can attach its exposed plug-type conductor firmly for a reliable connection.

Гніздовий роз'єм

Гніздовий роз'єм – це тип роз'єму, який складається з гнізда, в яке можна вставити штекер. Зазвичай він присутній на кінці кабелю або іншого обладнання, щоб забезпечити надійне фізичне та електричне з'єднання між двома або більше пристроями. Чоловічий роз'єм можна перетворити на жіночий і навпаки за допомогою інструменту, який називається гендер-чейнджер.

Гніздовий роз'єм – це роз'єм, який використовується для електричної, фізичної передачі або передачі даних. Гніздовий роз'єм має один або кілька отворів, в які чоловічий роз'єм може міцно вставити свій відкритий провідник штекерного типу для надійного з'єднання.

Fencepost Error

A fencepost error is a specific type of off-by-one error that has to do with unlikely or misunderstood algorithms for development.

Fencepost errors are also known as telegraph pole errors and lamppost errors.

At the heart of the fencepost error is the idea that the number of posts used for a fence project differs based on whether the fence is long with two opposite ends, or whether it circles back to a closed loop.

Помилка парканного стовпа

Помилка «стовпчик» – це специфічний тип помилок, які пов'язані з малоймовірними або неправильно зрозумілими алгоритмами розробки.

Помилки парканного стовпа також відомі як помилки телеграфного стовпа і помилки ліхтарного стовпа.

В основі помилки fencepost лежить ідея, що кількість стовпів, які використовуються для проекту огорожі, відрізняється залежно від того, чи є паркан довгим з двома протилежними кінцями, чи він замикається в петлю.

Fiber Laser

A fiber laser is a special type of laser in which the beam delivery as well as the laser cavity is integrated into a single system inside an optical fiber with the beam generated within the fiber, unlike conventional lasers where the beam is generated outside and sent into the system. Considered as a special category of solid state laser, fiber lasers provide many benefits compared with other laser technologies, such as:

- Maintenance-free operation
- Ease of use
- High reliability
- High integration capability

Волоконний лазер

Волоконний лазер – це особливий тип лазера, в якому доставка променя, а також лазерна порожнина інтегровані в єдину систему всередині оптичного волокна, причому промінь генерується всередині волокна, на відміну від звичайних лазерів, в яких промінь генерується ззовні і спрямовується в систему. Волоконні лазери, що розглядаються як особлива категорія твердотільних лазерів, мають багато переваг у порівнянні з іншими лазерними технологіями, такими як

- Експлуатація без технічного обслуговування
- Простота використання
- Висока надійність
- Висока інтеграційна здатність

Fiber Media Converter

A fiber media converter is a networking device that allows connecting two different media types, such as a twisted pair or coaxial cable to a fiber-optic cable. This type of device is very important as it allows interconnecting fiber-optic networks and cable systems with pre-existing copper-based cabling systems. This allows for partial upgrades of network infrastructure into fiber-optic technology and for interconnection with other types of communication networks.

Fiber media converters are designed to support most data communication protocols such as Ethernet and Fast Ethernet, Gigabit Ethernet, E3/DS3 and T1/J1/E1. To support a wide variety of communication protocols, they must

Оптоволоконний медіаконвертер

Оптоволоконний медіаконвертер – це мережевий пристрій, який дозволяє з'єднати два різних типи носіїв, наприклад, виту пару або коаксіальний кабель з оптоволоконним кабелем. Цей тип пристроїв дуже важливий, оскільки дозволяє з'єднувати волоконно-оптичні мережі та кабельні системи з мідними кабельними системами. Це дозволяє частково модернізувати мережеву інфра-структуру до волоконно-оптичної технології та з'єднати її з іншими типами мереж зв'язку.

Оптоволоконні медіаконвертери призначені для підтримки більшості протоколів передачі даних, таких як Ethernet і Fast Ethernet, Gigabit Ethernet, E3/DS3 і T1/J1/E1. Щоб

also support the cable types supported by those protocols such as coaxial and twisted pair to be connected to single- or multi-mode fiber-optic cables.

Fiber Optic Adapter

A fiber optic adapter or coupler is a special connector designed to mate or connect two ends of a fiber optic cable with high precision. The adapter uses a simple design: the ends of two separate fiber optic cables with fiber optic connectors fit into two slots opposite each other. The slots are designed to precisely align the two ends so that there is minimal to no signal loss.

Fiber optic adapters mate two ends of different fibers; hence they are also called couplers. There are versions that connect single fibers together (simplex); others connect two fibers for duplex mode, and some even connect up to four fibers.

Precision mating is done through the alignment sleeves, which are made of either ceramic or metal such as copper in order to provide rigid support for the connectors, whereas the body of the connector itself is made of plastic. There are fiber optic adapters/couplers made for every type of fiber optic connector available.

підтримувати широкий спектр протоколів зв'язку, вони також повинні підтримувати типи кабелів, що підтримуються цими протоколами, такі як коаксіальна і вита пара для підключення до одно- або багатомодових волоконно-оптичних кабелів.

Волоконно-оптичний адаптер

Волоконно-оптичний адаптер або з'єднувач – це спеціальний з'єднувач, призначений для з'єднання двох кінців волоконно-оптичного кабелю з високою точністю. Адаптер має просту конструкцію: кінці двох окремих волоконно-оптичних кабелів з волоконно-оптичними роз'ємами вставляються в два гнізда навпроти один одного. Гнізда призначені для точного вирівнювання двох кінців, так що втрати сигналу зводяться до мінімуму або взагалі відсутні.

Волоконно-оптичні адаптери з'єднують два кінці різних волокон, тому їх ще називають з'єднувачами. Існують версії, які з'єднують окремі волокна разом (симплекс); інші з'єднують два волокна для режиму двостороннього зв'язку, а деякі навіть з'єднують до чотирьох волокон.

Точне з'єднання здійснюється за допомогою вирівнювальних вставок, які виготовляються з кераміки або металу, наприклад, міді, щоб забезпечити жорстку підтримку роз'ємів, тоді як корпус самого роз'єму виготовляється з пластику. Існують волоконно-оптичні адаптери/ з'єднувачі для кожного типу волоконно-оптичних роз'ємів.

Fiber Optic Coupler

A fiber optic coupler is an optical device capable of connecting one or more fiber ends in order to allow the transmission of light waves in multiple paths. The device is capable of combining two or more inputs into a single output and also dividing a single input into two or more outputs. Compared to a splice or connector, the signal can be more attenuated by fiber optic couplers, as the input signal can be divided amongst the output ports.

Fiber optic couplers can broadly be classified as active or passive devices. An external power source is required for active fiber optic couplers, whereas no power is required for operation of passive fiber optic couplers. There are different types of fiber optic couplers such as X couplers, combiners, splitters, stars and trees.

Волоконно-оптичний з'єднувач

Волоконно-оптичний з'єднувач – це оптичний пристрій, здатний з'єднати один або кілька кінців волокна, щоб забезпечити передачу світлових хвиль у декількох напрямках. Пристрій здатний об'єднувати два або більше входів в один вихід, а також розділяти один вхід на два або більше виходів. У порівнянні зі з'єднувачем або роз'ємом, оптоволоконні муфти дозволяють послабити сигнал, оскільки вхідний сигнал може бути розподілений між вихідними портами.

Волоконно-оптичні з'єднувачі можна класифікувати як активні або пасивні пристрої. Для активних волоконно-оптичних з'єднувачів потрібне зовнішнє джерело живлення, тоді як для роботи пасивних волоконно-оптичних з'єднувачів живлення не потрібне. Існують різні типи волоконно-оптичних з'єднувачів, такі як Х-подібні з'єднувачі, комбінатори, розгалужувачі, зірки і дерева.

Fiber Optic Sensor

A fiber optic sensor is a sensing device that uses fiber optic technology for measuring physical quantities such as temperature, pressure, strain, voltages and acceleration, to name a few. In particular, it uses an optical fiber as the sensing element, called an intrinsic sensor, or uses it to transport signals from the remote sensor to the signal processing module (extrinsic sensor). Fiber optic sensors are immune to electromagnetic interference and can handle extreme conditions, so they are gaining popularity as the sensor of choice for many industries.

Волоконно-оптичний датчик

Волоконно-оптичний датчик – це чутливий пристрій, який використовує волоконно-оптичну технологію для вимірювання фізичних величин, таких як температура, тиск, деформація, напруга, прискорення та інші. Зокрема, він використовує оптичне волокно як чутливий елемент, який називається внутрішнім датчиком, або використовує його для транспортування сигналів від віддаленого датчика до модуля обробки сигналів (зовнішній датчик). Оптоволоконні датчики несприйнятливі до електромагнітних

Sensors use optical fibers in different ways, depending on the application of the former. Primarily, an optical fiber is used because of its small size or because it has little to no power requirement at the remote location. Another reason, however, is that many sensors can be multiplexed along the length of the fiber by using a different light wavelength shift for each sensor or by sensing the time it takes for light to travel along the fiber through each different sensor.

перешкод і можуть працювати в екстремальних умовах, тому вони набувають все більшої популярності як датчики вибору для багатьох галузей промисловості.

Датчики використовують оптичні волокна по-різному, залежно від їхнього застосування. В першу чергу, оптичне волокно використовується через його малий розмір або через те, що воно майже не потребує живлення у віддаленому місці. Інша причина полягає в тому, що багато датчиків можна об'єднати по довжині волокна, використовуючи різний зсув довжини світлової хвилі для кожного датчика або вимірюючи час, необхідний для проходження світла по волокну через кожен окремий датчик.

Fiber Optic Switch

A fiber optic switch is a communication control device used in different applications across different sectors, but it is mostly known for optical fiber networking.

In computer networking, a fiber optic switch is used to send and receive data transmissions as well as to determine where each data packet needs to go, much like a common networking switch. The advantage lies in the speed and bandwidth that is available to an optical fiber network. Reliability is also enhanced since light signals are not affected by interference from electromagnetic waves, so noise is not an issue with fiber optic technology.

Оптоволоконний комутатор

Оптоволоконний комутатор – це пристрій управління зв’язком, який використовується в різних сферах застосування в багатьох галузях, але найбільше він відомий завдяки оптоволоконним мережам.

У комп’ютерних мережах оптоволоконний комутатор використовується для надсилання та отримання даних, а також для визначення місця призначення кожного пакета даних, подібно до звичайного мережевого комутатора. Перевага полягає у швидкості та пропускній здатності, які забезпечує оптоволоконна мережа. Надійність також підвищується, оскільки на світлові сигнали не впливають перешкоди від електромагнітних хвиль, тому шум не є проблемою для волоконно-оптичної технології.

Fiber Optic Termination

Fiber optic termination refers to the physical termination of a length of a fiber optic cable into one of many types of connectors. The type of connector to be used in the termination depends on the type of cable and application. The reason for the termination is either to create a connection to a device or transceiver, to splice two cables into one longer cable or to multiplex a cable so that it can move more branches.

Fiber optic termination is a necessary step for installing a fiber optic network. Since any mistakes may result in the system functioning unreliably, this step must be performed correctly. Much attention has been given to this area, so more and more products are being developed to make the process easier and more accurate.

Закінчення волоконно-оптичного кабелю

Волоконно-оптичне закінчення – це фізичне закінчення довжини волоконно-оптичного кабелю в один з багатьох типів конекторів. Тип роз'єму, який буде використовуватися при термінації, залежить від типу кабелю і застосування. Причиною закінчення є або створення з'єднання з пристроєм або приймачем, або з'єднання двох кабелів в один довший кабель, або багатоканальне розділення кабелю, щоб він міг переміщати більше відгалужень.

Закінчення оптоволокна є необхідним етапом для встановлення оптоволоконної мережі. Оскільки будь-які помилки можуть викликати ненадійну роботу системи. Цей крок повинен бути виконаний правильно. Цьому питанню приділяється багато уваги, тому розробляється все більше і більше продуктів, щоб зробити цей процес простішим і точнішим.

Fiber Optic Transceiver

A fiber optic transceiver is a device that uses fiber optical technology to send and receive data. The transceiver has electronic components to condition and encode/decode data into light pulses and then send them to the other end as electrical signals. To send data as light, it makes use of a light source, which is controlled by the electronic parts, and to receive light pulses, it makes use of a photodiode semiconductor.

Data can usually travel only one way in a fiber optic cable, so most transceivers have two ports for bidirectional communication: one for sending and the other for receiving signals. Alternatively, a single cable can

Оптоволоконний приймач

Оптоволоконний приймач – це пристрій, який використовує оптоволоконну технологію для надсилання та отримання даних. Приймач має електронні компоненти, які формують і кодують/декодують дані у світлові імпульси, а потім надсилають їх на інший кінець у вигляді електричних сигналів. Для надсилання даних у вигляді світла використовується джерело світла, яке контролюється електронними компонентами, а для отримання світлових імпульсів – напівпровідниковий фотодіод.

Зазвичай дані можуть рухатися лише в одному напрямку по оптоволоконному кабелю, тому більшість

be used, but it can only send or receive data at a time but not both. The opposite end of the transceiver has a special connector for fitting it into specific models of enterprise-grade Ethernet switches, firewalls, routers and network interface cards.

приймачів мають два порти для двонаправленого зв'язку: один для надсилання, а інший – для прийому сигналів. Крім того, можна використовувати один кабель, але він може одночасно надсилати або приймати дані, але не те й інше. Протилежний кінець приймача має спеціальний роз'єм для підключення до певних моделей Ethernet-комутаторів, брандмауерів, мережевих інтерфейсних карт корпоративного класу.

Fiber Pigtail

A fiber pigtail is a specific hardware connection used for cable termination. On a fiber pigtail, one end of the wire is simply exposed fiber and the other end has a pre-installed connector on it. Fiber pigtails are commonly spliced onto individual strands of a multi-fiber trunk cable.

One of the ideas behind fiber pigtails is that, by splicing the various wires of a multi-fiber trunk, network professionals can create a set of connections to end-point devices. These installations may also be connected to patch panels or used to achieve mounting where precision alignment of hardware components is important. Fiber pigtails may be used in the process of cable jetting, where communications engineers use modern methods to install cables in hard-to-reach areas.

Оптоволоконний косинець

Оптоволоконний косинець – це специфічне апаратне з'єднання, яке використовується для термінації кабелю. На волоконному косинці один кінець дроту – це просто відкрите волокно, а інший кінець має попередньо встановлений з'єднувач. Волоконні косички зазвичай зрощуються на окремих нитках багатоволоконного магістрального кабелю.

Одна з ідей волоконно-оптичних косичок полягає в тому, що, зрощуючи різні дроти багатоволоконної магістралі, мережеві фахівці можуть створити набір з'єднань з кінцевими пристроями. Ці установки також можуть бути підключені до комутаційних панелей або використані для монтажу, де важливим є точне вирівнювання апаратних компонентів. Оптоволоконні косички можуть використовуватися в процесі струменевого прокладання кабелю, коли інженери зв'язку застосовують сучасні методи для прокладання кабелів у важкодоступних місцях.

File

A file is a container in a computer system for storing information. Files used in computers are similar in features to that of paper documents used in library and office files. There are different types of files such as text files, data files, directory files, binary and graphic files, and these different types of files store different types of information. In a computer operating system, files can be stored on optical drives, hard drives or other types of storage devices.

Файл

Файл – це контейнер у комп'ютерній системі для зберігання інформації. Файли, які використовуються в комп'ютерах, схожі на паперові документи, що зберігаються у бібліотеках та офісах. Існують різні типи файлів, такі як текстові файли, файли даних, файлові каталоги, бінарні та графічні файли, і ці різні типи файлів зберігають різну інформацію. У комп'ютерній операційній системі файли можуть зберігатися на оптичних носіях, жорстких дисках або інших типах пристроїв зберігання даних.

File Transfer Protocol With SSL Security

File Transfer Protocol with SSL Security (FTPS) is an extension to the FTP protocol that adds Secure Socket Layer (SSL)/Transport Layer Security (TLS)-based mechanisms/capabilities on a standard FTP connection. It mainly enables performing or delivering standard FTP communication on top of an SSL-based security connection.

FTPS is also known as FTP Secure.

FTPS is mainly used to provide secure server-to-server communication; however, it can also be used to access a server from desktop or end-user devices.

FTPS uses a combination of symmetric (Data Encryption Standard (DES)/Advance Encryption Standard (AES)) and asymmetric (Rivest-Shamir-Adleman (RSA)/Digital Signature Algorithm (DSA)) algorithms to deliver security and uses X.509 certificates for authentication.

Протокол передачі файлів із захистом SSL

Протокол передачі файлів із захистом SSL (FTPS) – це розширення протоколу FTP, яке додає до стандартного FTP-з'єднання механізми/можливості, засновані на захисті на рівні захищених сокетів (SSL) і транспортному рівні (TLS). Він головним чином дозволяє здійснювати або передавати стандартне FTP-з'єднання на основі захищеного SSL-з'єднання.

FTPS також відомий як FTP Secure.

FTPS в основному використовується для забезпечення безпечної серверної комунікації «сервер-сервер», однак він також може використовуватися для доступу до сервера з настільних або кінцевих користувацьких пристроїв. FTPS використовує комбінацію симетричних (Data Encryption Standard (DES)/Advanced Encryption Standard (AES)) та асиметричних (Rivest-Shamir-Adleman (RSA)/Digital Signature Algorithm (DSA)) алгоритмів для забезпечення безпеки і використовує сертифікати X.509 для автентифікації.

Filler Text

Filler text is text that has all the characters of a language, but they are randomly written in such a way that they do not make any sense to the reader. Filler text is most commonly used in prototype layouts by publishers or designers to show what the text would look like in terms of fonts and formatting.

Filler text is also known as dummy text or placeholder text.

Filler text is type of sample text displayed to test the fonts and layout of a project. It is also sometimes used to spoof email spam filters. The characters in filler text are arranged such that they do not form coherent words in the readers' language — as in case of lorem ipsum, a commonly used filler text scheme derived from Latin.

Філерний текст (текстовий заповнювач)

Філерний текст – це текст, який містить усі символи мови, але вони написані випадково так, що не мають сенсу для читача. Філерний текст найчастіше використовується в прототипах макетів видавцями або дизайнерами, щоб показати, як текст виглядатиме з точки зору шрифтів і форматування.

Філерний текст також відомий як фіктивний текст або текстовий заповнювач.

Філерний текст – це тип зразкового тексту, який відображається для тестування шрифтів і макета проекту. Його також іноді використовують для обману спам-фільтрів електронної пошти. Символи у філерному тексті розташовані таким чином, що вони не утворюють зв'язних слів мовою читача, як у випадку з lorem ipsum, широко використовуваною схемою філерного тексту, що походить від латини.

Finger Vein Recognition

Finger vein recognition is a process wherein a person's finger vein patterns are used as a basis for biometric authentication. Images are taken of one's finger vein patterns and then verified through pattern-recognition techniques.

The algorithm used for pattern matching varies from vendor to vendor. However, differences in apparatus do not affect the output since the basis for authentication — one's veins — remains relatively the same. Compared to commonly used biometric authentication methods, finger vein recognition has a higher security level because it is found inside the body and cannot be duplicated or removed.

Розпізнавання вен на пальцях

Розпізнавання вен на пальцях – це процес, в якому візерунки вен на пальцях людини використовуються як основа для біометричної автентифікації. Зображення візерунків вен на пальцях рук фотографуються, а потім перевіряються за допомогою методів розпізнавання образів.

Алгоритм, що використовується для зіставлення зразків, відрізняється в різних виробників. Однак відмінності в обладнанні не впливають на результат, оскільки основа для автентифікації – вени – залишається відносно однаковою. Порівняно із загальновживаними методами біометричної автентифікації, розпізнавання вен на пальцях має вищий рівень безпеки, оскільки вони знаходяться всередині тіла і не можуть бути скопійовані або видалені.

Finite Element Analysis

Finite element analysis (FEA) is a computerized analysis method to envisage how a manufactured product will react to the physical world. The analysis includes bringing the product in contact with force, heat, vibration, fluid flow and other such physical conditions. The FEA can predict if the product is likely to break, tear, wear or behave the way it is manufactured to.

First developed in 1943 by R. Courant, finite element analysis is a part of the manufacturing process in order to help predict how an object would react to real-world conditions when used. FEA also helps solid-state scientists to improve the quality and function of an object.

Скінченно-елементний аналіз

Скінченно-елементний аналіз (СЕА) – це комп'ютерний метод аналізу, який дозволяє передбачити, як виготовлений продукт реагуватиме на фізичний світ. Аналіз включає вплив на продукт сили, тепла, вібрації, потоку рідини та інших подібних фізичних умов. FEA може передбачити, чи може продукт зламатися, порватися, зноситися або поводитися так, як передбачено при його виготовленні.

Розроблений у 1943 році Р. Курантом, скінченно-елементний аналіз є частиною виробничого процесу, який допомагає прогнозувати, як об'єкт реагуватиме на реальні умови під час використання. СЕА також допомагає вченим у галузі фізики твердого тіла покращувати якість і функціональність об'єкта.

Five Nines

Five nines is the term used for describing the availability of a computer or a service at 99.999 percent of the time it is required. In other words, the system or service is only unavailable for 5.39 minutes throughout the year for planned or unplanned downtime. Five nines is recommended and required for mission-critical requirements and for certain areas such as e-commerce. However, five nines availability has always been a challenge for a service or network and is often impossible to guarantee.

Five nines ensures high availability and reliability of the computer or service. It is often the desired percentage availability of a given system or service. However, there is no ruling committee or

«П'ять дев'яток»

«Five Nines» (або «п'ять дев'яток») – це термін, що використовується для опису доступності комп'ютера або сервісу на рівні 99,999% від необхідного часу. Іншими словами, система або сервіс недоступні лише протягом 5,39 хвилин на рік через заплановані або незаплановані простої. Такий рівень доступності рекомендується та є необхідним для критично важливих задач і для певних сфер, таких як електронна комерція. Однак досягнення п'яти дев'яток завжди є складним завданням для будь-якої служби чи мережі, і часто його неможливо гарантувати.

«Five Nines» гарантує високу доступність і надійність комп'ютера

body which formalizes the meaning or definition of five nines. In order to achieve five nines, most employ monitoring systems in order to proactively resolve all issues.

або сервісу. Це часто бажаний рівень доступності для певної системи чи сервісу. Однак немає офіційного комітету або органу, який би формалізував значення або визначення «п'яти дев'яток». Щоб досягти такого рівня, зазвичай використовуються системи моніторингу для проактивного вирішення всіх проблем.

Flash Storage

Flash storage describes any type of long-term storage repository supported by flash memory. Flash storage may also be referred to as solid state storage.

Unlike traditional hard disk drive storage, flash storage has no mechanical parts which makes it a good choice for storage in mobile technology. Flash storage comes in a variety of formats and prices, ranging from inexpensive consumer-grade USB drives to enterprise-level all flash arrays.

Flash storage makes use of flash memory, which stores data in an array of memory cells. The cells can range from traditional single cell to multi-level cells.

Compared to hard drives, flash storage drives provides many advantages, including faster read and write times. Flash memory's quick access to stored data and fast processing capabilities makes it more business-friendly than traditional storage options.

Флеш-накопичувач

Флеш-накопичувач описує будь-який тип сховища даних довготривалого зберігання, що підтримується флеш-пам'яттю. Флеш-накопичувач також може називатися твердотільною пам'яттю.

На відміну від традиційних жорстких дисків, флеш-накопичувач не має механічних частин, що робить його гарним вибором для зберігання даних у мобільних пристроях. Флеш-накопичувачі бувають різних форматів і цін, від недорогих USB-накопичувачів споживчого класу до флеш-масивів корпоративного рівня.

У флеш-накопичувачі використовується флеш-пам'ять, яка зберігає дані в масиві комірок пам'яті. Комірки можуть бути як традиційними одинарними, так і багаторівневими. Порівняно з жорсткими дисками, флеш-накопичувачі мають багато переваг, зокрема швидший час читання та запису. Швидкий доступ флеш-пам'яті до збережених даних і швидкі можливості обробки роблять її більш зручною для бізнесу порівняно з традиційними варіантами зберігання.

Flat Panel Display

A flat panel display is a television, monitor or other display appliance that uses a thin panel design instead of a traditional cathode ray tube (CRT) design. These screens are much lighter and thinner, and can be much more portable than traditional televisions and monitors. They also have higher resolution than older models.

New flat panel displays utilize a liquid crystal display (LCD) display. This system lights up various pixels on the screen. The simple and small infrastructure of flat panel displays allows for the manufacturing of extremely light and portable screens, which are popular for personal and business use.

Плоский дисплей

Плоский дисплей – це телевізор, монітор або інший пристрій відображення, який використовує тонку панель замість традиційної електронно-променевої трубки (ЕПТ). Ці екрани набагато легші і тонші, і можуть бути набагато більш портативними, ніж традиційні телевізори і монітори. Вони також мають вищу роздільну здатність, ніж старі моделі.

У нових плоских дисплеях використовується рідкокристалічний дисплей (РК-дисплей). Ця система підсвічує різні пікселі на екрані. Проста і невелика інфраструктура плоских дисплеїв дозволяє виготовляти надзвичайно легкі і портативні екрани, які популярні для особистого і ділового використання.

FOAF

FOAF (friend of a friend) protocol is an RDF-based schema that uses semantic Web syntax to describe individuals and social networks. Experts describe it as an “ontology” that helps to order digital representations of relationship models.

Part of the idea behind FOAF is that semantic Web technologies and new syntactical systems facilitate a kind of “revolution” in data connection. Internet guru Tim Berners-Lee has written about how technologies like FOAF will change the ordering of data systems. One example is the use of FOAF in JSON-LD, a resource for adding linked data to online data models.

FOAF

Протокол FOAF (friend of a friend) – це схема на основі RDF, яка використовує синтаксис семантичного вебу для опису людей і соціальних мереж. Експерти описують його як «онтологію», яка допомагає впорядкувати цифрові представлення моделей взаємовідносин.

Частково ідея FOAF полягає в тому, що технології семантичної павутини і нові синтаксичні системи сприяють своєрідній «революції» в передачі даних. Інтернет-гуру Тім Бернерс-Лі писав про те, як технології на кшталт FOAF змінять упорядкування систем даних. Одним із прикладів є використання FOAF в JSON-LD, ресурсі для додавання пов’язаних даних до онлайн-моделей даних.

Folder

In computers, a folder is the virtual location for applications, documents, data or other sub-folders. Folders help in storing and organizing files and data in the computer. The term is most commonly used with graphical user interface operating systems.

Folders in computer science function similarly to real-world physical folders. Folders can store and organize different types of applications, files or libraries. Folders can also contain other folders, which in turn could contain other folders or files. Due to the manner in which folders organize and store data within the file system of the storage media, folders are also known as file directories or simply directories. There is no limit on the number of folders or sub-folders that can be created. Upon opening a folder, one can see how the data or files are organized.

Папка

У комп'ютерах папка – це віртуальне місце для зберігання програм, документів, даних або інших підпапок. Папки допомагають зберігати та організовувати файли та дані на комп'ютері. Цей термін найчастіше використовується в операційних системах з графічним інтерфейсом користувача.

Папки в інформатиці функціонують подібно до реальних фізичних папок. Вони можуть зберігати та організовувати різні типи програм, файлів або бібліотек. Папки можуть також містити інші папки, які, у свою чергу, можуть містити ще папки або файли. Завдяки способу, яким папки організовують і зберігають дані у файловій системі носія, папки також називають файловими каталогами або просто каталогами. Немає обмежень на кількість папок або підпапок, які можна створити. Відкривши папку, користувач може побачити, як організовані дані або файли.

Font Family

A font family is a set of fonts that have a common design. Fonts within a family, however, differ from each other in style such as the weight (light, normal, bold, semi-bold, etc.) and the slant (roman or upright, italic and oblique). An example of a font family is Times New Roman, which consists of a roman, italic, bold and bold italic version of the same typeface.

The stroke width and serif characteristics of a font differ from family to family. In Windows, fonts are categorized into six font family names:

- Decorative (a novelty font)

Сімейство шрифтів

Сімейство шрифтів – це набір шрифтів, які мають спільний дизайн. Однак шрифти в межах сімейства відрізняються один від одного за стилем, наприклад, за нахилом (світлий, звичайний, напівжирний тощо) та кеглем (курсив, прямий, похилий). Прикладом сімейства шрифтів є Times New Roman, яке складається з романської, курсивної, напівжирної та напівжирної курсивної версій того самого шрифту.

Ширина штрихів і характеристики зарубок шрифту відрізняються у різних

• Modern (a monospaced, fixed-width or non-proportional font)
• Roman (a proportional serif font)
• Script (a cursive or handwriting-like font)
• Swiss (a proportional sans serif font)
• Dontcare (a generic font)

сімействах. У Windows шрифти поділяються на шість сімейств:
• Декоративні (нові шрифти)
• Modern (моноширинний, фіксованої ширини або непропорційний шрифт)
• Roman (пропорційний шрифт із зарубками)
• Script (курсивний або рукописний шрифт)
• Swiss (пропорційний шрифт без зарубок)
• Dontcare (універсальний шрифт)

For Loop

For loop is a programming language conditional iterative statement which is used to check for certain conditions and then repeatedly execute a block of code as long as those conditions are met.

The for loop is distinguished from other looping statements through an explicit loop counter or loop variable which allows the body of the loop to know the exact sequencing of each iteration.

The For loop is used in many imperative programming languages notably C and C++ and comes from the English word ‘for’ which is used to state the purpose of an object or action, in this case the purpose and details of the iteration.

Цикл For

Цикл For – це умовний повторюваний оператор мови програмування, який використовується для перевірки певних умов, а потім циклічно виконує блок коду до тих пір, поки ці умови виконуються.

Цикл For відрізняється від інших операторів циклу наявністю видимого лічильника циклу або змінної циклу, яка дозволяє тілу програми знати точну послідовність кожного повторення.

Цикл For використовується в багатьох мовах машинного програмування, зокрема в C і C++, і походить від англійського слова «for», яке використовується для вказівки призначення об’єкта або дії, в даному випадку – мети і деталей виконання.

Force Touch

Force Touch is a feature promoted by Apple for use in its phone and smartwatch designs. It brings a new kind of functionality to the conventional touchpad and touchscreen, which are standard features in modern mobile devices.

Force Touch

Force Touch – це функція, яку компанія Apple просуває для використання в своїх телефонах і смарт-годинниках. Вона надає новий вид функціональності звичайній сенсорній панелі та сенсорному екрану,

The idea behind Force Touch is that touchpad users can apply different amounts of pressure on the screen and the operating system can sense the varying degrees of pressure applied to implement different commands. This brings a whole new dimension to touchpad control, opening doors for a more diverse set of commands based on a more diverse set of gestures.

Ідея Force Touch полягає в тому, що користувачі тачпаду можуть натискати на екран з різною силою, а операційна система може відчувати різний ступінь натискання для виконання різних команд. Це привносить абсолютно новий вимір в управління тачпадом, відкриваючи двері для більш різноманітного набору команд, заснованих на більш різноманітному наборі жестів.

Forensic Animation

Forensic animation refers to the recreation of crime scenes and scenarios using 3-D graphic tools to help investigators and police in solving crimes. Animation is done by experts using high tech software and actual images of crime scenes from various dimensions. Animators are chosen based on who can produce the best and most appropriate animation work.

Forensic animation is a widely used and successful method of solving crimes such as robbery, murder and accidents. It uses full-motion computer graphics to re-create events using the same scene and scenario as the actual events.

Криміналістична анімація

Криміналістична анімація – це відтворення місць і сценаріїв злочинів за допомогою тривимірних графічних інструментів, які допомагають слідчим і поліції в розкритті злочинів. Анімація створюється експертами з використанням високотехнологічного програмного забезпечення та реальних зображень місць злочинів у різних вимірах. Аніматорів обирають на основі того, хто може створити найкращу та найбільш відповідну анімаційну роботу.

Судова анімація – це широко використовуваний і успішний метод розкриття таких злочинів, як пограбування, вбивства та нещасні випадки. Вона використовує комп'ютерну графіку повного руху для відтворення подій, використовуючи ту саму сцену і сценарій, що й реальні події.

Formula And Recipe Management

Formula and recipe management is the use of various software programs for confirmation of process manufacturing in industries. It usually comprises a number of process management software

Управління формулами та рецептурами

Управління формулами та рецептурами – це використання різних програмних продуктів для підтвердження виробничих процесів у промисловості. Зазвичай воно складається з

implementations that collaboratively work to validate formulations to support production and regulatory needs. Many food and beverage processing industries use high-tech formula and recipe management techniques for formula or recipe calculation.

Formula and recipe management makes use of software and processes that are able to improve formulas, define and optimize formulation variables, forecast the demand and supply, manage proper classification and categorization of useful content, preparing inventory lists and accommodating changes in formulations and recipes.

декількох програмних реалізацій для управління процесами, які спільно працюють над перевіркою рецептур для забезпечення виробничих і регуляторних потреб. Багато галузей харчової промисловості та виробництва напоїв використовують високотехнологічні методи управління формулами та рецептурами для розрахунку формул або рецептів.

Управління формулами і рецептурами використовує програмне забезпечення і процеси, які здатні вдосконалювати формули, визначати і оптимізувати змінні формули, прогнозувати попит і пропозицію, управляти належною класифікацією і категоризацією корисного вмісту, готувати інвентаризаційні списки і вносити зміни в формули і рецепти.

Forward Compatible

Forward compatible is the ability of an IT system to be compatible with or to support a similar version of itself in the future.

Unlike backward compatibility, forward compatibility ensures the integration of or interoperability support for newer versions of an IT system with existing ones.

Forward compatible is also known as upward compatible, future-time compatible or newer-version compatible.

Forward compatibility primarily ensures that an existing IT system is able to operate with subsequent releases of itself. This compatibility is planned out during the system design phase. Typically, to support forward compatibility, the hardware/software must also be backward compatible.

«Сумісність у майбутньому»

Сумісність – це здатність інформаційних систем бути сумісними з аналогічними версіями в майбутньому або підтримувати їх у майбутньому.

На відміну від зворотної сумісності, пряма сумісність забезпечує інтеграцію або підтримку сумісності нових версій інформаційних систем з існуючими.

Сумісність уперед також відома як висхідна сумісність, сумісність з майбутнім часом або сумісність з новими версіями.

Перспективна сумісність в першу чергу гарантує, що існуюча інформаційна система може працювати з наступними версіями самої себе. Ця сумісність планується на етапі проектування системи. Як правило, для підтримки сумісності в майбутньому, апаратне/ програмне забезпечення повинно бути сумісним і в минулому.

Forward Slash

The forward slash is an ASCII text character that is used for punctuation, alphanumerical representations in mathematics, general-purpose coding and other aspects of digital text and design. It is also the common format for file and folder designations in command line systems.

The forward slash is also known simply as the slash or, less commonly, the oblique stroke.

One common use of the forward slash is in fractions, where the number that goes on top of the fraction is represented to the left of forward slash, and the number that goes in the bottom of the fraction is represented to the right of the forward slash. This usage goes back to early typewriters and typesetting, but is still used today. A newer use of the forward slash is the file and folder designations mentioned above. It is also commonly used to demarcate comments in many programming languages — in other words, between two sets of forward slashes, there are words and symbols that humans can look at, but the computer does not consider as part of functional programming.

Пряма похила риска

Пряма похила риска – це текстовий символ у кодуванні ASCII, який використовується для пунктуації, алфавітно-цифрових позначень у математиці, кодуванні загального призначення та інших аспектах цифрового тексту і дизайну. Це також загальний формат для позначення файлів і папок у системах командного рядка.

Пряма похила риска також відома просто як похила риска або, рідше, коса риска.

Одна з найпоширеніших форм використання прямої похилої риски – у дробах, де число, що стоїть у верхній частині дробу, подається ліворуч від прямої похилої риски, а число, що стоїть у нижній частині дробу, подається праворуч від прямої похилої риски. Таке використання сходить до ранніх друкарських машинок і друкарського набору, але все ще використовується і сьогодні. Новіше використання прямої похилої риски – це згадані вище позначення файлів і папок. Вона також широко використовується для розмежування коментарів у багатьох мовах програмування – іншими словами, між двома наборами прямих косих рисок є слова і символи, на які людина може дивитися, але комп'ютер не вважає їх частиною функціонального програмування.

Foundation Framework

The Foundation framework is a front-end framework that integrates the classic Web design languages HTML and Cascading Style Sheets (CSS) with other tools and controls to provide a responsive environment for design. This

Фреймворк Foundation

Фреймворк Foundation – це інтерфейсний фреймворк, який інтегрує класичні мови веб-дизайну HTML та каскадні таблиці стилів (КТС) з іншими інструментами та елементами керування, щоб забезпечити адаптивне

open-source technology is maintained by ZURB since its development several years ago; several subsequent versions were released in 2011, 2012, 2013 and 2014 and another one planned for 2015.

Essentially, Foundation is built on two languages called Sass (Syntactically Awesome Style Sheets) and SCSS (Sassy CSS). These languages are based on CSS, but offer different types of accessibility. The idea is that developers can use Foundation and other Sass/SCSS tools to do things more quickly or efficiently than if they were only using CSS as a Web design language.

середовище для дизайну. Ця технологія з відкритим вихідним кодом підтримується ZURB з моменту її розробки кілька років тому; кілька наступних версій були випущені в 2011, 2012, 2013 і 2014 роках і ще одна запланована на 2015 рік.

По суті, Foundation побудований на двох мовах, які називаються СЧТС (Синтаксично чудові таблиці стилів) і SCSS (Сміливі CSS). Ці мови засновані на CSS, але пропонують різні типи доступності. Ідея полягає в тому, що розробники можуть використовувати Foundation та інші інструменти Sass/ SCSS, щоб робити речі швидше та ефективніше, ніж якби вони використовували лише CSS як мову веб-дизайну.

Frame Synchronization

The term frame synchronization is used in two different contexts. In the case of video, it refers to the process of synchronizing display pixel scanning to a synchronization source. In the case of telecommunication, it is the process by which incoming framed data are extracted for decoding with the help of frame alignment signals. This process is called as such because framing and synchronization must be carried out whenever a bit slip event occurs during data transmission.

Frame synchronization can be defined as the process of identifying valid data from a framed data transmission. When data frames are transmitted to a receiver from the sender but get interrupted, the receiver must resynchronize.

Синхронізація кадрів

Термін «синхронізація кадрів» використовується у двох різних контекстах. У випадку відео він означає процес синхронізації розгортки пікселів дисплея з джерелом синхронізації. У випадку телекомунікацій – це процес, за допомогою якого вхідні кадрові дані виділяються для декодування за допомогою сигналів вирівнювання кадрів. Цей процес називається так тому, що кадрування і синхронізація повинні виконуватися щоразу, коли під час передачі даних відбувається подія бітового зсуву.

Синхронізацію кадрів можна визначити як процес ідентифікації достовірних даних з кадрової передачі даних. Коли кадри даних передаються від відправника до одержувача, але перериваються, одержувач повинен виконати повторну синхронізацію.

Frameset

A frameset is an element in hypertext markup language (HTML) which contains the different frame elements. It is used to inform the browser of the division of the screen into different split windows, and prohibits any content inside the body associated with a page.

A frameset can be divided into rows and columns. It is denoted by the “frameset” tag and makes use of a special frameset-specific doctype. The “frameset” tag provides the specification of number of columns and rows in the frameset and also space in pixels occupied by them.

Набір кадрів

Набір кадрів – це елемент мови гіпертекстової розмітки (HTML), який містить різні елементи фреймів. Він використовується для інформування браузера про поділ екрану на різні розділені вікна і забороняє будь-який вміст всередині тіла, пов’язаного зі сторінкою.

Набір фреймів можна розділити на рядки і стовпці. Він позначається тегом «frameset» і використовує спеціальну доктрину, специфічну для фреймворків. Тег «frameset» забезпечує специфікацію кількості стовпців і рядків у наборі, а також займаного ними простору у пікселях.

Free Lossless Audio Codec

Free Lossless Audio Codec (FLAC) is an open-source codec that is used for compressing audio data without any loss in audio quality. Similar to the MP3 audio format, it is specifically designed for audio and supports album art and audio tags, and is suitable for listening, archiving and recording.

Free Lossless Audio Codec is supported by a number of hardware devices. It is totally lossless as the encoding of the audio data has no loss and decoded data is identical to the encoder input. The format uses an MD5-based signature to ensure the integrity of the audio data. Free Lossless Audio Codec supports fast sample-accurate seeking. This makes the format favorable for editing applications, along with playback options.

Безкоштовний аудіокодек без втрат

Безкоштовний аудіокодек без втрат (БАБВ) – це кодек з відкритим вихідним кодом, який використовується для стиснення аудіоданих без втрати якості звуку. Подібно до аудіоформату MP3, він спеціально розроблений для аудіо і підтримує обкладинки альбомів та аудіотеги, а також підходить для прослуховування, архівування та запису.

Безкоштовний аудіокодек без втрат підтримується низкою апаратних пристроїв. Він повністю позбавлений втрат, оскільки при кодуванні аудіоданих не відбувається жодних втрат, а декодовані дані ідентичні вхідним. Формат використовує підпис на основі MD5 для забезпечення цілісності аудіоданих. Безкоштовний аудіокодек без втрат підтримує швидкий пошук з точністю до зразка. Це робить формат сприятливим для додатків для редагування, а також для відтворення.

FreeDOS

FreeDOS is a free and open-source operating system that is designed to provide a DOS-compatible environment. It was initially developed for IBM PCs and supports running legacy software, games and build embedded systems.

FreeDOS was released in 1998 and is also known as PD-DOS.

FreeDOS was primarily designed to provide a DOS environment similar to MS-DOS. It can run all the applications and commands that are supported by MS-DOS. FreeDOS has the ability to provide multiboot on Windows NT and 9X Oss and supports FAT32 and large disk support with long file names and more.

FreeDOS

FreeDOS – це вільна операційна система з відкритим вихідним кодом, розроблена для забезпечення DOS-сумісного середовища. Спочатку вона була розроблена для IBM PC і підтримує застаріле програмне забезпечення, ігри та збірку вбудованих систем.

FreeDOS була випущена у 1998 році і також відома як PD-DOS.

FreeDOS було розроблено для забезпечення середовища DOS, подібного до MS-DOS. У ній можна запускати всі програми і команди, які підтримуються MS-DOS. FreeDOS має можливість забезпечувати мультизавантаження на Windows NT і 9X, підтримує FAT32 і великі диски з довгими іменами файлів тощо.

Frequency Modulation

Frequency modulation (FM) is a technique used to encode data on an alternating digital or analog signal. The method includes varying the frequency of the carrier wave on which useful information is imposed or impressed upon. The signal on which data is imposed is known as the carrier signal and the resulting signal with variable frequency is called a frequency modulated signal.

Frequency modulation is widely used for radio transmission due to the fact that the signal-to-noise ratio (SNR) is large in this method of modulation and hence radio frequency interference is minimized.

Частотна модуляція

Частотна модуляція (ЧМ) – це метод, який використовується для кодування даних у змінному цифровому або аналоговому сигналі. Метод включає в себе зміну частоти несучої хвилі, на яку накладається корисна інформація. Сигнал, на який накладаються дані, називається несучим сигналом, а результуючий сигнал зі змінною частотою називається частотно-модульованим сигналом.

Частотна модуляція широко використовується для радіопередачі через те, що відношення сигнал/шум (ВСШ) при цьому методі модуляції велике, а отже, радіочастотні перешкоди зведені до мінімуму.

Frequency Modulation Synthesis

Frequency modulation (FM) synthesis is a popular technique used for generating rich sound palettes in the process of sound synthesis. Initially implemented in analog systems, FM synthesizers are now implemented digitally. FM synthesizers using analog oscillators suffer from pitch instability; as a result, digital implementations are favored. The latter are helpful in creating un-pitched and metallic tones rather than standard subtractive sounds. FM synthesizers are used to create more lifelike sounds. The simple plain input waveform is changed by modulating its frequency using an FM synthesizer to create more complex waveforms for lifelike sound generation.

Синтез частотної модуляції

Синтез частотної модуляції (ЧМ) – це популярна техніка, яка використовується для створення багатих звукових палітр у процесі синтезу звуку. Спочатку вона була реалізована в аналогових системах, але зараз ЧМ-синтезатори реалізовані цифровим способом. Аналогові ЧМ-синтезатори мають проблему з нестабільністю тону; тому віддають перевагу цифровим реалізаціям. Останні корисні для створення звуків без певної висоти або металевих тонів, а не стандартних субтрактивних звуків. ЧМ-синтезатори використовуються для створення більш реалістичних звуків. Проста хвиля, яка використовується як вхідний сигнал, змінюється шляхом модуляції її частоти за допомогою ЧМ-синтезатора для створення більш складних звукових форм для реалістичної генерації звуку.

Fuel Cell

A fuel cell is a device that converts chemical energy into electricity. It consists of an electrolyte and two electrodes. It generates electricity by means of chemical reactions occurring at the electrodes. The electrolyte carries electrically charged particles from one electrode, thus producing electricity. A chemical catalyst may be used to speed up the chemical reaction in the cell. It produces electricity without combustion and is hence less polluting.

The fuel cell was first devised by Sir William Grove in 1839. William Grove postulated that by reversing the electrolysis process, electricity and water could be produced.

Паливний елемент

Паливний елемент – це пристрій, який перетворює хімічну енергію на електричну. Він складається з електроліту та двох електродів. Електрика виробляється завдяки хімічним реакціям, що відбуваються на електродах. Електроліт переносить електрично заряджені частинки від одного електрода, таким чином створюючи електричний струм. Для прискорення хімічної реакції в елементі може використовуватися хімічний каталізатор. Він виробляє електрику без спалювання, тому є менш забруднюючим.

Паливний елемент був вперше розроблений сером Вільямом Гроувом у 1839 році. Вільям Гроув припустив, що шляхом обернення процесу електролізу можна виробляти електрику та воду.

Function Key

A function key refers to one of the twelve keys present on the top row of a common PC keyboard. Labeled from F1–F12, these function keys are responsible for performing shortcut tasks like printing or saving files. Different operating systems, for example Windows and Mac OS, have separate uses for function keys.

A function key is also known as a soft key.

