

**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

© Пальчевська О., 2025
© Добровольська С., 2025
© Маланюк М., 2025
© Губич П., 2025
© ЛДУ БЖД, 2025

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 англomовних 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 англomовною 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.

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

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.

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

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: КПП 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., Гришук 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., Євсєєв С. П., Аксьонова І. В. Кібербезпека та новітні технології захисту інформації: навчальний посібник / за ред. С. П. Євсєєва. 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., Євсєєв С. П., Король О. Г. Кібербезпека: сучасні технології 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. Indianapolis: 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

Access Control Facility	5
Accessibility Testing	5
Account Hijacking	6
Active Directory Monitoring (AD monitoring)	7
Alureon	8
Analog	8
Analytical Engine	9
Android Fragmentation	10
Anomaly Detection	10
Anti-phishing Service	11
Application Clustering	12
Application Infrastructure Provider	13
Armstrong's Axiom	13
Asset Management Software	14
Asset Tracking	15
Attribute-Based Access Control	16
Auto Scaling	16
Automated Business Process Discovery	17
Automated Data Tiering	17
Automated feature engineering	18
Automatic Failover	19
B2 security	20
B3 security	21
Back at keyboard	22
Back Orifice	22
Back quote	23
Backchannel	24
Backend	24
Back-end developer	25
Backscatter	26
Backup and Recovery Test	26
Backup Appliance	27
Backup Copy	28
Backup Storage	29
Beep Code	29
Beginning Of File (BOF)	30
Bi-directional predictive frame	30
Big Data Management	31
Big data mining	32
Big Data Platform	32
Big Data Storage	32
Big-endian	34

Binary-Coded Decimal (BCD)	34
Biohacking	35
Biometric Authentication	35
Biometric Verification	36
BIOS	37
BITNET	37
Blackphone	37
Blended Networking	38
Blockchain	38
Blue Noise	39
Blue Wire	39
Blue-Box	40
BlueJ	40
Body Area Network (BAN)	41
Bogon Filtering	41
Bohr Bug	42
Bonephones	43
Boolean Expression	43
Botnet Attack	44
Bottom-up Testing	44
Bounced email	45
Brain Dump	45
Browser Caching	46
Browser Security Test	46
BSD daemon	47
BTS	48
Bunny Suit	48
Business continuity and disaster recovery	49
Business Intelligence Reporting	50
Business process	50
Camper	51
Capacitive Touch Screen	51
Chipset	52
Cisco EnergyWise	52
Class C Network	53
Clean Computing	53
Collaboration Data Objects	53
Commerce Server	54
CompactFlash	55
Computational Origami	55
Concerns about Facial Recognition	55
Criticality Level	56
Cyberbullying	56
Data Access	57

Data Administration	58
Data Breach (Data Spill)	58
Data Deduplication	59
Data Transfer Rate	59
Decision Table	59
Decryption	60
Dedicated IP Address	60
Desktop Environment (DE)	61
Digital	61
DNS Cache Poisoning	62
Domain Name System (DNS)	62
Electronic Discovery Reference Model (EDRM)	64
Electronic Textile (E-textile)	64
Electronics disposal efficiency (EDE)	64
Email Server Mean	65
Email Thread	65
Engineer-to-Order Enterprise Resource Planning (ETO ERP)	65
Enterprise data quality	66
Enterprise Information System (EIS) Tier	66
ERP Software	67
Event Queue	67
Events Per Second	67
Exbibyte	68
Exception	68
Exchangeable image file format (EXIF)	68
Explicit Enhancement Point	69
External Cloud	69
Extremely Large Database (XLDB)	69
Fabric-Based Infrastructure	70
Facebook Like-Gating	70
Facebook Official	71
Facsimile	71
Factory Reset	72
Failure Mode and Effects Analysis	73
Failure-Directed Testing	73
Fax Server	73
Federal Communications Commission	74
Federated Application Life Cycle Management	74
Feed Aggregator	75
Female Connector	76
Fencepost Error	76
Fiber Laser	77
Fiber Media Converter	77
Fiber Optic Adapter	78