Function keys are present on all modern Mac and Windows keyboards. On some laptop keyboards, however, they are not separate keys but are sub-functions of other keys and can be activated with the help of a separate key, usually the Fn key. In the top row of a regular keyboard, function keys help with the performance of various functions; for example, Microsoft Windows users can press ALT + F4 to close the program currently active. Apple computers did not have function keys in earlier models, but current keyboards feature the function keys on the top row similar to the standard PC keyboard.

Функціональна клавіша

Функціональна клавіша – це одна з дванадцяти клавіш, розташованих у верхньому ряду стандартної клавіатури ПК. Позначені від F1 до F12, ці функціональні клавіші відповідають за виконання таких завдань, як друк або збереження файлів. Різні операційні системи, наприклад Windows і Mac OS, мають різне використання функціональних клавіш.

Функціональна клавіша також відома як м'яка клавіша.

Функціональні клавіші присутні на всіх сучасних клавіатурах Mac і Windows. Однак на деяких ноутбуках вони не є окремими клавішами, а є підфункціями інших клавіш і можуть бути активовані за допомогою окремої клавіші, зазвичай клавіші Fn. У верхньому ряду звичайної клавіатури функціональні клавіші допомагають виконувати різні функції; наприклад, користувачі Microsoft Windows можуть натиснути ALT + F4 для закриття активної програми. Перші моделі комп'ютерів Apple не мали функціональних клавіш, але сучасні клавіатури мають функціональні клавіші у верхньому ряду, подібні до стандартної клавіатури ПК.

Function Point

A function point (FP) is a component of software development which helps to approximate the cost of development early in the process. It is a process which defines the required functions and their complexity in a piece of software in order to estimate the software's size and scope upon completion.

Функціональна точка

Функціональна точка (ФТ) – це компонент розробки програмного забезпечення, який допомагає наближено оцінити вартість розробки на ранній стадії процесу. Це процес, який визначає необхідні функції та їхню складність у програмному забезпеченні, щоб оцінити розмір та обсяг

A function point calculates software size with the help of logical design and performance of functions as per user requirements. It also helps in determining the business functionality of a software application. A function point has a number of benefits, including increase in productivity and reduction in the risk of inflation of created code.

програмного забезпечення після завершення розробки.

Функціональна точка розраховує розмір програмного забезпечення за допомогою логічного дизайну та виконання функцій відповідно до вимог користувача. Це також допомагає визначити бізнес-функціональність програмного додатку. Функціональна точка має ряд переваг, включаючи підвищення продуктивності та зменшення ризику розростання створеного коду.

G

Gamification

Gamification refers to the use of game design principles to improve customer engagement in non-game businesses. The specific methods used range from the creation of reward schedules to creating levels of achievement via status and badges. Companies use gaming principles to increase interest in a product or service, or simply to deepen their customers' relationship with the brand.

Гейміфікація

Гейміфікація – це використання принципів ігрового дизайну для покращення залучення клієнтів у неігрових бізнесах. Конкретні методи, що використовуються, варіюються від створення графіків винагород до створення рівнів досягнень за допомогою статусів та бейджів. Компанії використовують ігрові принципи, щоб підвищити інтерес до продукту чи послуги або просто поглибити стосунки своїх клієнтів з брендом.

Generic Access Network (GAN)

In telecommunication systems, a generic access network (GAN) is used by cellular device users to connect and interact with other types of communication devices. GAN protocols primarily evolved for communication session. Modern GAN technology permits a subscriber to interact via voice, data, IP

Мережа загального доступу

У телекомунікаційних системах мережа загального доступу використовується користувачами мобільних пристроїв для підключення та взаємодії з функції між бездротовими локальними мережами і глобальними мережами не перериваючи сеанс зв'язку. Сучасна технологія мережі

multimedia subsystem and Session Initiation Protocol (SIP) applications.

Prior to 2005, a generic access network was commercially known as unlicensed mobile access (UMA).

загального доступу дозволяє абоненту взаємодіяти за допомогою голосу, даних, мультимедійної підсистеми IP і додатків з протоколом ініціювання сеансу (SIP).

До 2005 року мережа загального доступу була комерційно відома як неліцензійний мобільний доступ (UMA).

Global Assembly Cache (GAC)

The Global Assembly Cache (GAC) is a folder in Windows directory to store the .NET assemblies that are specifically designated to be shared by all applications executed on a system.

Глобальний кеш збірки (Global Assembly Cache, GAC)

Глобальний кеш збірки (Global Assembly Cache, GAC) – це папка в каталозі Windows для зберігання збірок НЕТ, які спеціально призначені для спільного використання всіма програмами, що виконуються в системі.

GNU Project

The GNU Project refers to the collaborative development of the GNU OS. Designed as a free Unix alternative, the GNU Project was launched by Richard Stallman, founder of the Free Software Foundation (FSF), in January 1984. The recursive GNU acronym represents the phrase "GNU's Not Unix."

In the GNU Project context, free software refers to liberty (versus price).

Проект GNU

Проект GNU – це спільна розробка операційної системи GNU. Розроблений як вільна альтернатива Unix, проект GNU був започаткований Річардом Столлманом, засновником Фонду вільного програмного забезпечення (FSF), у січні 1984 року. Рекурсивна абревіатура GNU представляє фразу «GNU – це не Unix».

У контексті проекту GNU вільне програмне забезпечення означає свободу (у порівнянні з ціною).

Goldmine

Goldmine is a customer relationship management (CRM) system software package produced by Frontrange Solutions. Like other CRM products on the market, it has been specifically designed for organizing and tracking sales, storing and managing contact information, reporting, follow-up and

«Голдмайн»

«Голдмайн» – це програмний пакет для управління взаємовідносинами з клієнтами (CRM), розроблений компанією «Фронтранж Солюшнс». Як і інші CRM-продукти на ринку, він був спеціально розроблений для організації та відстеження продажів, зберігання та управління контактною

integration with other software products. Goldmine software has been acknowledged as one of the earliest pioneers in the area of contact management and customer relationship management. Goldmine software was originally released in 1989.

інформацією, звітності, подальших дій та інтеграції з іншими програмними продуктами. Програмне забезпечення Голдмайн визнано одним з перших піонерів у сфері управління контактами та взаємовідносинами з клієнтами. Програмне забезпечення Goldmine було вперше випущено в 1989 році.

Google Swiffy

Google Swiffy is a software tool released by Google Labs in June 2011. Swiffy is used to convert an Adobe Flash/Flex project into HTML5.

Google Swiffy allows a developer to convert a Flash animation into a browser viewable format, eliminating the need for a Flash player plug-in.

Гугл Свіффі

Гугл Свіффі – це програмний інструмент, випущений Google Labs у червні 2011 року. Свіффі використовується для перетворення проектів Adobe Flash/Flex у HTML5.

Гугл Свіффі дозволяє розробнику конвертувати флеш-анімацію у формат, придатний для перегляду браузером, усуваючи необхідність у плагіні для флеш-плеєра.

Google Wallet

Google Wallet is smartphone software developed for Google Android phones and designed to replace credit card processing. Google Wallet technology allows a user to make a payment by tapping a smartphone and entering a four-digit security code during checkout. Google Wallet also includes SingleTap capabilities, in which the Wallet software stores a user's digital coupons, loyalty points and Groupon-style deals. This information facilitates transactions.

Google Гаманець

Google Гаманець – це програмне забезпечення для смартфонів, розроблене для телефонів Google Android і покликане замінити обробку кредитних карток. Технологія Google Гаманця дозволяє користувачеві здійснити платіж, доторкнувшись до смартфону і ввівши чотиризначний код безпеки під час оформлення замовлення. Google Гаманець також включає в себе можливості SingleTap.

Grinding

Grinding refers to the playing time spent doing repetitive tasks within a game to unlock a particular game item or to build the experience needed to progress smoothly through the game. Grinding most commonly involves killing the same set of opponents over

Гриндинг

Гриндинг – це ігровий час, витрачений на виконання повторюваних завдань у грі, щоб розблокувати певний ігровий предмет або накопичити досвід, необхідний для безперешкодного проходження гри. Найчастіше гриндинг передбачає

and over in order to gain experience points or gold. Although other game genres require some grinding, role-playing games (RPG) – specifically massively multiplayer online role-playing games – are the most notorious for requiring this type of time investment from players.

вбивство одного і того ж набору супротивників знову і знову, щоб отримати очки досвіду або золото. Хоча інші ігрові жанри вимагають певного шліфування, рольові ігри (RPG) – зокрема, масові багатокористувацькі рольові онлайн-ігри – найбільш відомі тим, що вимагають від гравців таких витрат часу.

Guard Band

A guard band is a narrow frequency range that separates two ranges of wider frequency. This ensures that simultaneously used communication

channels do not experience interference, which would result in decreased quality for both transmissions.

Guard bands are used in frequency division multiplexing (FDM).

Захисна смуга

Захисна смуга – це вузький діапазон частот, який розділяє два діапазони більш широких частот. Це гарантує, що одночасно використовувані канали зв'язку не зазнають інтерференції, яка б призвела до зниження якості обох передач.

Захисні смуги використовуються в мультиплексуванні з частотним розділенням каналів (FDM).

H

Hack/Phreak/Virii/Crack/Anarchy (H/P/V/C/A)

Hack/phreak/virii/crack/anarchy (H/P/V/C/A) is a collective term used to describe various malicious, unethical, and underground computer-related activities. These actions are often carried out by individuals or groups with extensive technical knowledge, usually for illegal or unauthorized purposes. This term encompasses hacking, phone phreaking, virus creation, software cracking, and cyber-anarchist acts.Each part of the acronym represents a different aspect of this subculture. "Hack" is sometimes associated with creative problem-solving or unauthorized system

Хакерство, фрікінг, віруси, злом і анархія

Хакерство, фрікінг, віруси, злом і анархія Hack/phreak/virii/crack/anarchy (H/P/V/C/A) — це загальний термін, що описує різноманітну зловмисну, неетичну й підпільну діяльність у сфері комп'ютерних технологій. Такі дії зазвичай виконують особи або групи з глибокими технічними знаннями, часто з метою порушення законів або несанкціонованого доступу до систем. Кожна складова цього терміна означає певну частину субкультури. "Hack" іноді асоціюється з креативним вирішенням проблем або несанкціонованим доступом до систем. "Phreak"

access. “Phreak” refers to the manipulation of telecommunication systems. “Virii” (a stylized plural of virus) indicates malware creation. “Crack” involves bypassing software protection. “Anarchy” symbolizes anti-system behavior or ideology in the tech world. These practices vary in severity — with hacking sometimes viewed as relatively harmless, while virus creation and software cracking are typically seen as highly destructive and illegal.

– це маніпуляції з телекомунікаційними системами. “Virii” (стилізований варіант множини від “virus”) означає створення шкідливих програм. “Crack” передбачає злом або обхід захисту програмного забезпечення. “Anarchy” відображає антиурядову або антисистемну ідеологію в IT-середовищі. Ці дії мають різний ступінь небезпеки – від відносно нешкідливого хакерства до потенційно руйнівних вірусів і зломів.

Hadapt

Hadapt is a company that developed a big data platform integrating SQL with Apache Hadoop. The platform removes the need for connecting traditional relational databases with big data analytics tools. Acquired by Teradata in 2014, Hadapt originated from a group of Yale scientists and played a role in transforming business intelligence by improving access to large-scale data.

Hadapt

Hadapt – це компанія, що розробила платформу для роботи з великими даними, яка поєднує SQL та Apache Hadoop. Ця платформа усуває необхідність з’єднання традиційних реляційних баз даних із аналітичними інструментами для великих даних. Компанію придбала Teradata у 2014 році. Hadapt заснували вчені з Єльського університету, і вона зробила внесок у трансформацію бізнес-аналітики, покращивши обробку великих обсягів даних.

Hand Coding

Hand coding refers to the manual process of writing code or layout instructions using original programming languages, without relying on automated tools or visual editors. In the past, languages like BASIC and FORTRAN were always hand coded, and even today, professional developers continue to use hand coding for greater control, precision, and understanding of the code. Though modern tools such as WYSIWYG editors allow users to create layouts visually without writing actual

Ручне кодування

Ручне кодування — це процес написання коду або інструкцій для верстки вручну за допомогою оригінальних мов програмування, без використання автоматизованих інструментів або візуальних редакторів. У минулому мови, як-от BASIC та FORTRAN, писалися виключно вручну. Навіть сьогодні професійні розробники часто обирають ручне кодування для досягнення точності, повного контролю над програмою та кращого розуміння її структури. Хоча сучасні редактори типу

code, many still prefer hand coding for its flexibility and direct interaction with the software's logic.

WYSIWYG дозволяють створювати інтерфейси без знання коду, ручне кодування залишається незамінним у багатьох сферах.

Hard Drive Recovery

Hard drive recovery refers to the process of retrieving lost or inaccessible data and restoring a hard drive to a previous working state after it experiences a failure, crash, or corruption. This process allows users to regain access to important files and return the drive to normal operation. It is especially useful in cases where data has been accidentally deleted, damaged by viruses, or lost due to hardware failure. Hard drive recovery can be performed using specialized software tools that repair logical errors and recover data, as long as the sectors haven't been overwritten. In cases of physical damage, such as mechanical failure or broken components, the drive often needs professional repair before the data can be accessed again. The recovery process may involve connecting the damaged drive to another system using interfaces like SATA, ATA, or USB.

Відновлення жорсткого диска

Відновлення жорсткого диска — це процес відновлення втрачених або недоступних даних і повернення жорсткого диска до попереднього робочого стану після збою, аварії або пошкодження. Цей процес дозволяє знову отримати доступ до важливих файлів і відновити нормальну роботу диска. Це особливо важливо, коли дані були випадково видалені, пошкоджені вірусами або втрачені через апаратні несправності. Відновлення може здійснюватися за допомогою спеціалізованого програмного забезпечення, що виправляє логічні помилки та витягує дані, якщо сектори ще не були перезаписані. У разі фізичного пошкодження, наприклад, механічної несправності або зламаних компонентів, диск часто потребує професійного ремонту для отримання доступу до даних. Також відновлення може включати підключення несправного диска до іншої системи через інтерфейси, як-от SATA, ATA або USB.

Hardcoding

Hardcoding is the practice of embedding fixed values or logic directly into the source code of a program. These values cannot be changed unless the source code is manually edited and recompiled. It is typically used for constants such as mathematical values (e.g., Pi) or system parameters that must remain the same under all conditions. Although hardcoding can be practical for small, unchanging data, it is generally discouraged in modern development due

Хардкод (жорстке кодування)

Хардкод (жорстке кодування) — це вбудовування фіксованих значень або логіки безпосередньо у вихідний код програми. Такі значення не можна змінити без ручного редагування коду та повторної компіляції. Найчастіше хардкод використовують для незмінних констант, як-от математичні величини (наприклад, число Пі), або для системних параметрів, які не повинні змінюватися. Хоча це може бути зручним для невеликих програм, у

to its lack of flexibility and maintainability. However, in some cases, such as embedding license keys or identifiers, hardcoding is still used deliberately.

сучасному програмуванні хардкод вважається поганою практикою, оскільки ускладнює оновлення та супровід. Утім, у певних випадках (наприклад, серійні номери або ідентифікатори) хардкод застосовується навмисно.

Hierarchical Temporal Memory

Hierarchical temporal memory is a biomimetic model that simulates how the human neocortex processes information. Developed by Jeff Hawkins and Dileep George, it represents a universal learning approach in artificial intelligence. It uses deep learning templates at different levels to understand how the brain perceives and assembles information. The theory suggests that the neocortex uses a unified framework for diverse tasks like vision and motor activity.

Ієрархічна тимчасова пам’ять

Ієрархічна тимчасова пам’ять — це біоміметична модель, що імітує обробку інформації неокортексом людського мозку. Розроблена Джеффом Хокінсом і Діліпом Джорджем, вона репрезентує універсальний підхід до навчання в штучному інтелекті. Використовує шаблони глибокого навчання на різних рівнях, щоб зрозуміти, як мозок сприймає та збирає інформацію. Теорія передбачає, що неокортекс використовує єдину структуру для різних завдань, як-от зір чи рухова активність.

High Availability Cluster (HA cluster)

High Availability Cluster (HA cluster) is a group of connected computers or hardware systems designed to minimize downtime and maintain continuous operations even during hardware or software failures. These clusters are typically used by organizations that require uninterrupted access to their services. The cluster automatically switches operations to another system in the event of a failure, a process known as “failover.” Components in an HA cluster usually share the same virtualization environment and have access to common storage systems through high-speed connections like fibre channel or SCSI.

Кластер високої доступності (HA-кластер)

Кластер високої доступності (HA-кластер) – це об’єднання декількох апаратних систем або комп’ютерів, створене для забезпечення безперебійної роботи навіть у разі відмови частини обладнання чи програмного забезпечення. Такі кластери особливо важливі для організацій, які не можуть допустити простоїв у роботі. У разі збою одна система автоматично передає свої функції іншій, що називається “перемиканням на резервну систему”. Компоненти кластера зазвичай використовують спільне віртуалізоване середовище та мають доступ до загального сховища через високошвидкісні канали передачі даних, як-от оптоволокно або інтерфейс SCSI.

High Sierra Format (HSF)

High Sierra Format (HSF) is an early file storage format for CD-ROMs. Although obsolete, it served as the foundation for the ISO 9660 standard. It was introduced to unify CD-ROM file storage and reduce compatibility issues. Adopted in 1985, it made file organization across discs more consistent.

Формат High Sierra (HSF)

Формат High Sierra (HSF) — це ранній формат зберігання файлів на CD-ROM. Хоча він застарілий, саме на ньому базується стандарт ISO 9660. Його було введено для уніфікації зберігання файлів на CD-ROM і зменшення проблем сумісності. У 1985 році він був прийнятий як стандарт, що забезпечив узгоджене зберігання файлів.

High-definition Audio (HD audio)

High-definition audio (HD audio) refers to high-bandwidth audio used in recorded music. It is usually sampled above 44100 Hz with more than 16-bit depth. It is used in commercial applications to reduce data loss and enhance quality. Formats include FLAC, ALAC, WAV, AIFF, and DSD. However, not all files in these formats are truly HD.

Аудіо високої чіткості (HD-аудіо)

Аудіо високої чіткості (HD-аудіо) – це широкосмуговий звук, який використовується у записаній музиці. Зазвичай дискретизується на частоті понад 44100 Гц і має глибину понад 16 біт. Його використовують у комерційних цілях для зменшення втрати даних і підвищення якості. До форматів належать FLAC, ALAC, WAV, AIFF і DSD. Проте не кожен файл у цих форматах є дійсно HD-аудіо.

HIPAA-compliant Email

A HIPAA-compliant email is a service that ensures security measures to comply with the Health Insurance Portability and Accountability Act (HIPAA), which regulates the use of sensitive health data.

Providers can ensure compliance by using encryption, creating secure systems, or requiring client consent. HIPAA also applies to third-party providers like ISPs and email hosts. End-to-end encryption is often used to prevent unauthorized access.

Електронна пошта, що відповідає вимогам HIPAA

Електронна пошта, що відповідає вимогам HIPAA – це сервіс, який забезпечує відповідні заходи безпеки для дотримання Закону про переносимість і відповідальність за медичне страхування (HIPAA), що регулює використання конфіденційної медичної інформації.

Постачальники можуть забезпечити відповідність HIPAA за допомогою шифрування, створення захищених систем або отримання згоди клієнта. HIPAA також охоплює сторонні сервіси, такі як інтернет-провайдери та поштові хости. Часто використовується наскрізне шифрування для захисту даних.

Home Key

The Home key is found on most keyboards and is supported by many operating systems and applications. Its main function is to move the cursor to the beginning of a line, document, page, screen, or worksheet cell. It is often used for navigation in word processors. It performs the opposite of the End key. On keyboards without a Home key, its function can be replaced with a combination of function and arrow keys. In read-only documents, it scrolls to the beginning. In editable ones, it moves the cursor to the beginning.With Shift, it may select all text before the cursor. In some software, it may open a menu screen.

Клавіша Home

Клавіша Home є на більшості клавіатур і підтримується багатьма операційними системами та програмами. Її основна функція – перемістити курсор на початок рядка, документа, сторінки, екрана або комірки. Часто використовується для навігації в текстових редакторах. Виконує протилежну функцію клавіші End. На клавіатурах без клавіші Home її функцію можна замінити поєднанням функціональної клавіші та клавіші зі стрілкою. У нередагованих документах прокручує на початок. У редагованих – переміщує курсор на початок. У поєднанні з Shift може виділити весь текст перед курсором. У деяких програмах може відкривати меню.

HomePlug

HomePlug refers to devices that transmit data like Ethernet, USB, or Wi-Fi via electrical wiring in a building to connect computers and other devices. Introduced in 2001, HomePlug became a standard supported by the HomePlug Powerline Alliance. It allows easy Ethernet connection by plugging into a regular power socket.

HomePlug

HomePlug – це пристрої, які передають дані (Ethernet, USB, Wi-Fi) через електропроводку будинку для з'єднання комп'ютерів та інших пристроїв. Представлений у 2001 році, HomePlug став стандартом, підтримуваним альянсом HomePlug Powerline Alliance. Дозволяє легко підключатися до Ethernet через звичайну розетку.

Hosted Virtual Desktop (HVD)

A Hosted Virtual Desktop (HVD) is a type of virtual desktop infrastructure (VDI) where the desktop environment is hosted on a remote server in a data center instead of being locally installed on the user's device. The user accesses this desktop through a client, usually over the internet. The HVD provides the user with a fully functional desktop experience, but the computing power, storage, and

Віртуальний робочий стіл

Віртуальний робочий стіл, що розміщується на сервері (Hosted Virtual Desktop, HVD) – це тип інфраструктури віртуальних робочих столів (VDI), де робоче середовище розміщується на віддаленому сервері в дата-центрі, а не на локальному пристрої користувача. Користувач отримує доступ до цього робочого столу через клієнтське програмне

processing are handled by the server, not the local machine. This allows for easier management, better security, and remote access from any device.

забезпечення, зазвичай через Інтернет. HVD надає користувачу повноцінний досвід роботи на робочому столі, але обчислювальна потужність, зберігання та обробка даних здійснюються сервером, а не локальною машиною. Це дозволяє простіше управляти, забезпечує кращу безпеку та можливість віддаленого доступу з будь-якого пристрою.

Hot Add

Hot add refers to the ability to dynamically add hardware, virtual or physical, to a running system without downtime. This allows system administrators to reallocate resources and services without shutting down operations. It often requires checking system resources, processor compatibility, and scheduling impact. Hot add is widely used in virtualization environments to efficiently manage computing power and memory.

Гаряче додавання

Гаряче додавання – це можливість динамічного додавання обладнання, віртуального або фізичного, до працюючої системи без її зупинки. Це дозволяє системним адміністраторам повторно розподіляти ресурси та послуги без відключення систем. Часто потребує перевірки ресурсів системи, сумісності процесора та впливу на планувальники. Гаряче додавання широко використовується у віртуалізованих середовищах для ефективного керування обчислювальною потужністю та пам’яттю.

Hotlinking

Hotlinking refers to when a website uses a link to another website to generate images or other files, rather than saving a copy of these files and installing them locally. It effectively outsources the energy used to display images or to load other kinds of files.

Hotlinking can be prevented by methods such as using .Htaccess files. Some types of hotlinking are becoming more common due to enhanced tools in platforms like Facebook. The process involves referencing images from their original sources, made easier by improved internet and hosting services.

Гарячі посилання

Гарячі посилання – це коли вебсайт використовує посилання на інший вебсайт для завантаження зображень або інших файлів, замість збереження копії цих файлів і локального розміщення. Це фактично передає навантаження на інший сервер.

Гарячим посиланням можна запобігти, наприклад, за допомогою файлів Htaccess. Деякі типи гарячих посилань стали більш поширеними через удосконалення інструментів соціальних платформ. Це посилання на зображення з першоджерела, полегшене розвитком інтернет-технологій.

HTML Tag

An HTML tag is a set of characters forming a formatting command on a web page. Tags structure and define the visual content in HTML. They include elements like paragraphs, tables, headlines, and more. A tag usually consists of an opening and closing part (e.g., and), with optional attributes in the opening tag. HTML tags are fundamental in web development and often used with CSS for styling.

Тег HTML

Тег HTML – це набір символів, що формує команду форматування на вебсторінці. Теги структурують і визначають візуальний вміст у HTML. Вони охоплюють елементи, як-от абзаци, таблиці, заголовки тощо. Зазвичай тег має відкриваючу і закриваючу частини (наприклад, і) з можливими атрибутами у відкриваючому тегі. HTML-теги є основою веброзробки й часто використовуються разом із CSS для стилізації.

HTTP Headers

HTTP headers are metadata or key-value pairs that are sent between the client and the server in an HTTP request or response. They provide essential information about the request or response, such as content type, encoding, cache settings, cookies, and the status of the request. Headers allow for control over data transfer, security, and how the server handles requests. Examples include «Content-Type» (which specifies the type of content being sent) and «Authorization» (which provides authentication credentials).

HTTP-заголовки

HTTP-заголовки – це метадані або пари ключ-значення, які передаються між клієнтом і сервером у HTTP-запиті або HTTP-відповіді. Вони надають важливу інформацію про запит чи відповідь, таку як тип вмісту, кодування, налаштування кешування, cookies та статус запиту. Заголовки дозволяють контролювати передачу даних, безпеку та спосіб обробки запитів на сервері. Прикладами є заголовки «Content-Type» (який вказує тип відправленого вмісту) та «Authorization» (який містить дані для аутентифікації).

HTTP Request Header

An HTTP request header is a part of a network packet sent by a browser or client to a web server to request a specific page or data. It is used in web communications to deliver user requests. The header is plain text and includes details like the requested page (URI), the source IP and port, the host (destination

Заголовок HTTP-запиту

Заголовок HTTP-запиту – це частина мережевого пакета, який браузер або клієнт надсилає вебсерверу для отримання конкретної сторінки або даних. Він використовується у вебкомунікаціях для передачі запитів користувачів. Заголовок складається з простого тексту та містить такі дані:

server), accepted data types (e.g., HTML, XML), and the user's browser type. This helps the server understand and respond correctly to the request. After receiving the request, the server sends back a corresponding HTTP response header.

запитувана сторінка (URI), IP-адреса та порт відправника, хост (сервер призначення), типи даних, які браузер може прийняти (наприклад, HTML, XML), а також тип браузера користувача. Це дозволяє серверу коректно обробити запит і надіслати відповідь у вигляді HTTP-відповіді.

Hug of Death

In IT, the phrase "hug of death" describes a situation where posting content on a certain website leads to an exponential increase in traffic, eventually making the content inaccessible. It's usually the result of something going viral. Many cases are linked to Reddit, where content shared on the platform causes spikes in traffic to the original source. This can overwhelm servers or applications. To prevent this, webmasters must monitor CPU and memory resources.

«Обійми смерті»

В IT фраза «обійми смерті» описує ситуацію, коли розміщення матеріалу на певному сайті призводить до експоненційного зростання трафіку, внаслідок чого контент стає недоступним. Зазвичай це наслідок вірусного поширення. Багато випадків пов'язані з Reddit, де контент, розміщений на платформі, викликає сплески трафіку на оригінальному сайті. Це може перевантажити сервери або програми. Щоб уникнути цього, вебмайстрам слід стежити за ресурсами процесора й пам'яті.

Huge Pipes

"Huge pipes" refers to high-speed or high-bandwidth internet connections, also called fat pipes. It's often used in contrast to average connections, such as those replaced by Google Fiber's fiber optic lines.High bandwidth is essential for streaming, videoconferencing, backups, and professional use like telemedicine.

«Величезні труби»

«Величезні труби» означають високошвидкісне або високопродуктивне інтернет-з'єднання, також відоме як «товсті труби». Часто використовується на противагу звичайним з'єднанням, наприклад, тим, що їх замінює Google Fiber за допомогою оптоволокна. Висока пропускна здатність необхідна для потокового відео, відеозв'язку, резервного копіювання та професійного використання, наприклад, телемедицини.

Hyper-V virtual hard disk (VHDX)

A Hyper-V virtual hard disk (VHDX) is a disk image file format used to create a virtual hard disk within Windows Server 2012-based virtualization environments. VHDX allows the creation and provisioning of virtual or logical disk storage to virtual machines. It is an enhancement of the older VHD format from Windows Server 2008.

VHDX works like a standard virtual hard disk but is actually a file format. It can store up to 64 TB of data, supports differencing disks, and offers better protection against disk corruption.

It is created and managed using built-in Windows Server 2012 tools such as DiskPart, Hyper-V Manager, and Disk Manager.

The size of a VHDX file can be either fixed or dynamically adjusted depending on requirements.

Although VHDX is not backward compatible, older VHD formats can be converted to VHDX within the Windows Server 2012 environment.

Віртуальний жорсткий диск Hyper-V (VHDX)

Віртуальний жорсткий диск Hyper-V (VHDX) – це формат файлу образу диска, який використовується для створення віртуального жорсткого диска у середовищах віртуалізації на базі Windows Server 2012. VHDX дозволяє створювати та надавати віртуальним машинам віртуальний або логічний дисковий простір. Це вдосконалена версія формату VHD, який використовувався у Windows Server 2008.

Формат VHDX функціонує як звичайний віртуальний жорсткий диск, хоча насправді є форматом файлу. Він може зберігати до 64 ТБ даних, підтримує створення різних (відмінних) дисків і забезпечує кращий захист від пошкодження даних на диску.

VHDX створюється і керується за допомогою вбудованих інструментів Windows Server 2012, таких як DiskPart, Hyper-V Manager і Disk Manager.

Розмір файлу VHDX може бути фіксованим або динамічно змінюватися відповідно до потреб користувача чи навантаження системи.

Хоча VHDX не підтримує зворотну сумісність, попередні формати VHD можна конвертувати у VHDX у середовищі Windows Server 2012.

I

I2P

I2P – is an open source project attempting to create ananonymousnetwork for communicationover the Internet. Communication in I2P is encrypted to provide protection and security against attackers and hackers.

I2P is an open-source free technology. Many applications, such as mail, IRC chat, peer-to peer applications, file sharing and instant messenger, use I2P interface to allow anonymous communication and operation for both the individual users and organizations. I2P possesses its own internal network database, which is used to distribute contact and routing information in a securely.

I2P

I2P – це проект з відкритим вихідним кодом, який намагається створити анонімну мережу для спілкування в Інтернеті. Спілкування в I2P шифрується, щоб забезпечити захист від зловмисників і хакерів.

I2P – це безкоштовна технологія з відкритим вихідним кодом. Багато додатків, таких як пошта, IRC-чат, пірінгові програми, обмін файлами та миттєві повідомлення, використовують інтерфейс I2P для забезпечення анонімного спілкування та роботи як для окремих користувачів, так і для організацій. I2P має власну внутрішню мережеву базу даних, яка використовується для безпечного розповсюдження контактної та маршрутної інформації.

IBM PC

IBM PC is the brand name of the first popular commercial PC developed by the IBM Corporation. In 1981, the IBM PC was launched with the model number IBM 5150 in an attempt to set an industry benchmark subsequent to the IBM 5100 and several other computers.

The IBM PC was also code named Acorn.

IBM PC

IBM PC – торгова марка першого популярного комерційного комп'ютера, розробленого корпорацією IBM. У 1981 році IBM PC був випущений під номером моделі IBM 5150 у спробі встановити галузевий стандарт після IBM 5100 та кількох інших комп'ютерів.

IBM PC також мав кодову назву Acorn.

IceWM

IceWM is a windows manager graphical user interface (GUI) for the open-source X Window System, a technology that allows GUI development in networked computers. The IceWM GUI provides a light build along with customizable features, and runs on various operating systems, including Linux and Windows. The system requirements for successful operation are fairly minimal.

iCloud

iCloud is a cloud computing solution by Apple Computer Inc. that provides cloud storage and apps for desktop, tablet and mobile devices.

iCloud provides the ability to store documents, videos, photos, music and other data online and the ability to sync it between iOS-powered devices.

iCloud is a hybrid cloud solution that combines infrastructure and software services to provide a suite of apps and services, enabling users to add, remove and synchronize typical data files, contacts and bookmarks on selected Apple devices. This data is then stored and backed up on iCloud's remote storage server.

Ideavirus

An ideavirus is an idea that spreads through various networks like the Internet and grows rapidly within a target population. It usually comes from a single person. The term ideavirus was coined by

IceWM

IceWM – це графічний інтерфейс користувача (GUI) для менеджера вікон з відкритим вихідним кодом X Window System, технології, яка дозволяє розробляти GUI на мережевих комп'ютерах. Графічний інтерфейс IceWM має полегшену збірку з можливістю налаштування і працює на різних операційних системах, включаючи Linux і Windows. Системні вимоги для успішної роботи досить мінімальні.

iCloud

iCloud – це рішення для хмарних обчислень від Apple Computer Inc., яке надає хмарне сховище та додатки для настільних, планшетних і мобільних пристроїв.

iCloud надає можливість зберігати документи, відео, фотографії, музику та інші дані в Інтернеті, а також синхронізувати їх між пристроями на базі iOS.

iCloud – це гібридне хмарне рішення, яке поєднує в собі інфраструктуру та програмне забезпечення для надання набору додатків і сервісів, що дозволяє користувачам додавати, видаляти та синхронізувати типові файли даних, контакти та закладки на вибраних пристроях Apple. Потім ці дані зберігаються та створюються резервні копії на віддаленому сервері iCloud.

Ідеовірус

Ідеовірус – це ідея, яка поширюється через різні мережі, такі як Інтернет, і швидко зростає серед цільової аудиторії. Зазвичай вона походить від однієї людини. Термін

marketer Seth Godin in his book, "Unleashing the Ideavirus." Like a virus, an ideavirus infects and changes every individual it touches, even in just a very small way. The outcome of this infection may not be noticeable, or it can lead to the creation of new products or companies. With each person influenced, the idea is interpreted, modified and often improved before it is passed on.

«ідеовірус» ввів маркетолог Сет Годін у своїй книзі «Випустити на волю ідеовірус». Подібно до вірусу, ідеовірус інфікує і змінює кожну людину, якої він торкається, навіть у дуже незначній мірі. Результат цієї інфекції може бути непомітним, а може призвести до створення нових продуктів або компаній. З кожною людиною, на яку впливає ідея, вона інтерпретується, модифікується і часто вдосконалюється перед тим, як її передають далі.

Identifier

An identifier, in C#, is the user-defined name of a program element. It can be a namespace, class, method, variable or interface.

Identifiers are symbols used to uniquely identify a program element in the code. They are also used to refer to types, constants, macros and parameters. An identifier name should indicate the meaning and usage of the element being referred.

Ідентифікатор

Ідентифікатор у C# – це визначене користувачем ім'я елемента програми. Це може бути простір імен, клас, метод, змінна або інтерфейс.

Ідентифікатори – це символи, що використовуються для однозначної ідентифікації програмного елемента в коді. Вони також використовуються для посилання на типи, константи, макроси та параметри. Ім'я ідентифікатора повинно вказувати на значення та використання елемента, на який посилаються.

Identifier for Advertisers (IFA or IDFA)

Identifier for Advertisers (IFA or IDFA) is a temporary device identifier used by the Apple set of handheld devices. It provides device identification while giving end users the ability to limit the device/consumer information accessed by advertisers or apps. A successor of Unique Device Identifier (UDID), IFA is available on all devices with versions iOS 6 and later.

Ідентифікатор для рекламодавців (IFA або IDFA)

Ідентифікатор для рекламодавців (IFA або IDFA) – це тимчасовий ідентифікатор пристрою, який використовується в лінійці портативних пристроїв Apple. Він забезпечує ідентифікацію пристрою, надаючи кінцевим користувачам можливість обмежити доступ рекламодавців або додатків до інформації про пристрій/споживача. IFA є наступником унікального ідентифікатора пристрою (UDID) і доступний на всіх пристроях з версією iOS 6 і вище.

Identity Management (ID Management/IdM)

Identity management (ID Management/ IdM) is the process of identifying, authenticating and authorizing an individual or group of individuals on an application, system or comprehensive IT environment.

It is an information security domain that deals with the administrative tasks and processes of validating the identity and controlling the access of individuals/users for hardware or software.

Управління ідентифікацією (ID Management/IdM)

Управління ідентифікацією (ID Management/ IdM) – це процес ідентифікації, автентифікації та авторизації особи або групи осіб у додатку, системі або комплексному IT-середовищі.

Це сфера інформаційної безпеки, яка займається адміністративними завданнями та процесами перевірки ідентичності та контролю доступу осіб/користувачів до апаратного чи програмного забезпечення.

Identity Resolution

Identity resolution is a data management process through which an identity is searched and analyzed between disparate data sets and databases to find a match and/or resolve identities. Identity resolution enables an organization to analyze a particular individual’s or entity’s identity based on its available data records and attributes.

Розпізнавання ідентичності

Розпізнавання ідентичності – це процес управління даними, за допомогою якого здійснюється пошук та аналіз ідентичності між різними наборами даних і базами даних для пошуку збігів та/або розпізнавання ідентичності. Розв'язання ідентифікаційних даних дозволяє організації аналізувати ідентичність конкретної особи чи організації на основі наявних записів даних та атрибутів.

IEEE 488

IEEE 488 is a digital communications bus specification invented by Hewlett Packard and used to connect short range communication devices. This term is also known as the general purpose interface bus (GPIB) or the Hewlett Packard interface bus (HP-IB). The IEEE 488 has a 24-pin connector and is used for double headed design.

IEEE 488

IEEE 488 – це специфікація цифрової комунікаційної шини, винайдена компанією Hewlett Packard, яка використовується для з'єднання пристроїв зв'язку малого радіусу дії. Цей термін також відомий як інтерфейсна шина загального призначення (GPIB) або інтерфейсна шина Hewlett Packard (HP-IB).

IEEE 488 має 24-контактний роз'єм і використовується для подвійної конструкції.

IEEE 802.1 Working Group (IEEE 802.1)

The IEEE 802.1 Working Group (IEEE 802.1) is an IEEE Standards Association (IEEE-SA) group established to ensure network management and monitoring capabilities in networks developed according to IEEE 802 standards.

The Internetworking group handles overall architecture, link aggregation, protocol addressing, network path identification/ calculation and other technical practices and recommendations.

Робоча група IEEE 802.1 (IEEE 802.1)

Робоча група IEEE 802.1 (IEEE 802.1) – це група Асоціації стандартів IEEE (IEEE-SA), створена для забезпечення можливостей мережевого управління і моніторингу в мережах, розроблених відповідно до стандартів IEEE 802.

Група з питань Інтернет-мереж займається загальною архітектурою, агрегацією каналів, адресацією протоколів, ідентифікацією/ розрахунком мережевих шляхів та іншими технічними практиками і рекомендаціями.

IEEE 802.11

IEEE 802.11 refers to the set of standards that define communication for wireless LANs (wireless local area networks, or WLANs). The technology behind 802.11 is branded to consumers as Wi-Fi.

As the name implies, IEEE 802.11 is overseen by the IEEE, specifically the IEEE LAN/MAN Standards Committee (IEEE 802). The current version of the standard is IEEE 802.11-2007.

In other words, IEEE 802.11 is the set of technical guidelines for implementing Wi-Fi. Selling products under this trademark is overseen by an industry trade association by the name of the Wi-Fi Alliance.

IEEE 802.11

IEEE 802.11 відноситься до набору стандартів, які визначають зв'язок для бездротових локальних мереж (бездротових локальних мереж, або WLAN). Технологія, що лежить в основі 802.11, відома споживачам як Wi-Fi.

Як випливає з назви, IEEE 802.11 знаходиться під наглядом IEEE, зокрема, Комітету зі стандартів IEEE LAN/MAN (IEEE 802). Поточна версія стандарту – IEEE 802.11-2007.

Іншими словами, IEEE 802.11 – це набір технічних рекомендацій для реалізації Wi-Fi. Продаж продуктів під цією торговою маркою контролюється галузевою торговою асоціацією Wi-Fi Alliance.

IEEE 802.11a

IEEE 802.11a is an amendment to the 802.11 standard for wireless LANs. It is of of the specifications that is more commonly known as Wi-Fi.

802.11a uses radio frequencies in the 5 GHz band and supports theoretical throughput of up to 54 Mbps. The standard uses the same base protocol as the original 802.11 standard, but uses orthogonal frequency-division multiplexing (OFDM).

Also known as IEEE 802.11a-1999.

IEEE 802.11a

IEEE 802.11a – це поправка до стандарту 802.11 для бездротових локальних мереж. Це одна зі специфікацій, яка більш відома як Wi-Fi.

802.11a використовує радіочастоти в діапазоні 5 ГГц і підтримує теоретичну пропускну здатність до 54 Мбіт/с. Стандарт використовує той самий базовий протокол, що і оригінальний стандарт 802.11, але застосовує ортогональне мультиплексування з частотним розділенням каналів (OFDM).

Також відомий як IEEE 802.11a-1999.

IEEE 802.11ac

IEEE 802.11ac is a pending amendment to the IEEE 802.11 standard that defines proper implementation and/or deployment of wireless local area network (WLAN) technology.

IEEE 802.11ac

IEEE 802.11ac – це очікувана поправка до стандарту IEEE 802.11, яка визначає належне впровадження та/ або розгортання технології бездротових локальних мереж (WLAN).

IEEE 802.11b

IEEE 802.11b is an amendment to the 802.11 standard for wireless LANs. It is of of the specifications that is more commonly known as Wi-Fi.

802.11b uses the same unregulated radio frequency band of 2.4 GHz that was used by the original 802.11 standard, but operates at theoretical data throughput of 11 Mbps. 801.11.b was rolled up into 802.11-2007 along with amendments a, b, d, e, g, h, i, j.

This term is also known as IEEE 802.11b-1999

IEEE 802.11b

IEEE 802.11b – це поправка до стандарту 802.11 для бездротових локальних мереж. Це одна зі специфікацій, яка більш відома як Wi-Fi.

Стандарт 802.11b використовує ту ж саму нерегульовану смугу радіочастот 2,4 ГГц, що і оригінальний стандарт 802.11, але працює з теоретичною пропускною здатністю 11 Мбіт/с. 801.11.b був включений в стандарт 802.11-2007 разом з поправками a, b, d, e, g, h, i і j.

Цей термін також відомий як IEEE 802.11b-1999

IEEE 802.11d

IEEE 802.11d is an IEEE 802.11 amendment that adds geographical regulations to the original standard. IEEE 802.11d facilitates the development of wireless local area network (WLAN) devices that comply with the wireless communications regulations of their respective countries.

IEEE 802.11d is also known as IEEE 802.11d-2001.

IEEE 802.11d allows a device to self-configure and operate according to the regulations of its operating country and includes parameters like country name, channel quantity and maximum transmission level.

IEEE 802.11d

IEEE 802.11d – це поправка до стандарту IEEE 802.11, яка додає географічні правила до оригінального стандарту. IEEE 802.11d полегшує розробку пристроїв для бездротових локальних мереж (WLAN), які відповідають нормам бездротового зв'язку відповідних країн.

IEEE 802.11d також відомий як IEEE 802.11d-2001.

IEEE 802.11d дозволяє пристрою самостійно конфігуруватися і працювати відповідно до правил країни, в якій він експлуатується, і включає такі параметри, як назва країни, кількість каналів і максимальний рівень передачі.

IEEE 802.11g

IEEE 802.11g is an amendment to the 802.11 standard for wireless LANs. It is of of the specifications that is more commonly known as Wi-Fi.

IEEE 802.11g

IEEE 802.11g – це поправка до стандарту 802.11 для бездротових локальних мереж. Це одна зі специфікацій, яка більш відома як Wi-Fi.

IEEE 802.11h

IEEE 802.11h is an IEEE 802.11 amendment that specifies wireless local area network (WLAN) extensions. It addresses network spectrum interference issues and allows wireless IEEE 802.11 devices to work with other wireless technologies.

IEEE 802.11h is also known as IEEE 802.11h-2003.

IEEE 802.11h

IEEE 802.11h – це поправка до стандарту IEEE 802.11, яка визначає розширення бездротових локальних мереж (WLAN). Вона вирішує проблеми інтерференції мережевого спектру і дозволяє бездротовим пристроям IEEE 802.11 працювати з іншими бездротовими технологіями.

Поправка IEEE 802.11h також відома як IEEE 802.11h-2003.

IEEE 802.11i

IEEE 802.11i is an IEEE 802.11 amendment used to facilitate secure end-to-end communication for wireless local area networks (WLAN). IEEE 80211i improves mechanisms for wireless authentication, encryption, key management and detailed security.

IEEE 802.11i is also known as IEEE 802.11i-2004.

IEEE 802.11i also incorporates Temporal Key Integrity Protocol (TKIP) and Counter Mode/CBC-MAC Protocol (CCMP) for data transmission confidentiality, protection, packet authentication and encryption.

IEEE 802.11i

IEEE 802.11i – це поправка до стандарту IEEE 802.11, що використовується для полегшення безпечного наскрізного зв'язку в бездротових локальних мережах (WLAN). IEEE 80211i покращує механізми бездротової автентифікації, шифрування, управління ключами та детальну безпеку.

Поправка IEEE 802.11i також відома як IEEE 802.11i-2004.

IEEE 802.11i також включає протокол цілісності тимчасового ключа (Temporal Key Integrity Protocol, TKIP) і протокол лічильника/ CBC-MAC (CCMP) для забезпечення конфіденційності передачі даних, захисту, автентифікації пакетів і шифрування.

IEEE 802.11j

IEEE 802.11j is an IEEE 802.11 amendment that extends wireless communication and signaling for 4.9 GHz and 5 GHz band operations in Japan. IEEE 802.11j facilitates communications for outdoor, indoor and mobile applications that comply with wireless local area network (WLAN) regulations.

IEEE 802.11j is also known as IEEE 802.11j-2004.

IEEE 802.11j adds channels and frequencies to Japan’s 4.9 GHz and 5 GHz bands for improved performance and capacity and reduced interference with coexisting signals

IEEE 802.11j

IEEE 802.11j – це поправка до стандарту IEEE 802.11, яка розширює можливості бездротового зв'язку і сигналізації для роботи в діапазонах 4,9 ГГц і 5 ГГц в Японії. IEEE 802.11j полегшує зв'язок для зовнішніх, внутрішніх і мобільних додатків, які відповідають нормам бездротових локальних мереж (WLAN).