Fiber Optic Coupler	79
Fiber Optic Sensor	79
Fiber Optic Switch	80
Fiber Optic Termination	81
Fiber Optic Transceiver	81
Fiber Pigtail	82
File	83
File Transfer Protocol With SSL Security	83
Filler Text	84
Finger Vein Recognition	84
Finite Element Analysis	85
Five Nines	85
Flash Storage	86
Flat Panel Display	87
FOAF	87
Folder	88
Font Family	88
For Loop	89
Force Touch	89
Forensic Animation	90
Formula And Recipe Management	90
Forward Compatible	91
Forward Slash	92
Foundation Framework	92
Frame Synchronization	93
Frameset	94
Free Lossless Audio Codec	94
FreeDOS	95
Frequency Modulation	95
Frequency Modulation Synthesis	96
Fuel Cell	96
Function Key	97
Function Point	97
Gamification	98
Generic Access Network (GAN)	98
Global Assembly Cache (GAC)	99
GNU Project	99
Goldmine	99
Google Swiffy	100
Google Wallet	100
Grinding	100
Guard Band	101
Hack/Phreak/Virii/Crack/Anarchy (H/P/V/C/A)	101

Hadapt	102
Hand Coding	102
Hard Drive Recovery	103
Hardcoding	103
Hierarchical Temporal Memory	104
High Availability Cluster (HA cluster)	104
High Sierra Format (HSF)	105
High-definition Audio (HD audio)	105
HIPAA-compliant Email	105
Home Key	106
HomePlug	106
Hosted Virtual Desktop (HVD)	106
Hot Add	107
Hotlinking	107
HTML Tag	108
HTTP Headers	108
HTTP Request Header	108
Hug of Death	109
Huge Pipes	109
Hyper-V virtual hard disk (VHDX)	110
I2P	111
IBM PC	111
IceWM	112
iCloud	112
Ideavirus	112
Identifier	113
Identifier for Advertisers (IFA or IDFA)	113
Identity Management (ID Management/IdM)	114
Identity Resolution	114
IEEE 488	114
IEEE 802.1 Working Group (IEEE 802.1)	115
IEEE 802.11	115
IEEE 802.11a	116
IEEE 802.11ac	116
IEEE 802.11b	116
IEEE 802.11d	117
IEEE 802.11g	117
IEEE 802.11h	117

IEEE 802.11i	118
IEEE 802.11j	118
IEEE 802.11m	119
IEEE 802.11n	119
IEEE 802.11r	120
IEEE 802.11s	120
IEEE 802.11u	121
IEEE 802.1X	121
If Statement	122
IF Statement	122
Imaging software	123
Implementation	123
Implicit Enhancement Point	123
Inaccessible Member	124
In-app purchasing	124
In-cell Technology	124
Increment Operator	125
In-database Analytics	126
Independent Software Vendor (ISV)	126
Independent Variable	127
Indigo	127
Industrial, Scientific, and Medical Radio Band (ISM band)	127
Infected File	128
Information Architect	128
Information management (IM)	128
Information technology governance (IT governance)	129
Information Technology Infrastructure Library (ITIL) Change Management	129
Information Technology Infrastructure Library v3	130
Information technology management (IT management)	130
Information Technology Service Desk (IT service desk)	131
Information Technology Supervisor (IT supervisor)	131
Infotype	131
Inheritance	132
Inline Deduplication	132
In-memory Analytics	133
In-memory Computing	133