Поправка IEEE 802.11j також відома як IEEE 802.11j-2004.

IEEE 802.11j додає канали і частоти в японські діапазони 4,9 ГГц і 5 ГГц для підвищення продуктивності і пропускної здатності, а також зменшення інтерференції з існуючими сигналами.

IEEE 802.11m

IEEE 802.11m is an IEEE Task Group m (TGm) initiative geared toward maintaining the IEEE 802.11 standard and related documentation. It is comprised of all IEEE 802.11 amendments and revisions applied to the IEEE 802.11 standard for wireless local area network (WLAN) services and compatible devices.

IEEE 802.11m is also known as 802.11 Cleanup.

IEEE 802.11m is based on two documented initiatives: IEEE 802.11ma and IEEE 802.11mb. IEEE 802.11ma is comprised of the eight amendments (a, b, d, e, g, h, i, j) editorially applied through 2003. IEEE 802.mb is the current maintenance draft version.

IEEE 802.11m

IEEE 802.11m – це ініціатива IEEE Task Group m (TGm), спрямована на підтримку стандарту IEEE 802.11 і пов'язаної з ним документації. Ініціатива включає в себе всі зміни і доповнення до стандарту IEEE 802.11, що стосуються послуг бездротових локальних мереж (WLAN) і сумісних з нею пристроїв.

Ініціатива IEEE 802.11m також відома як 802.11 Cleanup.

IEEE 802.11m базується на двох задокументованих ініціативах: IEEE 802.11ma та IEEE 802.11mb. IEEE 802.11ma складається з восьми поправок (a, b, d, e, g, h, i, j), які редагувалися до 2003 року. IEEE 802.mb є поточною редакцією проекту стандарту.

IEEE 802.11n

IEEE 802.11n is an IEEE 802.11 amendment that modifies the physical and media access control (MAC) layer specifications to increase overall throughput for local area networks (LAN), metropolitan area networks (MAN) and wireless local area networks (WLAN).

IEEE 802.11n is also known as IEEE 802.11n-2009 or draft n.

IEEE 802.11n

IEEE 802.11n – це поправка до стандарту IEEE 802.11, яка змінює специфікації фізичного рівня і рівня керування доступом до середовища (MAC) для збільшення загальної пропускної здатності локальних мереж (LAN), міських мереж (MAN) і бездротових локальних мереж (WLAN).

Поправка IEEE 802.11n також відома як IEEE 802.11n-2009 або проект n.

IEEE 802.11r

IEEE 802.11r is an amendment to the 802.11 standard for the deployment of IP-based telephony over 802.11-based phone devices. The IEEE 802.11r amendment is designed to increase handoff speed between access points in a wireless local area network (WLAN).

IEEE 802.11r serves as a fast-roaming standard that addresses connectivity and is critical to applications that require high quality and low latency, particularly Voice over Internet Protocol (VoIP).

IEEE 802.11r is also known as the fast basic service set.

IEEE 802.11r

IEEE 802.11r – це поправка до стандарту 802.11 для розгортання IP-телефонії через телефонні пристрої на базі стандарту 802.11. Поправка IEEE 802.11r призначена для збільшення швидкості передачі даних між точками доступу в бездротовій локальній мережі (WLAN).

IEEE 802.11r слугує стандартом швидкого роумінгу, який забезпечує з'єднання і є критично важливим для додатків, що вимагають високої якості та низької затримки, зокрема, для передачі голосу через Інтернет-протокол (VoIP).

IEEE 802.11r також відомий як швидкий базовий набір послуг

IEEE 802.11s

IEEE 802.11s is an IEEE 802.11 amendment that specifies the creation of a wireless mesh network (WMN) in a wireless local area network (WLAN). It facilitates direct communication by provisioning multiple wireless nodes for interconnection and communication without a required access point (AP).

IEEE 802.11s extends the media access control (MAC) sublayer of the Open Systems Interconnection (OSI) model's data link layer by allowing self-configuration of IEEE 802.11 stations for multi-hop networks with multicast and unicast transmission support.

IEEE 802.11s

IEEE 802.11s – це поправка до стандарту IEEE 802.11, яка визначає створення бездротової комірчастої мережі (WMN) у бездротовій локальній мережі (WLAN). Вона полегшує прямий зв'язок, надаючи кілька бездротових вузлів для взаємозв'язку і комунікації без обов'язкової точки доступу (AP).

Стандарт IEEE 802.11s розширює підрівень керування доступом до середовища (MAC) канального рівня моделі взаємодії відкритих систем (OSI), дозволяючи станціям IEEE 802.11 самостійно конфігуруватися для створення багатохопових мереж з підтримкою багатоадресної та одноадресної передачі даних.

IEEE 802.11u

IEEE 802.11u is a standard for external networks. It is part of the greater 802.11u "family" of standards that governs the use of portable or mobile electronic devices in wireless network setups.

IEEE 802.11u

IEEE 802.11u – це стандарт для зовнішніх мереж. Він є частиною більшого "сімейства" стандартів 802.11u, яке регулює використання портативних або мобільних електронних пристроїв у бездротових мережах.

IEEE 802.1X

IEEE 802.1X is a standard component of the IEEE 802.11 network protocol group established by the Institute of Electrical and Electronics Engineers (IEEE). IEEE 802.1X adheres to IEEE 802.11 protocols to enhance wireless network security.

IEEE 802.1X controls access to wireless or virtual local area networks (VLAN) and applies traffic policies based on user identity and credentials. IEEE 802.1X ensures a user authentication framework where network access is denied upon failed authentication.

Built for wired networks, IEEE 802.1X requires very little processing power and is well-suited to wireless LAN applications.

IEEE 802.1X

IEEE 802.1X є стандартним компонентом групи мережевих протоколів IEEE 802.11, створеної Інститутом інженерів з електротехніки та електроніки (IEEE). IEEE 802.1X дотримується протоколів IEEE 802.11 для підвищення безпеки бездротових мереж.

IEEE 802.1X контролює доступ до бездротових або віртуальних локальних мереж (VLAN) і застосовує політики трафіку на основі ідентифікації користувача та його облікових даних. IEEE 802.1X забезпечує систему автентифікації користувачів, яка відмовляє в доступі до мережі в разі невдалої автентифікації.

Створений для дротових мереж, стандарт IEEE 802.1X потребує дуже мало обчислювальної потужності і добре підходить для додатків бездротових локальних мереж.

If Statement

An if statement, in C#, is a programming construct in C# used to selectively execute code statements based on the result of evaluating a Boolean expression. The Boolean expression must return either a true or false value.

The if statement is used as a control statement to branch to different sections of code depending on the result of the Boolean conditional expression. The expression is stated within parentheses and evaluated during execution. If the expression results in a true value, the code following the if statement is executed. Otherwise, the code following an optional “else” statement is executed. If there is no else statement, execution continues with the code after the if block.

Оператор if

Оператор if в C# – це конструкція програмування в C#, яка використовується для вибіркового виконання операторів коду на основі результату обчислення логічного виразу. Булевий вираз повинен повертати значення true або false.

Оператор if використовується як керуючий оператор для розгалуження на різні ділянки коду залежно від результату булевого умовного виразу. Вираз задається в круглих дужках і обчислюється під час виконання. Якщо результат виразу дорівнює true, виконується код, що слідує за оператором if. В іншому випадку виконується код після необов'язкового оператора else. Якщо оператор else відсутній, виконання продовжується з кодом після блоку if.

IF Statement

The if statement is a programming language test that is done to determine whether a condition holds true. If the condition that is being tested holds true, a certain code is executed by the programmer that differs if it holds false. The if statement can be described with the Boolean expression, which produces a true or false value based on evaluation. The if statement is part of this evaluation.

Оператор if

Оператор if – це тест у мові програмування, який виконується для визначення того, чи виконується умова. Якщо умова, що перевіряється, є істинною, програміст виконує певний код, який відрізняється від того, якщо вона є хибною. Оператор if можна описати за допомогою булевого виразу, який видає значення true або false на основі оцінки. Оператор if є частиною цього обчислення.

Imaging software

Imaging software is a type of graphic design software used to create, edit and manipulate images on a computer. Imaging software is designed to work on photographs for images created by digital cameras, camcorders or related devices.

Imaging software may also be called digital imaging software or image editing software.

Програмне забезпечення для роботи з зображеннями

Програмне забезпечення для роботи з зображеннями – це тип графічного програмного забезпечення, що використовується для створення, редагування та маніпулювання зображеннями на комп'ютері. Програмне забезпечення для обробки зображень призначене для роботи з фотографіями, створеними цифровими фотоапаратами, відеокамерами або подібними пристроями.

Програмне забезпечення для роботи з зображеннями також може називатися програмним забезпеченням для роботи з цифровими зображеннями або програмним забезпеченням для редагування зображень.

Implementation

Implementation is often used in the tech world to describe the interactions of elements in programming languages. In Java, where the word is frequently used, to implement is to recognize and use an element of code or a programming resource that is written into the program.

Реалізація

Реалізація часто використовується у світі технологій для опису взаємодії елементів у мовах програмування. У мові Java, де це слово часто використовується, реалізувати означає розпізнати і використати елемент коду або програмний ресурс, який вписаний у програму.

Implicit Enhancement Point

An implicit enhancement point is a source code plug-in point provided in Advanced Business Application Programming (ABAP) programmed SAP objects. Unlike an explicit enhancement point or explicit enhancement section, implicit enhancement points are usually provided and exist for almost all SAP objects. Implicit enhancement points are usually hidden and need to be specified by a user to make them visible.

Неявна точка розширення

Неявна точка розширення – це точка підключення вихідного коду, яка передбачена в об'єктах SAP, запрограмованих за допомогою розширеного програмування бізнес-додатків (Advanced Business Application Programming, ABAP). На відміну від явної точки розширення або явної секції розширення, неявні точки розширення зазвичай передбачені та існують майже для всіх об'єктів SAP. Неявні точки вдосконалення зазвичай приховані і повинні бути вказані користувачем, щоб зробити їх видимими.

Inaccessible Member

An inaccessible member, in the context of C#, is a member that cannot be accessed by a specific type. An inaccessible member that cannot be accessed by one type can be accessible by another type.

As per the accessibility constraint in C#, several constructs require a type to be at least as accessible as a member or another type. Additionally, if the member is a method, delegate, or indexer, the return type and parameter types must be at least as accessible as the member itself. Use of an inaccessible member will result in a compile time error.

Недоступний член в контексті C#

Недоступний член в контексті C# – це член, до якого не може отримати доступ певний тип. Недоступний член, недоступний для одного типу, може бути доступним для іншого типу.

Згідно з обмеженням доступності в C#, деякі конструкції вимагають, щоб тип був щонайменше таким же доступним, як член або інший тип. Крім того, якщо член є методом, делегатом або індексатором, тип, що повертається, і типи параметрів повинні бути щонайменше такими ж доступними, як і сам член. Використання недоступного члена призведе до помилки під час компіляції.

In-app purchasing

In-app purchasing refers to the ability of a smartphone or mobile device to facilitate the sale of products or services within a specific application or "app." This added functionality has opened many new markets for the makers of various mobile applications. In-app purchasing functionality can take many forms in different applications, with different methodologies, functional features, and integration into an interface.

Внутрішні покупки

Внутрішні покупки – це здатність смартфона або мобільного пристрою полегшувати продаж товарів або послуг у певному додатку або "додатку". Ця додаткова функціональність відкрила багато нових ринків для розробників різних мобільних додатків. Функціонал купівлі через додаток може приймати різні форми в різних додатках, з різними методологіями, функціональними можливостями та інтеграцією в інтерфейс.

In-cell Technology

In-cell technology refers to a standard of displays that emerged in 2012 and allow mobile devices, such as smartphones, to have thinner form factors. They also allow devices to keep a low weight even when the display increases in size.

In-cell technology may also be called in-cell touch technology.

Технологія In-cell

Технологія In-cell відноситься до стандарту дисплеїв, який з'явився у 2012 році і дозволяє мобільним пристроям, таким як смартфони, мати тонший форм-фактор. Вони також дозволяють пристроям зберігати малу вагу, навіть коли дисплей збільшується в розмірі.

Внутрішньоклітинна технологія може також називатися сенсорною технологією.

Increment Operator

The increment operator, in C#, is a unary operator represented by the symbols "++". This operator is used in C# to increment the value of its operand by one. The type of the resulting value is the same as that of its operand. The operand in an increment operation can be a variable, a property access or an indexer access.

This operator is often used in loop constructs, such as the "for" loop, to increment the loop counter after executing the code within the loop. An increment operator is also used to change the pointer location by a value that is equal to the memory size of the pointer type used. Except for a pointer of type "void", the increment operator can be used for all other types of pointers. When used on a pointer, no exception is generated even when there is an overflow in the pointer's domain.

Оператор інкременту

Оператор інкременту в мові C# – це унарний оператор, який позначається символами «++». Цей оператор використовується в C# для збільшення значення операнду на одиницю. Тип результуючого значення збігається з типом його операнду. Операндом в операції інкременту може бути змінна, доступ до властивості або доступ до індексатора.

Цей оператор часто використовується в конструкціях циклів, таких як цикл for, для збільшення лічильника циклу після виконання коду всередині циклу. Оператор інкременту також використовується для зміни місцезнаходження вказівника на величину, що дорівнює розміру пам'яті типу вказівника, який використовується. За винятком покажчика типу void, оператор інкременту можна використовувати для всіх інших типів покажчиків. При його застосуванні до вказівника не генерується виключення навіть у випадку переповнення області видимості вказівника.

In-database Analytics

In-database analytics refers to a model of analysis where data processing is performed within a database to eliminate the overhead of moving large data sets to analytic applications. In such a model, the analytic logic is built into a database instead of in a separate application. Advantages of in-database analytics include parallel processing, scalability, analytic optimization and partitioning.

An in-database analytics system contains an enterprise data warehouse integrated with an analytic database platform. In-database analytics is used in applications that require intensive processing, primarily because datasets and data marts are effectively consolidated in an enterprise's data warehouse system, which facilitates and secures data analysis, processing and retrieval.

Аналітика в базі даних

Аналітика в базі даних – це модель аналізу, в якій обробка даних виконується всередині бази даних, щоб усунути накладні витрати, пов'язані з переміщенням великих наборів даних до аналітичних додатків. У такій моделі аналітична логіка вбудована в базу даних, а не в окремий додаток. Переваги аналітики в базі даних включають паралельну обробку, масштабованість, аналітичну оптимізацію та розділення.

Система аналітики в базі даних містить корпоративне сховище даних, інтегроване з платформою аналітичної бази даних. Внутрішня аналітика використовується в додатках, які потребують інтенсивної обробки, насамперед тому, що набори даних і вітрини даних ефективно консолідуються в системі сховища даних підприємства, що полегшує і захищає аналіз, обробку і пошук даних.

Independent Software Vendor (ISV)

An independent software vendor (ISV) is an individual or business that builds, develops and sells consumer or enterprise software. Although ISV-provided software is consumed by end users, it remains the property of the vendor.

An ISV is also known as a software publisher.

Незалежний постачальник програмного забезпечення (ISV)

Незалежний постачальник програмного забезпечення (ISV) – це фізична або юридична особа, яка створює, розробляє та продає споживче або корпоративне програмне забезпечення. Хоча програмне забезпечення, надане ISV, споживається кінцевими користувачами, воно залишається власністю постачальника.

ISV також відомий як видавець програмного забезпечення.

Independent Variable

In computing, an independent variable is any variable that changes its value under a process, program, event, or any computing-specific interaction.

It is used in computer programming to be assigned to a variable value, entity or process, or to calculate the value of a dependent variable.

Незалежна змінна

В обчисленнях незалежна змінна – це будь-яка змінна, яка змінює своє значення під впливом процесу, програми, події або будь-якої специфічної для обчислень взаємодії.

Використовується в комп'ютерному програмуванні для присвоєння значення змінній, об'єкту або процесу, або для обчислення значення залежної змінної.

Indigo

Indigo is a Microsoft technology for developing service-oriented applications built on the .NET framework. It's goal is to enable efficient application interaction with Windows OS-compatible software and other platforms. Indigo facilitates the development and interoperability of reliable and secure transactional software services on all OSs.

Indigo

Indigo – це технологія Microsoft для розробки сервіс-орієнтованих додатків, побудованих на платформі .NET. Її мета – забезпечити ефективну взаємодію додатків з програмним забезпеченням, сумісним з ОС Windows, та іншими платформами. Indigo полегшує розробку та інтероперабельність надійних і безпечних транзакційних програмних сервісів на всіх операційних системах.

Industrial, Scientific, and Medical Radio Band (ISM band)

The industrial, scientific, and medical radio band (ISM band) refers to a group of radio bands or parts of the radio spectrum that are internationally reserved for the use of radio frequency (RF) energy intended for scientific, medical and industrial requirements rather than for communications. ISM bands are generally open frequency bands, which vary according to different regions and permits.

Смуга радіочастот для промислового, наукового та медичного використання (ISM-діапазон)

Смуга радіочастот для промислового, наукового та медичного використання (ISM-діапазон) – це група радіодіапазонів або частин радіочастотного спектра, які на міжнародному рівні зарезервовані для використання радіочастотної енергії (РЧ), призначеної для наукових, медичних та промислових потреб, а не для зв'язку. Смуги ISM – це, як правило, відкриті смуги частот, які варіюються залежно від регіону та дозволів.

Infected File

An infected file is a file that has been impacted by a computer virus in any of several ways. Anti-virus technologies work to quarantine an infected file, and may, in some cases, repair the file by removing the virus code. Infected files often come from remote sources through downloads to infect a host computer.

Заражений файл

Заражений файл – це файл, який був уражений комп'ютерним вірусом у будь-який з декількох способів. Антивірусні технології працюють над тим, щоб помістити заражений файл у карантин, а в деяких випадках можуть відновити його, видаливши вірусний код. Заражені файли часто надходять з віддалених джерел через завантаження для зараження комп'ютера.

Information Architect

An information architect is an individual who works to make information attractive and accessible to an audience. This type of role can include elements of technical writing or written format creation, as well as graphic design and Web development. Generally, information architecture means developing a better presentation for given data through attention to a digital landscape. Information architects are said to help develop a "user experience," which relates to both the content and the style of a Web page or site, or other facility like a company intranet.

Інформаційний архітектор

Інформаційний архітектор – це людина, яка працює над тим, щоб зробити інформацію привабливою та доступною для аудиторії. Ця роль може включати елементи технічного письма або створення письмових форматів, а також графічний дизайн і веброзробку. Загалом, інформаційна архітектура означає розробку кращої презентації для даних через увагу до цифрового ландшафту.

Вважається, що інформаційні архітектори допомагають розробити «користувацький досвід», який стосується як змісту, так і стилю вебсторінки, сайту чи іншого об'єкта, наприклад, інтрамережі компанії.

Information management (IM)

Information management (IM) is the process of collecting, storing, managing and maintaining information in all its forms. Information management is a broad term that incorporates policies and procedures for centrally managing and sharing information among different individuals, organizations and/or

Інформаційний менеджмент (IM)

Інформаційний менеджмент (IM) – це процес збору, зберігання, управління та підтримки інформації в усіх її формах. Управління інформацією – це широкий термін, який включає в себе політику і процедури для централізованого управління та обміну інформацією між різними особами,

information systems throughout the information life cycle.

Information management may also be called information asset management.

Information management is generally an enterprise information system concept, where an organization produces, owns and manages a suite of information.

організаціями та/або інформаційними системами протягом усього життєвого циклу інформації.

Управління інформацією може також називатися управлінням інформаційними активами.

Інформаційний менеджмент – це, як правило, концепція інформаційної системи підприємства, де організація виробляє, володіє і управляє набором інформації.

Information technology governance (IT governance)

Information technology governance (IT governance) is the collective tools, processes and methodologies that enable an organization to align business strategy and goals with IT services, infrastructure or the environment.

IT governance uses manages and optimizes IT in such a way that it supports, complements or enables an organization to achieve its goals and objectives.

Управління інформаційними технологіями (IT-управління)

Управління інформаційними технологіями (IT-управління) – це сукупність інструментів, процесів і методологій, які дозволяють організації узгоджувати бізнес-стратегію та цілі з IT-послугами, інфраструктурою або середовищем.

Управління IT використовує управління та оптимізацію IT таким чином, щоб вони підтримували, доповнювали або дозволяли організації досягати своїх цілей і завдань.

Information Technology Infrastructure Library (ITIL) Change Management

Information Technology Infrastructure Library (ITIL) change management is one of the processes of ITIL framework process areas that defines and provides standardized processes and techniques to handle and implement changes within an IT infrastructure with a minimum impact on business.

It enables organizations to create, assess, approve and implement changes within an IT environment under a controlled process. The change refers to any modification made to IT infrastructure

Управління змінами в Бібліотеці інфраструктури інформаційних технологій (ITIL)

Управління змінами в Бібліотеці інфраструктури інформаційних технологій (ITIL) – це один із процесів, що входить до структури ITIL, яка визначає та забезпечує стандартизовані процеси та методики для обробки та впровадження змін в IT-інфраструктурі з мінімальним впливом на бізнес.

Він дозволяє організаціям створювати, оцінювати, затверджувати та впроваджувати зміни в IT-середовищі в рамках контрольованого

regardless of if it is changed to an existing environment or the addition of a new IT component or process.

процесу. Під зміною розуміється будь-яка модифікація ІТ-інфраструктури, незалежно від того, чи це зміна існуючого середовища, чи додавання нового ІТ-компонента або процесу.

Information Technology Infrastructure Library v3

Information Technology Infrastructure Library v3 is the 2007 version of the original Information Technology Infrastructure Library (ITIL), which developed as a general service standard in the 1980s. It represents an update of a set of management practices that can help dovetail a business's technology needs and IT strategies.

Бібліотека інфраструктури інформаційних технологій v3

Бібліотека інфраструктури інформаційних технологій v3 – це версія 2007 року оригінальної Бібліотеки інфраструктури інформаційних технологій (ITIL), яка була розроблена як загальний стандарт обслуговування у 1980-х роках. Вона являє собою оновлення набору управлінських практик, які можуть допомогти узгодити технологічні потреби бізнесу та ІТ-стратегії.

Information technology management (IT management)

Information technology management (IT management) is the process whereby all resources related to information technology are managed according to an organization's priorities and needs. This includes tangible resources like networking hardware, computers and people, as well as intangible resources like software and data. The central aim of IT management is to generate value through the use of technology. To achieve this, business strategies and technology must be aligned.

Information technology management includes many of the basic functions of management, such as staffing, organizing, budgeting and control.

Управління інформаційними технологіями (ІТ-менеджмент)

Управління інформаційними технологіями (ІТ-менеджмент) – це процес, за допомогою якого всі ресурси, пов'язані з інформаційними технологіями, управляються відповідно до пріоритетів і потреб організації. Сюди входять матеріальні ресурси, такі як мережеве обладнання, комп'ютери та люди, а також нематеріальні ресурси, такі як програмне забезпечення та дані. Головною метою управління ІТ є створення цінності через використання технологій. Щоб досягти цього, бізнес-стратегії та технології повинні бути узгоджені.

Управління інформаційними технологіями включає в себе багато базових функцій менеджменту, таких як підбір персоналу, організація, бюджетування та контроль.

Information Technology Service Desk (IT service desk)

An information technology service desk (IT service desk) is a primary IT service management function that provides a single point of contact (SPOC) between users and IT employees or a business and customers. It is implemented by organizations that follow the practices of the Information Technology Infrastructure Library (ITIL).

Служба підтримки інформаційних технологій (IT-служба)

Служба підтримки інформаційних технологій (IT-служба) – це основна функція управління IT-послугами, яка забезпечує єдину точку контакту (SPOC) між користувачами та IT-працівниками або між бізнесом і клієнтами. Її впроваджують організації, які дотримуються практик Бібліотеки інфраструктури інформаційних технологій (ITIL).

Information Technology Supervisor (IT supervisor)

A information technology supervisor (IT supervisor) is responsible for installation, maintenance and upgrades of an organization's technology systems. An IT supervisor generally works with a team of information technology administrators and support personnel to oversee the day-to-day operations of information technology systems and components. They ensure that proper support is available for all activities in the information technology environment and that adequate skilled resources are present to ensure smooth functioning.

Керівник відділу інформаційних технологій (IT-менеджер)

Керівник відділу інформаційних технологій (IT-менеджер) відповідає за встановлення, обслуговування та модернізацію технологічних систем організації. IT-супервайзер зазвичай працює з командою адміністраторів інформаційних технологій та допоміжним персоналом для нагляду за повсякденною роботою інформаційних систем і компонентів. Він забезпечує належну підтримку всіх видів діяльності в інформаційно-технологічному середовищі та наявність достатньої кількості кваліфікованих ресурсів для забезпечення безперебійного функціонування.

Infotype

An infotype is an information unit used to maintain master data related to SAP human resource management systems (HRMS).

An infotypes contains a four-digit code with a related name and is capable of maintaining employee data.

Інфотип

Інфотип – це інформаційна одиниця, яка використовується для зберігання основних даних, пов'язаних із системами управління людськими ресурсами (HRMS) SAP.

Інфотипи містять чотиризначний код з відповідним ім'ям і здатні зберігати дані про співробітників.

In SAP, infotypes are capable of handling human resource (HR) information, which is often time-sensitive.

Infotypes allow users to conveniently maintain and retrieve HR information, while providing the consistency check required for a HRMS by auto-checking entries with preset values and conditions.

У SAP інфотипи здатні обробляти інформацію про людські ресурси (HR), яка часто є чутливою до часу.

Інфотипи дозволяють користувачам зручно зберігати та отримувати кадрову інформацію, забезпечуючи при цьому перевірку узгодженості, необхідну для HRMS, шляхом автоматичної перевірки записів на відповідність заданим значенням та умовам.

Inheritance

Inheritance, in C#, is the ability to create a class that inherits attributes and behaviors from an existing class. The newly created class is the derived (or child) class and the existing class is the base (or parent) class.

Inheritance is one of the key features of object-oriented programming. The benefits of inheritance are part of the reason why structural programming can be replaced with object-oriented programming.

Успадкування

Успадкування в C# – це можливість створення класу, який успадковує атрибути та поведінку від існуючого класу. Новостворений клас є похідним (або дочірнім) класом, а існуючий клас є базовим (або батьківським) класом.

Спадкування є однією з ключових особливостей об'єктно-орієнтованого програмування. Переваги успадкування є однією з причин, чому структурне програмування можна замінити об'єктно-орієнтованим.

Inline Deduplication

Inline deduplication refers to getting rid of redundant data in a data set as that data set is being transferred from one device to another, usually in a data backup system. This process cuts down on the bulk of a data set and makes storage more efficient.

Інтегрована дедуплікація

Інтегрована дедуплікація – це позбавлення набору даних від надлишкових даних під час перенесення їх з одного пристрою на інший, зазвичай у системі резервного копіювання даних. Цей процес зменшує обсяг набору даних і робить зберігання більш ефективним.

In-memory Analytics

In-memory analytics is an enterprise architecture (EA) framework solution used to enhance business intelligence (BI) reporting by querying data from system memory (RAM), versus the traditional hard disk drive medium. This approach significantly reduces querying time in an effort to facilitate efficient business decisions

Traditional BI incorporates dedicated, heavy resources for building data structures through online analytical processing (OLAP) programming or denormalized schemas.

Аналітика в пам'яті

Аналітика в пам'яті – це рамкове рішення для архітектури підприємства (EA), яке використовується для покращення звітності бізнес-аналітики (BI) шляхом запиту даних з системної пам'яті (оперативної пам'яті), а не з традиційного носія на жорсткому диску. Такий підхід значно скорочує час виконання запитів, що сприяє прийняттю ефективних бізнес-рішень

Традиційна аналітика включає в себе виділені, важкі ресурси для побудови структур даних за допомогою програмування онлайн-аналітичної обробки (OLAP) або денормалізованих схем.

In-memory Computing

In-memory computing is the storage of information in the main random access memory (RAM) of dedicated servers rather than in complicated relational databases operating on comparatively slow disk drives. In-memory computing helps business customers, including retailers, banks and utilities, to quickly detect patterns, analyze massive data volumes on the fly, and perform their operations quickly.

Обчислення в пам'яті

Обчислення в пам'яті – це зберігання інформації в оперативній пам'яті (ОЗП) виділених серверів, а не в складних реляційних базах даних, що працюють на порівняно повільних дискових накопичувачах. Обчислення в пам'яті допомагають бізнес-клієнтам, включаючи роздрібну торгівлю, банки та комунальні служби, швидко виявляти закономірності, аналізувати величезні обсяги даних «на льоту» та швидко виконувати свої операції.

In-memory Database (IMDB)

An in-memory database (IMDB) is a database management system that primarily depends on main memory for storing computer data. IMDBs are quicker than disk-optimized databases because they carry out fewer CPU instructions, and their internal optimization algorithms are much simpler. IMDB eradicates disk access by saving and manipulating data in the main memory. An IMDB commonly includes direct data manipulation and a dedicated memory-based architecture.

IMDBs are mainly used in applications where response time is crucial, such as telecommunications network devices and mobile ad networks.

База даних у пам'яті (БД)

База даних у пам'яті (БД) - це система керування базами даних, яка в першу чергу залежить від оперативної пам'яті для зберігання комп'ютерних даних. IMDB працюють швидше, ніж бази даних, оптимізовані для роботи на диску, оскільки вони виконують менше інструкцій процесора, а їхні внутрішні алгоритми оптимізації набагато простіші. IMDB виключає доступ до диска, зберігаючи та маніпулюючи даними в оперативній пам'яті. IMDB зазвичай включає пряму маніпуляцію даними та архітектуру на основі виділеної пам'яті.

IMDB в основному використовуються в додатках, де час відгуку має вирішальне значення, наприклад, в пристроях телекомунікаційних мереж і мобільних рекламних мережах.

Innovator's Patent Agreement (IPA)

The Innovator's Patent Agreement (IPA) is a new initiative that aims to change the way technology patents are assigned and controlled. Introduced by Twitter in April 2012, the IPA allows engineers and designers to maintain control of their patents, even when sold. This means that any company that uses the patents can only do so for defensive purposes. In other words, companies can only make claims for infringement if they are sued first.

Патентна угода інноватора (IPA)

Патентна угода інноватора (IPA) – це нова ініціатива, яка має на меті змінити спосіб передачі та контролю за технологічними патентами. Запроваджена компанією Twitter у квітні 2012 року, IPA дозволяє інженерам та дизайнерам зберігати контроль над своїми патентами навіть після їх продажу. Це означає, що будь-яка компанія, яка використовує патенти, може робити це лише в оборонних цілях. Іншими словами, компанії можуть подавати позови про порушення прав, тільки якщо на них подали позов першими.

Input Device

An input device is a term for a physical piece of hardware that connects to a primary device, such as a computer, in order to provide user input.

Input devices are generally a class of peripheral devices that connect to the primary device.

Пристрій введення

Пристрій введення – це термін для позначення фізичного пристрою, який підключається до основного пристрою, наприклад, комп'ютера, щоб забезпечити введення даних користувачем.

Пристрої введення – це, як правило, клас периферійних пристроїв, які підключаються до основного пристрою.

Input/Output (I/O) Device

An input/output (I/O) device is a hardware device that has the ability to accept inputted, outputted or other processed data. It also can acquire respective media data as input sent to a computer or send computer data to storage media as storage output.

An I/O device is also known as an IO device.

Input devices provide input to a computer, while output devices provide a way for a computer to output data for communication with users or other computers. An I/O device is a device with both functionalities.

Пристрій вводу/виводу

Пристрій вводу/виводу – це апаратний пристрій, який має можливість приймати введені, виведені або інші оброблені дані. Він також може отримувати відповідні дані з носія як вхідні дані, що надсилаються до комп'ютера, або надсилати комп'ютерні дані на носій як вихідні дані.

Пристрій вводу/виводу також відомий як пристрій вводу/виводу Пристрої вводу забезпечують введення даних до комп'ютера, а пристрої виводу дають змогу комп'ютеру виводити дані для зв'язку з користувачами або іншими комп'ютерами. Пристрій вводу/виводу – це пристрій з обома функціями.

Input/output Operations per Second (IOPS)

Input/output operations per second (IOPS) is the measure of how many input/output operations a storage device can complete within one second. It is a standard performance benchmark for hard drives, solid state drives, flash drives and even network attached storage (NAS) devices. Although IOPS is a common performance indicator, performance measures for the same device can vary from system to system based on other factors.

Операції вводу/виводу за секунду (IOPS)

Операції вводу/виводу за секунду (IOPS) – це показник того, скільки операцій вводу/виводу може виконати пристрій зберігання даних за одну секунду. Це стандартний показник продуктивності для жорстких дисків, твердотільних накопичувачів, флеш-накопичувачів і навіть мережевих пристроїв зберігання даних (NAS). Хоча IOPS є загальним показником продуктивності, показники продуктивності для одного і того ж пристрою можуть відрізнятися в різних системах залежно від інших факторів.

Insert

Insert is a widely-used command in the Structured Query Language (SQL) data manipulation language (DML) used by SQL Server and Oracle relational databases. The insert command is used for inserting one or more rows into a database table with specified table column values. The first DML command executed immediately after a table creation is the insert statement

Insert operations can result in errors from defined column constraint violations or database inactivity. In both cases, exceptions are thrown and handled by error handlers that set appropriate values for error text, native errors, state and SQL code.

Вставка

Вставка – це широко використовувана команда в мові маніпулювання даними (DML) мови структурованих запитів (SQL), яка використовується в реляційних базах даних SQL Server і Oracle. Команда вставки використовується для вставки одного або декількох рядків у таблицю бази даних із зазначеними значеннями стовпців таблиці. Першою командою DML, яка виконується відразу після створення таблиці, є оператор вставки

Операції вставки можуть призвести до помилок через порушення визначених обмежень стовпців або неактивність бази даних. В обох випадках генеруються винятки, які обробляються обробниками помилок, які встановлюють відповідні значення для тексту помилки, власних помилок, стану і коду SQL.

Integer

An integer, in the context of computer programming, is a data type used to represent real numbers that do not have fractional values. The use of integers as variables supports programming in various ways.

Ціле число

Ціле число в контексті комп'ютерного програмування – це тип даних, що використовується для представлення дійсних чисел, які не мають дробових значень Використання цілих чисел як змінних підтримує програмування різними способами.

Integrated Circuit (IC)

An integrated circuit (IC) is a small semiconductor-based electronic device consisting of fabricated transistors, resistors and capacitors. Integrated circuits are the building blocks of most electronic devices and equipment.

Інтегральна схема (IC)

Інтегральна схема (IC) – це невеликий напівпровідниковий електронний пристрій, що складається з виготовлених транзисторів, резисторів і конденсаторів. Інтегральні схеми є будівельними блоками більшості електронних пристроїв та обладнання.

An integrated circuit is also known as a chip or microchip.

A integrated circuit is built with the primary objective of embedding as many transistors as possible on a single semiconductor chip.

Інтегральна схема також відома як чіп або мікросхема.

Інтегральна схема створюється з головною метою – розмістити якомога більше транзисторів на одному напівпровідниковому чіпі.

Integrated Cloud Service Management (ICSM)

Integrated cloud service management (ICSM) refers to the centralized management of a cloud computing solutions portfolio through purpose-built software tools and methodologies. ICSM is an approach used in cloud computing to manage the commissioning, decommissioning and overall maintenance of a suite of cloud products and services sourced by an organization. ICSM also ensures the maximum level of authority, control and governance of all cloud resourcesand the hosted/deployed data by a particular organization.

Інтегроване управління хмарними сервісами (ICSM)

Інтегроване управління хмарними сервісами (ICSM) – це централізоване управління портфелем рішень для хмарних обчислень за допомогою спеціально розроблених програмних інструментів і методологій. ICSM – це підхід, який використовується в хмарних обчисленнях для управління введенням в експлуатацію, виведенням з експлуатації та загальним обслуговуванням набору хмарних продуктів і сервісів, наданих організацією. ICSM також забезпечує максимальний рівень повноважень, контролю та управління всіма хмарними ресурсами та розміщеними/ розгорнутими даними конкретної організації.

Integrated threat management (ITM)

Integrated threat management (ITM) is a security approach that consolidates different security components into a single platform or application for an enterprise IT architecture. ITM evolved as a response to increasingly complex and frequent malicious attacks by hackers and others intent on damaging systems.

ITM is also known as threat management, unified threat management (UTM), universal threat management (UTM) and security threat management (STM).

Інтегроване управління загрозами (ІУЗ)

Інтегроване управління загрозами (ІУЗ) – це підхід до безпеки, який об'єднує різні компоненти безпеки в єдину платформу або додаток для корпоративної ІТ-архітектури. ITM розвивався як відповідь на дедалі складніші та частіші зловмисні атаки хакерів та інших осіб, що мають на меті пошкодити системи.

ITM також відомий як управління загрозами, уніфіковане управління загрозами (UTM), універсальне управління загрозами (UTM) та управління загрозами безпеці (STM).

Integration middleware

Integration middleware is the alternate term used for middleware as the purpose of middleware is mainly integration. Integration middleware represents software systems that offer runtime services for communications, integration application execution, monitoring and operations.

The key function of middleware is to help make application development simpler. This is done by offering common programming abstractions, covering up heterogeneity, delivering fundamental operating systems and hardware, and masking low-level programming details.

Інтеграційне проміжне програмне забезпечення

Інтеграційне проміжне програмне забезпечення – це альтернативний термін, який використовується для проміжного програмного забезпечення, оскільки метою проміжного програмного забезпечення є переважно інтеграція. Інтеграційне проміжне програмне забезпечення являє собою програмні системи, які пропонують послуги часу виконання для комунікацій, виконання інтеграційних додатків, моніторингу та операцій.

Ключова функція проміжного програмного забезпечення – допомогти спростити розробку додатків. Це досягається за допомогою загальних абстракцій програмування, приховування гетерогенності, надання фундаментальних операційних систем та апаратного забезпечення, а також маскування деталей низькорівневого програмування.

Integrity

Integrity, in the context of computer systems, refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification.

Integrity is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, confidentiality and nonrepudiation.

Цілісність

У контексті комп'ютерних систем цілісність означає методи забезпечення того, що дані є реальними, точними та захищеними від несанкціонованої модифікації користувачем.

Доброчесність є одним з п'яти стовпів забезпечення інформаційної безпеки (ІБ). Інші чотири – автентифікація, доступність, конфіденційність і неспростування.

Intel Virtualization Technology (Intel VT or IVT)

Intel Virtualization Technology (Intel VT or IVT) is a capability provided in Intel processors that enables multiple operating systems and environments to consolidate and host on a single processor.

Intel virtualization technology is the processor's hardware ability to divide and isolate its computing capacity for multiple host virtual machines and their operating systems. Intel virtualization technology was formerly known as Vanderpool.

Intel virtualization technology is a hardware virtualization technique that works in cohesion with software and operating system virtualization to create pool of typical or virtual computing environments on top of it.

Технологія віртуалізації Intel (Intel VT або IVT)

Технологія віртуалізації Intel (Intel VT або IVT) – це можливість, що надається процесорами Intel, яка дозволяє консолідувати та розміщувати декілька операційних систем та середовищ на одному процесорі.

Технологія віртуалізації Intel – це апаратна здатність процесора розділяти та ізолювати свою обчислювальну потужність для декількох хост-віртуальних машин та їхніх операційних систем. Технологія віртуалізації Intel раніше була відома як Vanderpool.

Технологія віртуалізації Intel – це апаратна технологія віртуалізації, яка працює в поєднанні з віртуалізацією програмного забезпечення та операційної системи, створюючи пул типових або віртуальних обчислювальних середовищ на їх основі.

Intellectual Property Attaché Act (IP Attaché Act or IPPA)

The Intellectual Property Attaché Act (IP Attaché Act or IPPA) is a new anti-piracy bill introduced July 9, 2012. IPPA's current text provides that oversight of the U.S. Patent and Trademark Office's (USPTO) Overseas Intellectual Property Rights (IPR) Attaché program would transfer to the Commerce Department.

Закон про аташе з питань інтелектуальної власності (IP Attaché Act або IPPA)

Закон про аташе з питань інтелектуальної власності (IP Attaché Act або IPPA) – це новий антипіратський законопроект, представлений 9 липня 2012 року. Нинішній текст IPPA передбачає, що нагляд за програмою Аташе з питань інтелектуальної власності (IPR) Відомства США з патентів і торговельних марок (USPTO) за кордоном буде передано Міністерству торгівлі.

Intelligence-bearing emanations

Intelligence-bearing emanations are signal emissions/emanations caused by any information processing device or equipment. This term can be used to refer to any wireless signal emanation that is carrying confidential or private information that gives off emissions that could be intercepted.

Розвідувальні випромінювання

Розвідувальні випромінювання – це сигнальні випромінювання/ випромінювання, спричинені будь-яким пристроєм або обладнанням для обробки інформації. Цей термін можна використовувати для позначення будь-якого випромінювання бездротового сигналу, який несе конфіденційну або приватну інформацію, що спричиняє випромінювання, які можуть бути перехоплені.

Intelligent Agent

An intelligent agent is a type of software application that searches, retrieves and presents information from the Internet. This application automates the process of extracting data from the Internet, such as information selected based on a predefined criterion, keywords or any specified information/ entity to be searched. Intelligent agents are often used as Web browsers, news retrieval services and online shopping.

An intelligent agent may also be called an agent or bot.

Інтелектуальний агент

Інтелектуальний агент – це тип програмного забезпечення, який здійснює пошук, вилучення та представлення інформації з Інтернету. Ця програма автоматизує процес вилучення даних з Інтернету, наприклад, інформації, відібраної на основі заздалегідь визначеного критерію, ключових слів або будь-якої іншої інформації/об'єкта для пошуку. Інтелектуальні агенти часто використовуються як веббраузери, служби пошуку новин та інтернет-магазини.

Інтелектуальний агент може також називатися агентом або ботом.

Intelligent Database

An intelligent database is a full-text database with artificial intelligence (AI) components that interact with users to ensure that users are supplied all relevant information. The AI portion is most often seen during searches providing intellectual operations and knowledge representations that are usually based on the connectionist neural network models. So, an intelligent database is a

Інтелектуальна база даних

Інтелектуальна база даних – це повнотекстова база даних з компонентами штучного інтелекту (ШІ), які взаємодіють з користувачами, щоб гарантувати, що користувачі отримують всю необхідну інформацію. Частину штучного інтелекту найчастіше можна побачити під час пошуку, забезпечуючи інтелектуальні операції та представлення знань, які зазвичай

system that manages information, rather than simple data, and presents it in such a way that is natural and informative for users. As a result, its capacity is far beyond simple record keeping.

ґрунтуються на моделях нейронних мереж, що базуються на зв'язках. Отже, інтелектуальна база даних – це система, яка управляє інформацією, а не простими даними, і представляє їх у природній та інформативній для користувачів формі. Як наслідок, її можливості виходять далеко за межі простого ведення записів.

Intelligent Network (IN)

An intelligent network (IN) is a network that provides specific technical capabilities or services outside the conventional network standard spectrum. This term is often linked with telecom networks, as recent innovation has expanded telecom's capabilities beyond its original primary function of facilitating phone calls.

Інтелектуальна мережа (ІМ)

Інтелектуальна мережа (ІМ) – це мережа, яка надає специфічні технічні можливості або послуги, що виходять за межі стандартного спектру звичайних мереж. Цей термін часто пов'язують з телекомунікаційними мережами, оскільки нещодавні інновації розширили можливості телекомунікацій за межі їх первісної основної функції – полегшення телефонних дзвінків.

Interaction Design (IxD)

Interaction design (IxD) is a process in which technology products and solutions are designed to center on the human behavior, interaction and utilization of a product. IxD enables the building of a technology product by focusing on its visual interface and interaction, rather than the underlying functionality.

Інтерактивний дизайн (IxD)

Інтерактивний дизайн (IxD) – це процес, в якому технологічні продукти та рішення розробляються з урахуванням поведінки, взаємодії та використання продукту людиною. IxD дозволяє створювати технологічний продукт, зосереджуючись на його візуальному інтерфейсі та взаємодії, а не на базовій функціональності.

Inter-exchange carrier (IXC)

An inter-exchange carrier (IXC) is a telephone company providing connections between local exchanges in different geographic areas. They also provide local access and transport area

Оператор міжміського зв'язку (ОМЗ)

Оператор міжміського зв'язку (ОМЗ) – це телефонна компанія, що забезпечує з'єднання між місцевими АТС у різних географічних регіонах. Вони також надають послуги місцевого

services as per the Telecommunication Act of 1996. They are commonly referred to as long distance carriers. U.S. legal and regulatory term used by telecommunication companies for long distance telephone Companies including MCI, Sprint and formerly AT&T. They are defined as any carriers providing local access and transport area (LATA) communication.

доступу та транспортної зони відповідно до Закону про телекомунікації від 1996 року. Їх зазвичай називають операторами міжміського зв'язку.

Американський юридичний та нормативний термін, що використовується телекомунікаційними компаніями для позначення компаній міжміського телефонного зв'язку, включаючи MCI, Sprint і раніше AT&T. Вони визначаються як будь-які оператори, що надають місцевий доступ і транспортну зону зв'язку (LATA).

Interface

Interface, in C#, is a code structure that defines a contract between an object and its user. It contains a collection of semantically similar properties and methods that can be implemented by a class or a struct that adheres to the contract.

In general, an interface is used to describe a set of related functionalities that can be implemented in a class or struct. It enables a class to inherit multiple behaviors defined in multiple interfaces. It also helps to resolve the name ambiguity that arises while using multiple methods with same names existing in different interfaces.

Інтерфейс

Інтерфейс у мові C# – це структура коду, яка визначає контракт між об'єктом та його користувачем. Він містить набір семантично схожих властивостей і методів, які можуть бути реалізовані класом або структурою, що дотримується контракту.

Загалом, інтерфейс використовується для опису набору пов'язаних функціональних можливостей, які можуть бути реалізовані в класі або структурі. Інтерфейс дозволяє класу успадковувати декілька типів поведінки, визначених у декількох інтерфейсах. Це також допомагає вирішити проблему неоднозначності імен, яка виникає при використанні декількох методів з однаковими іменами, що існують у різних інтерфейсах.

Interface Message Processor (IMP)

The interface message processor (IMP) was the first packet-router. It was part of the ARPANET, the the precusor to today’s Internet. IMPs monitored

Процесор інтерфейсних повідомлень (IMP)

Процесор інтерфейсних повідомлень (IMP) був першим пакетним маршрутизатором. Він був частиною ARPANET, попередника сучасного

network status and gathered statistics. They were also the heart of the ARPANET from its launch until it was decomissioned in 1989. They also represent the first generation of the gateways that are now known as routers.

Інтернету. IMP відстежував стан мережі та збирав статистику. Вони також були серцем ARPANET від її запуску до виведення з експлуатації в 1989 році. Вони також представляють перше покоління шлюзів, які зараз відомі як маршрутизатори.

Intergalactic Computer Network

The Intergalactic Computer Network is a name that Joseph Carl Robnett Licklider gave to a conceptual network in a memo. The memo, and Licklider himself, inspired the creation of ARPANET, a network that eventually evolved into a system that is now the modern-day Internet.

Міжгалактична комп'ютерна мережа

Міжгалактична комп'ютерна мережа – це назва, яку Джозеф Карл Робнетт Ліклайдер дав концептуальній мережі у своїй записці. Ця записка і сам Ліклайдер надихнули на створення ARPANET, мережі, яка з часом перетворилася на систему, що сьогодні є сучасним Інтернетом.

Interim Standard 95 (IS-95)

Interim Standard 95 (IS-95) is a second generation (2G) mobile telecommunications standard based on code division multiple access (CDMA) technology, which guarantees multiple access when sending voice and data between mobile phones and cell sites. IS-95 operates in the 800 MHz and 1900 MHz frequency bands.

IS-95 is also known as TIA/EIA-95. It is marketed under the brand name CDMA One (cdmaOne).

IS-95 is the first Qualcomm standard under CDMA digital cellular technology, but the term generally applies to a protocol revision (P_REV=1) that was developed by the Telecommunications Industry Association (TIA).

Interim Standard 95 (IS-95)

Interim Standard 95 (IS-95) – це стандарт мобільного зв'язку другого покоління (2G), заснований на технології множинного доступу з кодовим поділом каналів (CDMA), який гарантує множинний доступ при передачі голосу і даних між мобільними телефонами і сайтами стільникового зв'язку. IS-95 працює в діапазонах 800 МГц і 1900 МГц.

IS-95 також відомий як TIA/EIA-95. Він продається під торговою маркою CDMA One (cdmaOne).

IS-95 є першим стандартом Qualcomm для цифрової технології стільникового зв'язку CDMA, але цей термін зазвичай застосовується до версії протоколу (P_REV=1), яка була розроблена Асоціацією телекомунікаційної індустрії (TIA).

Internal

Internal, in C#, is a keyword used to declare the accessibility of a type or type member such that the access is limited to the assembly in which it is declared.

An internal modifier is used to prevent the use of a public modifier, which allows access to other assemblies wherever necessary

Внутрішній

Внутрішній у C# – це ключове слово, яке використовується для оголошення доступності типу або члена типу таким чином, що доступ обмежується збіркою, в якій він оголошений.

Внутрішній модифікатор використовується для запобігання використанню загальнодоступного модифікатора, що дозволяє отримати доступ до інших збірок там, де це необхідно.

Internal Bus

An internal bus is a type of data bus that only operates internally in a computer or system. It carries data and operations as a standard bus; however, it is only used for connecting and interacting with internal computer components.

An internal bus is also known as an internal data bus, frontside bus (FSB) and local bus.

Внутрішня шина

Внутрішня шина – це тип шини даних, яка працює тільки всередині комп'ютера або системи. Вона передає дані та виконує операції як стандартна шина, але використовується лише для з'єднання та взаємодії з внутрішніми компонентами комп'ютера.

Внутрішня шина також відома як внутрішня шина даних, передня шина (FSB) і локальна шина.

Internal Hard Drive

An internal hard drive is the primary storage device located inside a computer system. It usually contains pre-installed software applications, the operating system and other files. Most desktop computers have several internal hard drives, allowing them to provide greater data storage. On the other hand, laptop computers can only accommodate one internal hard drive, forcing the user to add an external storage device to store data that exceeds the laptop's internal capacity.

Внутрішній жорсткий диск

Внутрішній жорсткий диск – це основний пристрій зберігання даних, розташований всередині комп'ютерної системи. Зазвичай він містить попередньо встановлені програми, операційну систему та інші файли. Більшість стаціонарних комп'ютерів мають кілька внутрішніх жорстких дисків, що дозволяє їм забезпечувати більший обсяг зберігання даних. З іншого боку, ноутбуки можуть вмістити лише один внутрішній жорсткий диск, що змушує користувача додавати зовнішній накопичувач для зберігання даних, які перевищують внутрішню ємність ноутбука.

Internal Tables

In ABAP programming, internal tables are dynamic data objects that are used to provide a mechanism of transferring data from a database or any other fixed structure to working memory for the purposes of array functionality. The data extracted is stored in memory, record by record. Internal tables are mainly used to process a dataset with a predefined structure within an ABAP program. With the help of internal tables, SAP developers can store and format data within a program extracted from a database table. Due to their dynamic nature, they also save programmers from having to worry about dynamic memory management, which would otherwise be a concern.

Внутрішні таблиці

У ABAP-програмуванні внутрішні таблиці – це динамічні об'єкти даних, які використовуються для забезпечення механізму передачі даних з бази даних або будь-якої іншої фіксованої структури в оперативну пам'ять для цілей функціонування масивів. Витягнуті дані зберігаються в пам'яті, запис за записом. Внутрішні таблиці в основному використовуються для обробки набору даних із заздалегідь визначеною структурою в ABAP-програмі. За допомогою внутрішніх таблиць розробники SAP можуть зберігати і форматувати дані в програмі, витягнуті з таблиці бази даних. Завдяки своїй динамічній природі вони також позбавляють програмістів необхідності турбуватися про динамічне управління пам'яттю, що в іншому випадку могло б викликати занепокоєння.

International Committee for Information Technology Standards (INCITS)

The International Committee for Information Technology Standards (INCITS) is a forum that creates and manages standards in Information and Communications Technology (ICT). INCITS develops standards and products in data storage, processing, transfer, display, management an retrieval. It is pronounced as “insights” and was founded in 1960.

INCITS was previously known as the Accredited Standards Committee and the National Committee for Information Technology Standards (NCITS).

Міжнародний комітет зі стандартів інформаційних технологій (INCITS)

Міжнародний комітет зі стандартів інформаційних технологій (INCITS) – це форум, який створює та управляє стандартами в галузі інформаційно-комунікаційних технологій (ІКТ). INCITS розробляє стандарти та продукти для зберігання, обробки, передачі, відображення, управління та пошуку даних. Він вимовляється як "інсайт" і був заснований у 1960 році.

Раніше INCITS був відомий як Акредитований комітет зі стандартів та Національний комітет зі стандартів інформаційних технологій (NCITS).

International Electrotechnical Commission (IEC)

The International Electrotechnical Commission (IEC) is a global organization that publishes standards for electronic and technical equipment developed for consumer markets. IEC members include dozens of nations around the world. IEC standards lead to a more consistent core standard for different kinds of electronic and technical products.

Міжнародна електротехнічна комісія (IEC)

Міжнародна електротехнічна комісія (IEC) – це всесвітня організація, яка публікує стандарти для електронного та технічного обладнання, розробленого для споживчих ринків. Членами IEC є десятки країн по всьому світу. Стандарти IEC ведуть до створення більш узгодженого базового стандарту для різних видів електронної та технічної продукції.

International Mobile Telecommunications Advanced (IMT-Advanced)

International Mobile Telecommunications Advanced (IMT-Advanced) is a standard and system created by the International Telecommunication Union (ITU), for the creation, operation and management of next generation mobile networks and Internet communications. It provides higher quality mobile data and communication services than its predecessor. IMT-Advanced is largely incorporated.

IMT-Advanced is also known as 4G network.

International Mobile Telecommunications Advanced (IMT-Advanced)

International Mobile Telecommunications Advanced (IMT-Advanced) – це стандарт і система, розроблена Міжнародним союзом електрозв'язку (МСЕ), для створення, експлуатації та управління мобільними мережами наступного покоління та інтернет-зв'язком. Він забезпечує вищу якість мобільних послуг передачі даних і зв'язку, ніж його попередник. IMT-Advanced значною мірою інтегрований.

IMT-Advanced також відома як мережа 4G.

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a global agency that helps to provide diverse standards for industrial, commercial and public use. Some of these relate to manufacturing and other physical industries, while others apply to digital technologies and other aspects of modern IT. The ISO has helped to shape the face of modern technology and communications.

Міжнародна організація зі стандартизації (ISO)

Міжнародна організація зі стандартизації (ISO) – це міжнародна організація, яка допомагає створювати різноманітні стандарти для промислового, комерційного та громадського використання. Деякі з них стосуються виробництва та інших галузей фізичної промисловості, а інші – цифрових технологій та інших аспектів сучасних ІТ. ISO допомогла сформувати обличчя сучасних технологій та комунікацій.

International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is a globally managed agency of the United Nations that is responsible for the development, management and standardization of information and communication technology (ICT). The ITU collaborates and coordinates the use of satellite orbits and radio spectrum, the interconnectivity of different technologies, and the creation of ICT standards.

Міжнародний союз електрозв'язку (МСЕ)

Міжнародний союз електрозв'язку (МСЕ) – це глобальна організація ООН, яка відповідає за розвиток, управління та стандартизацію інформаційно-комунікаційних технологій (ІКТ). МСЕ співпрацює та координує використання супутникових орбіт та радіочастотного спектру, взаємозв'язок різних технологій та створення стандартів ІКТ.

Internet Art

Internet art is a kind of art that uses the Internet as its mode of dissemination. The art is often interactive and/or participatory in nature and may use a number of different mediums. This method strays from the traditional gallery and museum system and gives even small artists a way of sharing their work with a large audience. Artists who do this kind of art are usually called net artists.

Internet art is also known as Net art.

Інтернет-мистецтво

Інтернет-мистецтво – це вид мистецтва, що використовує Інтернет як спосіб поширення. Це мистецтво часто є інтерактивним та/ або партисипативним за своєю природою і може використовувати низку різних засобів. Цей метод відходить від традиційної галерейної та музейної системи і дає можливість навіть невеликим художникам ділитися своєю творчістю з великою аудиторією. Художників, які займаються цим видом мистецтва, зазвичай називають мережевими художниками.

Інтернет-мистецтво також відоме як мережеве мистецтво.

Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit public benefit corporation that develops policy on unique identifiers and coordinates the Internet's naming system. In other words, the ICANN is the overseeing body for the domain names on the Internet.

Інтернет-корпорація з присвоєння імен і номерів (ICANN)

Інтернет-корпорація з присвоєння імен і номерів (ICANN) – це некомерційна суспільно корисна корпорація, яка розробляє політику щодо унікальних ідентифікаторів і координує систему імен в Інтернеті. Іншими словами, ICANN є органом нагляду за доменними іменами в Інтернеті.

Internet Fax Product

An Internet fax product is a technology that uses the global IP network to send a fax instead of using traditional public switched telephone networks or fiber-optic land lines to send documents. A range of Internet fax tools help offices to receive faxes in digital form or as paper documents.

Інтернет-факсимільний продукт

Інтернет-факсимільний продукт – це технологія, яка використовує глобальну IP-мережу для надсилання факсу замість традиційних телефонних мереж загального користування або оптоволоконних наземних ліній для надсилання документів. Різноманітні інструменти інтернет-факсу допомагають офісам отримувати факсимільні повідомлення в цифровому вигляді або у вигляді паперових документів.

Internet Map

An Internet map is like any other map in function in that it displays an object's relative position based on other objects around it. However, it differs from an average map in a sense that an Internet map is not aligned on a surface, nor does it really show a physical location. It uses circles to depict websites, which varies according to its website traffic, and uses a bi-dimensional presentation of the connectors that links the websites, which forms the Internet as a whole.

Інтернет-карта

Інтернет-карта схожа на будь-яку іншу карту, оскільки вона відображає відносне розташування об'єкта на основі інших об'єктів навколо нього. Однак вона відрізняється від звичайної карти в тому сенсі, що інтернет-карта не вирівнюється на поверхні і не показує фізичне місцезнаходження. Вона використовує кола для зображення вебсайтів, кількість яких змінюється залежно від відвідуваності сайту, і використовує двовимірне представлення з'єднувачів, які з'єднують вебсайти, що формують Інтернет в цілому.

Internet Network Information Center (InterNIC)

The Internet Network Information Center (InterNIC) was set up by the National Science Foundation to provide for orderly domain name registration. The InterNIC provides a system called Whois that helps users get information on a given domain by entering the domain name or the IP address.

Інформаційний центр мережі Інтернет (InterNIC)

Інформаційний центр мережі Інтернет (InterNIC) був створений Національним науковим фондом для забезпечення впорядкованої реєстрації доменних імен. InterNIC надає систему під назвою Whois, яка допомагає користувачам отримати інформацію про певний домен, ввівши доменне ім'я або IP-адресу.

Internet of Things (IoT)

The Internet of Things (IoT) is a network of interconnected devices that can collect and share data over the Internet with minimal human involvement. In this context, a "thing" is an object that has a unique identifier and the ability to communicate over a network.

Internet phone (a broadband phone)

The Internet phone, also known as a broadband phone, is a digital communications device used for making phone calls via the Internet. It is also a commonly used Voice over Internet Protocol (VoIP) application device. When a call is made, the phone using VoIP converts the user's voice into several digital packets after an analog-to-digital conversion circuit processes it, and then sends the data over the Internet to be received by the other user.

And Internet phone is also known as a broadband phone or IP phone.

Internet Protocol Configuration (ipconfig)

Internet Protocol Configuration (ipconfig) is a Windows console application that has the ability to gather all data regarding current Transmission Control Protocol/Internet Protocol (TCP/IP) configuration values and then display this data on a screen. Ipconfig also refreshes the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) settings each time it is invoked.

Інтернет речей (IoT)

Інтернет речей (IoT) – це мережа взаємопов'язаних пристроїв, які можуть збирати та обмінюватися даними через Інтернет з мінімальною участю людини. У цьому контексті «річ» – це об'єкт, який має унікальний ідентифікатор і здатність спілкуватися через мережу.

Інтернет-телефон (широкосмуговий телефон)

Інтернет-телефон, також відомий як широкосмуговий телефон, – це цифровий комунікаційний пристрій, що використовується для здійснення телефонних дзвінків через Інтернет. Це також широко використовуваний прикладний пристрій для передачі голосу через Інтернет-протокол (VoIP). Під час дзвінка телефон, що використовує VoIP, перетворює голос користувача в кілька цифрових пакетів після обробки аналого-цифровим перетворювачем, а потім надсилає дані через Інтернет, щоб їх отримав інший користувач.

А інтернет-телефон також відомий як широкосмуговий телефон або IP-телефон.

Конфігурація інтернет-протоколу (ipconfig)

Конфігурація інтернет-протоколу (ipconfig) – це консольна програма Windows, яка має можливість збирати всі дані про поточні значення конфігурації протоколу управління передачею/інтернету (TCP/IP), а потім відображати ці дані на екрані. Ipconfig також оновлює налаштування системи доменних імен (DNS) і протоколу динамічної конфігурації хостів (DHCP) при кожному запуску.

Internet Protocol hijacking (IP hijacking)

Internet Protocol hijacking (IP hijacking) is a specific form of hacking that makes use of IP addresses to move data over the Internet. IP hacking exploits some vulnerabilities in general IP networking and the Border Gateway Protocol, a system used to designate paths for routed data packets.

Перехоплення Інтернет-протоколу (IP-хакінг)

Перехоплення Інтернет-протоколу (IP-хакінг) – це специфічна форма злому, яка використовує IP-адреси для переміщення даних через Інтернет. IP-хакінг використовує деякі вразливості в загальній IP-мережі та протоколі прикордонного шлюзу (Border Gateway Protocol) – системі, що використовується для визначення шляхів для пакетів даних, які маршрутизуються.

Internet Protocol Private Branch Exchange (IP PBX)

Internet Protocol Private Branch Exchange (IP PBX) is a PBX system that is built over IP-based architecture for delivering and managing voice communication services.

IP PBX provides IP telephony and switching services between an IP telephone network and a public switched telephone network (PSTN) system.

IP-АТС

IP-АТС – це система АТС, побудована на основі IP-архітектури для надання та управління послугами голосового зв'язку.

IP-АТС надає послуги IP-телефонії та комутації між IP-телефонною мережею та телефонною мережею загального користування (ТфОП).

Internet Protocol Telephony (IP Telephony)

Internet Protocol Telephony (IP Telephony) is the use of IP-based networks to build, provide and access voice, data or other forms of telephonic communications. IP telephony provides traditional telephonic communication over an IP-based network, the Internet – via an Internet service provider (ISP) – or directly from a telecommunications service provider.

Телефонія на основі Інтернет-протоколу (IP-телефонія)

Телефонія на основі Інтернет-протоколу (IP-телефонія) – це використання мереж на основі IP для побудови, надання та доступу до голосового зв'язку, передачі даних або інших форм телефонного зв'язку. IP-телефонія забезпечує традиційний телефонний зв'язок через IP-мережу, Інтернет – через Інтернет-провайдера (ISP) або безпосередньо від постачальника телекомунікаційних послуг.

Internet Relay Chat (IRC) Worm

The Internet Relay Chat (IRC) worm is a program that spreads via message forums or chat rooms by sending infected files or websites using IRC channels. The IRC network is connected to thousands of channels, making it susceptible to a worm attack. Before this worm can spread, it needs to establish a connection to the IRC network or drop detailed scripts to the IRC client directory. Next, when the infected client logs in to the IRC server and connects to any channel, the installed script will cause the client to send a copy of the infected file to other users in the same channel.

Хробак Internet Relay Chat (IRC)

Хробак Internet Relay Chat (IRC) – це програма, яка поширюється через форуми повідомлень або чати, надсилаючи заражені файли або вебсайти через канали IRC. Мережа IRC з'єднана з тисячами каналів, що робить її вразливою до атак черв'яків. Перед тим, як черв'як зможе поширюватися, йому необхідно встановити з'єднання з мережею IRC або скинути детальний сценарій в каталог клієнта IRC. Далі, коли заражений клієнт заходить на IRC-сервер і підключається до будь-якого каналу, встановлений скрипт змушує клієнта відправити копію зараженого файлу іншим користувачам того ж каналу.

Internet Relay Chat Bot (IRC bot)

An Internet relay chat bot (IRC bot) is a type of application that performs automated tasks within an IRC-based chat room or channel. It enables the performance of several channel specific tasks on behalf of the user and usually is configured as a channel operator.

An IRC bot is also known as an automaton.

Інтернет-ретрансляційний чат-бот (IRC-бот)

Інтернет-ретрансляційний чат-бот (IRC-бот) – це тип програми, яка виконує автоматизовані завдання в чаті або каналі на базі IRC. Він дозволяє виконувати кілька специфічних для каналу завдань від імені користувача і зазвичай налаштовується як оператор каналу.

IRC-бот також відомий як автомат.

Internet Security

Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol.

Безпека в Інтернеті

Безпека в Інтернеті – це загальний термін для позначення дуже широкого кола питань, що охоплюють безпеку транзакцій, які здійснюються в Інтернеті. Загалом, інтернет-безпека охоплює безпеку браузера, безпеку даних, що вводяться через вебформи, а також загальну автентифікацію і захист даних, що надсилаються через інтернет-протокол.

Internet Telephony

Internet telephony is a type of communications technology that allows voice calls and other telephony services like fax, SMS and other voice-messaging applications to be transmitted using the Internet as a connection medium. Software under this technology is cost-effective and convenient because it allow the user to communicate through fax, voice and video calls anywhere in the world as long as there is an Internet connection.

Інтернет-телефонія

Інтернет-телефонія – це тип комунікаційної технології, що дозволяє передавати голосові дзвінки та інші телефонні послуги, такі як факс, SMS та інші додатки для обміну голосовими повідомленнями, використовуючи Інтернет як середовище зв'язку. Програмне забезпечення за цією технологією є економічно ефективним і зручним, оскільки дозволяє користувачеві спілкуватися за допомогою факсу, голосових і відеодзвінків у будь-якій точці світу, якщо є підключення до Інтернету.

Internetwork Packet Exchange/ Sequenced Packet Exchange (IPX/ SPX)

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is a set of network protocols that provide packet switching and sequencing for small and large networks. IPX works at layer three of the Open Systems Interconnection (OSI) model and SPX works at layer 4.

SPX is connection-oriented and used for routing information and connection-related functions. Like IP, IPX is connectionless and contains end-user data, such as IP addresses.

Обмін пакетами міжмережевого обміну/впорядкований обмін пакетами (IPX/ SPX)

Обмін пакетами міжмережевого обміну/впорядкований обмін пакетами (IPX/SPX) – це набір мережевих протоколів, які забезпечують комутацію та впорядкування пакетів для малих і великих мереж. IPX працює на третьому рівні моделі взаємодії відкритих систем (OSI), а SPX – на четвертому.

SPX орієнтований на з'єднання і використовується для маршрутизації інформації та функцій, пов'язаних зі з'єднанням. Як і IP, IPX не потребує з'єднання і містить дані кінцевого користувача, такі як IP-адреси.

Interoperability Testing

Interoperability testing involves testing whether a given software program or technology is compatible with others and promotes cross-use functionality. This kind of testing is now important as many

Тестування інтероперабельності

Тестування інтероперабельності передбачає перевірку сумісності певного програмного забезпечення або технології з іншими та сприяє крос-використанню функціональності. Цей

different kinds of technology are being built into architectures made up of many diverse parts, where seamless operation is critical for developing a user base.

вид тестування зараз є важливим, оскільки багато різних видів технологій вбудовуються в архітектури, що складаються з багатьох різноманітних частин, де безперебійна робота є критично важливою для розвитку користувацької бази.

Interweb or "the Interweb"

Interweb or "the Interweb" is a colloquial term for the World Wide Web or Internet. This term, which combines the two formal names for today's global network of computers and servers, is often thought of as a slightly sarcastic reference to the Internet, implicating those who do not understand how it works.

Interweb або «павутиння»

Interweb або «павутиння» – це розмовний термін для позначення Всесвітньої павутини або Інтернету. Цей термін, що поєднує в собі дві офіційні назви сучасної глобальної мережі комп'ютерів і серверів, часто сприймається як дещо саркастичне посилання на Інтернет, що натякає на тих, хто не розуміє, як він працює.

Intexticated

Intexticated is a term coined to refer to an individual who is distracted by texting or composing an email on a handheld device while walking or driving, and is therefore unaware of the surroundings. As result, this person may move and/or react as if intoxicated, which is why the term combines the words "texting" and "intoxicated."

«Розсіяний»

«Розсіяний» – це термін, вигаданий для позначення людини, яка відволікається на текстові повідомлення або написання електронного листа на портативному пристрої під час ходьби або водіння, і тому не усвідомлює навколишню обстановку. Як наслідок, така людина може рухатися та/або реагувати так, ніби перебуває у стані алкогольного сп'яніння, тому цей термін поєднує в собі слова «текстові повідомлення» та «сп'яніння».

Intrusive testing

Intrusive testing is a kind of testing that involves adding or introducing unexpected external variables into a system. The test records the timing and processing information when the program is performed and executed and external elements are introduced, which might make certain changes in terms of how the program will behave in a real-time environment. This testing usually

Інтрузивне тестування

Інтрузивне тестування – це вид тестування, який передбачає додавання або введення в систему неочікуваних зовнішніх змінних. Під час тестування записується інформація про час та обробку даних під час виконання програми та введення зовнішніх елементів, які можуть внести певні зміни в те, як програма поводитиметься в реальному часі. Таке тестування

requires additional codes embedded in the software or has some other processes that run simultaneously with the program to be tested.

зазвичай потребує вбудовування додаткових кодів у програмне забезпечення або інших процесів, які виконуються одночасно з програмою, що тестується.

In-Vehicle Infotainment (IVI)

In-Vehicle Infotainment (IVI) is an auto industry term that refers to vehicle systems that combine entertainment and information delivery to drivers and passengers. IVI systems use audio/video (A/V) interfaces, touchscreens, keypads and other types of devices to provide these types of services.

Інформаційно-розважальні системи в автомобілі (IVI)

Інформаційно-розважальні системи в автомобілі (IVI) – це термін автомобільної промисловості, який позначає транспортні системи, що поєднують в собі розваги та надання інформації водіям і пасажирам. Системи IVI використовують аудіо/відео (A/V) інтерфейси, сенсорні екрани, клавіатури та інші типи пристроїв для надання таких послуг.

IP network

An IP network is a communication network that uses Internet Protocol (IP) to send and receive messages between one or more computers. As one of the most commonly used global networks, an IP network is implemented in Internet networks, local area networks (LAN) and enterprise networks. An IP network requires that all hosts or network nodes be configured with the TCP/IP suite.

The Internet is the largest and best known IP network.

IP-мережа

IP-мережа – це комунікаційна мережа, яка використовує Інтернет-протокол (IP) для надсилання та отримання повідомлень між одним або декількома комп'ютерами. Як одна з найпоширеніших глобальних мереж, IP-мережа реалізована в мережах Інтернету, локальних мережах (LAN) та корпоративних мережах. IP-мережа вимагає, щоб усі хости або вузли мережі були налаштовані за допомогою набору TCP/IP.

Інтернет – це найбільша і найвідоміша IP-мережа.

IP routing

IP routing is the process of transporting data from source to destination on a determined path across two or more networks. IP routing enables two or more devices on different TCP/IP networks to connect with each other. IP routing provides the path for reaching the destination device.

IP-маршрутизація

IP-маршрутизація – це процес транспортування даних від джерела до місця призначення за визначеним маршрутом через дві або більше мереж. IP-маршрутизація дозволяє двом або більше пристроям у різних мережах TCP/IP з'єднуватися один з одним. IP-маршрутизація забезпечує шлях для досягнення пристрою призначення.

iPhone 5

The iPhone 5 is the sixth iteration of the ever-popular Apple brand of touchscreen-based smartphones. Although upon first impression the iPhone 5 is not very different from its predecessor, the iPhone 4S, it is actually lighter and slimmer and has a higher resolution "retina" display. Several other subtle changes can be seen at closer inspection of its external structure, like the height of the front glass protrusion and the bevels of the edges. It comes equipped with the iOS 6 operating system.

iPhone 5

iPhone 5 – це шоста ітерація популярного бренду смартфонів з сенсорним екраном від Apple. Хоча на перший погляд iPhone 5 не дуже відрізняється від свого попередника, iPhone 4S, насправді він легший і тонший, а також має вищу роздільну здатність "сітчастого" дисплея. При уважному розгляді його зовнішньої структури можна помітити кілька інших тонких змін, таких як висота виступу переднього скла і скоси країв. Він оснащений операційною системою iOS 6.

ISO-IEC 24821-1

ISO-IEC 24821-1 is an international standard, which specifies a format for XML documents. It defines a standard for interpreting the XML information set (XML Infoset) with the help of binary encoding. The ASN.1 and ASN.1 Encoding Control Notation (ECN) are the widely used notations for specifying binary encodings.

This term is also known as Fast Infoset (FI).

ISO/IEC 24824-1 allows the use of dynamic tables (for representing both character strings and qualified names) and initial and external vocabularies.

ISO-IEC 24821-1

ISO-IEC 24821-1 – це міжнародний стандарт, який визначає формат XML-документів. Він визначає стандарт для інтерпретації інформаційного набору XML (XML Infoset) за допомогою двійкового кодування. Нотації ASN.1 і ASN.1 Encoding Control Notation (ECN) є широко використовуваними нотаціями для визначення двійкових кодувань.

Цей термін також відомий як Fast Infoset (FI).

ISO/IEC 24824-1 дозволяє використовувати динамічні таблиці (для представлення як символьних рядків, так і кваліфікованих імен), а також початкові та зовнішні словники.

IT Asset Management (ITAM)

IT Asset Management (ITAM) is a type of business management that is directly tied to an enterprise's IT infrastructure. With ITAM, professionals review the an organization's total business hardware and software inventory and make comprehensive decisions about sourcing, use and all other aspects related to an asset lifecycle.

Управління ІТ-активами (IT Asset Management, ITAM)

Управління ІТ-активами (IT Asset Management, ITAM) – це тип управління бізнесом, який безпосередньо пов'язаний з ІТ-інфраструктурою підприємства. За допомогою ITAM фахівці аналізують загальну інвентаризацію апаратного та програмного забезпечення організації та приймають комплексні рішення щодо джерел постачання, використання та всіх інших аспектів, пов'язаних з життєвим циклом активів.

IT Cost Transparency

IT cost transparency is a branch of IT management that combines finance and management accounting principles with the acquisition, maintenance and deployment of IT products and services used by large and small organizations.

IT cost transparency factors include licensing costs, IT personnel/labor, asset management and project portfolio management (PPM).

Прозорість витрат на ІТ

Прозорість витрат на ІТ – це галузь управління ІТ, яка поєднує принципи фінансового та управлінського обліку з придбанням, обслуговуванням та розгортанням ІТ-продуктів та послуг, що використовуються великими та малими організаціями.

Фактори прозорості ІТ-витрат включають витрати на ліцензування, ІТ-персонал/роботу, управління активами та управління портфелем проектів (УПП).

IT Management Service

IT management service refers to an ongoing service that manages and oversees the IT infrastructure of an organization responsible for network and data communication operations.

It is a broad term that encompasses all the IT-central technological, management and operational guidelines, policies and procedures performed by a service provider.

Послуга управління ІТ

Послуга управління ІТ відноситься до постійної послуги, яка управляє і контролює ІТ-інфраструктуру організації, що відповідає за мережеві операції і передачу даних.

Це широкий термін, який охоплює всі технологічні, управлінські та операційні настанови, політики та процедури, що виконуються постачальником послуг, пов'язані з інформаційними технологіями.

IT MOOSE Management

IT MOOSE management is a management viewpoint coined by Forrester Research to refer to the expenses necessary to keep an IT organization running. MOOSE stands for maintain and operate the organization, systems and equipment. IT MOOSE management refers to managing the costs associated with maintaining and operating the organization along with all of its equipment and different systems.

Управління IT MOOSE

Управління IT MOOSE – це управлінська точка зору, запропонована компанією Forrester Research для позначення витрат, необхідних для підтримки роботи IT-організації. MOOSE розшифровується як «утримання та експлуатація організації, систем та обладнання». Управління IT MOOSE – це управління витратами, пов'язаними з обслуговуванням та експлуатацією організації разом з усім її обладнанням та різними системами.

IT portfolio management

IT portfolio management is the process of supervising and maintaining the entire pool of IT resources across an enterprise in terms of their investment and financial viability.

IT portfolio management takes into account all the current and planned IT resources and provides a framework for analyzing, planning and executing IT portfolio's throughout the organization. IT portfolio management exists to create, provide and measure business value of IT.

IT portfolio management is built around tools that measure data such as the costs, risks and benefits associated with the implementation of certain IT resources spread throughout the enterprise.

Управління IT-портфелем

Управління IT-портфелем – це процес нагляду та підтримки всього пулу IT-ресурсів на підприємстві з точки зору їх інвестиційної та фінансової життєздатності.

Управління IT-портфелем враховує всі поточні та заплановані IT-ресурси і забезпечує основу для аналізу, планування та реалізації IT-портфелів в організації. Управління IT-портфелем існує для того, щоб створювати, надавати та вимірювати бізнес-цінність IT.

Управління IT-портфелем будується на основі інструментів, які вимірюють такі дані, як витрати, ризики та вигоди, пов'язані з впровадженням певних IT-ресурсів, розподілених по всьому підприємству.

IT Service Management (ITSM)

IT service management (ITSM) is the process of aligning enterprise IT services with business and a primary focus on the delivery of best services to end user.

IT service management deals with how IT resources and business practices together, are delivered in such a way that the end-user experience the most desired result from the accessed IT resource, application, business process or an entire solution stack.

Управління ІТ-послугами (ITSM)

Управління ІТ-послугами (ITSM) – це процес приведення ІТ-послуг підприємства у відповідність до потреб бізнесу, основна увага приділяється наданню найкращих послуг кінцевому користувачеві.

Управління ІТ-послугами стосується того, як ІТ-ресурси та бізнес-практики разом надаються таким чином, щоб кінцевий користувач отримував найбільш бажаний результат від доступу до ІТ-ресурсу, додатку, бізнес-процесу або цілого стеку рішень.

Iteration planning

Iteration planning is the process of discussing and planning the next cycle, phase or iteration of a software application that is under development. It is conducted through a meeting of the entire software development team at the starting point of each iteration to formally plan technical and non-technical processes.

Iteration planning is also known as iterative planning.

Планування ітерацій

Планування ітерацій – це процес обговорення та планування наступного циклу, фази або ітерації програмного додатку, що перебуває на стадії розробки. Він здійснюється шляхом зустрічі всієї команди розробників програмного забезпечення на початку кожної ітерації для формального планування технічних і нетехнічних процесів.

Ітераційне планування також відоме як ітераційне планування.

Iterative Development

Iterative development is a methodology of software development that divides a project into many releases. The main idea of iterative development is to create small projects that have a well-defined scope and duration and constantly do builds and updates as soon as possible.

A critic of iterative development would say it is simply releasing sloppy code done without proper planning. Iterative

Ітеративна розробка

Ітеративна розробка – це методологія розробки програмного забезпечення, яка розділяє проект на багато релізів. Основна ідея ітеративної розробки полягає у створенні невеликих проектів, які мають чітко визначений обсяг і тривалість, і постійно виконують збірки та оновлення в найкоротші терміни.

development is the opposite of a waterfall methodology and most closely aligned with agile development or extreme programming.

Критик ітеративної розробки скаже, що це просто випуск недбалого коду, зробленого без належного планування. Ітеративна розробка є протилежністю методології водоспаду і найбільш близька до гнучкої розробки або екстремального програмування.

Iterator, in the context of C#

An iterator, in the context of C#, is a block of code that returns an ordered sequence of values of a collection or array. It is a member function implemented using the iterator block, which contains one or more statements containing the "yield" keyword.

An iterator is used to enable consumers of a container class, containing a collection or array, to traverse the collection using the "foreach" statement in a simpler manner. It is used with strongly typed collection classes to iterate complex data structures like binary trees, which require recursive traversal and maintain the iteration state through the recursion. The concept of iterator is also used in implementing deferred execution in LINQ queries.

Ітератор в контексті C#

Ітератор в контексті C# – це блок коду, який повертає впорядковану послідовність значень колекції або масиву. Це функція-член, реалізована за допомогою блоку iterator, яка містить один або декілька операторів, що містять ключове слово yield.

Ітератор використовується для того, щоб дозволити споживачам класу-контейнера, що містить колекцію або масив, обходити колекцію за допомогою оператора foreach у більш простий спосіб. Він використовується зі строго типізованими класами колекцій для ітерації складних структур даних, таких як бінарні дерева, які потребують рекурсивного обходу та підтримки стану ітерації за допомогою рекурсії. Поняття ітератора також використовується для реалізації відкладеного виконання в LINQ-запитах.

ITU Telecommunication Standardization Sector (ITU-T)

The ITU Telecommunication Standardization Sector (ITU-T) is a sector within the International Telecommunication Union (ITU) which coordinates with all entities involved with creating standards in the telecommunications industry

Сектор стандартизації електрозв'язку МСЕ (МСЕ-Т)

Сектор стандартизації електрозв'язку МСЕ (МСЕ-Т) – це сектор Міжнародного союзу електрозв'язку (МСЕ), який координує роботу з усіма організаціями, що беруть участь у створенні стандартів у телекомунікаційній галузі.

Ivy Bridge

Ivy Bridge is a microprocessor architecture developed by Intel Corporation. It is the first processor architecture to implement 3-D or Tri-Gate transistors. Ivy Bridge was developed in 2011 as a successor to the Sandy Bridge microprocessor

Ivy Bridge processors are designed to provide enhanced computing and graphical performance and are considerably smaller than their predecessors.

Ivy Bridge

Ivy Bridge – мікропроцесорна архітектура, розроблена корпорацією Intel. Це перша процесорна архітектура, яка реалізує 3-D або Tri-Gate транзистори. Ivy Bridge був розроблений у 2011 році як наступник мікропроцесора Sandy Bridge.

Процесори Ivy Bridge розроблені для забезпечення підвищеної обчислювальної та графічної продуктивності і мають значно менші розміри, ніж їхні попередники.

J

Java Card

Java Card is a Java technology used for tiny applications, known as applets, on extremely resource-limited devices. Like other Java applications, Java Card applets feature write-once-run-anywhere capabilities. Java Card technology is widely used, with manufacturers accounting for over 90% of the smart card industry. Java Card bytecode is very small; only a subset of Java API is used. Source code is saved as .java, compiled to .class, then converted to .cap for installation. A complete Java Card application includes a back-end app, a host app, an interface device, and the applet.

Java Card

Java Card – це технологія Java, яка використовується для мініатюрних додатків, відомих як аплети, на пристроях з дуже обмеженими ресурсами. Як і інші Java-додатки, аплети Java Card мають можливість запису та запуску будь-де. Технологія Java Card широко використовується, а виробники Java Card складають понад 90% індустрії смарт-карт. Байт-код Java Card дуже малий; використовується лише підмножина Java API. Вихідний код зберігається як .java, компілюється в .class, потім конвертується у .cap для встановлення. Повна Java Card-програма включає внутрішній додаток, хост-додаток, інтерфейсний пристрій та аплет.

Java Foundation Classes (JFC)

Java Foundation Classes (JFC) are a set of graphical user interface (GUI) components for Java applications that streamline software and cloud application development. JFC contains the Abstract Window Toolkit (AWT), Java 2D and Swing. Because of its cross-platform capabilities, Java applications run on any OS without source code changes. Developers may choose between a uniform GUI across platforms or a native look and feel. A key advantage of JFC is its pluggable components and predictable performance across systems.

Базові класи Java (JFC)

Базові класи Java (JFC) – це набір компонентів графічного інтерфейсу користувача (GUI) для Java-додатків, які спрощують розробку програмного забезпечення та хмарних сервісів. До JFC входять Abstract Window Toolkit (AWT), Java 2D та Swing. Завдяки кросплатформності, додатки Java працюють на будь-якій ОС без змін у вихідному коді. Розробники можуть обрати єдиний вигляд інтерфейсу або зовнішність, що відповідає системі. Головна перевага JFC – підєднувальні компоненти і передбачувана робота незалежно від ОС.

Java ME WTK

Java ME WTK is a toolkit for developing wireless applications based on CLDC and MIDP. It is part of Java ME SDK 3.0. Can be used standalone via KToolbar or command line. Can create Java Archives, Descriptors, or mobile apps.When integrated into an IDE, developers use menus or CLI. Components: UI (for MIDP tasks), Emulator (mobile simulation), Utilities (SMS console, crypto tools).

Java ME WTK

Java ME WTK – це інструментарій для розробки бездротових додатків на основі CLDC і MIDP. Він є частиною Java ME SDK 3.0. Можна використовувати окремо через KToolbar або командний рядок. Можна створювати архіви Java, дескриптори або мобільні додатки. При інтеграції в IDE розробники використовують меню або командний інтерфейс. Компоненти: інтерфейс (для завдань MIDP), емулятор (імітація мобільного), утиліти (консоль SMS, криптоінструменти).

Java Zero Day

Java zero day refers to a threat that surrounds the Java programming language and Java objects, such as applets that work with various Web browsers. It also represents an important issue for Java users and systems that are vulnerable to cyberattacks because they use Java functionality. With its

Нульовий день Java

Нульовий день Java – це загроза, яка оточує мову програмування Java та об'єкти Java, такі як аплети, що працюють з різними веббраузерами. Це також є важливою проблемою для користувачів Java та систем, які вразливі до кібератак, оскільки використовують функціональність

straightforward syntax and a versatile application to Web design, many developers use Java to build applications for the Web. Java has come under fire for a variety of security problems. On zero day, a Java security problem is identified, and IT professionals begin working to resolve the issue.

Java. Завдяки простому синтаксису та універсальному застосуванню до вебдизайну багато розробників використовують Java для створення додатків для Інтернету. Java піддавалася критиці через різні проблеми з безпекою. У день нульової вразливості виявляється проблема безпеки Java, і IT-фахівці починають працювати над її вирішенням.

Jet Propulsion Laboratory (JPL)

Jet Propulsion Laboratory (JPL) is a U.S. federally funded R&D center operated by Caltech for NASA.

JPL focuses on robotic space exploration and partners with global scientists.

It's founded in the 1940s for missile technology, JPL now develops spacecraft for exploring the Solar System.

Лабораторія реактивного руху (JPL)

Лабораторія реактивного руху (JPL) – центр досліджень і розробок США, що фінансується державою та управляється Caltech для NASA.

Основна діяльність JPL – роботизоване дослідження космосу. Лабораторія співпрацює з науковцями з усього світу.

Заснована в 1940-х для розробки ракетної техніки, JPL сьогодні створює апарати для дослідження Сонячної системи.

Jimmy Wales

Jimmy Wales is an American Internet entrepreneur best known as the co-founder of Wikipedia, the nonprofit open-content encyclopedia. He launched Wikipedia in 2001 with Larry Sanger, initially to support Nupedia, a peer-reviewed online encyclopedia. Before that, Wales worked as a financial trader and later founded Bomis, a web portal with user-generated content. Wikipedia quickly became the largest online reference source.

Джиммі Вейлз

Джиммі Вейлз – американський інтернет-підприємець, найбільш відомий як співзасновник Вікіпедії, некомерційної енциклопедії з відкритим контентом. Він запустив Вікіпедію 2001 року разом з Ларрі Сенгером, спочатку як підтримку Nupedia – рецензованої онлайн-енциклопедії. До цього Вейлз працював фінансовим трейдером і заснував портал Bomis з контентом користувачів. Вікіпедія швидко стала найбільшим онлайн-довідником.

John McCarthy

John McCarthy was a computer scientist and one of the founders of artificial intelligence. He coined the term "artificial intelligence" and developed the Lisp programming language, widely used in AI research. He organized the 1956 Dartmouth Conference, which marked AI as a research field. McCarthy also proposed the idea of utility computing, a precursor to cloud computing.

Джон Маккарті

Джон Маккарті – вчений-комп'ютерник, один із засновників штучного інтелекту. Він ввів термін «штучний інтелект» і розробив мову програмування Lisp, широко використовувану в дослідженнях ШІ. Організував Дартмутську конференцію 1956 року, що започаткувала ШІ як напрям. Також запропонував ідею utility computing – прототип хмарних обчислень.

Joli OS

Joli OS, developed by Jolicloud, provides file sharing and access to Web applications and desktops from the cloud. Based on the Ubuntu Linux kernel, it enables netbooks and low-end processors to run Web apps without hardware upgrades. Formerly known as Jolicloud. Joli OS is installed as a thin client on a host desktop and offers access to Web apps like Gmail, Dropbox, Google Docs and Flickr. It includes a launcher for adding apps and social bookmarking features for sharing.

Joli OS

Joli OS, розроблена компанією Jolicloud, забезпечує обмін файлами та доступ до веб-додатків і настільних комп'ютерів із хмари. Заснована на ядрі Ubuntu Linux, вона дозволяє нетбукам і слабким комп'ютерам використовувати веб-додатки без оновлення «заліза». Раніше відома як Jolicloud. Joli OS встановлюється як тонкий клієнт і надає доступ до вебдодатків, таких як Gmail, Dropbox, Google Docs і Flickr. Має панель запуску для додавання програм та функцію соціальних закладок для спільного використання.

Joystick

A joystick is an input device used to control a pointer by moving a lever. It is mostly used in gaming and sometimes in graphic applications.

Useful for people with mobility issues. Types include hand, finger, thumb-operated, and isometric joysticks.

Similar to a mouse, includes buttons (triggers). Joystick movement continues until stopped, unlike the mouse.

Джойстик

Джойстик – пристрій введення для керування курсором за допомогою важеля. Його переважно використовують у відеоіграх і графічних програмах.

Корисний для людей з обмеженими руховими можливостями. Існують різні типи: з ручним, пальцевим, ізометричним керуванням тощо.

Provides quick interaction needed for gaming. It is easy to use and often inexpensive.

Not ideal for menu selection. Some limit direction (no diagonal). Less precise and harder to control than a mouse.

Схожий на мишу, має кнопки (тригери). Рух триває доти, доки джойстик не буде зупинено, на відміну від миші.

Забезпечує швидку взаємодію, потрібну в іграх. Простий у користуванні та зазвичай недорогий.

Не зручний для вибору з меню. Деякі мають обмеження в напрямках. Менш точний і важчий у керуванні, ніж миша.

jQuery

jQuery is a concise and fast JavaScript library that simplifies event handling, HTML traversal, Ajax and animation for Web development. It's open-source, free, and dual-licensed under the GNU GPL. jQuery is widely used and popular due to its simple functions. Developers can create plug-ins for animations, effects and widgets. The modular design supports efficient, powerful Web application creation. jQuery can be used with various technologies like ASP, PHP, JSP, and Servlets.

jQuery

jQuery – це лаконічна і швидка бібліотека JavaScript, яка спрощує обробку подій, роботу з HTML, Ajax та анімацію при створенні вебдодатків. Вона безкоштовна, з відкритим кодом і подвійною ліцензією GNU GPL. Завдяки простоті функцій jQuery дуже популярна. Розробники можуть створювати плагіни для анімації, ефектів і віджетів. Модульна структура полегшує створення потужних вебдодатків. jQuery сумісна з ASP, PHP, JSP, Servlets та іншими мовами вебпрограмування.

Julian Date (or Day)

Julian date (or day) counts days since the start of a 7980-year cycle. Introduced by Joseph Scaliger in 1538. Used in computers and astronomy.

Often confused with the Julian calendar (introduced by Julius Caesar in 45 B.C.).

Julian date measures time difference in days from the cycle's start. Based on solar, lunar, and tax cycles with 7980 as common multiple.

The current cycle began on Jan 1, 4713 B.C. and ends Jan 22, 3268 A.D.

Юліанська дата (або день)

Юліанська дата (або день) – це кількість днів від початку 7980-річного циклу. Запроваджена Йозефом Скалігером у 1538 році. Використовується в ІТ та астрономії.

Часто плутають із юліанським календарем, запровадженим Юлієм Цезарем у 45 р. до н.е.

Вимірює різницю в часі у днях від початку циклу. Базується на сонячному, місячному та податковому циклах, кратних 7980.

Поточний цикл розпочався 1 січня 4713 р. до н.е. і завершиться 22 січня 3268 р. н.е.

Jupyter Notebook

Jupyter Notebook is an interactive Python-based environment for writing and executing code, especially useful for data analysis, machine learning, and visualization tasks. It allows users to combine live code, equations, visualizations, and narrative text in a single document.

Jupyter Notebook

Jupyter Notebook – це інтерактивне середовище на основі Python для написання й виконання коду, особливо корисне для аналізу даних, машинного навчання та візуалізації. Дозволяє поєднувати код, рівняння, візуалізації та текст у одному документі.

Justin Sun

Justin Sun is a Chinese tech entrepreneur best known for founding the Tron blockchain platform and leading major crypto projects like BitTorrent. He is a controversial but influential figure in the cryptocurrency world.

Джастін Сан

Джастін Сан – китайський технологічний підприємець, найвідоміший як засновник блокчейн-платформи Tron та керівник проєктів на кшталт BitTorrent. Він є суперечливою, але впливовою фігурою у світі криптовалют.

Jython

Jython is an open-source implementation of Python written in Java. It provides access to Java libraries and is integrated with the Java Platform. It allows using Java components, applets, and servlets while coding in Python. Jython was originally developed in 1997 by Jim Hugunin. It supports dynamic compilation to Java bytecode for better performance. Java classes can be extended, and static compilation is available.

Jython

Jython – це реалізація Python з відкритим вихідним кодом, написана на Java. Вона надає доступ до бібліотек Java та інтегрована з Java Platform. Дозволяє використовувати компоненти, аплети та сервлети Java, програмуючи на Python. Jython був спочатку розроблений у 1997 році Джимом Хугуніним. Підтримує динамічну компіляцію в байт-код Java для кращої продуктивності.Можна розширювати Java-класи, доступна статична компіляція.

K

Kanban

Kanban is a visual signal used to tell a producer what, when and how much to produce. Originating from Japan, it means "card you can see." Modern e-kanban systems improve upon manual methods. The process starts with customer orders, making it a "pull system." Initially introduced by Toyota in the 1950s, it standardized the flow of parts. A kanban card indicates a part number and is detached during use to signal restocking. One example is the three-bin system for factory, store, and supplier.

Канбан

Канбан – це візуальний сигнал, який повідомляє виробнику, що, коли і в якій кількості виготовляти. Походить з Японії і означає «видима картка». Сучасні електронні системи замінюють ручні. Відправна точка – замовлення клієнтів, тому це «система витягування». Вперше запроваджений Toyota у 1950-х для стандартизації потоку деталей. Картка канбан вказує номер деталі і використовується для сигналізації про потребу у поповненні. Приклад – система з трьома контейнерами: цех, склад, постачальник.

Katmai

Katmai is the code name for Microsoft SQL Server 2008, announced in 2007 and released in 2008 as the 10th major version. It introduced features like improved security, reliability, performance, management, development, data warehousing, and full-text search. It also added support for new data types (e.g., FILESTREAM, GEOGRAPHY, GEOMETRY) and resource governance. Katmai was replaced by SQL Server 2008 R2 (Kilimanjaro) in 2010.

Katmai

Katmai – кодова назва Microsoft SQL Server 2008, анонсована у 2007 році та випущена у 2008 як 10-та основна версія. Вона додала покращену безпеку, надійність, продуктивність, управління, розвиток, сховища даних та повнотекстовий пошук. Також з'явились нові типи даних (наприклад, FILESTREAM, GEOGRAPHY, GEOMETRY) та контроль ресурсів. Katmai було замінено на SQL Server 2008 R2 (Kilimanjaro) у 2010 році.

Key Performance Indicators (KPI)

Key performance indicators (KPI) are measurements used to identify and quantify business performance. KPIs are selected through a management framework. To identify and establish the critical KPIs, an enterprise process must

Ключові показники ефективності (КПЕ)

Ключові показники ефективності (КПЕ) – це показники, які використовуються для визначення та кількісної оцінки ефективності бізнесу. КПЕ обираються за допомогою системи управління. Для визначення та встановлення критичних КПЕ

be created to meet the following requirements:

• Contain clear objectives

• Be measurable, quantitatively and qualitatively

• Identify and resolve organizational variances.

A KPI can really be anything that an organization identifies as being an important driver of the business. . While this term is business-oriented in nature, many IT Professionals would come across it because of its use in business intelligence (BI).

необхідно створити процес на підприємстві, який відповідатиме таким вимогам: Містити чіткі цілі; Бути вимірюваним, кількісно і якісно; Визначати та вирішувати організаційні розбіжності. Ключовим показником ефективності може бути будь-що, що організація визначає як важливий фактор розвитку бізнесу. Незважаючи на те, що це дещо гучне слово, ідея полягає в тому, що якщо щось не вимірюється, воно не покращується. KPI слугує для вимірювання результатів, а потім швидко позначає їх, якщо вони потребують уваги. Хоча цей термін є бізнес-орієнтованим за своєю природою, багато IT-спеціалістів стикалися з ним через його використання в бізнес-аналітиці (BI).

Keyboard, Video, Mouse (KVM)

A KVM switch is a hardware device that connects a keyboard, video display, and mouse to multiple computers, letting one set of input/output devices control them all. It helps save space, reduce cost, and avoid clutter. KVMs are used in data centers and homes. Connections vary: USB, DVI, VGA, or IP. Some allow switching with hotkeys. Modern KVMs support many PCs and peripherals.

Клавіатуру, монітор, мишка (КММ)

KVM-перемикач – це пристрій, що з'єднує клавіатуру, монітор і мишу з кількома комп’ютерами, дозволяючи керувати ними з одного комплекту пристроїв введення/виведення. Він економить простір, зменшує витрати і захаращення. Застосовується у дата-центрах і вдома. Підключення можливе через USB, DVI, VGA або IP. Деякі КММ дозволяють перемикання за допомогою гарячих клавіш. Сучасні КММ підтримують багато ПК та периферії.

Keyword

A keyword is a word or phrase used in SEO to describe the content of a webpage. It helps search engines match the page with relevant queries. While keywords used to be essential for ranking, misuse led to reduced importance in modern SEO. They still matter but are no longer the only ranking factor.

Ключове слово

Ключове слово – це слово або фраза, що описує зміст вебсторінки в контексті SEO. Вони допомагають пошуковим системам зіставляти сторінки з відповідними запитами. Хоча раніше ключові слова були важливими для ранжування, їхнє зловживання призвело до зменшення їхнього значення. Вони залишаються важливими, але не єдині у SEO.

KidsRuby

KidsRuby is a simplified version of the Ruby programming language made for younger users. It supports different coding styles (procedural, functional) and is based on the object-oriented Ruby language. KidsRuby makes it easier for beginners to learn coding. Ruby, created in the 1990s, is similar to Perl and an alternative to Python. Ruby on Rails is a well-known framework built on Ruby.

KidsRuby

KidsRuby – спрощена версія мови програмування Ruby для молодших користувачів. Вона підтримує різні стилі кодування (процедурне, функціональне) та базується на об'єктно-орієнтованій Ruby. KidsRuby полегшує вивчення коду для початківців. Ruby створено у 1990-х, вона схожа на Perl і є альтернативою Python. Ruby on Rails – відомий фреймворк, створений на базі Ruby.

Kirchhoff's Laws (or Circuit Laws)

Kirchhoff's Laws, or circuit laws, are two mathematical equality equations that deal with electricity, current and voltage (potential difference) in the lumped element model of electrical circuits. Described in 1845 by Gustav Kirchhoff, a German physicist, these laws are considered corollaries of the Maxwell equations for the low-frequency limit for alternating current (AC) circuits. The equations are perfectly accurate for direct current (DC) circuits. Kirchhoff's Laws are also known as Kirchhoff's Voltage Law and Kirchhoff's Laws For Current And Voltage. Kirchhoff's laws are fundamental laws used in electrical engineering and related fields, as well as in formulating proper circuits.

Закони Кірхгофа (або закони ланцюга)

Закони Кірхгофа, або закони ланцюга, – це два математичні рівняння рівності, які стосуються електрики, струму та напруги (різниці потенціалів) в моделі електричних ланцюгів з кускових елементів. Описані в 1845 році Густавом Кірхгофом, німецьким фізиком, ці закони вважаються наслідками рівнянь Максвелла для низькочастотної межі для кіл змінного струму (ЗС). Рівняння є абсолютно точними для кіл постійного струму (DC). Закони Кірхгофа також відомі як закон напруги Кірхгофа і закони Кірхгофа для струму і напруги. Закони Кірхгофа – це фундаментальні закони, що використовуються в електротехніці та суміжних галузях, а також при складанні правильних схем.

Knowledge Discovery in databases (KDD)

Knowledge discovery in databases (KDD) is the process of discovering useful knowledge from a collection of data. This widely used data mining technique is a process that includes data preparation and selection, data cleansing, incorporating prior knowledge on data sets and interpreting accurate solutions from the observed

Виявлення знань у базах даних (KDD)

Виявлення знань у базах даних (KDD) – це процес виявлення корисних знань з набору даних. Цей широко використовуваний метод інтелектуального аналізу даних – це процес, який включає підготовку та відбір даних, очищення даних, включення попередніх знань про набори даних та інтерпретацію точних

results. Major KDD application areas include marketing, fraud detection, telecommunication and manufacturing. Traditionally, data mining and knowledge discovery was performed manually. As time passed, the amount of data in many systems grew to larger than terabyte size, and could no longer be maintained manually. Moreover, for the successful existence of any business, discovering underlying patterns in data is considered essential. As a result, several software tools were developed to discover hidden data and make assumptions, which formed a part of artificial intelligence.

рішень на основі спостережуваних результатів. Основні сфери застосування KDD включають маркетинг, виявлення шахрайства, телекомунікації та виробництво. Традиційно інтелектуальний аналіз даних та виявлення знань виконувалися вручну. З часом обсяги даних у багатьох системах зросли до терабайтних розмірів, і їх уже не можна було підтримувати вручну. Для успішного існування будь-якого бізнесу виявлення основних закономірностей у даних є необхідним. У результаті було розроблено кілька програмних інструментів для виявлення прихованих даних і формування припущень, які стали частиною штучного інтелекту.

Knowledge, Skills and Abilities (KSA)

KSA is a competency model used in hiring and retaining qualified staff. It includes job-related knowledge, learned skills, and measurable abilities. Originally required in U.S. government hiring, KSAs were narrative-based but are now embedded in job ads. Key types: technical (knowledge, skills) and behavioral (attitude, collaboration).

Знання, навички та вміння (ЗНВ)

ЗНВ – це модель компетенцій для найму та утримання кваліфікованого персоналу. Вона охоплює професійні знання, набуті навички та вимірювані здібності. Раніше вимагалися в заявках на роботу в уряд США як описові тексти, тепер включені у вакансії. Основні типи: технічні (знання, навички) і поведінкові (ставлення, співпраця).

Kyoto Cooling

Kyoto Cooling is an energy-efficient alternative to traditional cooling systems for data centers and IT infrastructure. It uses a rotating heat wheel (Kyoto wheel) to transfer heat from the warm return air to the cooler outside air, significantly reducing the need for mechanical refrigeration.

Кіотське охолодження

Кіотське охолодження – це енергоефективна альтернатива традиційним системам охолодження для центрів обробки даних та IT-інфраструктури. Воно використовує обертове теплове колесо (кіотське колесо) для перенесення тепла з теплого зворотного повітря до холоднішого зовнішнього, що значно знижує потребу в механічному охолодженні.

L

Lambda Calculus

Lambda calculus is a formal system in mathematical logic used in computer science to define and apply functions, including recursion. It inspired functional programming, which models software development with predictable and transparent computation. Unlike imperative programming, which can change program state and produce different outcomes, functional programming ensures consistent results and can be applied in any language, even those not originally designed for it.

Лямбда-числення

Лямбда-числення – це формальна система математичної логіки, що використовується в інформатиці для визначення та застосування функцій, зокрема рекурсії. Вона стала основою функціонального програмування, яке забезпечує прозору та передбачувану обробку даних. На відміну від імперативного підходу, який змінює стан програми і дає різні результати, функціональне програмування гарантує сталість результатів і може застосовуватися в будь-якій мові, навіть не орієнтованій на нього.

Lead Nurturing

Lead nurturing is the marketing process of building relationships with potential clients who may not be ready to buy yet. Its goal is to increase a company's visibility and influence the client’s future purchasing decisions. Once a company has a client’s contact information, it can personalize communication through simple updates or more complex educational campaigns. While lead nurturing is a traditional practice, modern tools like social media have expanded its role by helping companies build communities around their products.

Лідогенерація

Розвиток потенційних клієнтів – це маркетинговий процес встановлення відносин із потенційними клієнтами, які ще не готові до покупки. Його мета – підвищити впізнаваність компанії та вплинути на майбутні рішення клієнтів щодо покупки. Отримавши контактну інформацію клієнта, компанія може персоналізувати комунікацію через прості оновлення або складніші освітні кампанії. Хоча лідогенерація – традиційна практика, сучасні інструменти, такі як соціальні мережі, розширили її можливості, дозволяючи створювати спільноти навколо брендів.

Lightweight Thread

A lightweight thread is a user-level thread that shares address space and resources with other threads, reducing context switching time. Compared to heavyweight threads, lightweight

Полегшений потік

Полегшений потік – це потік користувацького рівня, який спільно використовує адресний простір і ресурси з іншими потоками, що зменшує час перемикання контексту. У

threads require less processing time. The efficiency of thread processing also depends on the programming language, with languages like C# offering better performance for multi-threaded programs. Modern operating systems, such as macOS, support multiple threads in the same address space, but this alone doesn't fully utilize the advantages of multithreading.

порівнянні з важкими потоками, полегшені потоки потребують менше часу на обробку. Ефективність роботи потоків також залежить від мови програмування – наприклад, C# забезпечує високу продуктивність для багатопотокових програм. Сучасні операційні системи, як-от macOS, підтримують кілька потоків в одному адресному просторі, хоча це само по собі не забезпечує повного використання переваг багатопотоковості.

LinkedIn

LinkedIn (LI) is a professional networking site founded in 2002, focused on helping users create and maintain career-oriented connections and promote their skills or services. LinkedIn is also widely used by recruiters and agencies thanks to its extensive, searchable professional data. One of its most popular features is job searching and matching. The “Follow” feature lets users receive updates on job postings and news from specific organizations. LinkedIn also includes other features that support networking and career development.

LI’s other notable features are:

- Members can post photos and view the profiles and photos of other users.
- Members can view how many people have searched for and viewed them recently, although more detailed information requires a paid upgrade to a premium account.
- Employers can list jobs and openings and search for potential candidates.

Це вебсайт для професійного спілкування

LinkedIn (LI) – це професійна мережа, заснована у 2002 році, що допомагає користувачам створювати та підтримувати ділові зв’язки, а також просувати свої навички й послуги. Завдяки великій кількості доступної для пошуку професійної інформації, платформа стала корисним інструментом для рекрутерів, агентств і пошукачів роботи. Однією з найпопулярніших функцій є можливість пошуку й розміщення вакансій. Також є функція «Follow», яка дозволяє отримувати оновлення про вакансії й новини компаній. LinkedIn має й інші функції, що сприяють розвитку професійної кар’єри та налагодженню контактів.

Іншими важливими функціями LI є такі:

- користувачі можуть публікувати фотографії та переглядати профілі і фотографії інших користувачів;
- користувачі можуть бачити, скільки людей шукали і переглядали їх останнім часом, хоча більш детальна інформація вимагає платного переходу на преміум-аккаунт;
- роботодавці можуть розміщувати вакансії та шукати потенційних кандидатів.

Linux Console Terminal

A Linux console terminal is a system console in the Linux kernel that handles input and output operations. Similar to the Windows command line, it offers full control over the system without requiring a graphical interface. It is commonly used for text-based applications, system configuration, file management, data sharing, and system monitoring. Unlike virtual consoles, the console terminal has its own dedicated screen.

Консольний термінал Linux

Консольний термінал Linux – це системна консоль ядра Linux, яка виконує операції введення та виведення. Подібно до командного рядка в Windows, він забезпечує повний контроль над системою без необхідності графічного інтерфейсу. Його використовують для роботи з текстовими додатками, налаштування системи, керування файлами, обміну даними та моніторингу системи. На відміну від віртуальних консолей, консольний термінал має власний екран.

List Processing

List processing refers to programming operations involving abstract data structures used to compute variables in a specific order, allowing repeated values. Static lists permit only inspection and enumeration, while dynamic lists allow insertion, replacement, and deletion. Each ordered sequence of variables, or tuple, is an instance of a list. Items, entries, and elements all refer to values within a list, with repeated values treated as separate entities. Abstract lists like linked lists are implemented through various data structures. Many programming languages support lists, using commas, semicolons, or spaces to separate elements, and often allow indexing and slicing operations.

Обробка списку

Обробка списків – це операції програмування, що працюють із абстрактними структурами даних для обчислення змінних у певному порядку з можливістю повторення значень. У статичних списках дозволені лише перегляд і перелік елементів, тоді як у динамічних – також вставка, заміна та видалення. Послідовність змінних називається кортежем. Терміни «елемент», «запис» і "значення" позначають окремі елементи списку, навіть якщо вони повторюються. Абстрактні списки, як-от зв'язані списки, реалізуються через різні структури даних. Багато мов програмування підтримують спискові типи даних із розділенням елементів комами, крапками з комами або пробілами, а також дозволяють операції індексації й нарізки.

Logical OR Symbol

The logical OR symbol is a conditional operator used to test the validity of two statements, returning true if at least one is true. It belongs to Boolean algebra and is fundamental in programming and electronic circuits. In programming, it is often represented by one or two vertical bars (| or ||). Many languages distinguish between bitwise OR (|) and logical OR (||), with logical OR often using short-circuit evaluation, meaning if the first condition is false, the second may not be evaluated. C language is a typical example of this distinction.

Символ логічного OR (або)

Логічний оператор OR – це умовний оператор, що перевіряє істинність двох висловлювань і повертає true, якщо хоча б одне з них істинне. Він належить до алгебри Булева і є фундаментальним у програмуванні та електронних схемах. У мовах програмування логічний OR зазвичай позначається однією або двома вертикальними рисками (| або ||). Багато мов розрізняють побітовий OR (|) і логічний OR (||). Логічний OR часто використовує коротке замикання: якщо перша умова хибна, друга може не перевірятися. Прикладом такої реалізації є мова програмування C.

LotusScript

LotusScript is an object-oriented scripting language developed by IBM for its Lotus programs and application suites. Based on BASIC, LotusScript has a coding syntax and structure almost identical to Visual Basic, allowing easy code export between the two. Its GUI is built within the Lotus Domino Designer environment. LotusScript is mainly used in Lotus Notes, Domino, and SmartSuite applications. It supports both front-end and back-end services and integrates with Object Linking and Embedding (OLE) databases, offering strong support for Lotus applications.

Об'єктно-орієнтована мова сценаріїв

LotusScript – це об’єктно-орієнтована скриптова мова, розроблена IBM для програм і пакетів Lotus. Вона базується на BASIC і має майже ідентичний синтаксис та структуру з Visual Basic, що дозволяє легко переносити код між ними. Інтерфейс LotusScript побудований у середовищі Lotus Domino Designer. Мову переважно використовують у додатках Lotus Notes, Domino та SmartSuite. LotusScript підтримує як фронтенд, так і бекенд сервіси, а також інтеграцію з базами даних через технологію Object Linking and Embedding (OLE), надаючи широкі можливості для роботи з додатками Lotus.

M

Malicious Active Content

Malicious active content refers to harmful code embedded in scripting languages like JavaScript, often downloaded without a user's knowledge when visiting interactive websites. Once on a user's system, it can launch attacks, spread worms or viruses, and steal sensitive data. It commonly hides in features like weather widgets, stock tickers, polls, or embedded objects.

JavaScript is especially vulnerable due to its widespread use and flexibility. Attackers often encode the malicious code in formats like Hex or UTF-8 to avoid detection, making it difficult to distinguish from legitimate content. Even tools designed to filter active content, such as ProxySG, can sometimes be bypassed.

ActiveX plug-ins are also known for being easy targets for such attacks. Once infected, a system can be used to impersonate the user, accessing secure websites and stealing passwords – often without any immediate signs, making detection and response difficult.

Because of this, experts recommend using multiple layers of protection, since no single tool can block all types of malicious scripts.

Шкідливий активний вміст

Шкідливий активний контент – це шкідливий код, вставлений у скриптові мови, як-от JavaScript. Його часто завантажують у веббраузер без відома користувача при відвідуванні інтерактивних сайтів. Потрапивши на комп'ютер, такий код може запускати віруси та красти особисті дані.

JavaScript вважається особливо вразливим, оскільки широко використовується та має гнучкий синтаксис. Зловмисники часто шифрують шкідливий код у форматах Hex або UTF-8, що ускладнює виявлення, навіть для захисних систем, таких як ProxySG.

Деякі інтерактивні елементи на сайтах – карти погоди, біржові тікери, опитування – також можуть містити шкідливий активний контент. Плагіни, як-от ActiveX, мають погану репутацію через свою вразливість до таких атак.

Один із найнебезпечніших аспектів – це те, що після зараження система може видавати себе за користувача, входити на захищені сайти й красти паролі, не залишаючи явних слідів. Тому фахівці радять використовувати багаторівневий захист, адже жоден інструмент не гарантує повного захисту від усіх типів шкідливих скриптів.

Many-to-Many Relationship

A many-to-many relationship in a database occurs when multiple records in one table are associated with multiple records in another. This is common in real-world scenarios. For example, in a school system, a student can enroll in multiple subjects, and each subject can be taken by many students.

To represent this type of relationship in a relational database, an intermediary table (also called a junction or bridge table) is used. In the student-subject example, this table could include fields like Student_ID, Subject_ID, Semester, and Year. This table connects each student to the subjects they are enrolled in for a specific term.

Another common example is between employees and departments. An employee might work in multiple departments, and each department may have many employees. Again, an intermediate table using Employee_ID and Department_ID allows for this many-to-many link.

Зв'язок «багато-до-багатьох»

Зв'язок «багато-до-багатьох» у базі даних виникає тоді, коли кілька записів в одній таблиці пов'язані з кількома записами в іншій таблиці. Це типова ситуація у реальному житті. Наприклад, у шкільній системі один студент може вивчати кілька предметів, а кожен предмет викладається багатьом студентам.

Щоб реалізувати такий зв’язок у реляційній базі даних, створюється проміжна таблиця (також її називають таблицею-зв’язком). У випадку зі студентами та предметами така таблиця може містити поля: Student_ID, Subject_ID, Semester, Year. Кожен рядок у цій таблиці вказує, який студент вивчає який предмет у певному семестрі й році.

Інший приклад – співробітники та відділи. Один співробітник може працювати в кількох відділах, а у відділі можуть працювати багато співробітників. Щоб реалізувати цей зв’язок, створюється проміжна таблиця з полями Employee_ID і Department_ID.

MapReduce

MapReduce is a programming model developed by Google to process and generate large datasets using clusters of computers. Originally created to improve Google’s web indexing system, it simplifies the development of parallel programs by handling communication, task monitoring, and error recovery internally. It runs on many standard (commodity) machines and is highly scalable, supporting various programming languages like Java, C++, and C#.

Модель програмування, створена компанією Google

MapReduce – це модель програмування, розроблена Google для обробки та генерації великих обсягів даних у кластерах комп’ютерів. Спочатку вона була створена для вдосконалення системи індексації вебсторінок Google і замінила попередні алгоритми. Ця модель спрощує створення паралельних програм, оскільки сама відповідає за комунікацію між вузлами, моніторинг завдань та обробку збоїв.

The framework consists of two key functions:

- Map, which processes input data across multiple nodes,
- Reduce, which aggregates the results into a final output.

Its main strength is fault tolerance – if a node fails or becomes unresponsive, the system automatically reassigns the task. Inspired by functional programming concepts, MapReduce handles data stored in file systems or databases, converting input key-value pairs into output key-value pairs.

Google runs thousands of MapReduce jobs daily for tasks such as data sorting, log analysis, graph processing, and machine learning. Developers can use it effectively without deep knowledge of distributed systems, as the runtime manages data partitioning, scheduling, and communication.

MapReduce працює на великій кількості звичайних (недорогих) машин і легко масштабується. Її реалізації доступні у різних мовах програмування, таких як Java, C++ і C#.

Фреймворк має дві основні функції:

- Map – розподіляє обробку даних між різними вузлами кластера,
- Reduce – об'єднує результати у фінальний вихід.

Головна перевага MapReduce – відмовостійкість. Якщо один із вузлів не відповідає, головний вузол (master) автоматично перенаправляє завдання на інший. Ідея моделі походить з функціонального програмування: вона обробляє дані у форматі пар «ключ-значення», зберігаючи їх у файлових системах або базах даних.

Google щодня виконує тисячі завдань MapReduce для таких задач, як сортування даних, аналіз логів, обробка графів, кластеризація документів, машинне навчання та статистичний переклад. Навіть розробники без досвіду у розподілених системах можуть ефективно використовувати цей фреймворк завдяки автоматичному керуванню процесами.

Marshalling

Marshalling is the process of converting an object’s in-memory structure into a format that can be easily stored or sent across systems or networks. This process enables communication between different software applications, especially when objects need to be transmitted remotely. The serialized format created during marshalling can be transferred and later restored.

Маршалінг (процес перетворення об'єкта в пам'яті в інший формат)

Маршалінг – це процес перетворення об’єкта в оперативній пам’яті у формат, придатний для зберігання або передачі іншим програмам чи системам. Цей процес уможливлює зв'язок між різними програмними додатками, особливо коли об'єкти потрібно передавати віддалено. Серіалізований формат, створений під час маршалінгу, може бути переданий і пізніше відновлений.

The reverse process is called unmarshalling, which converts the serialized data back into its original object or structure.

These two processes are exact opposites: any transformation done during marshalling is undone during unmarshalling.

Marshalling is essential in remote procedure calls (RPCs), where different systems or processes need to understand each other's data formats. It is also widely used in technologies like Microsoft's COM (Component Object Model) and NET, where managed and unmanaged code need to exchange data.

Зворотний процес називається демаршалізація (unmarshalling), який перетворює серіалізовані дані назад у вихідний об'єкт або структуру.

Обидва процеси – маршалізація і демаршалізація – є взаємно зворотними: усе, що додається або змінюється під час маршалізації, скасовується під час демаршалізації.

Маршалінг є важливим у віддалених викликах процедур (RPC), де різні процеси чи системи мають різні формати даних. Він також широко використовується в таких технологіях, як COM (Component Object Model) від Microsoft та NET, де керований і некерований код повинні обмінюватися даними.

Mashup

Мешап (техніка, за допомогою якої вебсайт або вебдодаток використовує дані)

A mashup is a web-based technique where data or features from different sources are combined to create a new, more useful application. These sources usually share their information through public APIs or web services, allowing developers to access and use them freely. Mashups are often visual and interactive, offering users a more engaging experience. They are also popular with developers because they reduce the amount of code needed, making development faster. The term mashup became popular with the rise of Web 2.0, which emphasizes interaction and collaboration online. For example, Google Maps is often used in mashups, helping developers build apps that show restaurants, traffic updates, or event locations using its map features.

Мешап – це вебтехніка, яка об'єднує дані або функції з кількох джерел для створення нового, більш корисного застосунку. Джерела зазвичай надають доступ через публічні API або вебсервіси, що дозволяє розробникам безкоштовно використовувати їх. Мешапи часто мають візуальний та інтерактивний вигляд, забезпечуючи кращу взаємодію з користувачем. Вони також зручні для розробників, оскільки потребують менше коду, що пришвидшує процес створення. Термін став популярним у період розвитку Web 2.0, який передбачає більшу взаємодію між сайтами та користувачами. Наприклад, Google Maps часто використовується у мешапах для створення застосунків, які показують ресторани, стан доріг або визначні місця.

Massively Multiplayer Online Role-Playing Game

A massively multiplayer online role-playing game (MMORPG) is a video game set in a persistent world with thousands or millions of players developing characters through ongoing interactions. The world continues evolving even when players are offline. Unlike traditional RPGs, MMORPGs focus on emergent gameplay shaped by player cooperation and conflict. Players complete tasks to gain experience, wealth, and skills, form alliances, customize avatars, and sometimes create game content. MMORPGs also feature virtual economies, with in-game currencies sometimes exchanged for real money, and even the hiring of other players ("farmers") to level up characters.

Багатокористувацька онлайн-рольова гра

MMORPG (масова багато-користувацька онлайн-рольова гра) – це відеогра у постійно змінюваному світі, де тисячі або мільйони гравців розвивають своїх персонажів через взаємодію з іншими. Світ гри продовжує змінюватися навіть тоді, коли гравець не в мережі. На відміну від традиційних рольових ігор, MMORPG акцентують увагу на ігровому процесі, що виникає завдяки співпраці та суперництву гравців. Гравці виконують завдання, щоб отримувати досвід, багатство та навички, створюють альянси, налаштовують аватари та навіть створюють власний контент. У MMORPG також існують віртуальні економіки, де ігрову валюту іноді обмінюють на реальні гроші, а також практикується найм «фермерів» для прокачування персонажів.

Member Server

A member server is a Windows-based server that belongs to an Active Directory (AD) domain but is not a domain controller. It provides various network services such as file storage, application hosting, email, databases, and more. Unlike domain controllers, which handle authentication and security policy enforcement, member servers focus on operational services that support users and business functions.

Once a server joins an AD domain, it becomes a member server and can support both local and domain logins. Member servers are essential in enterprise IT environments, often running critical

Сервер-учасник

Сервер-учасник (Member Server) — це сервер на базі Windows, який входить до домену Active Directory (AD), але не є контролером домену. Він виконує різноманітні функції, такі як зберігання файлів, розміщення додатків, електронна пошта, робота з базами даних тощо. Контролер домену відповідає за автентифікацію користувачів і політику безпеки, а сервер-учасник – за обробку сервісів і бізнес-функцій.

Після приєднання до домену сервер отримує статус сервера-учасника та підтримує як локальний, так і доменний вхід. У більшості

systems like financial applications, human resources platforms, SQL databases, web services, and more.

Because these servers manage sensitive operations, securing them is crucial. Security configurations for member servers include managing user rights, service permissions, ports, and local accounts. These are typically controlled using Group Policy, which ensures consistent settings across the domain or specific organizational units.

компаній сервери-учасники є основою інфраструктури, забезпечуючи роботу ключових систем: фінансових, кадрових, вебсервісів, баз даних SQL тощо.

Через важливість виконуваних функцій безпека серверів-учасників має велике значення. Необхідно правильно налаштовувати права користувачів, порти, дозволи для сервісів і локальні облікові записи. Основним інструментом керування безпекою в середовищі AD є групова політика (Group Policy), яка дозволяє централізовано застосовувати налаштування для сайтів, доменів і організаційних підрозділів.

Memory Address

A memory address serves as a unique identifier used by the CPU or hardware device to track the location of data stored in memory. It is essential for the efficient functioning of modern computing systems. Memory is typically addressed in terms of bytes, with each byte assigned a unique memory address. If data exceeds one byte, it is divided into multiple segments, each having its own memory address.

This system allows the CPU to efficiently access and process data. Memory addresses are allocated during the boot process, with different hardware components receiving their own specific addresses. Initially, the video memory (VRAM) is assigned, followed by addresses for expansion card ROM, RAM modules, and other system components. During the boot process, the ROM BIOS on the motherboard assigns the first memory addresses, with the video ROM and RAM being

Адреса пам'яті

Адреса пам'яті є унікальним ідентифікатором, що використовується процесором або апаратними пристроями для відстеження розташування даних, збережених у пам'яті. Це критично важливо для ефективного функціонування сучасних комп'ютерних систем. Пам'ять зазвичай адресована в термінах байтів, і кожен байт отримує унікальну адресу пам'яті. Якщо дані перевищують один байт, вони розподіляються на кілька сегментів, кожен з яких має свою адресу пам'яті.

Ця система дозволяє процесору ефективно отримувати доступ до даних і обробляти їх. Адреси пам'яті призначаються під час процесу завантаження, при цьому різні апаратні компоненти отримують свої конкретні адреси. Спочатку призначається адреса для відеопам'яті (VRAM), а потім – для ROM розширювальних карт, модулів оперативної пам'яті та інших компонентів системи. Під час процесу

prioritized to enable immediate video display capability.

Once the system is operational, the CPU uses these allocated memory addresses to access data from various components, such as the keyboard, stored software, and secondary storage. These addresses are handled by data buses, which help in retrieving and storing data during the execution of programs. The allocation of memory addresses is critical to system performance, as it ensures that each component is correctly accessed without conflicts, allowing for efficient processing and communication between the CPU and the system's memory.

завантаження ROM BIOS на материнській платі призначає перші адреси пам'яті, причому відео ROM та оперативна пам'ять мають пріоритет, щоб забезпечити негайну можливість відображення відео.

Коли система працює, процесор використовує ці призначені адреси пам'яті для доступу до даних з різних компонентів, таких як клавіатура, збережене програмне забезпечення та вторинне сховище. Ці адреси обробляються через системні шини, що допомагають отримувати та зберігати дані під час виконання програм. Виділення адрес пам'яті є критично важливим для продуктивності системи, оскільки це забезпечує правильний доступ до кожного компонента без конфліктів, дозволяючи ефективну обробку та комунікацію між процесором та пам'яттю системи.

Message Queue

A message queue is a software tool that allows programs or different parts of a program to communicate by sending and receiving messages in an organized way. It works asynchronously, meaning the sender doesn’t need the receiver to be available right away –the message is stored in a queue until the receiver is ready. Message queues are commonly used in operating systems, applications, or between different computers to ensure smooth and independent communication. This method helps reduce delays and keeps systems flexible and efficient. Middleware, like message-oriented middleware, helps manage these queues across different networks and systems, even if they use different technologies.

Черга повідомлень

Черга повідомлень – це програмний інструмент, який дозволяє програмам або частинам програми обмінюватися повідомленнями у впорядкований спосіб. Вона працює асинхронно, тобто відправнику не потрібно чекати, поки отримувач буде готовий – повідомлення зберігається в черзі, доки його не буде отримано. Черги повідомлень широко використовуються в операційних системах, додатках або між різними комп’ютерами для забезпечення незалежної та ефективної комунікації. Такий підхід зменшує затримки та підвищує гнучкість систем. Проміжне програмне забезпечення (middleware), як-от орієнтоване на повідомлення, допомагає керувати цими чергами в мережах з різними платформами та технологіями.

Metacomputing

Metacomputing is a technology that connects multiple computing systems to work together, often across different locations. It is used in areas such as business, industry, and software development to process, analyze, and share data efficiently. The idea is to use all available computing resources as if they were one large system. First introduced in the late 1980s at the National Center for Supercomputing Applications, metacomputing now supports large-scale computer grids that act like virtual supercomputers. These systems consist of loosely connected nodes and a set of services that allow them to perform tasks beyond the power of a single computer. Benefits include better graphics, solving complex problems, handling large data loads, and reducing bandwidth usage.

Метаобчислення

Метаобчислення – це технологія, яка об'єднує кілька обчислювальних систем для спільної роботи, часто на великих відстанях. Вона застосовується в бізнесі, промисловості та розробці програмного забезпечення для ефективної обробки, аналізу та обміну даними. Ідея полягає в тому, щоб використовувати всі доступні обчислювальні ресурси як єдину велику систему. Концепція з'явилася наприкінці 1980-х у Національному центрі суперкомп'ютерних застосунків (NCSA). Сучасні системи метакомп'ютингу включають великі обчислювальні мережі, що працюють як віртуальні суперкомп'ютери. Такі системи складаються з слабо пов'язаних вузлів і набору служб, які дозволяють виконувати завдання, що перевищують можливості одного комп'ютера. Переваги включають покращену графіку, вирішення складних задач, обробку великих обсягів даних і зменшення використання пропускної здатності.

Method Stub

A method stub is a placeholder in software development that mimics the behavior of actual code. It's often used when the real functionality is not yet implemented or is temporarily unavailable. A stub only includes the method's name and its parameters, with minimal code to allow successful compilation and linking. Developers use stubs for testing, porting, or during distributed computing, especially when parts of a program are still under construction. Stubs let the rest of the system run without waiting for full code completion.

Метод Заглушки

Метод Заглушки – це тимчасовий код, що використовується в розробці програмного забезпечення для імітації роботи справжньої функціональності. Він застосовується, коли основний код ще не написаний або тимчасово недоступний. Заглушка містить лише назву методу та список параметрів, а також мінімальний код, необхідний для компіляції та зв'язування з іншими частинами програми. Її часто використовують для тестування, перенесення програм або в розподілених обчисленнях, щоб інші частини системи могли працювати, поки справжня реалізація ще створюється.

Methods for Testing and Specification

Methods for Testing and Specification (MTS) is a technical committee within the European Telecommunications Standards Institute (ETSI). It focuses on creating rules, methods, and tools for testing and specifying telecommunications standards. MTS plays a key role in ensuring that communication technologies meet quality and interoperability requirements through well-defined testing procedures.

Its responsibilities include defining advanced testing methods, developing methodologies for future standards, applying global testing standards within ETSI frameworks, and conducting real-world tests. MTS also contributes to the development of specification languages used in major communication technologies like Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE), Digital Enhanced Cordless Telecommunication (DECT) ensuring consistent and reliable standardization across Europe and beyond.

Методи тестування та специфікації

Методи тестування та специфікації (MTS) – це технічний комітет у складі Європейського інституту стандартів зв’язку (ETSI), який займається розробкою правил, методів і засобів для тестування та стандартизації телекомунікаційних технологій. Основна мета MTS – забезпечення якості та сумісності стандартів шляхом створення чітких процедур тестування.

Комітет відповідає за визначення сучасних методів тестування, розробку методологій для майбутніх стандартів, адаптацію міжнародних норм до вимог ETSI та проведення польових випробувань нових рішень. Значна частина роботи MTS пов’язана з мовами специфікацій, які застосовуються в ключових технологіях зв’язку, таких як Глобальна система мобільного зв'язку (GSM), Універсальна система мобільного зв'язку (UMTS), Довгострокова еволюція (LTE), Цифровий вдосконалений бездротовий зв'язок (DECT), сприяючи уніфікації стандартів у Європі та за її межами.

Metro Ethernet

Metro Ethernet refers to the use of carrier Ethernet technology to provide connectivity in metropolitan areas, connecting local area networks (LANs) in businesses, academic institutions, and government offices to the Internet or wide area networks (WANs). It typically involves layer 2 or layer 3 switches and routers connected via optical fiber.

Metro Ethernet networks can use various topologies, such as ring, star, or mesh. The service can be delivered over

Міський Ethernet

Міський Ethernet (Metro Ethernet) – це використання технології Ethernet оператора для забезпечення зв’язку в межах великих міст, з’єднуючи локальні мережі (LAN) підприємств, навчальних закладів і урядових установ з Інтернетом або широкосмуговими мережами (WAN). Зазвичай це мережі, що використовують оптоволоконні комутатори та маршрутизатори 2-го або 3-го рівня.

Ethernet, SDH (Synchronous Digital Hierarchy), MPLS (Multiprotocol Label Switching), or DWDM (Dense Wavelength Division Multiplexing). Pure Ethernet is cheaper but less scalable and reliable, making it suitable for smaller or experimental setups. SDH-based deployments are more reliable and are used by large service providers when there's an existing SDH infrastructure.

Мережі Metro Ethernet можуть використовувати різні топології, такі як кільце, зірка чи сітка. Послуги можуть надаватись через Ethernet, SDH (Синхронна цифрова ієрархія), MPLS (Мультипротокольне міткове перемикання) або DWDM (Щільне мультиплексування з довжинами хвиль). Чистий Ethernet дешевший, але менш масштабований та надійний, тому він більше підходить для невеликих або експериментальних установок. Рішення на базі SDH більш надійні і використовуються великими постачальниками послуг, коли вже є встановлена інфраструктура SDH.

Metro Ethernet Forum

Metro Ethernet Forum (MEF) – неприбуткова організація

The Metro Ethernet Forum (MEF) is a nonprofit organization that seeks to accelerate the use of carrier class Ethernet networks and services worldwide, especially those used by large telecommunications providers. Formed in 2001, MEF includes service providers, hardware makers, and other industry players working together to improve Ethernet technology. MEF also sets its own technical guidelines and works with existing standards organizations. Another group, the Ethernet First Mile Alliance (EFMA), merged into MEF after the IEEE introduced standard 802.3ah in 2005. MEF publishes white papers to help users and businesses understand Ethernet services more clearly.

Metro Ethernet Forum (MEF) – це неприбуткова організація, яка прагне прискорити використання мереж і послуг Ethernet операторського класу в усьому світі, особливо класу операторського рівня. Форум був створений у 2001 році та об'єднує постачальників послуг зв'язку, виробників мережевого обладнання, тестового обладнання та інші компанії, зацікавлені у вдосконаленні технології Ethernet. MEF розробляє власні технічні специфікації та співпрацює з міжнародними органами стандартизації. Інша організація – Ethernet First Mile Alliance (EFMA), яка зосереджувалась на стандартах для першої милі мережі, стала частиною MEF після затвердження стандарту IEEE 802.3ah у 2005 році. MEF також публікує аналітичні матеріали (white papers), які допомагають користувачам і компаніям краще зрозуміти доступні послуги Ethernet.

Micro Fuel Cell

A micro fuel cell (MFC) is a compact power source that converts chemical energy – usually from hydrogen or methanol – into electrical energy. These cells are ideal for powering small electronic devices such as laptops, cameras, and portable radios. Unlike traditional batteries that require recharging, MFCs continuously generate electricity as long as they receive a steady fuel supply.

MFCs are miniaturized versions of hydrogen fuel cells used in vehicles. They have a membrane between two water layers that helps trigger a chemical reaction. As the fuel reacts, the anode releases electrons and protons, generating carbon dioxide. The electrons travel through an external circuit to the cathode, powering connected devices. At the cathode, the electrons and protons combine with oxygen, producing water vapor and heat.

Since MFCs are refillable and not rechargeable like conventional batteries, they offer quick fuel replenishment and long operational life. They typically deliver under 50 watts of power. As technology progresses and demand increases, the cost of MFCs is expected to decrease.

Мікропаливний елемент

Мікропаливний елемент (MFC) — це компактне джерело живлення, яке перетворює хімічну енергію (зазвичай із водню або метанолу) в електричну. Такі елементи використовуються для живлення невеликих електронних пристроїв, таких як ноутбуки, камери та портативні радіо. На відміну від традиційних акумуляторів, які потребують підзарядки, MFC постійно виробляють електроенергію за умови безперервного подавання палива.

MFC — це зменшена версія водневих паливних елементів, які застосовуються в транспорті. Усередині знаходиться мембрана між шарами води, яка сприяє хімічній реакції. Під час розряду анод виробляє електрони, протони та вуглекислий газ. Електрони проходять через зовнішній ланцюг до катода, забезпечуючи живлення пристроїв. На катоді електрони й протони з'єднуються з киснем, утворюючи водяну пару та тепло.

MFC не потребують підзарядки, а лише дозаправки, що робить їх швидкими у використанні й довговічними. Зазвичай вони забезпечують потужність менше 50 ват. Із розвитком технологій і зростанням ринку очікується зниження вартості таких елементів.

Mobile Code

Mobile code refers to any software or content that can move across systems and execute itself on a local machine, often without the user's direct permission. It is

Мобільний код

Мобільний код – це будь-яка програма або вміст, здатні переміщатися між системами та виконуватись на локальному комп'ютері, часто без

commonly embedded in emails, documents, or websites and can travel via networks or devices like USB drives. While mobile code can serve useful purposes, the term is often associated with malicious activities. Harmful mobile code can replicate itself and cause serious damage to systems, such as corrupting files or stealing data. It may be hidden in plug-ins or downloads involving technologies like ActiveX, Flash, or JavaScript. For example, a user might download a song from an infected website, not knowing that the file contains harmful code.

прямого дозволу користувача. Зазвичай він вбудовується в електронні листи, документи або вебсайти та може поширюватися через мережу або пристрої, як-от USB-накопичувачі. Хоча мобільний код може мати корисне призначення, термін часто пов'язують із шкідливою активністю. Такий код може швидко розмножуватись і завдавати серйозної шкоди системі – наприклад, псувати файли або красти дані. Шкідливий код часто приховується у плагінах або завантаженнях, пов'язаних з ActiveX, Flash або JavaScript. Наприклад, користувач може завантажити пісню з зараженого сайту, не підозрюючи, що файл містить небезпечний код.

Mobile Instant Messaging

Mobile Instant Messaging (MIM) is a form of instant messaging designed specifically for mobile devices. It allows real-time communication using technologies such as text messaging, Wireless Access Protocol (WAP), and General Packet Radio Service (GPRS). Unlike standard SMS, MIM can show the availability status of contacts, letting users know who is online.

MIM services can be stand-alone apps or browser-based tools. Some well-known MIM apps include Meebo, Trillian, Beejive, Google Talk, and BlackBerry Messenger. The first three are compatible with Android, iOS, and BlackBerry, while BlackBerry Messenger is exclusive to BlackBerry devices.

Мобільний обмін миттєвими повідомленнями

Мобільний обмін миттєвими повідомленнями (MIM) — це форма миттєвого обміну повідомленнями, призначена для мобільних пристроїв. Вона забезпечує спілкування в реальному часі за допомогою таких технологій, як текстові повідомлення, бездротовий протокол доступу (WAP) та пакетна передача даних (GPRS). На відміну від звичайних SMS, MIM показує статус доступності контактів — хто онлайн, а хто ні.

Деякі MIM-додатки є окремими програмами, інші працюють у веббраузері. Серед найпопулярніших додатків — Meebo, Trillian, Beejive, Google Talk та BlackBerry Messenger. Перші три працюють на Android, iOS і BlackBerry, а останній — лише на пристроях BlackBerry.

Monolithic Kernel

A monolithic kernel is a type of operating system core that has full control over system resources, including memory, input/output devices, and hardware management. It handles various low-level operations directly within the kernel space, making it large in size. This architecture is used in older or traditional systems like Linux, Unix, MS-DOS, and early Mac OS. However, due to its size and complexity, adding new features or fixing bugs often requires recompiling the kernel, which can be time-consuming and difficult to maintain.

Modern operating systems tend to use hybrid or microkernel architectures, where only essential functions remain in the kernel, and other services run in user space. This allows for easier updates, better system stability, and improved security. Despite its limitations, the monolithic kernel is still widely used in systems like Linux, where its design is constantly evolving, and updates are frequent. Thanks to its efficient structure, Linux manages to keep the monolithic kernel lightweight and adaptable.

Монолітне ядро

Монолітне ядро – це тип ядра операційної системи, який має повний доступ до системних ресурсів, таких як пам’ять, пристрої введення/виведення та керування апаратним забезпеченням. Воно виконує багато низькорівневих операцій безпосередньо в ядрі, що робить його досить великим за розміром. Таку архітектуру використовували в традиційних системах, як-от Linux, Unix, MS-DOS і старі версії Mac OS. Проте через складність і великий обсяг коду додавання нових функцій або виправлення помилок часто вимагає перекомпіляції ядра, що ускладнює обслуговування.

Сучасні операційні системи частіше використовують гібридні або мікроядра, де в ядрі залишаються лише основні функції, а решта працює в просторі користувача. Це спрощує оновлення, підвищує стабільність і безпеку системи. Попри недоліки, монолітне ядро досі активно використовується, особливо в системах на базі Linux, де його структура постійно вдосконалюється, а оновлення відбуваються регулярно. Завдяки оптимізованій будові Linux вдається зберігати монолітне ядро легким і гнучким.

Multihomed

Multihomed refers to the configuration of a host computer or network with two or more network connections, which may involve connections to the same type of network or different types, such as LAN segments or connections to multiple ISPs. The primary benefit of multihoming is to

Multihomed (конфігурація, що описує налаштування комп'ютер з двома або більше мережевими адресами)

Термін «мультимодова конфігурація» описує налаштування комп'ютера або мережі з двома або більше з'єднаннями, які можуть бути з'єднаннями одного типу мережі або різних типів, таких як сегменти LAN або з'єднання з кількома Інтернет-

eliminate Single Point of Failure (SPOF) issues by providing alternate data transmission paths in case one path fails. This can enhance both the performance and reliability of network connections, ensuring fault tolerance.

There are several types of multihoming setups, including:

1. Single Link with Multiple IP Addresses: Using one network link but assigning multiple IP addresses to it.
2. Multiple Links with Multiple IP Addresses: Several network connections, each with its own IP address.
3. Multiple Interfaces with Single IP Address per Interface: Each network interface on the host has a single IP address.
4. Multiple Links with Single IP Address: Each connection has one shared IP address.

послугами (ISP). Основна перевага мультимодових з'єднань – усунення проблем з єдиною точкою відмови (SPOF), надаючи альтернативні шляхи передачі даних у випадку відмови одного шляху. Це може підвищити як продуктивність, так і надійність мережевих з'єднань, забезпечуючи толерантність до збоїв.

Є кілька типів мультимодових налаштувань, серед яких:

1. Один лінк з кількома IP-адресами: використовується одне з'єднання з кількома IP-адресами.
2. Кілька лінків з кількома IP-адресами: кілька з'єднань, кожне з власною IP-адресою.
3. Кілька інтерфейсів з однією IP-адресою на інтерфейс: кожен мережевий інтерфейс на хості має одну IP-адресу.
4. Кілька лінків з однією IP-адресою: кожне з'єднання має одну спільну IP-адресу.

Multivalued Field

A multivalued field (MVF) allows a single database field to store multiple values, which can simplify some operations, such as managing many-to-many relationships. However, MVFs are controversial because they violate a key principle of relational database design defined by E.F. Codd, which states that each data value should be atomic and accessible using a table name, primary key, and column name.

While MVFs can make certain tasks easier, they can also complicate SQL queries, potentially causing inaccurate results. MVFs are sometimes referred to as multivalued dependencies.

A notable implementation of MVFs appeared in Microsoft Access 2007, where they were used to improve

Багатозначне поле

Багатозначне поле (MVF) дозволяє зберігати кілька значень в одному полі бази даних. Це може спростити роботу з багатьма задачами, наприклад, реалізацію зв’язків «багато-до-багатьох». Проте MVF викликає суперечки, оскільки порушує основний принцип реляційного моделювання, сформульований Е.Ф. Коддом: кожне значення має бути атомарним і однозначно доступним через назву таблиці, первинний ключ і назву стовпця.

Хоча MVF можуть полегшити розробку, вони можуть також ускладнювати SQL-запити і призводити до помилкових результатів. Інша назва для MVF – багатозначна залежність.

compatibility with SharePoint. For example, in a company intranet, tasks might be assigned to multiple people from a preset list. MVFs allow storing all those people in one field instead of managing a separate relationship table.

Despite this convenience, MVFs are not widely supported. While databases like Oracle allow them, Microsoft SQL Server, as of 2011, still did not support MVFs.

Найвідомішим прикладом використання MVF є Microsoft Access 2007, де ця функція була реалізована для кращої інтеграції з SharePoint. Наприклад, на корпоративному інтернет-порталі завдання можуть призначатися кільком особам із певного списку. MVF дозволяє зберігати ці імена в одному полі, замість створення окремої таблиці зв'язків.

Незважаючи на таку зручність, MVF не мають широкої підтримки. Хоча такі бази даних, як Oracle, дозволяють їх використовувати, Microsoft SQL Server, станом на 2011 рік, все ще не підтримував MVF.

N

Napster

Napster, currently an online music store owned by Best Buy, began in 1999 as a free peer-to-peer (P2P) file-sharing platform founded by Shawn Fanning and Sean Parker. It revolutionized music sharing by enabling users to exchange MP3 files directly, often without respecting copyright laws. This led to major legal issues, especially from the Recording Industry Association of America (RIAA), and culminated in the landmark *A&M Records, Inc. vs. Napster, Inc.* case. Napster was forced to shut down its free service, pay millions in settlements, and later relaunched as a paid music subscription platform. By 2008, Best Buy acquired Napster for $121 million.

Napster's early popularity was driven by its unique focus on MP3s, attracting users looking for rare or live recordings.

Інтернет-магазин музики

Napster – це онлайн-магазин музики, який належить компанії Best Buy. Спочатку він був створений у 1999 році Шоном Феннінгом і Шоном Паркером як безкоштовна платформа для обміну MP3-файлами через P2P-мережу. Napster дозволяв користувачам завантажувати музику без дозволу правовласників, що призвело до масштабного порушення авторських прав.

Найбільш резонансною справою стала *A&M Records проти Napster*, за результатами якої компанія була зобов'язана виплатити $26 мільйонів компенсації й припинити безкоштовне надання музики. У 2001 році сервіс було зупинено, а згодом перетворено на платну підписну платформу. У 2008 році Napster було придбано компанією Best Buy за $121 мільйон.

However, its widespread use overloaded university networks and drew widespread piracy accusations. Although Napster no longer offers free music downloads, it helped shape the future of digital music distribution.

У перші роки Napster здобув величезну популярність серед меломанів, які шукали рідкісні або концертні записи. Незважаючи на юридичні проблеми, він значно вплинув на розвиток цифрової музики та моделі онлайн-стримінгу.

Net Neutrality

Network neutrality is the principle that governments and Internet service providers (ISPs) should not limit or control users' access to online content, services, platforms, or devices. It ensures that all Internet traffic is treated equally, without discrimination or preference. This means that users with the same subscription level should receive the same quality of access, regardless of what they are doing online.

The main aspects of net neutrality include:

1. Non-Discrimination: ISPs should not block or slow down access to any websites or services, and users should be free to publish or access content without bias.
2. Content Diversity: Providers must not alter website content or favor specific content providers.
3. Commercial Use: Online businesses and e-commerce platforms should operate without unfair restrictions or favoritism.
4. IP Telephony: Services like Skype or voice chat using VoIP (Voice over IP) should remain accessible without limitations.

Net neutrality supports open access to information, freedom of expression, and fair competition online.

Мережевий нейтралітет

Мережевий нейтралітет – це принцип, за яким уряди та постачальники інтернет-послуг (ISP) не повинні обмежувати доступ користувачів до вмісту, сайтів, сервісів або пристроїв в Інтернеті. Усі дані повинні передаватися в мережі однаково, без преференцій або упередженого ставлення. Це означає, що користувачі з однаковими тарифними планами повинні мати однаковий рівень доступу до Інтернету.

Основні положення мережевого нейтралітету:

1. Недискримінація:
постачальники не повинні блокувати або сповільнювати доступ до жодних сайтів чи сервісів. Користувачі можуть вільно створювати блоги, коментарі та здійснювати пошук без упередженості.
2. Різноманітність контенту: провайдери не мають права змінювати вміст сайтів або надавати перевагу окремим джерелам.
3. Комерційне використання: підприємці та власники інтернет-магазинів можуть вільно працювати без обмежень з боку провайдерів.
4. IP-телефонія: сервіси на кшталт Skype або голосових чатів, які працюють на основі VoIP, мають залишатися доступними без обмежень.

Мережевий нейтралітет сприяє вільному доступу до інформації, свободі слова та чесній конкуренції в Інтернеті.

Netbook

A netbook is a compact, lightweight mini-laptop with lower processing power and storage capacity compared to traditional laptops. Netbooks typically lack CD/DVD drives, but include small keyboards and are optimized for basic tasks such as web browsing, word processing, and cloud computing.

Originally intended for education as secondary devices, netbooks became popular with students, bloggers, and mobile users. They are also referred to as mini-notebooks, ultra-portables, or cloud books.

Netbooks often run Linux, Windows XP, or Chrome OS. Their functions include:

- Accessing the web
- Using Microsoft Office tools
- Managing photos and multimedia
- Working in cloud-based environments

They are ideal for users who don't require heavy computing power and benefit from portability and long battery life. Over time, spec differences between netbooks and notebooks have narrowed.

Нетбук (міні-ноутбук)

Нетбук – це компактний, легкий міні-ноутбук, який має меншу потужність і менший обсяг пам'яті, ніж звичайний ноутбук. Більшість нетбуків не мають CD/DVD-приводів, але оснащені невеликою клавіатурою, що підходить для базових завдань, таких як веб-серфінг, обробка текстів та робота в хмарі.

Спочатку створені для освітнього ринку як другорядні пристрої, нетбуки стали популярними серед студентів, блогерів та користувачів у дорозі. Також їх називають міні ноутбуками, ультрапортативними або хмарними комп'ютерами.

Нетбуки зазвичай працюють на Linux, Windows XP або Chrome OS. Основні функції:

- перегляд інтернету
- робота з програмами Microsoft Office
- управління фотографіями та медіа
- використання хмарних сервісів

Нетбуки ідеальні для хмарних обчислень, адже вони зменшують ризики втрати даних, проблем із сумісністю програм або збоїв у друку. Специфікації нетбуків і ноутбуків поступово стають схожими, що робить нетбуки хорошою альтернативою.

NetMeeting

NetMeeting was a Microsoft Windows application for audio/video conferencing, instant messaging (IM), chat, desktop sharing, and file transfer. It

Популярна програма для проведення аудіо- та відео-конференцій і обміну миттєвими повідомленнями

NetMeeting – це програма для аудіо- та відеоконференцій, обміну повідомленнями, чатів, спільного використання робочого столу та

was available from Windows 95 OSR2 through Windows XP, and was later replaced by Windows Meeting Space in Windows Vista.

Key points:

- Offered real-time communication features before modern IM tools became popular.
- Integrated with Internet Explorer 3 and 4.

Today, NetMeeting is obsolete and no longer in common use.

передачі файлів, яка входила до складу Microsoft Windows (від Windows 95 OSR2 до Windows XP). У Windows Vista її замінили на Windows Meeting Space.

Основні моменти:

- NetMeeting забезпечував спілкування в реальному часі ще до появи сучасних месенджерів.
- інтегрувався з Internet Explorer 3 та 4.

На сьогодні вийшов з ужитку і майже не використовується.

Netscape Communicator

Netscape Communicator was a suite of Internet applications released by Netscape in 1997. It included several tools:

- Netscape Navigator (web browser)
- Netscape Messenger (email client)
- Netscape Collabra (discussion groups)
- Netscape Address Book
- Netscape Composer (HTML editor)
- Netscape Netcaster (push content)
- Netscape Conference (video/audio communication)
- Netscape Calendar

Although it introduced useful updates, Netscape Communicator marked the end of Netscape's dominance as Microsoft began bundling Internet Explorer (IE) with Windows, leveling the playing field. In 1998, AOL bought Netscape and later shut down the browser business. However, the Netscape codebase lived on through the Mozilla open-source project, which eventually led to the development of Mozilla Firefox.

Пакет інтернет-додатків

Netscape Communicator – це набір інтернет-додатків, випущений компанією Netscape у 1997 році. До нього входили такі компоненти:

- Netscape Navigator – веббраузер
- Netscape Messenger – поштовий клієнт
- Netscape Collabra – інструмент для дискусійних груп
- Netscape Address Book – адресна книга
- Netscape Composer – редактор HTML
- Netscape Netcaster – передача контенту ("push" технологія)
- Netscape Conference – відео та аудіозв'язок
- Netscape Calendar – календар

Хоча програма мала важливі оновлення, Netscape втратив лідерство, коли Microsoft почала постачати Internet Explorer разом із Windows. У 1998 році Netscape була куплена AOL, яка згодом припинила розвиток браузера. Проте кодова база Netscape Navigator стала основою відкритого проєкту Mozilla, який призвів до створення браузера Firefox.

Network Computer

A network computer is a cost-effective, simplified personal computer designed to operate within a centrally managed network. It lacks typical hardware like disk drives or CD-ROMs and relies on a network server for storage and processing. Often called a *thin client*, *diskless node*, or *Internet appliance*, it's primarily used in businesses or environments where full-featured PCs are unnecessary or vulnerable to damage.

Advantages include:

- Lower production and operating cos
- Quiet operation
- Reduced total cost of ownership (TC

Мережевий комп'ютер

Мережевий комп'ютер – це недорогий персональний комп'ютер, створений для роботи в централізованій мережі. Він не має жорсткого диска, CD-ROM або слотів для розширення, і залежить від мережевого сервера для зберігання даних та обчислень. Такий пристрій ще називають *тонким клієнтом*, *вузлом без диска* або *інтернет-пристроєм*.

Переваги:

- Низька вартість виробництва та обслуговування
- Тиха робота
- Зменшення загальної вартості володіння (TCO)

Network Interface Card

A Network Interface Card (NIC) is a hardware component that enables a computer to connect to a network, supporting both wired and wireless connections. It is also called a network adapter, LAN card, or network controller.

Key points:

- Modern computers often have built-in NICs, either integrated into the motherboard or as a separate chip (via PCI or PCI Express).
- NICs may also be found in routers, printers, or USB devices.
- Many NICs have LED indicators to show network activity and data transfer.
- Typical data transfer speeds include 10, 100, or 1000 Mbps (Megabits per second).

Мережева карта

Мережева карта (NIC) – це апаратний компонент, який дозволяє комп'ютеру підключатися до мережі як через дріт, так і бездротово. Інші назви: мережевий адаптер, LAN-карта, контролер мережевого інтерфейсу.

Основні моменти:

- сучасні комп'ютери зазвичай мають вбудовану мережеву карту – у материнську плату або окремим чипом (через PCI або PCI Express).
- NIC також може бути частиною роутерів, принтерів або USB-пристроїв.
- більшість NIC мають світлодіодні індикатори, які показують активність мережі або передачу даних.

Швидкість передачі даних зазвичай становить 10, 100 або 1000 Мбіт/с.

Network Layer

The network layer is the third layer (Layer 3) of the OSI Model, responsible for routing and transferring data packets across different networks. It establishes

Мережевий рівень

Мережевий рівень – це третій рівень (Рівень 3) моделі OSI, що відповідає за маршрутизацію та передачу пакетів даних між різними пристроями та

logical paths, assigns IP addresses, forwards packets, and reports delivery errors. Layer 3 enables communication between heterogeneous networks and supports either connection-oriented or connectionless transmission, but not both at the same time.

Key responsibilities:

- Routing and logical path selection
- Packet forwarding between nodes
- Error reporting via protocols like ICMP
- Quality of Service (QoS) for prioritizing traffic

мережами. Вона визначає логічні шляхи передачі, призначає IP-адреси, пересилає пакети та повідомляє про помилки доставки. Мережевий рівень забезпечує з'єднання між різними мережами, використовуючи або орієнтований на з'єднання, або безз'єднаний тип передавання (але не одночасно обидва).

Основні функції:

- вибір найкращого логічного маршруту
- пересилання пакетів між вузлами
- звітність про помилки доставки (через ICMP)
- пріоритезація трафіку (QoS)

Network PC

A Network PC (Net PC) is a compact, low-cost computer developed in the late 1990s for centralized management in business environments. Unlike traditional computers, Net PCs lack disk drives, CD-ROM drives, and expansion slots, though they include hard disks for caching and performance. Introduced in 1997 by Microsoft and Intel, Net PCs were designed with sealed cases to prevent user modification and were primarily used in settings like banking, retail, and online transaction processing. They were meant to compete with network computers and reduce the complexity and cost of maintaining multiple desktops.

Мережевий ПК (Net PC)

Мережевий ПК (Net PC) — це компактний і недорогий комп’ютер, розроблений у кінці 1990-х для централізованого управління в бізнес-середовищі. На відміну від звичайних ПК, Net PC не має дисководів, CD-ROM або слотів розширення, але оснащений жорстким диском для кешування й підвищення продуктивності. Представлені у 1997 році компаніями Microsoft та Intel, Net PC мали герметичні корпуси, щоб запобігти модифікаціям користувачів, і використовувалися переважно у сфері банківських послуг, торгівлі та онлайн-операцій. Вони були створені як конкурентна альтернатива мережевим комп’ютерам, орієнтована на зниження витрат і спрощення адміністрування.

Nickel-Cadmium Battery

A nickel-cadmium battery (NiCd or NiCad) is a rechargeable battery commonly used in portable electronics like laptops, power tools, and camcorders. It consists of nickel oxide hydroxide and

Нікель-кадмієвий акумулятор

Нікель-кадмієвий акумулятор (NiCd або NiCad) – це акумуляторна батарея, що широко використовується в портативних пристроях, зокрема ноутбуках, електроінструментах та

metallic cadmium electrodes, with potassium hydroxide as the electrolyte. Invented by Waldemar Junger in 1899, NiCd batteries offer stable power output throughout discharge and support deep discharge cycles.

Key advantages:

- Long lifespan due to more charge/discharge cycles
- High energy density, compact, and lightweight
- Works well in applications where size and weight matter (e.g. aviation)
- Lower self-discharge rate than NiMH batteries

Drawbacks include:

- Toxicity of nickel and cadmium
- High cost of materials
- Can overheat and self-destruct if improperly charged (e.g., using a dynamo)
- Require thermal cutoffs for safety

відеокамерах. Складається з електродів із гідроксиду нікелю, металевого кадмію та лужного електроліту – гідроксиду калію. Її винайшов Вальдемар Юнґнер у 1899 році.

Переваги NiCd акумуляторів:

- стійка напруга під час розрядки
- стійкі до глибоких розрядок
- довговічні – витримують більше циклів заряд/розряд
- легкі та компактні, ідеальні для авіації
- нижчий саморозряд, ніж у батарей NiMH (20% проти 30% на місяць)

Недоліки:

- висока токсичність нікелю та кадмію
- дорожчі у виробництві
- можуть перегріватися та вибухати при неправильному заряджанні (особливо з динамо)
- потребують внутрішнього термозахисту для безпечної експлуатації.

Nokia N8

The Nokia N8, released on September 23, 2010, was Nokia's flagship smartphone and the first to run the Symbian 3 operating system. Key features included:

- Capacitive multitouch screen: allowed finger gestures like tap, swipe, pinch, and zoom.
- 12 MP camera with Carl Zeiss optics and Xenon flash: enabled high-quality photography even in low light.
- HDMI output: could connect to TVs or projectors for HD video (720p) and Dolby Digital Plus audio.
- ARM11 680 MHz CPU: provided solid performance for its time.
- Integrated social networking: support for apps combining Facebook and Twitter.

Nokia N8 (перший смартфон під управлінням операційної системи Symbian)

Nokia N8, випущений 23 вересня 2010 року, став флагманським смартфоном Nokia і першим, що працював на операційній системі Symbian 3.

Основні характеристики:

- ємнісний мультисенсорний екран: підтримує жести пальцями (дотик, змахування, масштабування).
- камера на 12 МП з оптикою Carl Zeiss і спалахом Xenon: забезпечує високу якість фото навіть при слабкому освітленні.
- HDMI-вихід: дає змогу підключати телефон до телевізорів або проекторів для перегляду відео у форматі 720p з аудіо Dolby Digital Plus.
- процесор ARM11 680 МГц: забезпечує хорошу продуктивність.

• Voice-guided navigation: a standout feature for mobile navigation.

Although Nokia had released touch phones earlier, the N8 was only its second with a capacitive screen, offering a more modern user experience compared to older resistive screens.

• інтеграція з соціальними мережами: підтримка додатків Facebook і Twitter.

• навігація з голосовими підказками: одна з найбільш рекламованих функцій.

Хоча Nokia вже випускала сенсорні телефони, N8 був лише другим з ємнісним екраном, що покращувало взаємодію користувача.

Nuker

A nuker is a type of hacker or malicious program that aims to crash or disable a computer by sending corrupted or invalid data, often using a modified *ping* tool to repeatedly send harmful Internet Control Message Protocol (ICMP) packets. Some nukers exploit messaging apps using macros or scripts to repeatedly send infected messages. While modern systems are generally protected against such attacks, nukers can still target vulnerable ports to launch denial of service (DoS) attacks and shut down websites.

One of the earliest and most notorious nuker attacks was WinNuke, which affected Windows 95, NT, and 3.1x. It sent out-of-band data that caused system crashes and displayed the "blue screen of death." Microsoft later released patches to stop such attacks, especially on ports 135–139 and 445.

Consumers who are concerned about DoS attacks should contact their Internet service provider for assistance in combating these types of attacks.

Нукер – тип хакера

Нукер (Nuker) – це тип хакера або шкідливої програми, яка намагається вивести комп'ютер з ладу, надсилаючи пошкоджені або неправильні дані. Часто для цього використовується модифікована утиліта *ping*, яка надсилає шкідливі ICMP-пакети. Деякі нукери використовують програми обміну повідомленнями, надсилаючи інфіковані повідомлення за допомогою макросів або скриптів. Хоча сучасні системи мають захист від таких атак, нукери досі можуть використовувати вразливі порти для атак типу відмова в обслуговуванні (DoS), щоб зупинити роботу сайтів.

Однією з перших і найнебезпечніших атак була WinNuke, яка вражала системи Windows 95, NT і 3.1x. Вона надсилала позасмугові (out-of-band) дані, що призводило до збою системи та появи «синього екрану смерті». Microsoft випустила патчі для захисту від таких DoS-атак, зокрема для портів 135–139 і 445.

Споживачі, які занепокоєні DoS-атаками, повинні звернутися до свого інтернет-провайдера за допомогою в боротьбі з цими типами атак.

O

Object Linking and Embedding

Object Linking and Embedding (OLE) is a Microsoft technology that allows sharing and inserting data or objects from different applications. Linking connects two files, while embedding places data directly into a host document.

OLE is commonly used for compound documents and drag-and-drop or clipboard operations.

OLE objects can appear as:

- Icons (double-click to open or edit).
- Content (like charts or graphs embedded into a document).

Example: An Excel chart embedded into a Word file can be edited directly in Word.

Applications supporting OLE include Word, Excel, PowerPoint, Adobe Acrobat, AutoCAD, and multimedia tools.

Disadvantages:

- Embedded objects increase file size.
- Linked objects may break if files are moved.
- Objects can't be edited if the original application isn't available.

Зв'язування та вбудовування об'єктів

Зв'язування та вбудовування об'єктів (OLE) – це технологія Microsoft, що дозволяє обмінюватися та вставляти дані чи об'єкти з різних програм. Зв'язування створює посилання між файлами, а вбудовування вставляє дані безпосередньо в документ.

OLE використовується для роботи зі складеними документами, перетягуванням об'єктів та операціями з буфером обміну.

Об'єкти OLE можуть виглядати як:

- піктограма (подвійне клацання відкриває або дозволяє редагувати).
- вміст (наприклад, діаграма чи графік у документі).

Приклад: Діаграма з Excel, вставлена у Word, може редагуватися прямо у Word.

Програми, що підтримують OLE: Word, Excel, PowerPoint, Adobe Acrobat, AutoCAD та мультимедійні застосунки.

Недоліки:

- вбудовані об'єкти збільшують розмір файлу.
- зв'язані об'єкти можуть не працювати при переміщенні файлів.

Об'єкти не редагуються без початкової програми.

On-Demand Self Service

On-demand self-service is a key cloud computing feature that lets users access and manage cloud resources (like computing power and storage) as needed

Самообслуговування на вимогу

Самообслуговування на вимогу – це ключова функція хмарних технологій, яка дозволяє користувачам самостійно отримувати доступ до ресурсів

through an online control panel. Users can scale resources up or down without interrupting services.

This model supports flexible use, starting with minimal resources and expanding over time. It works with a pay-as-you-grow system, meaning users only pay for what they use, similar to utility computing.

(обчислювальна потужність, сховище тощо) через онлайн-панель, масштабуючи їх за потреби без переривання роботи.

Цей підхід забезпечує гнучкість: користувачі починають з мінімальних ресурсів і поступово їх збільшують. Модель працює за принципом «оплата за використання», подібно до комунальних послуг.

On-Demand Service

On-demand service is a key feature of cloud computing that lets users instantly access computing, storage, software, and other resources when needed. Resources can be added without interrupting current operations.

Cloud computing makes it easy to deploy and manage essential applications, much like signing up for email. It also allows flexible scaling – companies can increase or reduce resources based on demand, making on-demand service highly efficient and cost-effective.

Сервіс на вимогу

Сервіс на вимогу – це ключова функція хмарних технологій, яка дозволяє користувачам миттєво отримувати доступ до обчислювальних ресурсів, сховищ, програмного забезпечення та іншого, коли це потрібно. Додавання ресурсів відбувається без перерв у роботі.

Хмарні обчислення забезпечують легке розгортання важливих додатків, подібно до реєстрації поштової скриньки. Також можливе гнучке масштабування – компанії можуть швидко збільшувати або зменшувати ресурси відповідно до потреб, що робить цей сервіс ефективним і економним.

Open Enterprise Server

Open Enterprise Server (OES) is a server OS by Novell that combines features of NetWare and SUSE Linux Enterprise Server. It can be installed as either OES-Linux or OES-NetWare.

OES merges NetWare's networking strengths with SUSE's server management. It includes tools like eDirectory, iFolder, iManager, and cluster/user management, making it suitable for enterprise environments.

Серверна операційна система

Open Enterprise Server (OES) – це серверна операційна система від Novell, яка поєднує можливості NetWare та SUSE Linux Enterprise Server. Її можна встановити як OES-Linux або OES-NetWare.

OES поєднує мережеві функції NetWare з інструментами керування сервером від SUSE. До її складу входять eDirectory, iFolder, iManager та інструменти для керування користувачами та кластерами, що робить її придатною для підприємств.

Open Mobile Alliance

The Open Mobile Alliance (OMA) is an organization that develops open standards to support interoperability in mobile services globally. It helps grow the mobile market by promoting standards for data, entertainment, and communication.

OMA has around 200 members, including mobile operators, IT firms, and content providers. It emerged from earlier initiatives like WAP and SyncML and works with other bodies such as 3GPP and CEA.

Its working groups focus on areas like architecture, messaging, device management, and mobile commerce.

Організація, що займається розробкою специфікацій для мобільного зв'язку

Open Mobile Alliance (OMA) — це організація, яка розробляє відкриті стандарти для забезпечення сумісності мобільних сервісів у всьому світі. Вона сприяє розвитку мобільного ринку, просуваючи стандарти для даних, розваг та комунікацій.

OMA об’єднує близько 200 учасників: мобільних операторів, IT-компаній та контент-провайдерів. Вона утворилася на основі таких ініціатив, як WAP та SyncML, і співпрацює з організаціями, зокрема з 3GPP та CEA.

Групи OMA займаються питаннями архітектури, обміну повідомленнями, керування пристроями та мобільної комерції.

Open Source Initiative

The Open Source Initiative (OSI) is a non-profit organization founded in 1998 by Bruce Perens and Eric Raymond to promote open-source software. Raymond, a key figure in the open-source movement, served as OSI president until 2005. OSI should not be confused with the OSI Model used in networking.

Inspired by Netscape’s release of its source code, Perens and Raymond created OSI to coordinate open-source development. By 2011, Michael Tiemann was president, and OSI was based in San Francisco.

OSI differs from the Free Software Foundation (FSF), led by Richard Stallman. While both support open

Неприбуткова організація, що займається просуванням програмного забезпечення з відкритим вихідним кодом.

Open Source Initiative (OSI) – неприбуткова організація, заснована у 1998 році Брюсом Перенсом і Еріком Реймондом для просування відкритого програмного забезпечення. Реймонд, важлива постать у русі відкритого коду, був президентом OSI до 2005 року. Не слід плутати OSI з моделлю OSI в мережевих технологіях.

Після того як Netscape відкрив код свого браузера, Перенс і Реймонд створили OSI для координації розробки відкритого ПЗ. У 2011 році президентом був Майкл Тіманн, а штаб-квартира OSI була розташована в Сан-Франциско.

software, OSI takes a more business-oriented approach, whereas FSF is based on moral principles. Despite philosophical differences, the two groups have collaborated.

OSI promotes open-source awareness, education, and certification. It maintains the Open Source Definition and certifies software licenses that allow free use, modification, and distribution.

OSI відрізняється від Free Software Foundation (FSF), яку очолює Річард Столмен. Хоча обидві організації підтримують відкритість, OSI орієнтована на практичний і бізнесовий підхід, тоді як FSF – на моральні принципи. Попри розбіжності, вони співпрацювали над спільними проєктами.

OSI займається популяризацією відкритого ПЗ, освітою та сертифікацією. Вона підтримує Визначення відкритого ПЗ і сертифікує ліцензії, які дозволяють вільне використання, зміну та розповсюдження програм.

OpenGL for Embedded Systems

OpenGL ES (OpenGL for Embedded Systems) is a lightweight, cross-platform API used for 3D graphics on embedded devices like smartphones, game consoles, and PDAs. It uses minimal power and storage, making it ideal for mobile platforms.

As a low-level, royalty-free API, OpenGL ES enables developers to create advanced 3D graphics. It acts between applications and graphics engines. With better mobile hardware, it supports powerful graphics. The Khronos Group manages OpenGL ES.

OpenGL для вбудованих систем

OpenGL ES (OpenGL для вбудованих систем) – це полегшений кросплатформенний API для 3D-графіки на вбудованих пристроях, таких як смартфони, ігрові консолі та КПК. Він споживає мало енергії та пам’яті, що підходить для мобільних платформ.

Як низькорівневий та безоплатний API, OpenGL ES дає змогу створювати просунуту 3D-графіку. Він працює між додатками та графічними рушіями. Його розвиток підтримує група Khronos.

Operating System

An Operating System (OS) is software that manages hardware and software resources on a computing device and enables the running of other applications. It controls input/output devices, network connections, storage, and allocates system resources like CPU and memory to active programs.

Операційна система

Операційна система (OS) – це програма, яка керує апаратними та програмними ресурсами комп’ютера і дозволяє запускати інші програми. Вона контролює ввід/вивід пристроїв, мережеві з’єднання, сховища, а також розподіляє ЦП та пам’ять між активними додатками.

Key points:

- Ensures that multiple applications can run efficiently and simultaneously.
- Acts as an intermediary between hardware and software, simplifying application development.
- Common OS examples: Windows, Linux, macOS, iOS, Android.

Early OSs emerged in the 1950s, evolving from simple libraries to full systems.

Основні моменти:

- забезпечує одночасну та ефективну роботу кількох програм.
- є посередником між програмами та апаратним забезпеченням, спрощуючи розробку ПЗ.
- популярні ОС: Windows, Linux, macOS, iOS, Android.

Перші ОС з'явилися у 1950-х роках.

Operators

In C#, operators are symbols used to perform operations in expressions. They work with operands like literals, variables, and expressions to perform tasks such as calculations, assignments, or comparisons.

C# supports:

- Unary (1 operand),
- Binary (2 operands), and
- Ternary (3 operands) operators.

Operators can be overloaded for user-defined types using the operator keyword. For example, overloading == lets you compare values instead of references.

C# also has operator precedence and associativity, which define the evaluation order.

The various types of C# operators that are used for specific functionalities include:

- Assignment (=) : used to assign the result of an expression to a variable
- Short-hand assignment(+=,-=,*=,/=,%=,&=,|=,^=,<<=,>>=): for shortening the common assignment operations
- Arithmetic (+,-,*,/,%) : for constructing mathematical expressions

Оператори

У C# оператори – це символи, які використовуються для виконання операцій в виразах. Вони працюють з операндами (літералами, змінними, виразами) для виконання обчислень, присвоєнь чи порівнянь.

C# підтримує:

- унарні (1 операнд),
- бінарні (2 операнди),
- тернарні (3 операнди) оператори.

Оператори можна перевантажувати для користувацьких типів за допомогою ключового слова operator. Наприклад, перевантаження == дозволяє порівнювати значення, а не посилання.

Також у C# є пріоритет і асоціативність операторів, що визначають порядок обчислень.

Існують різні типи операторів C#, які використовуються для виконання певних функцій:

- присвоєння (=): використовується для присвоєння результату виразу змінній
- скорочене присвоювання(+=,-=,*=,/=,%=,&=,|=,^=,<<=,>>=): для скорочення звичайних операцій присвоювання

- Increment and decrement operators (++ and –): shortcut for incrementing or decrementing the value by 1
- Comparison (==,>,<,>=,<=,!=): for performing comparison that control the program flow
- Boolean logical operator (!, &&, ||, ^): for performing Boolean logical operations
- Bitwise manipulation (&,|,^,>>,<<): for manipulating each bit of integer values
- Type testing(is, as): to check or convert the type of an object
- Pointer manipulation(*,&,->,[]): for operations performed directly on pointers in unsafe context
- Overflow exception (checked and unchecked): option to check or avoid checking overflow on values

Ternary operator (?:):used for making decisions

- арифметика (+,-,*,/,%): для побудови математичних виразів
- оператори інкременту та декременту (++ та -): скорочення для збільшення або зменшення значення на 1
- порівняння (==,>,<,>=,<=,!=): для виконання порівнянь, які керують ходом програми
- булевий логічний оператор (!, &&, ||, ^): для виконання булевих логічних операцій
- побітова маніпуляція (&,|,^,>>,<<): для маніпуляції з кожним бітом цілочисельних значень
- перевірка типів (is, as): для перевірки або перетворення типу об'єкта
- маніпуляції з вказівниками (*,&,->,[]): для операцій, що виконуються безпосередньо над вказівниками у небезпечному контексті
- виключення переповнення (з перевіркою та без перевірки): опція для перевірки або уникнення перевірки переповнення значень
- тернарний оператор (?:): використовується для прийняття рішень

Optical Fiber Amplifier

An optical fiber amplifier boosts optical signals directly without converting them to electrical signals. It's essential in long-distance fiber optic communication, where amplifiers are placed along the cable to maintain signal strength.

The first type, erbium-doped fiber amplifier (EDFA), appeared in the late 1980s. These amplifiers use silica-based fibers and a pump light source to provide gain.

Оптоволоконний підсилювач

Оптоволоконний підсилювач підсилює оптичні сигнали без їх перетворення в електричні. Це ключовий елемент у системах волоконно-оптичного зв’язку на великі відстані, де підсилювачі розміщують уздовж кабелю для збереження сили сигналу.

Перший тип – волоконний підсилювач, допований ербієм (EDFA) – з’явився наприкінці 1980-х років. Підсилювачі використовують волокна

Types of optical fiber amplifiers:

- Doped Fiber Amplifiers (DFA): Use doped fibers with ions and pump lasers to amplify signals. Typical noise is 6–8 dB.
- Semiconductor Optical Amplifiers: Use laser diode structures with improved coatings to reduce reflection.
- Raman Amplifiers: Use nonlinear fiber and pump wavelengths to amplify signals; can be distributed or lumped.
- Optical Parametric Amplifiers: Use nonlinear optical media for wide-band signal amplification via non-collinear geometry.

із силікатного скла й джерело накачування для створення посилення.

Типи оптичних волоконних підсилювачів:

- доповані волоконні підсилювачі (DFA): використовують доповане волокно та лазери накачування. Типовий рівень шуму – 6–8 дБ.
- Напівпровідникові оптичні підсилювачі: побудовані на основі лазерних діодів із покращеним антивідбивним покриттям.
- раманівські підсилювачі: використовують нелінійні волокна й довжини хвиль накачування; можуть бути розподілені або зосереджені.

Оптичні параметричні підсилювачі: застосовують нелінійні середовища та неколінеарну геометрію для широкосмугового підсилення.

Oracle OpenWorld

Щорічна подія, на якій демонструються можливості продуктів та інші новини від корпорації Oracle

Oracle OpenWorld is an annual, multi-day event held in cities like San Francisco, São Paulo, and Shanghai, organized by Oracle Corporation. It showcases Oracle's products, technologies, and acquisitions, targeting IT professionals and business decision-makers.

The event features keynotes by Oracle executives, product demos, lab sessions, and seminars. For example, in 2010, Oracle highlighted the integration of Sun Microsystems' technologies like Java and Solaris. The event plays a key role in Oracle's strategy to reach corporate users, as the company focuses on business software.

Oracle OpenWorld – це щорічна багатоденна подія, яка проходить у таких містах, як Сан-Франциско, Сан-Паулу та Шанхай, організована компанією Oracle. Захід демонструє продукти, технології та нові придбання Oracle, орієнтуючись на ІТ-фахівців і керівників бізнесу.

Програма включає виступи керівників Oracle, демонстрації продуктів, лабораторні сесії та семінари. Наприклад, у 2010 році Oracle зосередила увагу на інтеграції технологій Sun Microsystems, таких як Java і Solaris. Подія є важливою частиною стратегії компанії, яка зосереджена на корпоративних клієнтах.

Organic Search Engine Optimization

Organic SEO refers to unpaid techniques used to improve a website's ranking in search engine results. Common methods include keyword optimization, backlinking, and creating high-quality content. Some unethical "black hat" tactics like keyword stuffing may boost rankings temporarily but can harm a site's reputation or get it banned.

The term "organic" implies that the site grows and evolves naturally over time, adapting to user needs.

Key organic SEO strategies:

- Use relevant content
- Spread backlinks
- Add metatags and descriptive attributes

Benefits of organic SEO:

- Brings more clicks due to content relevance
- Results last longer than paid ads
- Builds trust with users

More cost-effective than paid listings.

Органічна пошукова оптимізація

Органічна SEO – це безоплатні методи покращення позицій сайту в пошукових системах. До них належать оптимізація ключових слів, зворотні посилання та якісний контент. Нечесні методи (чорна SEO), як-от надмірне використання ключових слів, можуть тимчасово підвищити рейтинг, але зрештою шкодять сайту або навіть призводять до його блокування.

Термін «органічна» означає, що сайт природно розвивається та змінюється відповідно до потреб користувачів.

Основні стратегії органічної SEO:

- використання релевантного контенту
- поширення зворотних посилань
- додавання метатегів та атрибутів

Переваги органічної SEO:

- більше кліків завдяки актуальності контенту
- довготривалий ефект у видачі пошуковиків
- формує довіру користувачів

Значно дешевша за платну рекламу.

Orkut

Orkut was a social networking site developed by Google, enabling users to connect, share videos and pictures, and chat via GTalk. It was especially popular in Brazil and India.

The platform was created by Orkut Buyukkokten, a Turkish engineer and Google product manager. He had previously developed social networks like inCircle. In 2004, Google faced a lawsuit alleging orkut copied inCircle code.

Despite gaining over 100 million users by 2011, orkut struggled with

Соціальна мережа

Orkut – соціальна мережа, розроблена компанією Google, яка дозволяла спілкування, обмін відео й фото, а також чат через GTalk. Найбільшу популярність мала в Бразилії та Індії.

Платформу створив Оркут Бююккоктен, турецький інженер і менеджер проєктів у Google. Раніше він розробив мережу inCircle. У 2004 році проти Google подали позов, звинувативши у копіюванні коду inCircle.

security issues like hacking and spam. Google took steps to improve security. Over time, many users began shifting to Facebook, especially in Brazil and India.

Попри те, що до 2011 року orkut нараховував понад 100 мільйонів користувачів, він стикався з проблемами безпеки – хакерством і спамом. Google вживала заходів для їх вирішення. Згодом багато користувачів почали переходити до Facebook, особливо в Бразилії та Індії.

Orphan File

An orphan file is a leftover file, often a .dll, remaining after its original application has been uninstalled – usually due to an incomplete or manual removal.

While safe deletion is possible, it should be done with caution, as some orphan files may still be used by other programs or the operating system. In many cases, it's safer to leave them, especially if they're small in size.

Спадковий файл

Спадковий файл – це залишковий файл (часто з розширенням .dll), який лишився після видалення пов'язаної програми, особливо якщо видалення було неповним або ручним.

Такі файли можна видаляти обережно, але варто переконатися, що вони не потрібні іншим програмам чи самій системі. Часто краще залишити їх, особливо якщо вони займають мало місця.

Outsourced Product Development

Outsourced Product Development (OPD) involves hiring a third-party provider to develop products and services in fields like IT, business, communication, HR, and idea generation. Successful OPD relies on strategic planning, communication, collaboration, and specialized resources.

Key factors for successful OPD include continuous communication between decision-makers (managers, engineers, business owners) to ensure quality production and customer satisfaction.

Recommendations for OPD success:

- Develop during daylight hours, test in the evening.
- Outsource to locations that minimize time zone differences.

Аутсорсингова розробка продукту

Аутсорсинг розробки продуктів (OPD) – це практика, коли організація наймає третю сторону для розробки продуктів і послуг у таких сферах, як IT, бізнес, комунікації, HR та генерування ідей. Успіх OPD залежить від стратегічного планування, комунікації, співпраці та спеціалізованих ресурсів.

Ключові фактори для успішної реалізації OPD включають безперервну комунікацію між основними учасниками (менеджерами, інженерами, власниками бізнесу) для забезпечення якості продукції та задоволення клієнтів.

Рекомендації для успіху OPD:

- Розробка протягом дня, тестування – в вечірні години.

- Recruit high-quality team members to foster innovation.
- Small teams are more efficient, so balance is needed for synergy.
- Intellectual Property (IP) costs should be accounted for.
- Focus on monitoring the impact on quality and customer satisfaction.

The IT industry, including offshore offices of companies like Microsoft and Cisco, makes up about 15% of the OPD market.

- Аутсорсинг у місця з мінімальною різницею в часі.
- Найм високоякісних учасників для стимулювання інновацій.
- Маленькі команди працюють ефективніше, тому необхідно забезпечити синергію.
- Враховувати витрати на інтелектуальну власність (IP).
- Основна увага – на моніторинг впливу на якість продукції та задоволеність клієнтів.

ІТ-індустрія, включаючи офшорні офіси таких компаній, як Microsoft і Cisco, становить близько 15% ринку OPD.

P

Pasta Theory

Pasta theory is a programming analogy that compares code structures to pasta dishes:

- Spaghetti code: Unstructured and hard to read or update.
- Lasagna code: Layered and readable, but difficult to change due to hidden dependencies.
- Ravioli code: Clean, object-oriented code that's easy to maintain; interfaces act like "sauce" connecting the parts.

Many programmers spend time rewriting spaghetti or lasagna code into better object-oriented (OOP) code or replacing it completely.

Теорія макаронів

Теорія макаронів (пасти) – це аналогія в програмуванні, яка порівнює структуру коду з видами пасти:

- код-спагеті: неструктурований, важкий для читання та оновлення.
- код-лазанья: має шари та зрозумілий, але важко змінюється через приховані залежності.
- код-равіолі: чистий об'єктно-орієнтований код, яким легко керувати; інтерфейси – це «соус» між частинами.

Багато програмістів займаються переписуванням коду-спагеті чи лазаньї в кращий ООП-код, або створюють нову програму з нуля.

Patch

A patch is a software update that modifies or replaces part of a program's code. It is usually used to:

- Fix bugs or security issues
- Add new features or drivers
- Improve software stability or performance

Patches can be downloaded from the Internet and may be free or available only to registered users. Modern patches often install automatically.

Patches are usually small, but large updates (especially in Windows) are called service packs.

Патч (оновлення програмного забезпечення, що складається з коду, який вставляється (або виправляється) в код виконуваної програми)

Патч – це оновлення програмного забезпечення, яке змінює або замінює частину коду програми. Його використовують для:

- виправлення помилок або вразливостей безпеки
- додавання нових функцій чи драйверів
- поліпшення стабільності чи продуктивності

Патчі зазвичай завантажуються з Інтернету та можуть бути безкоштовними або доступними лише для зареєстрованих користувачів. Сучасні патчі часто встановлюються автоматично.

Зазвичай патчі маленькі, але великі оновлення (наприклад, у Windows) називають пакетами оновлень (*service packs*).

Pay Per Click

Pay Per Click (PPC) is an online advertising model where advertisers pay each time someone clicks on their ad. It is often used in search advertising, where companies bid on keywords.

Publishers usually sell ads by cost per impression (CPM), but not all ad space is sold that way, so some is sold via PPC. PPC and cost per click (CPC) are often used interchangeably. PPC refers to the model in general, while CPC is the price paid per click. For example, Google is a major PPC provider, and a CPC might be $0.25 per click.

Оплата за клік

PPC (оплата за клік) – це модель онлайн-реклами, коли рекламодавець платить кожного разу, коли користувач клікає на його оголошення. Часто використовується в пошуковій рекламі, де йде аукціон за ключові слова.

Рекламні майданчики зазвичай продають рекламу за CPM (ціна за тисячу показів), але частину простору віддають під PPC. PPC – це загальна назва моделі, а CPC означає конкретну вартість одного кліка, наприклад $0.25. Google – один із головних постачальників PPC-реклами.

Personal Digital Assistant

A Personal Digital Assistant (PDA) is a portable device used for managing personal information. PDAs support web browsing, office apps, multimedia, and sometimes phone functions. Common features include touchscreens, Bluetooth, Wi-Fi, memory card slots, and synchronization with desktop or cloud data.

The line between PDAs and smartphones has blurred, as many smartphones now include PDA functions. Early notable PDAs include the Apple Newton, Nokia 9000 Communicator, and Palm Pilot.

Персональний цифровий асистент

Персональний цифровий асистент (PDA) –портативний пристрій для керування особистою інформацією. PDA підтримують веббраузинг, офісні програми, мультимедіа та іноді функції телефону. Звичайні функції – сенсорний екран, Bluetooth, Wi-Fi, слоти для карт пам'яті та синхронізація з ПК або хмарою.

Різниця між PDA та смартфонами стирається, адже багато смартфонів мають функції PDA. Відомі ранні PDA – Apple Newton, Nokia 9000 Communicator і Palm Pilot.

PHP: Hypertext Preprocessor 3.0

PHP 3.0 (Hypertext Preprocessor) is a free, server-side scripting language created by Rasmus Lerdorf. It can be embedded into HTML to make dynamic web pages and supports databases like MySQL, Oracle, and PostgreSQL.

Inspired by Perl, Java, and C, PHP 3.0 is easy to learn and use. It handles complex math, file uploads, cookies, and user authentication. It also supports HTTP authentication and error reporting (e.g., function errors, warnings, parser errors, notices).

PHP 3.0 includes regular expression functions for advanced string operations, such as ereg, eregi, and split.

PHP: Препроцесор гіпертексту 3.0

PHP 3.0 (Hypertext Preprocessor) – це безкоштовна серверна мова сценаріїв, створена Расмусом Лердорфом. Її можна вбудовувати в HTML для створення динамічних вебсторінок. Вона підтримує бази даних, зокрема MySQL, Oracle та PostgreSQL.

PHP 3.0 заснований на ідеях з Perl, Java і C, тому його легко вивчити. Він підтримує складні обчислення, завантаження файлів, кукі-файли та автентифікацію користувачів. Також доступна система звітності про помилки (наприклад, помилки функцій, попередження, синтаксичні помилки, повідомлення).

PHP має функції для регулярних виразів, які використовуються для роботи зі строками – наприклад, ereg, eregi, split.

Pierre Salinger Syndrome

Pierre Salinger Syndrome is a term for people who believe everything they read on the Internet. It comes from former White House Press Secretary Pierre Salinger, who wrongly claimed the 1996 TWA Flight 800 crash was caused by a U.S. Navy missile.

Although Salinger got the information from security sources—not the Internet—people believed he had found it online. The incident became linked to online misinformation. Critics said Salinger didn't verify the story properly. The real cause of the crash was later found to be a fuel tank explosion.

This syndrome is mostly seen in inexperienced Internet users who can't tell real news from hoaxes.

Синдром П'єра Селінджера

Синдром П'єра Саліджера – це термін, що описує людей, які вірять у все, що читають в Інтернеті. Назва походить від П'єра Саліджера, прес-секретаря Білого дому, який помилково заявив, що катастрофа рейсу TWA 800 у 1996 році сталася через ракету ВМС США.

Хоча Саліджер отримав цю інформацію не з Інтернету, багато хто вважав, що він знайшов її онлайн. Це стало символом дезінформації в Інтернеті. Насправді причиною катастрофи був вибух паливного бака.

Найчастіше цей синдром зустрічається у недосвідчених користувачів Інтернету, які не вміють відрізняти факти від вигадок.

Pipe

A pipe is a method of passing data from one program process to another, usually offering one-way communication. The system temporarily holds the data until the receiving process reads it. Pipes are common in Unix and Linux programming.

In shell scripts, a pipe is represented by a vertical bar |. It sends the output of one command as the input to another, allowing more complex processing. Two pipes can be used for two-way communication.

Труба

Труба (pipe) – це метод передачі даних від одного процесу програми до іншого, зазвичай в одному напрямку. Дані тимчасово зберігаються в системі, поки їх не зчитає інший процес. Канали часто використовуються в Unix та Linux.

У скриптах оболонки Unix канал позначається вертикальною рискою |. Він передає вивід однієї команди як вхід для іншої, що дозволяє створювати складніші обробки. Для двосторонньої передачі можна використати два канали.

Planking

Planking is a game where a person lies face down with arms at the sides and feet stretched out, often in strange or dangerous places. A photo is taken and

Планкінг

Планкінг – це гра, де людина лягає обличчям донизу з витягнутими руками вздовж тіла і ногами, зазвичай у незвичних або небезпечних місцях.

shared online. It is also called the lying down game.

The term became popular in Australia in 2011, but it may have started earlier in England with Gary Clarkson and Christian Langdon. Planking quickly spread on social media, with people doing it in extreme locations like the Taj Mahal or aircraft engines. In 2011, a man in Australia died while trying to plank on a seventh-story balcony, bringing attention to the dangers.

Потім її фотографують, і знімок публікують в Інтернеті. Інша назва – гра лежачи.

Термін став популярним в Австралії у 2011 році, хоча саму ідею, ймовірно, започаткували в Англії Ґері Кларксон і Крістіан Ленгдон. Через соцмережі планкінг швидко поширився, іноді до небезпечних крайнощів (наприклад, на Тадж-Махалі чи двигуні літака). У 2011 році один чоловік загинув, намагаючись зробити фото на сьомому поверсі.

Private Automatic Branch Exchange

Private Automatic Branch Exchange (PABX) is a telephone system used by large organizations to manage internal and external calls. It allows:

- One access number to connect to many external callers.
- Internal calls between staff using extensions.
- Automatic switching of calls without manual help.

PABX is an upgraded version of PBX and uses computers to manage calls. It is owned and controlled by the organization. Operators are rarely needed, except to help new users.

Приватна АТС

Автоматична приватна телефонна станція (АТС) – це телефонна система, яку використовують великі організації для керування внутрішніми та зовнішніми дзвінками. Вона забезпечує:

- один номер для багатьох зовнішніх дзвінків.
- внутрішні дзвінки між співробітниками.
- автоматичне з'єднання без участі оператора.

АПТС – це вдосконалена версія ТС, яка використовує комп'ютери для керування дзвінками. Система належить організації. Оператор потрібен лише у виняткових випадках.

Proof of work

Proof of Work (PoW) is a consensus mechanism used in blockchain networks to securely validate transactions and add new blocks. Miners compete to solve complex cryptographic puzzles using computational power. The first miner to solve the puzzle earns the right to add the block and receives rewards in cryptocurrency and transaction fees. This

Доказ роботи

Proof of Work (PoW) – це механізм консенсусу, який використовується в блокчейн-мережах для безпечної валідації транзакцій та додавання нових блоків. Майнери змагаються у розв'язанні складних криптографічних задач, використовуючи обчислювальні потужності. Перший майнер, який розв'язує задачу, отримує право додати

process ensures the blockchain remains decentralized and trustless, meaning users don't need to rely on a central authority. PoW was originally designed to prevent spam and denial-of-service attacks and was adapted for cryptocurrencies by Hal Finney and later popularized by Bitcoin's creator, Satoshi Nakamoto.

While PoW provides strong security, it requires significant energy because many computers continuously work to solve puzzles. This energy consumption has led to alternative consensus methods like Proof of Stake (PoS) and Proof of Authority (PoA), which are less resource-intensive. Despite its drawbacks, PoW remains one of the most proven methods for maintaining blockchain integrity and preventing fraud. The system also includes a "halving" event, where mining rewards are cut in half approximately every four years to control supply and inflation. Overall, PoW is central to many cryptocurrencies and blockchain platforms, balancing security and decentralization through computational effort.

блок і винагороду у вигляді криптовалюти та комісій за транзакції. Цей процес забезпечує децентралізацію блокчейну і робить систему «без довіри», тобто користувачам не потрібно покладатися на центральний орган управління. PoW спочатку був розроблений для запобігання спаму та атакам типу відмова в обслуговуванні, а потім адаптований для криптовалют Хелом Фінні та пізніше популяризований творцем Біткоїна – Сатоші Накамото.

Хоча PoW забезпечує високий рівень безпеки, він потребує значних енергетичних затрат, оскільки багато комп'ютерів безперервно працюють над розв'язанням задач. Через це з'явилися альтернативні механізми консенсусу, такі як Proof of Stake (PoS) та Proof of Authority (PoA), які менш енергозатратні. Незважаючи на недоліки, PoW залишається одним із найперевіреніших методів для підтримки цілісності блокчейну та запобігання шахрайству. У системі також є подія «халвінг», коли винагороди за майнінг зменшуються вдвічі приблизно кожні чотири роки для контролю над пропозицією та інфляцією. Загалом, PoW є ключовим для багатьох криптовалют і блокчейн-платформ, балансуючи між безпекою та децентралізацією через обчислювальні зусилля.

Protocol Stack

A protocol stack is a group of network protocols that work together in layers (such as in the OSI or TCP/IP models). Each layer handles specific tasks, like data transport or addressing. For successful communication, all protocols in the stack must be interoperable – able to connect both between layers (vertically) and across network devices (horizontally).

Стек протоколів

Стек протоколів – це набір мережевих протоколів, які працюють разом у шарах (наприклад, у моделях OSI або TCP/IP). Кожен шар виконує певні функції, як-от передача даних чи адресація. Для ефективного обміну даними протоколи мають бути сумісними – тобто взаємодіяти як між

The stack allows different systems to share data even if they use different hardware or transmission methods. Each layer uses its own protocols, and these layers must work together. This layered approach keeps network communication organized and flexible.

шарами, так і між пристроями в мережі.

Стек дозволяє різним системам обмінюватися даними, навіть якщо вони використовують різне обладнання або способи передачі. Кожен шар має свої протоколи, які працюють спільно для забезпечення загальної функції – передавання даних через мережу.

Q

Q-learning

Q-learning is a term for an algorithm structure representing model-free reinforcement learning. By evaluating policy and using stochastic modeling, Q-learning finds the best path forward in a Markov decision process.

Q-навчання

Q-навчання – це термін для позначення структури алгоритму, що представляє безмодельне навчання з підкріпленням. Оцінюючи політику та використовуючи стохастичне моделювання, Q-навчання знаходить найкращий шлях у процесі прийняття рішень за Марковом.

QR code phishing (quishing)

QR code phishing, also known as quishing, is a type of cyberattack that involves tricking someone into scanning a malicious QR code

Фішинг QR-кодів (квішинг)

Фішинг QR-кодів, також відомий як квішинг, – це тип кібератаки, який полягає в тому, щоб обманом змусити когось відсканувати шкідливий QR-код.

Quadtree

A quadtree is a type of data structure where each original or parent node has four lower-level or subsequent child nodes, where each element is continually split into four pieces. Expressed in mathematical equations or in a visual way, a quadtree has many data analysis applications.

Дерево квадрантів (Quadtree)

Quadtree (дерево квадрантів) – це тип структури даних, де кожен початковий або батьківський вузол має чотири нижчих або наступних дочірніх вузли, де кожен елемент постійно розбивається на чотири частини. Квадродерево, виражене в математичних рівняннях або у візуальному вигляді, має багато застосувань для аналізу даних.

Quantization

Quantization is a process aimed at simplifying data representation by reducing precision – the number of bits used. This process involves approximating a continuous range of values with a smaller set of discrete options.

Квантифікація

Квантифікація – це процес, спрямований на спрощення представлення даних шляхом зменшення точності – кількості використовуваних бітів. Цей процес передбачає апроксимацію безперервного діапазону значень меншим набором дискретних параметрів.

Quantization Error

The definition of quantization error is the difference between the original continuous signal *(infinite precision*) and its quantized representation (*limited precision*). When rounding to the nearest quantization level, there's always a discrepancy between the original and its quantized version.

Похибка квантування

Похибка квантування – це різниця між вихідним неперервним сигналом (нескінченна точність) і його квантованим представленням (обмежена точність). При округленні до найближчого рівня квантування завжди існує розбіжність між оригіналом та його квантованою версією.

Quantum Internet

The quantum internet is an idea based on the theoretical use of quantum computers to construct a new kind of network. In contrast to the traditional internet which operates through the use of binary signals in data packets, the quantum internet would utilize quantum signals instead.

Квантовий інтернет

Квантовий інтернет – це ідея, заснована на теоретичному використанні квантових комп'ютерів для побудови нового типу мережі. На відміну від традиційного інтернету, який працює завдяки використанню двійкових сигналів у пакетах даних, квантовий інтернет буде використовувати квантові сигнали.

Query Plan Monitoring

Query plan monitoring is the act of monitoring the performance and output of a query during execution. A query plan provides clear, logical steps to perform tasks such as querying databases and retrieving data. Just like creating a query plan is a complex task, monitoring it for

Моніторинг плану запиту

Моніторинг плану запиту – це відстеження продуктивності та результатів виконання запиту під час його виконання. План запиту містить чіткі, логічні кроки для виконання таких завдань, як створення запитів до баз даних і отримання даних. Так само,

performance and output is a complex process. Monitoring is a multidimensional task and the plan needs to monitor multiple aspects of a query such as performance, nested steps and their performance, and speed of retrieval.

як створення плану запиту є складним завданням, так само складним процесом є моніторинг його виконання та результатів. Моніторинг є багатовимірним завданням, і план повинен відстежувати різні аспекти запиту, такі як продуктивність, вкладені кроки та їхня продуктивність, а також швидкість пошуку.

R

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) refers to technologies that use wireless communication between an object (tag) and an interrogating device (reader) to automatically identify and track the physical location of each object. A tag's transmission range is limited to several meters from the reader and a clear line of sight between the tag and reader is not necessarily required.

Радіочастотна ідентифікація (RFID)

Радіочастотна ідентифікація (RFID) – це технологія, яка використовує бездротовий зв'язок між об'єктом (міткою) і опитувальним пристроєм (зчитувачем) для автоматичної ідентифікації та відстеження фізичного місцезнаходження кожного об'єкта. Діапазон передачі мітки обмежений кількома метрами від зчитувача, і не обов'язково, щоб між міткою та зчитувачем була пряма видимість.

Radio Frequency Identification Tag (RFID tag)

A Radio Frequency Identification Tag (RFID tag) is an electronic tag that exchanges data with a radio frequency identification (RFID) reader by using radio waves.

Радіочастотна ідентифікаційна мітка (RFID-мітка)

Радіочастотна ідентифікаційна мітка (RFID-мітка) – це електронна мітка, яка обмінюється даними зі зчитувачем радіочастотної ідентифікації (RFID) за допомогою радіохвиль.

Rational Rose

Rational Rose is an object-oriented programming (OOP) and unified modeling language (UML) tool to design enterprise-level software applications and

Rational Rose

Rational Rose – це об'єктно-орієнтоване програмування (ООП) та уніфікована мова моделювання (UML) для розробки програмних додатків та

components. It creates visual software application models under object-oriented principles. Example application models include the creation of actors, use cases, relationships, objects, entities, etc. Rational Rose uses classical UML concepts to graphically model software applications. This facilitates documenting the environment, requirements and overall design.

компонентів корпоративного рівня. Він створює візуальні моделі програмних додатків на основі об'єктно-орієнтованих принципів. Приклади моделей додатків включають створення акторів, варіантів використання, зв'язків, об'єктів, сутностей тощо. Rational Rose використовує класичні концепції UML для графічного моделювання програмних додатків. Це полегшує документування середовища, вимог і загального дизайну.

Record

In relational databases, a record is a group of related data held within the same structure. More specifically, a record is a grouping of fields within a table that reference one particular object. The term record is frequently used synonymously with row.

Запис

У реляційних базах даних запис – це група пов'язаних даних, що зберігаються в одній структурі. Точніше кажучи, запис – це група полів у таблиці, які посилаються на один конкретний об'єкт. Термін «запис» часто використовується як синонім терміну «рядок».

Region of Interest (ROI)

A region of interest (ROI) is a subset of an image or a dataset identified for a particular purpose.

Регіон інтересу (ROI)

Регіон інтересу (ROI) – це підмножина зображення або набору даних, визначена для певної мети.

Registered Jack-11 (RJ-11)

A registered jack-11 (RJ-11) is a 6-position 2-conductor telephone connector/ jack (6P2C) with 4 positions unused. In the United States, RJ-11 is commonly used to connect the telephone handset to the base unit, and the entire telephone to the wall outlet.

Іменний роз'єм-11 (RJ-11)

Іменний роз'єм-11 (RJ-11) – це 6-позиційний 2-провідний телефонний роз'єм (6P2C), 4 позиції якого не використовуються. У Сполучених Штатах RJ-11 зазвичай використовується для підключення телефонної трубки до базового блоку, а всього телефону до розетки.

Registered jack-45 (RJ45)

Registered jack-45 (RJ45) refers to a cable termination specification that specifies physical male and female connectors and the pin assignments of wires-in telephone cables and other networks that use RJ45 connections.

Release management

Release management is the part of the software management process dealing with development, testing, deployment and support of software releases to the end user. The team involved in this process is referred to as the release management team.

Remote Desktop

A remote desktop is a separate program or feature found on most operating systems that allows a user to access an operating computer system's desktop. The access occurs via the Internet or through another network in another geographical location and allows users to interact with that system as if they were physically at their own computer. USB devices with the ability to recreate a remote user's desktop are commonly called secure portable offices.

Іменований роз'єм RJ45 (Registered jack-45)

Іменований роз'єм RJ45 (Registered jack-45) – це специфікація кабельних закінчень, яка визначає фізичні чоловічі і жіночі роз'єми і призначення контактів проводів в телефонних кабелях та інших мережах, які використовують з'єднання RJ45.

Управління випусками

Управління випусками – це частина процесу управління програмним забезпеченням, що займається розробкою, тестуванням, розгортанням і підтримкою випусків програмного забезпечення для кінцевого користувача. Команда, яка бере участь у цьому процесі, називається командою управління випуском.

Віддалений робочий стіл

Віддалений робочий стіл – це окрема програма або функція в більшості операційних систем, яка дозволяє користувачеві отримати доступ до робочого столу операційної комп'ютерної системи. Доступ відбувається через Інтернет або через іншу мережу в іншому географічному місці і дозволяє користувачам взаємодіяти з цією системою так, ніби вони фізично перебувають за власним комп'ютером. USB-пристрої з можливістю відтворення робочого столу віддаленого користувача зазвичай називають захищеними портативними офісами.

Route Control

Route control is a specialized type of network management that aims to improve Internet connectivity, and reduce bandwidth cost and overall internetwork operations.

Керування маршрутом (маршрутизація)

Маршрутизація – це спеціалізований тип управління мережею, який має на меті покращити підключення до Інтернету, зменшити витрати на пропускну здатність і загальну роботу мережі.

Router

A router is a device that analyzes the contents of data packets transmitted within a network or to another network. Routers determine whether the source and destination are on the same network or whether data must be transferred from one network type to another, which requires encapsulating the data packet with routing protocol header information for the new network type.

Маршрутизатор

Маршрутизатор – це пристрій, який аналізує вміст пакетів даних, що передаються всередині мережі або в іншу мережу. Маршрутизатори визначають, чи знаходяться джерело і пункт призначення в одній мережі, чи потрібно передати дані з одного типу мережі в інший, що вимагає інкапсуляції пакета даних з інформацією заголовка протоколу маршрутизації для нового типу мережі.

RSA Identification Verification for Health Care

RSA identification verification for health care is a real-time identity authentication product produced by RSA Security Inc. RSA identification verification enlists knowledge-based authentication (KBA) to help ensure that sensitive electronic health records (EHR) are accessed only by authorized users.

Перевірка ідентифікації RSA для охорони здоров'я

Перевірка ідентифікації RSA для охорони здоров'я – це продукт для автентифікації особи в режимі реального часу, вироблений компанією RSA Security Inc. Перевірка ідентифікації RSA використовує автентифікацію на основі знань (KBA), щоб забезпечити доступ до конфіденційних електронних медичних записів (ЕМД) лише авторизованим користувачам.

RTP Control Protocol (RTCP)

RTP Control Protocol (RTCP) is a real time transport protocol (RTP) component of voice over Internet protocol (VoIP) communication.

RTP протокол контролю (RTCP)

RTP протокол контролю (RTCP) – це компонент транспортного протоколу реального часу (RTP), що входить до складу голосового зв'язку через Інтернет-протокол (VoIP).

S

Scrum

Scrum is an iterative and incremental framework for project management mainly deployed in agile software development. The scrum methodology emphasizes functional software, the flexibility to change along with emerging business realities, communication and collaboration.

Скрам

Скрам – це ітеративний та інкрементний фреймворк для управління проектами, який в основному використовується в гнучкій розробці програмного забезпечення. Методологія скраму робить акцент на функціональному програмному забезпеченні, гнучкості до змін відповідно до нових бізнес-реалій, комунікації та співпраці.

Self-join (Inner Join)

A self-join, also known as an inner join, is a structured query language (SQL) statement where a queried table is joined to itself. The self-join statement is necessary when two sets of data, within the same table, are compared.

Самооб'єднання (внутрішнє об'єднання)

Самооб'єднання, також відоме як внутрішнє об'єднання, – це оператор мови структурованих запитів (SQL), за допомогою якого запитувана таблиця об'єднується сама з собою. Оператор самооб'єднання необхідний, коли порівнюються два набори даних в одній таблиці.

Simple IT Infrastructure Definition

The simple IT infrastructure definition is the combined set of hardware, software, network resources, and services (like CRM solutions) required for the operation, management, and support of an organization's IT environment. This includes servers, storage, networking devices, and software applications.

Essentially, IT infrastructure is the foundation for all of an organization's IT services and operations. It ensures data flows smoothly, applications run efficiently, and IT services are reliable and secure. It supports daily operations,

Просте визначення IT-інфраструктури

Просте визначення IT-інфраструктури – це сукупність обладнання, програмного забезпечення, мережевих ресурсів і сервісів (наприклад, CRM-рішень), необхідних для роботи, управління та підтримки IT-середовища організації. Сюди входять сервери, сховища, мережеві пристрої та програмне забезпечення.

По суті, IT-інфраструктура є основою для всіх IT-сервісів та операцій організації. Вона забезпечує безперебійний потік даних, ефективну роботу додатків, надійність та безпеку

facilitates communication and collaboration, and allows organizations to adapt quickly to market changes.

IT-сервісів. Вона підтримує щоденні операції, полегшує комунікацію та співпрацю, а також дозволяє організаціям швидко адаптуватися до ринкових змін.

Single Inline Memory Module (SIMM)

Single inline memory module (SIMM) is a type of RAM (random access memory) that was popular in the early 1980s to late 1990s. SIMMs have 32-bit data paths and were standardized under the JEDEC JESD-21C standard. Non-IBM PC computers, UNIX workstations and the Mac IIfx used the non-standard SIMMS.

Одиночний модуль пам'яті (SIMM)

Одиночний модуль пам'яті (SIMM) – це тип оперативної пам'яті (пам'яті з довільним доступом), який був популярний на початку 1980-х - наприкінці 1990-х років. SIMM мають 32-розрядні канали передачі даних і були стандартизовані за стандартом JEDEC JESD-21C. Комп'ютери PC інших виробників, робочі станції UNIX та Mac IIfx використовували нестандартні SIMMS.

Smartphone

A smartphone is a mobile phone with highly advanced features. A typical smartphone has a high-resolution touch screen display, WiFi connectivity, Web browsing capabilities, and the ability to accept sophisticated applications. The majority of these devices run on any of these popular mobile operating systems: Android, Symbian, iOS, BlackBerry OS and Windows Mobile.

Смартфон

Смартфон – це мобільний телефон з високорозвиненими функціями. Типовий смартфон має сенсорний дисплей з високою роздільною здатністю, підключення до Wi-Fi, можливість перегляду вебсторінок і здатність приймати складні додатки. Більшість цих пристроїв працюють на одній з цих популярних мобільних операційних систем: Android, Symbian, iOS, BlackBerry OS та Windows Mobile.

Software Development Kit (SDK)

A software development kit (SDK) is a set of tools used for developing applications provided by hardware and software providers. SDKs are usually comprised of application programming interfaces (APIs), sample code, documentation, etc.

Комплект для розробки програмного забезпечення (SDK)

Комплект для розробки програмного забезпечення (SDK) – це набір інструментів для розробки додатків, що надаються постачальниками апаратного та програмного забезпечення. SDK зазвичай складаються з інтерфейсів прикладного програмування (API), зразків коду, документації тощо.

Software Modem

A software modem is a modem with minimum hardware capability designed to work using a host computer's resources. Softare modems are capable of a majority of tasks performed by a traditional hardware modem, but use the host computer's processor to carry out the signal processing required to modulate and demodulate data signals.

This term is also known as win modem, soft modem and driver based modem.

Програмний модем

Програмний модем – це модем з мінімальними апаратними можливостями, призначений для роботи з використанням ресурсів комп'ютера. Програмні модеми здатні виконувати більшість завдань, які виконує традиційний апаратний модем, але використовують процесор комп'ютера для обробки сигналів, необхідних для модуляції та демодуляції сигналів даних.

Цей термін також відомий як win-модем, програмний модем і модем на основі драйверів.

Software Switch

A software switch is an Internet Protocol (IP) application programming interface (API), which bridges software and hardware systems. The device was developed by the International Softswitch Consortium (ISC), which was formed in May 1999.

Програмний комутатор

Програмний комутатор – це інтерфейс прикладного програмування (API) Інтернет-протоколу (IP), який з'єднує програмне та апаратне забезпечення. Пристрій був розроблений Міжнародним консорціумом програмних комутаторів (ISC), який був сформований у травні 1999 року.

Sound Card

A sound card is an expansion component used in computers to receive and send audio. Sound cards are configured and utilized with the help of a software application and a device driver. The input device attached to receive audio data is usually a microphone, while the device used to output audio data is generally speakers or headphones.

Звукова карта

Звукова карта – це компонент розширення, який використовується в комп'ютерах для отримання та надсилання звуку. Звукові карти налаштовуються і використовуються за допомогою програмного забезпечення та драйвера пристрою. Пристроєм введення для отримання аудіоданих зазвичай є мікрофон, а пристроєм виведення аудіоданих – динаміки або навушники.

Sprite Effects

Sprite effects are graphical images normally found on gaming multimedia that rotate in relation to the user's movement or camera rotation. A sprite contains a series of pictures that display themselves as one picture or animation.

Ефекти спрайтів

Ефекти спрайтів – це графічні зображення, які зазвичай зустрічаються в ігрових мультимедіа, що обертаються відповідно до руху користувача або повороту камери. Спрайт містить серію зображень, які відображаються як одна картинка або анімація.

SQL injection

An SQL injection is a computer attack in which malicious code is embedded in a poorly-designed application and then passed to the backend database. The malicious data then produces database query results or actions that should never have been executed.

SQL-ін'єкція

SQL-ін'єкція – це комп'ютерна атака, при якій шкідливий код вбудовується в погано розроблений додаток, а потім передається до внутрішньої бази даних. Шкідливі дані потім створюють результати запитів до бази даних або дії, які ніколи не повинні були виконуватися.

Steganography

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

Стеганографія

Стеганографія – це дані, приховані в даних. Стеганографія – це метод шифрування, який можна використовувати разом з криптографією як додатковий метод захисту даних.

Strongly typed

Strongly typed is a concept used to refer to a programming language that enforces strict restrictions on intermixing of values with differing data types. When such restrictions are violated and error (exception) occurs.

Строга типізація

Сильно типізована – це поняття, що використовується для позначення мови програмування, яка накладає суворі обмеження на змішування значень з різними типами даних. Порушення цих обмежень призводить до виникнення помилки (виключення).

Superkey

A superkey is a combination of columns that uniquely identifies any row within a relational database management

Суперключ

Суперключ – це комбінація стовпців, яка однозначно ідентифікує будь-який рядок у таблиці реляційної

system (RDBMS) table. A candidate key is a closely related concept where the superkey is reduced to the minimum number of columns required to uniquely identify each row.

системи управління базами даних (СКБД). Ключ-кандидат – це тісно пов'язане поняття, де суперключ зводиться до мінімальної кількості стовпців, необхідних для однозначної ідентифікації кожного рядка.

Suspend Mode

Suspend mode is a low-power computer setting that helps reduce electrical power consumption by shutting down devices that are not in use. Most laptops automatically enter suspend mode when the system runs on batteries or the lid is closed. This status is often signaled by a pulsing LED-powered light.

Режим очікування

Режим очікування – це режим низького енергоспоживання комп'ютера, який допомагає зменшити споживання електроенергії, вимикаючи пристрої, які не використовуються. Більшість ноутбуків автоматично переходять у режим очікування, коли система працює від батарей або закривається кришка. Про цей стан часто сигналізує пульсуючий світлодіодний індикатор.

T

Tablet

A tablet is a wireless touch screen personal computer (PC) that is smaller than a notebook but larger than a smartphone. Modern tablets are built with wireless Internet or local area networks (LAN) and a variety of software applications, including business applications, Web browsers and games.

Планшет

Планшет – це бездротовий персональний комп'ютер (ПК) з сенсорним екраном, менший за ноутбук, але більший за смартфон. Сучасні планшети оснащені бездротовим Інтернетом або локальною мережею (LAN) і різноманітними програмними додатками, включаючи бізнес-додатки, веббраузери та ігри.

Telecommunications

Telecommunications refers to the exchange of information by electronic and electrical means over a significant distance. A complete telecommunication

Телекомунікації

Телекомунікації – це обмін інформацією за допомогою електронних та електричних засобів на значні відстані. Повна телекомунікаційна

arrangement is made up of two or more stations equipped with transmitter and receiver devices. A single co-arrangement of transmitters and receivers, called a transceiver, may also be used in many telecommunication stations.

система складається з двох або більше станцій, оснащених передавальними та приймальними пристроями. У багатьох телекомунікаційних станціях може також використовуватися один спільний пристрій передавачів і приймачів, який називається прийомопередавачем.

Temporal Key Integrity Protocol (TKIP)

Temporal Key Integrity Protocol (TKIP) is a wireless network security protocol of the Institute of Electrical and Electronics Engineers (IEEE) 802.11. TKIP encryption is more robust than Wired Equivalent Privacy (WEP), which was the first Wi-Fi security protocol.

Протокол цілісності тимчасового ключа

Протокол цілісності тимчасового ключа (Temporal Key Integrity Protocol, TKIP) – це протокол безпеки бездротових мереж Інституту інженерів з електротехніки та електроніки (IEEE) стандарту 802.11. Шифрування TKIP є більш надійним, ніж дротовий еквівалент конфіденційності (WEP), який був першим протоколом безпеки Wi-Fi.

Terminal Node Controller (TNC)

A terminal node controller (TNC) is a radio network device used to communicate with AX.25 packet radio networks. Typically this device consists of a dedicated microprocessor, a modem, flash memory and software that uses AX.25 protocol and provides a command line interface to the user. Typically TNC interfaces between a dumb computer terminal providing the data and a radio transceiver. The transceiver modulates and transmits the analogue radio signal containing the data provided by the TNC.

Контролер термінального вузла (TNC)

Контролер термінального вузла (TNC) – це радіомережевий пристрій, який використовується для зв'язку з пакетними радіомережами AX.25. Зазвичай цей пристрій складається зі спеціального мікропроцесора, модему, флеш-пам'яті та програмного забезпечення, яке використовує протокол AX.25 і надає користувачеві інтерфейс командного рядка. Зазвичай TNC є інтерфейсом між комп'ютерним терміналом, що надає дані, і радіоприймачем. Приймач модулює і передає аналоговий радіосигнал, що містить дані, отримані від ЧПК.

The Green Grid

The Green Grid is a nonprofit, open industry consortium consisting of end users, policymakers, technology providers, facility architects and utility companies. It is a joint collaboration that aims to improve the energy efficiency of data centers and business computing systems.

Зелена мережа

Зелена мережа – це неприбутковий відкритий галузевий консорціум, що складається з кінцевих користувачів, політиків, постачальників технологій, архітекторів об'єктів та комунальних компаній. Це спільна співпраця, спрямована на підвищення енергоефективності центрів обробки даних і бізнес-обчислювальних систем.

The Institute of Electrical and Electronic Engineers (IEEE)

The Institute of Electrical and Electronic Engineers (IEEE) is a global association and organization of professionals working toward the development, implementation and maintenance of technology-centered products and services.

IEEE primarily innovates new electronic products and services, designs the standards that govern them and imparts, publishes and promotes industry knowledge through publications, conferences and partnering with academic institutes.

Інститут інженерів з електротехніки та електроніки (IEEE)

Інститут інженерів з електротехніки та електроніки (IEEE) – це всесвітня асоціація та організація професіоналів, які працюють над розробкою, впровадженням та підтримкою технологічних продуктів і послуг.

IEEE займається, насамперед, інноваційними розробками нових електронних продуктів і послуг, розробляє стандарти, які ними керують, а також поширює, публікує і просуває галузеві знання за допомогою публікацій, конференцій і партнерства з академічними установами.

Third Generation Wireless

3rd Generation Mobile Telecommunications (3G), is a set of standards that came about as a result of the International Telecommunication Union's (ITU) initiative known as IMT-2000 (International Mobile Telecommunications-2000). 3G systems are expected to deliver quality multimedia to mobile devices by way of faster and

Бездротовий зв'язок третього покоління

Мобільний зв'язок третього покоління (3G) – це набір стандартів, що з'явився в результаті ініціативи Міжнародного союзу електрозв'язку (МСЕ), відомої як IMT-2000 (International Mobile Telecommunications-2000).
Очікується, що системи 3G дозволять передавати якісні мультимедійні дані

easier wireless communications as well as “anytime, anywhere” services.

на мобільні пристрої за допомогою швидшого і простішого бездротового зв'язку, а також надавати послуги "будь-де і будь-коли".

Three Easily Defined Operating System Components

Kernel:
The kernel controls computer hardware by managing memory, processing tasks, and handling input/output from devices like monitors, keyboards, and networks. Monolithic kernels are large and unified, while microkernels are smaller and use message passing between components.

User Interface (UI):

The UI lets users interact with the system via a Command Line Interface (CLI) or a Graphical User Interface (GUI). CLI uses typed commands, while GUI uses icons and menus.

Application Programming Interface (API):
APIs let developers create modular applications by defining how software components interact.

Три компоненти операційної системи, які легко визначити

Ядро:
Ядро керує апаратним забезпеченням комп’ютера: управляє пам’яттю, виконує завдання та обробляє введення/виведення з таких пристроїв, як монітор, клавіатура та мережа. Монолітні ядра великі й цілісні, а мікроядра менші та використовують обмін повідомленнями між компонентами.

Інтерфейс користувача (UI):

Інтерфейс дозволяє користувачу взаємодіяти з системою через командний рядок (CLI) або графічний інтерфейс (GUI). CLI використовує текстові команди, а GUI – піктограми та меню.

Інтерфейс прикладного програмування (API): API дозволяє розробникам створювати модульні програми, визначаючи, як програмні компоненти взаємодіють між собою.

Three-finger Salute

The three-finger salute refers to the original PC-compatible system command to reboot or restart a computer by pressing three keys simultaneously: Control, Alt and Delete. The three-key combination is specifically designed to be impossible to execute with one hand in order to avoid the potential for accidental reboots.

Трипальцеве вітання

Трипальцеве вітання – це оригінальна системна команда для перезавантаження або перезавантаження комп'ютера шляхом одночасного натискання трьох клавіш: Control, Alt і Delete. Комбінація з трьох клавіш спеціально розроблена таким чином, щоб її неможливо було виконати однією рукою, щоб уникнути можливості випадкового перезавантаження.

Time Division Multiplexing (TDM)

Time division multiplexing (TDM) is a communications process that transmits two or more streaming digital signals over a common channel. In TDM, incoming signals are divided into equal fixed-length time slots. After multiplexing, these signals are transmitted over a shared medium and reassembled into their original format after de-multiplexing. Time slot selection is directly proportional to overall system efficiency.

Мультиплексування з часовим розділенням каналів (TDM)

Мультиплексування з часовим розділенням каналів (TDM) – це комунікаційний процес, який передає два або більше потокових цифрових сигналів по спільному каналу. У TDM вхідні сигнали поділяються на рівні часові інтервали фіксованої довжини. Після мультиплексування ці сигнали передаються через спільне середовище і знову збираються в початковий формат після демультиплексування. Вибір часових інтервалів прямо пропорційний загальній ефективності системи.

Time-domain Reflectometry (TDR)

Time-domain reflectometry (TDR) identifies and measures errors related to aerial and underground cable and fiber optic wiring through the analysis of pulse reflection polarity.

Часова рефлектометрія (TDR)

Часова рефлектометрія (TDR) виявляє і вимірює помилки, пов'язані з повітряною і підземною кабельною і волоконно-оптичною проводкою, шляхом аналізу полярності відбиття імпульсів.

To boot up

To boot up is to start up a computer system by providing it with the required electrical power and loading the startup services until the operating system is loaded. It refers to the process of starting a computer from a dead or offline state, thus making it available to perform any computing operation. The boot-up sequence typically includes a power-on self-test (POST) to verify hardware functionality, initialization of peripheral devices, and the loading of the boot loader, which in turn loads the operating system kernel and essential system processes. This fundamental process is

Завантаження (комп'ютерної системи)

Завантаження комп'ютерної системи відбувається шляхом подачі необхідної електричної енергії та завантаження стартових служб до завантаження операційної системи. Це процес запуску комп'ютера з вимкненого або офлайн стану, що робить його готовим до виконання будь-яких обчислювальних операцій. Послідовність завантаження зазвичай включає самотестування при включенні (POST) для перевірки працездатності обладнання, ініціалізацію периферійних пристроїв та завантаження завантажувача, який, своєю чергою,

also referred to as booting, bootstrapping, or system startup and is essential for any computer to become operational.

завантажує ядро операційної системи та основні системні процеси. Цей фундаментальний процес також називають бутінгом, бутстрапінгом або запуском системи і є необхідним для того, щоб будь-який комп'ютер став працездатним.

Transact-SQL (T-SQL)

Transact-SQL (T-SQL) is Microsoft's proprietary version of ANSI SQL for its SQL Server relational database.

Transact-SQL (T-SQL)

Transact-SQL (T-SQL) – це власна версія ANSI SQL від Microsoft для реляційної бази даних SQL Server.

Transport Right

A transport right is the lending of digital transfer rights to various media. A transport right occurs when an owner of intellectual property legally consents to the lending, copying or transferring of a protected work.

Право на передачу

Право на передачу – це надання прав на передачу цифрових даних на різні носії. Право на передачу виникає тоді, коли власник інтелектуальної власності дає законну згоду на передачу, копіювання або передачу захищеного твору.

Trust Anchor

A trust anchor is a public key and its associated accompanying information. Public keys act as an authority to verify a digital signature's authenticity. The data associated with a public key delineates what types of information the trust anchor can rule over or what actions it can allow or disallow.

Якір довіри

Якір довіри – це відкритий ключ і пов'язана з ним супровідна інформація. Відкриті ключі діють як авторитет для перевірки автентичності цифрового підпису. Дані, пов'язані з відкритим ключем, визначають, якими типами інформації може керувати якір довіри або які дії він може дозволити чи заборонити.

Two-phase Commit

A two-phase commit is a standardized protocol that ensures that a database commit is implementing in the situation where a commit operation must be broken into two separate parts.

Двофазна фіксація

Двофазна фіксація – це стандартизований протокол, який забезпечує реалізацію фіксації бази даних в ситуації, коли операцію фіксації необхідно розбити на дві окремі частини.

U

Ubuntu

Ubuntu is an open-source operating system (OS) based on the Debian GNU/Linux distribution.

Ubuntu incorporates all the features of a Unix OS with an added customizable GUI, which makes it popular in universities and research organizations. Ubuntu is primarily designed to be used on personal computers, although a server editions does also exist.

Ubuntu

Ubuntu – це операційна система (ОС) з відкритим вихідним кодом, заснована на дистрибутиві Debian GNU/Linux.

Ubuntu включає в себе всі можливості ОС Unix з додатковим графічним інтерфейсом, що налаштовується, що робить її популярною в університетах і дослідницьких організаціях. Ubuntu в першу чергу призначена для використання на персональних комп'ютерах, хоча існує також серверна версія.

Unified Process (UP)

Unified process (UP) is an architecture-centric, use-case driven, iterative and incremental development process that leverages unified modeling language and is compliant with the system process engineering metamodel. Unified process can be applied to different software systems with different levels of technical and managerial complexity across various domains and organizational cultures.

Уніфікований процес (UP)

Уніфікований процес (UP) – це архітектурно-орієнтований, орієнтований на варіанти використання, ітеративний та інкрементальний процес розробки, який використовує уніфіковану мову моделювання та відповідає метамоделі інженерії системних процесів. Уніфікований процес може бути застосований до різних програмних систем з різними рівнями технічної та управлінської складності в різних галузях та організаційних культурах.

Unique Constraint

A unique constraint is a type of column restriction within a table, which dictates that all values in that column must be unique though may be null.

Унікальне обмеження

Унікальне обмеження – це тип обмеження стовпця в таблиці, який передбачає, що всі значення в цьому стовпці повинні бути унікальними, хоча можуть бути і нульовими.

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is an Internet protocol set primarily for home networks permitting devices to access the network. These include PCs, printers, Internet gateways, Wi-Fi access points and mobile devices which connect automatically. This then allows them to share data, communications and entertainment media such as television, radio, music and other audio.

Універсальне підключення та відтворення

Універсальне підключення та відтворення (Universal Plug and Play, UPnP) – це інтернет-протокол, створений в першу чергу для домашніх мереж, що дозволяє пристроям отримувати доступ до мережі. До них відносяться ПК, принтери, інтернет-шлюзи, точки доступу Wi-Fi та мобільні пристрої, які підключаються автоматично. Це дозволяє їм обмінюватися даними, комунікаціями та розважальними медіа, такими як телебачення, радіо, музика та інші аудіоматеріали.

Universally Unique Identifier (UUID)

A universally unique identifier (UUID) is a 128-bit number that identifies unique Internet objects or data. A UUID is generated by an algorithm with values that are based on a machine's network address.

Універсальний унікальний ідентифікатор

Універсальний унікальний ідентифікатор (UUID) – це 128-бітне число, яке ідентифікує унікальні об'єкти або дані в Інтернеті. UUID генерується алгоритмом, значення якого базуються на мережевій адресі комп'ютера.

Unlocked Cellphone

An unlocked cellphone is a cellphone that will work with any network service provider. Mobile phone carriers typically offer subscribers a locked phone, essentially restricting its use to specific carriers and/or countries.

Розблокований мобільний телефон

Розблокований мобільний телефон – це телефон, який буде працювати з будь-яким оператором мобільного зв'язку. Оператори мобільного зв'язку зазвичай пропонують абонентам заблоковані телефони, по суті, обмежуючи їх використання певними операторами та/або країнами.

“Update” Statement

The “update” statement is a Structured Query Language (SQL) statement used to change or update values in a table. It is usually suffixed with a WHERE clause to restrict the change to a set of values that meet a specific set of criteria.

«Оновлення»

«Оновлення» – це оператор мови структурованих запитів (SQL), який використовується для зміни або оновлення значень у таблиці. Зазвичай до нього додається вираз WHERE, щоб обмежити зміну набором значень, які відповідають певному набору критеріїв.

Usability

Usability is the degree of ease with which products such as software and Web applications can be used to achieve required goals effectively and efficiently. Usability assesses the level of difficulty involved in using a user interface. Although usability can only be quantified through indirect measures and is therefore a nonfunctional requirement, it is closely related to a product’s functionality.

Зручність використання

Зручність використання – це ступінь легкості, з якою продукти, такі як програмне забезпечення та вебдодатки, можуть бути використані для ефективного та результативного досягнення необхідних цілей. Юзабіліті оцінює рівень складності використання інтерфейсу користувача. Хоча юзабіліті можна оцінити кількісно лише за допомогою непрямих показників і, отже, це нефункціональна вимога, воно тісно пов'язане з функціональністю продукту.

User acceptance testing (UAT)

User acceptance testing (UAT) is an important phase of the software development process that verifies whether a product or software is fit for the purpose it was built for in the first place – namely, that it: fulfills business requirements; provides a good user experience (UX) for end-users.

Користувацьке тестування (UAT)

Користувацьке тестування (UAT) – це важливий етап процесу розробки програмного забезпечення, який перевіряє, чи відповідає продукт або програмне забезпечення тій меті, для якої воно було створено, а саме:

- відповідає бізнес-вимогам;
- забезпечує хороший користувацький досвід (UX) для кінцевих користувачів.

V

Variable

In mathematics, a variable is a quantity that can change. Letters are used to represent these changing, unknown quantities.

Змінна

У математиці змінна – це величина, яка може змінюватися. Для позначення цих мінливих, невідомих величин використовуються літери.

Vector Graphics Rendering

Vector graphics rendering is the process of generating models from geometrical primitives such as lines, points, curves and shapes to represent images in computer graphics.

Візуалізація векторної графіки

Візуалізація векторної графіки – це процес створення моделей з геометричних примітивів, таких як лінії, точки, криві та фігури, для представлення зображень у комп'ютерній графіці.

Video Graphics Array (VGA) Connector

A video graphics array (VGA) connector is a 15-pin D-subminiature set of male and female electrical connectors that relays data from a computer to an output device. VGA connectors are used for LCD monitors, projectors, high definition televisions and so on. IBM designed the D-subminiature 15-pin VGA connector in 1987, and it became the standard connector for VGA output devices.

Роз'єм відеографічної матриці (VGA)

Роз'єм відеографічної матриці (VGA) – це 15-контактний D-подібний набір електричних роз'ємів, який передає дані від комп'ютера до пристрою виводу. Роз'єми VGA використовуються в РК-моніторах, проекторах, телевізорах високої чіткості тощо. IBM розробила 15-контактний D-подібний роз'єм VGA у 1987 році, і він став стандартним роз'ємом для пристроїв виводу VGA.

Video on Demand (VoD)

Video on demand (VoD) is a system that allows users to select and watch video content of their choice on their TVs or computers. Video on demand is one of the dynamic features offered by Internet Protocol TV. VoD provides users with a menu of available videos

Відео за запитом (VoD)

Відео за запитом (VoD) – це система, яка дозволяє користувачам вибирати і переглядати відеоконтент за власним бажанням на своїх телевізорах або комп'ютерах. Відео на вимогу – це одна з динамічних функцій, яку пропонує інтернет-телебачення. VoD надає

from which to choose. The video data is transmitted via Real-Time Streaming Protocol.

користувачам меню доступних відео, з якого вони можуть вибирати. Відеодані передаються через протокол потокового передавання в реальному часі.

Virtual Data Room (VDR)

A virtual data room (VDR) is a secure, online repository for data and documents pertinent to business, legal transactions or proceedings. The VDR uses a central server and extranet connection, which is an Internet connection with very controlled access. This Internet connection uses a secure log-on supplied by the appropriate overseeing vendor or authority responsible for disabling or enabling, the secure log-on at any time.

Віртуальна кімната даних (VDR)

Віртуальна кімната даних (VDR) – це захищене онлайн-сховище даних і документів, що стосуються бізнесу, юридичних транзакцій або судових розглядів. ВДР використовує центральний сервер і екстранет-з'єднання, яке є інтернет-з'єднанням з дуже контрольованим доступом. Це підключення до Інтернету використовує захищений вхід, який надається відповідним постачальником або органом, відповідальним за вимкнення або ввімкнення захищеного входу в будь-який час.

Virtual Memory (VM)

Virtual memory (VM) is a feature developed for the kernel of an operating system (OS) that simulates additional main memory such as RAM (random access memory) or disc storage. This technique involves the manipulation and management of memory by allowing the loading and execution of larger programs or multiple programs simultaneously. It also allows each program to operate as if it had infinite memory, and is often considered more cost effective than purchasing additional RAM.

Віртуальна пам'ять (ВП)

Віртуальна пам'ять (ВП) – це функція, розроблена для ядра операційної системи (ОС), яка імітує додаткову основну пам'ять, таку як оперативна пам'ять (ОЗП) або дисковий накопичувач. Ця технологія передбачає маніпуляції з пам'яттю та управління нею, дозволяючи завантажувати та виконувати більші програми або декілька програм одночасно. Це також дозволяє кожній програмі працювати так, ніби вона має нескінченну пам'ять, і часто вважається більш економічно ефективним, ніж придбання додаткової оперативної пам'яті.

Virtual Network Computing (VNC)

A virtual network computing (VNC) is a graphical desktop-sharing application that uses remote frame buffer protocol to

Віртуальні мережеві обчислення (VNC)

Віртуальні мережеві обчислення (VNC) – це графічна програма для спільного використання робочого столу,

remotely control another computer. This form of desktop sharing transmits keyboard and mouse events from one system to another over the network based on screen updates.

яка використовує протокол віддаленого буфера кадрів для віддаленого керування іншим комп'ютером. Ця форма спільного використання робочого столу передає події клавіатури і миші з однієї системи на іншу через мережу на основі оновлень екрану.

Virtualization Stack

A virtualization stack is a group of software components used to support a virtual environment. Items include the management console, virtual machine processes, emulated devices, management services and the user interface combined with the hypervisor.

Стек віртуалізації

Стек віртуалізації – це група програмних компонентів, які використовуються для підтримки віртуального середовища. До них належать консоль керування, процеси віртуальної машини, емульовані пристрої, служби керування та користувацький інтерфейс у поєднанні з гіпервізором.

VMware

VMware is a cloud computing and virtualization company founded in 1998 that has been instrumental in changing how hardware setups power workloads and support architectures.

VMware

VMware – це компанія, що займається хмарними обчисленнями та віртуалізацією, заснована в 1998 році, яка відіграла важливу роль у зміні того, як апаратне забезпечення забезпечує потужність робочих навантажень та архітектур підтримки.

Voice over Internet Protocol (VoIP) Trunk Gateway

VoIP (Voice over Internet Protocol) trunk gateway is an interface that allows for the interface of PSTN equipment to a voice over Internet Protocol network.

Магістральний шлюз VoIP («голос через Інтернет-протокол»)

Магістральний шлюз VoIP ("голос через Інтернет-протокол") – це інтерфейс, який забезпечує зв'язок між обладнанням ТфОП і мережею передачі голосу через Інтернет-протокол.

Voice over Internet Protocol Caller Identification (VoIP caller ID)

Voice over Internet Protocol Caller Identification (VoIP caller ID) is a type of application found in VoIP phones that allows the person being contacted to view the caller's phone number and in most cases, the name of the caller, through a console from where the communication is established. Caller identification is an added value service provided by telecommunications companies. Furthermore, the caller's personal identification information can also be withheld on some outgoing calls. This is usually done by dialing a special code before connecting with the recipient's phone number.

Ідентифікація абонента за допомогою Інтернет-телефонії (VoIP Caller ID)

Ідентифікація абонента за допомогою Інтернет-телефонії (VoIP Caller ID) – це тип програми, що використовується в телефонах VoIP, яка дозволяє абоненту, з яким зв'язуються, бачити номер телефону абонента і, в більшості випадків, ім'я абонента, через консоль, з якої встановлюється зв'язок. Ідентифікація абонента є додатковою послугою, яку надають телекомунікаційні компанії. Крім того, особиста ідентифікаційна інформація абонента може бути прихована під час деяких вихідних дзвінків. Зазвичай це робиться шляхом набору спеціального коду перед з'єднанням з телефонним номером абонента.

Vulcan Nerve Pinch

The Vulcan Nerve Pinch is a keyboard combination that hinders a user's ability to complete complicated command functions with a single-hand or accidental keypress.

Вулканський зажим нервів

Вулканський зажим нервів – це комбінація клавіш, яка перешкоджає користувачеві виконувати складні командні функції однією рукою або випадковим натисканням клавіш.

W

Wallpaper

Wallpaper, in the context of computing, refers to the image behind the area where menus, icons and shortcuts are displayed. Wallpaper is usually in either a .jpeg or .gif file format and is customizable in most operating systems (OSs).

Шпалери

Шпалери в контексті комп'ютерних технологій – це зображення за областю, де відображаються меню, піктограми та ярлики. Зазвичай шпалери мають формат .jpeg або .gif і можуть налаштовуватися в більшості операційних систем (ОС).

Watchdog Timer (WDT)

A watchdog timer (WDT) is an embedded timing device that automatically prompts corrective action upon system malfunction detection. If software hangs or is lost, a WDT resets the system microcontroller via a 16-bit counter.

Сторожовий таймер (WDT)

Сторожовий таймер (WDT) – це вбудований пристрій синхронізації, який автоматично пропонує коригувальні дії при виявленні несправності системи. Якщо програмне забезпечення зависає або втрачається, WDT скидає системний мікроконтролер за допомогою 16-розрядного лічильника.

Wavelength Division Multiplexing (WDM)

Wavelength division multiplexing (WDM) is a technology or technique modulating numerous data streams, i.e. optical carrier signals of varying wavelengths (colors) of laser light, onto a single optical fiber. WDM enables bi-directional communication as well as multiplication of signal capacity.

Мультиплексування з поділом по довжині хвилі (WDM)

Мультиплексування з поділом по довжині хвилі (WDM) – це технологія або метод модуляції численних потоків даних, тобто оптичних несучих сигналів різної довжини хвилі (кольору) лазерного світла, в одному оптичному волокні. WDM забезпечує двосторонній зв'язок, а також збільшує пропускну здатність сигналу.

Web Development

Web development is the process of developing websites or web applications that run on the Internet (or an Intranet). It can take various forms, including database management, web programming, and web design, among others.

Веброзробка

Веброзробка – це процес створення вебсайтів або вебдодатків, які працюють в Інтернеті (або інтрамережі). Він може набувати різних форм, включаючи управління базами даних, вебпрограмування та вебдизайн, серед іншого.

Web-based training (WBT)

Web-based training (WBT) is an internet browser-based learning which is also available on local intranet. WBT technologies include streaming audio/ video, webinars, forums and instant messaging.

Вебнавчання (WBT)

Вебнавчання (WBT) – це навчання через інтернет-браузер, яке також доступне в локальній інтрамережі. Технології WBT включають потокове аудіо/відео, вебінари, форуми та обмін миттєвими повідомленнями.

Wiki

A wiki is a website that allows the site visitors to add and edit content. Generally, site visitors use their browser to edit text without requiring HTML code. Additionally, some Wikis allow adding and editing of graphics, tables and interactive components.

Вікі

Вікі – це вебсайт, який дозволяє відвідувачам додавати та редагувати контент. Як правило, відвідувачі сайту використовують свій браузер для редагування тексту, не вимагаючи HTML-коду. Крім того, деякі вікі дозволяють додавати і редагувати графіку, таблиці та інтерактивні компоненти.

Windows Internet Naming Service (WINS)

The Windows Internet Naming Service (WINS) converts NetBIOS host names into IP addresses. It allows Windows machines on a given LAN segment to recognize Windows machines on other LAN segments.

Служба імен в Інтернеті Windows (WINS)

Служба імен в Інтернеті Windows (WINS) перетворює імена хостів NetBIOS в IP-адреси. Це дозволяє комп'ютерам Windows у певному сегменті локальної мережі розпізнавати комп'ютери Windows в інших сегментах локальної мережі.

Word Processor

A word processor is a type of software application used for composing, editing, formatting and printing documents. Word processors have a variety of uses and applications within the business environment, at home and in educational contexts.

Текстовий процесор

Текстовий процесор – це тип програмного забезпечення, що використовується для створення, редагування, форматування та друку документів. Текстові процесори мають різноманітне застосування в діловому середовищі, вдома та в освітньому контексті.

Workaround

A workaround is a concept that describes a short-term or temporary solution to a problem. Often the software development lifecycle for a product is very short and the development team may face many critical issues if the project of a similar nature has not been undertaken in the past by the organization. Under such circumstances, the project manager is expected to generate or formulate a workaround as a solution unless the team can concentrate on the exact solution.

Обхідний шлях

Обхідний шлях – це поняття, яке описує короткострокове або тимчасове вирішення проблеми. Часто життєвий цикл розробки програмного забезпечення для продукту дуже короткий, і команда розробників може зіткнутися з багатьма критичними проблемами, якщо проект подібного характеру не виконувався організацією в минулому. За таких обставин очікується, що керівник проекту згенерує або сформулює обхідний шлях як рішення, якщо команда не може сконцентруватися на точному рішенні.

X

X.509 Certificate

X.509 is a standard defining the format of public key certificates used in many internet protocols, including SSL/TLS. These certificates authenticate the identity of websites and encrypt data transferred between clients and servers. X.509 certificates are issued by trusted Certificate Authorities (CAs) and are essential for secure communications.

X.509 – стандарт

X.509 – стандарт, що визначає формат публічних сертифікатів, які застосовуються в інтернет-протоколах, зокрема SSL/TLS. Вони підтверджують ідентичність сайтів та шифрують дані між клієнтом і сервером. Сертифікати видаються довіреними центрами сертифікації і є основою безпечного зв'язку.

XaaS – Anything as a Service

XaaS refers to a wide range of cloud-delivered services beyond traditional SaaS, PaaS, and IaaS. Under the XaaS umbrella, offerings can inc lude Database-as-a-Service (DBaaS), Security-as-a-Service (SECaaS), and Function-as-a-Service (FaaS), allowing businesses to consume IT resources on- demand without investing in infrastructure. This model supports scalability and cost efficiency across diverse cloud deployments.

XaaS – це бар'єрне поняття для широкого спектру ІТ-послуг

XaaS – це бар'єрне поняття для широкого спектру ІТ-послуг, які надаються «як сервіс» через хмару (наприклад, Бази-як-сервіс, Безпека-як-сервіс тощо), без потреби в інфраструктурних інвестиціях. Забезпечує гнучкість, масштабованість і економію.

XaaS Provider

An XaaS provider offers various cloud services that customers can access on-demand, covering everything from software to infrastructure. These providers maintain the underlying infrastructure, security, and updates, enabling clients to focus on business needs without managing hardware.

Провайдер XaaS

Провайдер XaaS надає різноманітні хмарні послуги за вимогою, від програмного забезпечення до інфраструктури. Він підтримує інфраструктуру, безпеку і оновлення, дозволяючи клієнтам зосередитись на бізнесі без турбот про обладнання.

XAI – Explainable Artificial Intelligence

Explainable AI refers to techniques and methods in AI that allow humans to understand and trust the decisions made by machine learning models. In cybersecurity, XAI helps analysts visualize why a detection system flagged unusual behavior, reducing false positives and increasing confidence in automated responses. It bridges the gap between black-box AI and human decision-making.

XAI – пояснювальна штучна інтелектуальна система

XAI – пояснювальна штучна інтелектуальна система, що робить алгоритми прозорими: фахівці бачать, чому спрацювала тривога або рекомендація, що зменшує кількість хибних спрацьовувань та підвищує довіру до автоматизації.

XDR – Extended Detection and Response

XDR is a cybersecurity approach that integrates detection and response tools across endpoints, networks, cloud workloads, and email. Rather than siloed solutions, XDR provides a unified view of threats, enabling faster investigation and remediation of sophisticated multi-vector attacks. Organizations using XDR gain improved threat visibility and coordinated defense.

XDR – розширена концепція виявлення та реагування

XDR – розширена концепція виявлення та реагування, яка поєднує інструменти безпеки для кінцевих точок, мереж, хмар і пошти в єдиний механізм аналізу загроз. Забезпечує швидше розслідування складних атак і ефективніше реагування.

XDR Detection

XDR detection refers to the process by which an Extended Detection and Response system identifies potential

XDR detection

XDR detection – це процес виявлення потенційних загроз системою Extended Detection and

security threats across multiple vectors like endpoints, networks, and cloud services. It uses advanced analytics and AI to correlate events and reduce false positives.

Response, що охоплює кінцеві точки, мережі і хмарні сервіси. Використовує аналітику та штучний інтелект для кореляції подій і зменшення хибних спрацьовувань.

XDR Platform

An XDR platform integrates multiple security products into a unified system for better threat detection and response. It collects data from endpoints, networks, servers, and cloud environments, providing security teams with a holistic view and automated responses to complex cyber threats.

Платформа XDR

Платформа XDR об'єднує різні продукти безпеки в єдину систему для покращеного виявлення та реагування на загрози. Вона збирає дані з кінцевих точок, мереж, серверів та хмар, надаючи безпековим командам повний огляд і автоматизовані відповіді на складні кібератаки.

XDR Response

XDR response is the set of automated or manual actions taken by an Extended Detection and Response system after identifying a threat. These can include isolating affected devices, blocking malicious IPs, or initiating incident response workflows to mitigate attacks swiftly.

XDR response

XDR response – це комплекс автоматизованих або ручних дій, які система Extended Detection and Response здійснює після виявлення загрози. Вони можуть включати ізоляцію пристроїв, блокування шкідливих IP-адрес або запуск процедур реагування для швидкого усунення атаки.

X-IDS – Explainable Intrusion Detection System

X-IDS denotes an IDS designed with explainable AI, so each alert is accompanied by human-understandable reasoning. Analysts working in SOCs can see why a particular packet or behavior triggered a rule, improving decision accuracy and enabling effective tuning of security controls. Such systems reduce dependence on opaque, deep-learning black boxes.

X-IDS – система виявлення вторгнень

X-IDS – система виявлення вторгнень із пояснювальною AI-логікою: кожне сповіщення супроводжується зрозумілим поясненням (наприклад, які пакети або поведінка викликали попередження), що допомагає аналітикам ухвалити рішення без довіри до «чорного ящика».

XML – eXtensible Markup Language

XML is a markup language designed to store and transport data in a format that is both human-readable and machine-readable. It is widely used in IT and cybersecurity for data exchange between systems, configuration files, and web services. XML's flexible structure allows developers to define custom tags suitable for their needs.

XML – розміткова мова

XML – розміткова мова, призначена для зберігання та передачі даних у форматі, зрозумілому як людям, так і машинам. Широко використовується в IT і кібербезпеці для обміну даними між системами, файлів конфігурації та вебсервісів. Гнучка структура XML дозволяє створювати власні теги під конкретні завдання.

XOR – Exclusive OR

XOR is a logical operation that outputs true only when inputs differ (one true and one false). In cybersecurity, XOR is often used in encryption algorithms and obfuscation techniques, as its reversibility allows simple encryption and decryption by applying the operation twice with the same key.

XOR – логічна операція

XOR – логічна операція «виключне АБО», що дає істину, коли вхідні значення різні (одне істинне, інше – хибне). В кібербезпеці XOR часто застосовується в алгоритмах шифрування та обфускації, бо операція є оборотною: застосування двічі з тим самим ключем повертає початкові дані.

XPC –Cross-Process Communication

Cross-Process Communication (XPC) is a mechanism that allows different software processes to exchange data securely and efficiently. In cybersecurity, managing XPC properly is crucial to prevent unauthorized data leaks between applications running on the same system.

XPC

XPC – це механізм, що дозволяє різним процесам обмінюватися даними безпечно і ефективно. У кібербезпеці правильне керування XPC важливе для запобігання несанкціонованим витокам даних між додатками, які працюють на одній системі.

XSS – Cross-Site Scripting

Cross-Site Scripting is a common web application vulnerability that allows attackers to inject malicious scripts into webpages viewed by other users. Through XSS, an attacker can hijack user sessions, deface websites, or redirect traffic. Defense involves input validation, output encoding, and use of Content Security Policy (CSP).

XSS – вразливість вебдодатків

XSS – вразливість вебдодатків, при якій зловмисник вставляє шкідливий JavaScript-код у сторінки, які відкривають інші користувачі. Це може призвести до викрадення сесій, фальсифікації вмісту або перенаправлення трафіку. Захист включає валідацію введення, кодування виводу та CSP.

XSS Attack Vector

An XSS attack vector describes the method or entry point through which Cross-Site Scripting attacks are carried out, such as through vulnerable form inputs, URL parameters, or HTTP headers. Understanding attack vectors helps in designing better defenses.

XSS attack vector

XSS attack vector – це спосіб чи точка входу, через яку здійснюється атака Cross-Site Scripting, наприклад, уразливі поля форм, параметри URL або HTTP-заголовки. Аналіз векторів атак допомагає розробляти ефективніші засоби захисту.

XSS Filter

An XSS filter is a security feature implemented by web browsers or web applications to detect and block Cross-Site Scripting attacks. It scans input and output data for suspicious scripts and neutralizes them before execution. Though helpful, filters are not foolproof and must be complemented with other security measures.

XSS-фільтр

XSS-фільтр – це функція безпеки в браузерах або вебдодатках, яка виявляє та блокує атаки Cross-Site Scripting. Фільтр перевіряє вхідні й вихідні дані на підозрілі скрипти і нейтралізує їх перед виконанням. Він допомагає, але не замінює повноцінні заходи захисту.

Y

Y2K Bug – Year 2000 Bug

The Y2K bug was a widespread computer issue where software represented years with only two digits, causing confusion when the year rolled over from 1999 to 2000. This glitch threatened to disrupt systems worldwide, including financial and infrastructure systems, but widespread remediation efforts largely prevented major failures. It remains a landmark case in software maintenance and cybersecurity awareness.

Y2K Bug

Y2K Bug – це проблема в комп'ютерах, коли рік записували двома цифрами, і при переході з 1999 на 2000 рік це могло викликати помилки у роботі систем. Глюк загрожував масштабними збоями в фінансових і інфраструктурних системах, але завдяки масштабним виправленням катастрофи вдалося уникнути. Це приклад важливості підтримки ПЗ і обізнаності в кібербезпеці.

YAGNI – You Aren't Gonna Need It

YAGNI is a software development principle advising developers not to add functionality until it is absolutely necessary. In cybersecurity projects, following YAGNI helps avoid unnecessary complexity, reducing potential security vulnerabilities and simplifying maintenance.

YAGNI

YAGNI – принцип розробки ПЗ, який радить не додавати функціонал, поки він дійсно не знадобиться. У кібербезпеці це допомагає уникнути зайвої складності, зменшуючи можливі вразливості і спрощуючи підтримку систем.

YAML – YAML Ain't Markup Language

YAML is a human-readable data serialization language commonly used for configuration files and data exchange in IT systems. It emphasizes simplicity and is often preferred over XML or JSON for its clarity and ease of editing. YAML is widely adopted in DevOps and cloud environments for defining infrastructure as code.

YAML

YAML – це мова серіалізації даних, зручна для читання людиною, яка часто використовується у конфігураційних файлах і обміні даними в IT-системах. Вона проста у використанні та зазвичай легша для редагування, ніж XML чи JSON. YAML широко застосовується у DevOps і хмарних технологіях для опису інфраструктури як коду.

YANG – Yet Another Next Generation

YANG is a data modeling language used to model configuration and state data manipulated by network management protocols like NETCONF. It allows network administrators to define device configurations in a standardized way, facilitating automation and interoperability in IT and cybersecurity infrastructures.

YANG

YANG – мова моделювання даних, яка використовується для опису конфігурації та стану мережевих пристроїв, керованих протоколами, наприклад NETCONF. Вона дозволяє адміністраторам стандартно описувати налаштування пристроїв, сприяючи автоматизації та сумісності в IT та кібербезпеці.

YARA – Yet Another Recursive Acronym

YARA is a tool widely used in cybersecurity to identify and classify malware by creating rules based on

YARA

YARA – це інструмент для кібербезпеки, який використовується для ідентифікації і класифікації

patterns in files or processes. It helps analysts detect malicious code by matching binary or textual patterns, improving threat hunting and incident response. YARA rules are flexible and can be customized for different malware families.

шкідливого ПЗ за допомогою правил, створених на основі патернів у файлах або процесах. Допомагає аналітикам швидко знаходити шкідливий код, покращуючи пошук загроз і реагування на інциденти. Правила YARA гнучкі і можуть налаштовуватись під різні сімейства вірусів.

YARN – Yet Another Resource Negotiator

YARN is a resource management platform used in big data environments, particularly with Apache Hadoop. It schedules and allocates resources to applications running in a distributed computing system, ensuring efficient use of cluster capacity and improving performance.

YARN

YARN – це платформа управління ресурсами, що застосовується у великих даних, особливо з Apache Hadoop. Вона розподіляє ресурси для додатків у розподіленій системі, забезпечуючи ефективне використання кластеру і підвищення продуктивності.

Yellow Card Alert

A Yellow Card Alert is a cybersecurity warning indicating a moderate level of threat that requires attention but is not critical. It helps security teams prioritize responses and allocate resources efficiently while monitoring for escalation.

Yellow Card Alert

Yellow Card Alert – це попередження про кіберзагрозу середнього рівня, що вимагає уваги, але не є критичною. Допомагає командам безпеки розставляти пріоритети та ефективно розподіляти ресурси, стежачи за розвитком ситуації.

Yellow Card Protocol

Yellow Card Protocol refers to a set of procedures for issuing warnings in cybersecurity incident management. It alerts teams to suspicious activities that may not be immediately harmful but require investigation and monitoring to prevent escalation.

Yellow Card Protocol

Yellow Card Protocol – це набір процедур для видачі попереджень у керуванні інцидентами кібербезпеки. Він сигналізує про підозрілі дії, які поки не є критичними, але потребують розслідування та спостереження, щоб запобігти загостренню.

Yellow Dog Attack

A Yellow Dog Attack is a type of cyberattack that involves compromising low-security or outdated systems to gain access to a larger network. Attackers exploit these "yellow dog" systems as stepping stones to escalate privileges and move laterally within an organization.

Yellow Dog Attack

Yellow Dog Attack – це тип кібератаки, коли зловмисники атакують системи з низьким рівнем безпеки або застарілі, щоб отримати доступ до більшої мережі. Ці системи використовуються як трампліни для підвищення прав доступу і руху всередині організації.

Yellow Hat Hacker

A Yellow Hat Hacker is a term sometimes used to describe ethical hackers focused on defense and improving system security, working alongside organizations to identify and fix vulnerabilities. Unlike Black Hat hackers who exploit systems, Yellow Hats operate with permission and promote cybersecurity awareness.

Yellow Hat Hacker

Yellow Hat Hacker – це етичний хакер, який займається захистом і підвищенням безпеки систем, співпрацюючи з організаціями для виявлення і усунення вразливостей. На відміну від Black Hat, Yellow Hat діють за згодою і сприяють підвищенню обізнаності в кібербезпеці.

Yellow PowerShell Warning

A Yellow PowerShell Warning is a non-critical alert generated during script execution that notifies users of potential issues without stopping the script. In cybersecurity, monitoring such warnings helps administrators catch miscon figurations or suspicious activity early.

Yellow PowerShell Warning

Yellow PowerShell Warning – це некритичне попередження під час виконання скрипта, яке повідомляє про потенційні проблеми, не припиняючи роботу скрипта. У кібербезпеці моніторинг таких попереджень допомагає адміністраторам вчасно виявляти помилки чи підозрілі дії.

Yellow Team

The Yellow Team is a cybersecurity group focused on ensuring compliance with legal and regulatory requirements. It bridges the gap between technical security teams (Red and Blue) and organizational policies, helping maintain risk management and governance. This team plays a crucial role in audits and maintaining certification standards.

Yellow Team

Yellow Team – це група в кібербезпеці, яка відповідає за дотримання юридичних та нормативних вимог. Вона працює на перетині технічних команд (Red і Blue) та політик організації, забезпечуючи управління ризиками і відповідність стандартам. Ця команда важлива під час аудитів і підтримки сертифікацій.

Yield

In cybersecurity and IT, yield refers to the effective output or performance achieved from a system or process, such as the proportion of successful detections in a threat detection system. Improving yield means increasing accuracy and efficiency of security measures.

Yield Curve Risk

Yield curve risk refers to potential financial losses arising from changes in the difference between long-term and short-term interest rates. In cybersecurity budgeting and financial planning for IT projects, understanding this risk helps manage funding uncertainties.

Yield Management

Yield management is a strategy used in IT service management and cloud computing to optimize resource allocation and pricing based on demand. By analyzing usage patterns, organizations can maximize revenue while efficiently managing computing resources and infrastructure costs.

Yottabyte

A yottabyte is a unit of digital information storage equivalent to one septillion bytes (10^24). It represents an extraordinarily large amount of data, far beyond typical current storage needs. Yottabytes are used to quantify data at global scales, such as total internet traffic or massive cloud storage capacities.

Yield

У кібербезпеці та IT yield означає ефективний результат або продуктивність системи чи процесу, наприклад, частку успішно виявлених загроз у системі детекції. Підвищення yield означає покращення точності та ефективності заходів безпеки.

Yield curve risk

Yield curve risk – це ризик фінансових втрат через зміни різниці між довгостроковими і короткостроковими відсотковими ставками. У плануванні бюджету кібербезпеки та IT-проектів цей ризик допомагає керувати невизначеністю фінансування.

Yield management

Yield management – це стратегія в управлінні IT-послугами та хмарними обчисленнями для оптимізації розподілу ресурсів і ціноутворення залежно від попиту. Аналізуючи використання, організації можуть максимізувати дохід та ефективно управляти витратами на інфраструктуру.

Йоттабайт

Йоттабайт – це одиниця виміру цифрової інформації, що дорівнює одному септильйону байтів (10^24). Це неймовірно великий обсяг даних, значно більший за звичайні потреби зберігання. Йоттабайти використовуються для оцінки даних на глобальному рівні, наприклад, загального трафіку інтернету чи величезних хмарних сховищ.

Yottacon

Yottacon is an annual cybersecurity conference focused on hacking, information security, and technology innovations. It brings together professionals to share knowledge, research, and strategies to tackle evolving cyber threats. The conference promotes community building and collaboration in the cybersecurity field.

Yottacon

Yottacon – це щорічна конференція з кібербезпеки, присвячена хакінгу, інформаційній безпеці та технологічним інноваціям. Вона збирає професіоналів для обміну знаннями, дослідженнями і стратегіями боротьби з кіберзагрозами. Конференція сприяє розвитку спільноти і співпраці у сфері кібербезпеки.

YouTube API

The YouTube API allows developers to integrate YouTube's video functionality into their own applications and websites. It provides access to upload, search, and manage videos, as well as retrieve analytics data, making it useful for cybersecurity tools monitoring video content or user activity.

YouTube API

YouTube API дозволяє розробникам інтегрувати функції YouTube у власні застосунки та сайти. Він надає можливість завантажувати, шукати та керувати відео, а також отримувати аналітику, що корисно для інструментів кібербезпеки, які відслідковують контент або активність користувачів.

Y-Path

Y-Path is a term used in malware analysis to describe a specific code execution path that branches like the letter "Y." Understanding Y-Paths helps cybersecurity experts trace how malicious code propagates and identify critical decision points for intervention.

Y-Path

Y-Path – термін у аналізі шкідливого ПЗ, що описує певний шлях виконання коду, який розгалужується у формі букви "Y". Вивчення Y-Path допомагає фахівцям з кібербезпеки відстежувати розповсюдження шкідливого коду і визначати ключові точки для втручання.

YubiKey

YubiKey is a hardware authentication device developed by Yubico that provides secure two-factor authentication (2FA). It supports multiple authentication protocols and is widely used to enhance login security for online services, including those in cybersecurity environments.

YubiKey

YubiKey – це апаратний пристрій аутентифікації від компанії Yubico, який забезпечує безпечну двофакторну аутентифікацію. Підтримує різні протоколи і широко застосовується для підвищення безпеки входу в онлайн-сервіси, у тому числі в кібербезпеці.

Z

Zero Fill

Zero Fill refers to overwriting unused storage locations with the character "0" as part of secure data wiping. This practice ensures that previously stored data cannot be recovered easily.

Zero Fill

Zero Fill – процес перезапису неактивних секторів сховища символом «0» для безпечного видалення даних. Це ускладнює їх можливе відновлення в майбутньому.

Zero Hour Attack

A zero hour attack refers to a cyberattack that occurs immediately after a vulnerability is disclosed, before patches are available. These attacks exploit the short window of opportunity when systems remain vulnerable. Organizations must act quickly to detect and mitigate such threats.

Zero hour attack

Zero hour attack – це кібератака, що відбувається одразу після виявлення уразливості, до появи патчів. Зловмисники використовують короткий проміжок часу, коли системи залишаються вразливими. Організаціям потрібно оперативно виявляти та нейтралізувати такі загрози.

Zero Knowledge Proof (ZKP)

Zero Knowledge Proof is a cryptographic method that allows one party to prove to another that they know a value without revealing the value itself. It is used in blockchain and cybersecurity to enhance privacy and secure authentication processes. ZKPs help reduce data exposure during verification.

Zero Knowledge Proof

Zero Knowledge Proof – це криптографічний метод, що дозволяє одній стороні довести іншій знання певного значення без розкриття самого значення. Використовується у блокчейні та кібербезпеці для підвищення приватності та безпечної аутентифікації. ZKP допомагає зменшити обсяг даних, що розкриваються під час перевірки.

Zero Trust Architecture

Zero Trust Architecture is a cybersecurity model that requires strict identity verification for every user and device trying to access resources, regardless of their location inside or outside the network perimeter. It

Zero Trust Architecture

Zero Trust Architecture – це модель кібербезпеки, яка вимагає суворої перевірки ідентичності кожного користувача і пристрою, що намагається отримати доступ до ресурсів, незалежно від їх розташування у мережі

assumes that threats can come from anywhere, emphasizing "never trust, always verify." This model reduces risk by minimizing implicit trust.

чи поза нею. Вона базується на припущенні, що загрози можуть надходити звідусіль, підкреслюючи принцип "ніколи не довіряй, завжди перевіряй". Ця модель знижує ризики, мінімізуючи приховану довіру.

Zero-Day Vulnerability

A zero-day vulnerability is a software security flaw that is unknown to the vendor and therefore has no patch or fix available. Attackers can exploit this vulnerability before developers become aware, making it extremely dangerous and valuable in cyberattacks. Zero-day exploits often lead to severe breaches before mitigation is possible.

Zero-day вразливість

Zero-day вразливість – це уразливість програмного забезпечення, невідома виробнику, через що не існує виправлення або патча. Зловмисники можуть скористатися нею до того, як розробники дізнаються про проблему, що робить такі атаки дуже небезпечними і цінними. Експлойти zero-day часто призводять до серйозних порушень безпеки до моменту їх усунення.

Zigbee

Zigbee is a wireless communication protocol used for creating personal area networks with small, low-power digital radios. It is commonly used in IoT devices for smart homes and industrial applications. However, due to its wireless nature, it can be a target for cybersecurity attacks if not properly secured.

Zigbee

Zigbee – це протокол бездротового зв’язку для створення персональних мереж із малопотужними цифровими радіомодулями. Часто застосовується у пристроях Інтернету речей (IoT) для розумних будинків та промисловості. Через бездротовий характер може стати об’єктом кібератак, якщо не захищений належним чином.

Zigbee Security

Zigbee Security refers to the built-in protection mechanisms of the Zigbee wireless protocol, such as encryption, authentication, and access control. These features safeguard communication among IoT devices, protecting against unauthorized access and data manipulation.

Zigbee Security

Zigbee Security – це вбудовані механізми захисту протоколу Zigbee: шифрування, аутентифікація та контроль доступу. Вони забезпечують безпечний зв’язок між IoT-пристроями, захищаючи від несанкціонованого проникнення і зміни даних.

Zip Bomb

A zip bomb is a malicious compressed file designed to overwhelm systems when decompressed, using minimal disk space but expanding to enormous size. It can crash antivirus software or drain resources, enabling further malware infiltration. It's often disguised as harmless.

Zip bomb

Zip bomb – це шкідливий архів, спеціально стиснутий для того, щоб при розпакуванні перевантажити систему: невеликий файл розширюється до величезного об'єму. Він може викликати збій антивірусів, витрачати ресурси системи і відкривати шлях для додаткового шкідливого ПЗ. Часто видається за нешкідливий.

ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)

ZK-SNARKs are cryptographic proofs that allow one party to prove possession of certain information without revealing the information itself and without interaction. Widely used in blockchain technology, they enhance privacy and scalability in secure transactions.

ZK-SNARKs

ZK-SNARKs – це криптографічні докази, які дозволяють одній стороні довести наявність інформації, не розкриваючи її і без взаємодії з іншою стороною. Широко застосовуються у блокчейні для підвищення приватності та масштабованості безпечних транзакцій.

Zombie (in cybersecurity context)

In cybersecurity, a zombie is a compromised computer controlled by attackers, forming part of a botnet. Zombies execute tasks like DDoS attacks or spamming without users' knowledge. They amplify scale and hide origin in malicious campaigns.

Зомбі

Зомбі – заражений комп'ютер, який використовується зловмисниками як частина ботнету. Виконує атаки типу DDoS або розсилки спаму без відома власника. Допомагає нарощувати масштаб і зберігати анонімність злочинців.

Zombie Network (Botnet)

A zombie network, or botnet, is a collection of compromised computers controlled remotely by attackers. These "zombie" devices perform coordinated malicious activities like DDoS attacks, spamming, or data theft without the owners' knowledge. Botnets pose significant cybersecurity threats due to their scale and stealth.

Zombie network або ботнет

Zombie network, або ботнет – це мережа скомпрометованих комп'ютерів, керованих віддалено зловмисниками. Ці «зомбі»-пристрої виконують скоординовані атаки, такі як DDoS, розсилання спаму чи викрадення даних, без відома власників. Ботнети є серйозною загрозою через свій масштаб і прихованість.

Zombie Process

A zombie process is a computer process that has completed execution but still has an entry in the process table. It occurs when the parent process has not yet read the child's exit status. In cybersecurity, numerous zombie processes may indicate system mismanagement or compromise.

Зомбі-процес

Зомбі-процес – це процес у комп'ютері, який завершився, але його запис залишився в таблиці процесів. Це трапляється, коли батьківський процес ще не отримав статус завершення дочірнього. У кібербезпеці велика кількість таких процесів може свідчити про неправильне керування системою або компрометацію.

Zone Transfer

Zone transfer is a process where DNS servers share the contents of their DNS zones to synchronize domain information. While legitimate zone transfers help manage domain data, attackers can abuse misconfigured zone transfers to gather intelligence about a network's infrastructure. Proper configuration is vital to prevent such leaks.

Zone transfer

Zone transfer – це процес, під час якого DNS-сервери обмінюються інформацією про зони DNS для синхронізації даних домену. Хоча легітимні трансфери допомагають керувати даними, зловмисники можуть використовувати неправильно налаштовані трансфери для збору інформації про інфраструктуру мережі. Важливо правильно налаштовувати їх, щоб запобігти витокам.

Zone-Based Firewall

A zone-based firewall divides a network into zones and controls traffic between these zones based on security policies. This method provides granular control and segmentation, helping prevent unauthorized access within different parts of the network. It is widely used in enterprise cybersecurity architectures.

Зонований файрвол

Зонований файрвол поділяє мережу на зони та контролює трафік між ними відповідно до політик безпеки. Такий підхід забезпечує детальний контроль і сегментацію, допомагаючи запобігти несанкціонованому доступу між різними частинами мережі. Широко застосовується в корпоративних архітектурах безпеки.

Zone-based Firewall

A zone-based firewall separates a network into zones and enforces security policies between zones. It allows granular control of traffic and limits lateral movement across network segments. Widely adopted in enterprise network architectures.

Метафорична «зонована» межа

Метафорична «зонована» межа, що поділяє мережу на секції та керує трафіком між ними. Забезпечує точний контроль доступу і запобігає розповсюдженню загроз у межах мережі.

Список використаних джерел

1. Василенко Л. С. Основи термінознавства в ІТ. Київ: ВЦ Академія, 2018. 192 с.
2. Гаврилюк В. О. Основи кібербезпеки для студентів ІТ-спеціальностей. Київ: КНУ, 2020. 320 с.
3. Гладун А. Я., Пучков О. О., Субач І. Ю., Хала К. О. Англо-український словник термінів з інформаційних технологій та кібербезпеки: словник-довідник. Київ: КПІ ім. І. Сікорського, 2018. 376 с.
4. Гринько О. П., Морозова О. І. Інформаційна безпека в підприємствах. Харків: ХНАДУ, 2019. 280 с.
5. Даник Ю. Г. Системи кібербезпеки: теорія та практика. Житомир: ЖНАЕУ, 2016. 280 с.
6. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія / за ред. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.
7. Кавун С. В., Носов В. В., Манжай О. В. Безпека інформаційно-комунікаційних систем: навчальний посібник. Частина 2. Харків: ХНЕУ, 2018. 196 с.
8. Коваленко Н. А., Мироненко С. П. Інформаційна безпека в державному секторі. Харків: ХНАДУ, 2020. 280 с.
9. Козак Л. М., Соколов В. В. Глосарій термінів з кібербезпеки. Львів: Новий Світ-2000, 2019. 160 с.
10. Костюк Ю. В., Складанний П. М., Бебешко Б. Т., Хорольська К. В., Рзаєва С. Л., Ворохоб М. В. Безпека інформаційно-комунікаційних систем: підручник. Київ: Київський столичний університет ім. Бориса Грінченка, 2025. 1016 с.
11. Кириченко Т. Ю., Левченко В. М. Захист інформації в комп'ютерних системах: навчальний посібник. Львів: ЛНУ ім. Івана Франка, 2017. 268 с.
12. Ковтун В. Ю., Євсеєв С. П., Аксьонова І. В. Кібербезпека та новітні тех нології захисту інформації: навчальний посібник / за ред. С. П. Євсеєва. Харків / Львів: НТУ «ХПІ» / Новий Світ, 2000, 2025. 285 с. Серія «Кібербезпека та штучний інтелект».
13. Лизанчук В. В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. І. Франка, 2017. 725 с.
14. Литвиненко М. Г. Безпека даних у цифровому середовищі. Київ: Наук. думка, 2021. 312 с.
15. Лісовська Ю. П. Інформаційна безпека України: навчальний посібник. Київ: Кондор, 2024. 172 с.
16. Мацкевич С. В., Кривенко А. П., Панченко І. В. Інформаційна безпека комп'ютерних мереж: навчальний посібник. Київ: КНЕУ, 2019. 352 с.
17. Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник. Київ: Інтертехнологія, 2010. 512 с.

18. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М., Петрик В. М. Інформаційна безпека: підручник. Київ: Ліра-К, 2021. 411 с.
19. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні техноло гії захисту. Навчальний посібник. Львів: Новий Світ-2000, 2024. 678 с.
20. Павленко О. В., Руденко С. І. Кіберзахист інформаційних систем. Харків: ХНУ імені В. Н. Каразіна, 2018. 450 с.
21. Пірог О. В. Безпека вебдодатків (вебзастосунків): навчальний посібник. Житомир: Житомирська політехніка, 2025. 290 с.
22. Тимошенко Н. П., Пономаренко І. В. Криптографія та захист інформації. Львів: ЛНУ, 2017. 210 с.
23. Шевченко О. М. Кібербезпека: теорія і практика. Харків: ХНУРЕ, 2021. 416 с.
24. Шевчук С. І. Основи кібербезпеки для початківців. Київ: КНЕУ, 2022. 220 с.
25. Зубок М. І. Інформаційна безпека в підприємницькій діяльності: підручник. Житомир, 2015. 200 с.
26. Ahmed M., Mahmood A. N., Hu J. A Survey of Network Anomaly Detection Techniques // Journal of Network and Computer Applications. 2016. Vol. 60. P. 19 - 31.
27. Andress J. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014. 320 p.
28. Antonucci D. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. Hoboken, NJ: Wiley, 2017. 448 p.
29. Bayuk J. L. Cybersecurity Policy Guidebook. Hoboken, NJ: Wiley, 2012. 336 p.
30. Blokdyk G. Cybersecurity: A Complete Guide, 2020 Edition. n.p.: Emereo Publishing, 2021. 305 p.
31. Brooks C. J., Grow C., Craig P., Short D. Cybersecurity Essentials. Indianap olis: Wiley, 2018. 784 p.
32. Buchanan B. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, MA: Harvard University Press, 2022. 432 p.
33. Chen G. Et al. Cybersecurity Threats, Malware Trends, and Strategies. Packt Publishing, 2020. 428 p.
34. Chen T. M., Abu-Nimeh S. Lessons from Stuxnet // Computer. 2011. Vol. 44, No. 4. P. 91-93.
35. Dudley R., Golden D. The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime. New York: Farrar, Straus and Giroux, 2022. 368 p.
36. Goodrich M. T., Tamassia R. Introduction to Computer Security. Boston: Pearson Education, 2011. 557 p.
37. Grimes R. A. Cybersecurity Essentials. Indianapolis: Wiley, 2019. 320 p.
38. Gupta B. B. Cross-Site Scripting Attacks: Classification, Attack and Countermeasures. Boca Raton: CRC Press, 2020. 200 p.

39. Gupta B. B. Internet of Things Security: Principles, Applications, Attacks and Countermeasures. Boca Raton: CRC Press, 2020. 200 p.

40. Gupta B. B. Et al. A Beginner's Guide to Internet of Things Security: Attacks, Applications, Authentication Fundamentals and Security. Boca Raton: CRC Press, 2020. 200 p.

41. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. London: Chapman & Hall, 2020. 500 p.

42. Kim D., Solomon M. G. Fundamentals of Information Systems Security. Burlington: Jones & Bartlett Learning, 2018. 552 p.

43. Parker D. B. Fighting Computer Crime: A New Framework for Protecting Information. New York: Wiley, 1998. 507 p.

44. Perlroth N. This Is How They Tell Me the World Ends: The Cyber Weapons Arms Race. New York: Bloomsbury, 2021. 416 p.

45. Sadeghi A.-R., Wachsmann C., Waidner M. Security and Privacy Challenges in Industrial Internet of Things // Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). 2015. P. 1-6.

46. Sen J. Et al. Computer and Network Security. arXiv preprint, 2020. pages unspecified.

47. Sharp R. Introduction to Cybersecurity: A Multidisciplinary Challenge. Cham, Switzerland: Springer, 2023. 440 p.

48. Skoudis E., Liston T. Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Upper Saddle River, NJ: Prentice Hall, 2006. 752 p.

49. Stallings W. Network Security Essentials: Applications and Standards. 6th ed. Boston: Pearson, 2017. 496 p.

50. Vacca J. R. Computer and Information Security Handbook. Cambridge, MA: Academic Press, 2017. 1190 p.

51. Whitman M. E., Mattord H. J. Principles of Information Security. Boston: Cengage Learning, 2018. 672 p.

52. Xu S. Cybersecurity Dynamics: A Foundation for the Science of Cybersecurity. arXiv preprint, 2020. 200 p.

ПРЕДМЕТНИЙ ПОКАЖЧИК

Навчальне видання

Олександра ПАЛЬЧЕВСЬКА, Світлана ДОБРОВОЛЬСЬКА
Марія МАЛАНЮК, Петро ГУБИЧ

АНГЛО - УКРАЇНСЬКИЙ ГЛОСАРІЙ ТЕРМІНІВ ІТ-ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ

Літературний редактор **Галина Падик**

Технічний редактор
та комп'ютерна верстка **Маріанна Климус**

Друк **Назарій Петролюк**

Підписано до друку 06.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Папір офсетний. Друк цифровий. Ум. друк. арк. 16,6

Друк ЛДУБЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
Тел. /факс: (032)233-24-79
E-mail: vnrd@ldubgd.edu.ua
Свідоцтво суб'єкта видавничої справи ДК №7249 від 09.02.2021 р.