In-memory Database (IMDB)	134
Innovator's Patent Agreement (IPA)	134
Input Device	135
Input/Output (I/O) Device	135
Input/output Operations per Second (IOPS)	135
Insert	136
Integer	136
Integrated Circuit (IC)	136
Integrated Cloud Service Management (ICSM)	137
Integrated threat management (ITM)	137
Integration middleware	138
Integrity	138
Intel Virtualization Technology (Intel VT or IVT)	139
Intellectual Property Attaché Act (IP Attaché Act or IPPA)	139
Intelligence-bearing emanations	140
Intelligent Agent	140
Intelligent Database	140
Intelligent Network (IN)	141
Interaction Design (IxD)	141
Inter-exchange carrier (IXC)	141
Interface	142
Interface Message Processor (IMP)	142
Intergalactic Computer Network	143
Interim Standard 95 (IS-95)	143
Internal	144
Internal Bus	144
Internal Hard Drive	144
Internal Tables	145
International Committee for Information Technology Standards (INCITS)	145
International Electrotechnical Commission (IEC)	146
International Mobile Telecommunications Advanced (IMT-Advanced)	146
International Organization for Standardization (ISO)	146
International Telecommunication Union (ITU)	147
Internet Art	147
Internet Corporation for Assigned Names and Numbers (ICANN)	147
Internet Fax Product	148
Internet Map	148
Internet Network Information Center (InterNIC)	148
Internet of Things (IoT)	149

Internet phone (a broadband phone)	149
Internet Protocol Configuration (ipconfig)	149
Internet Protocol hijacking (IP hijacking)	150
Internet Protocol Private Branch Exchange (IP PBX)	150
Internet Protocol Telephony (IP Telephony)	150
Internet Relay Chat (IRC) Worm	151
Internet Relay Chat Bot (IRC bot)	151
Internet Security	151
Internet Telephony	152
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)	152
Interoperability Testing	152
Interweb or "the Interweb"	153
Intexticated	153
Intrusive testing	153
In-Vehicle Infotainment (IVI)	154
IP network	154
IP routing	154
iPhone 5	155
ISO-IEC 24821-1	155
IT Asset Management (ITAM)	156
IT Cost Transparency	156
IT Management Service	156
IT MOOSE Management	157
IT portfolio management	157
IT Service Management (ITSM)	158
Iteration planning	158
Iterative Development	158
An iterator, in the context of C#	159
ITU Telecommunication Standardization Sector (ITU-T)	159
Ivy Bridge	160
Java Card	160
Java Foundation Classes (JFC)	161
Java ME WTK	161
Java Zero Day	161
Jet Propulsion Laboratory (JPL)	162
Jimmy Wales	162
John McCarthy	163
Joli OS	163
Joystick	163
jQuery	164

Julian Date (or Day)	164
Jupyter Notebook	165
Justin Sun	165
Jython	165
Kanban	166
Katmai	166
Key Performance Indicators (KPI)	166
Keyboard, Video, Mouse (KVM)	167
Keyword	167
KidsRuby	168
Kirchhoff's Laws (or Circuit Laws)	168
Knowledge Discovery in databases (KDD)	168
Knowledge, Skills and Abilities (KSA)	169
Kyoto Cooling	169
Lambda Calculus	170
Lead Nurturing	170
Lightweight Thread	170
LinkedIn	171
Linux Console Terminal	172
List Processing	172
Logical OR Symbol	173
LotusScript	173
Malicious Active Content	174
Many-to-Many Relationship	175
MapReduce	175
Marshalling	176
Mashup	177
Massively Multiplayer Online Role-Playing Game	178
Member Server	178
Memory Address	179
Message Queue	180
Metacomputing	181
Method Stub	181
Methods for Testing and Specification	182
Metro Ethernet	182
Metro Ethernet Forum	183
Micro Fuel Cell	184
Mobile Code	184
Mobile Instant Messaging	185
Monolithic Kernel	186
Multihomed	186
Multivalued Field	187
Napster	188

Net Neutrality	189
Netbook	190
NetMeeting	190
Netscape Communicator	191
Network Computer	192
Network Interface Card	192
Network Layer	192
Network PC	193
Nickel-Cadmium Battery	193
Nokia N8	194
Nuker	195
Object Linking and Embedding	196
On-Demand Self Service	196
On-Demand Service	197
Open Enterprise Server	197
Open Mobile Alliance	198
Open Source Initiative	198
OpenGL for Embedded Systems	199
Operating System	199
Operators	200
Optical Fiber Amplifier	201
Oracle OpenWorld	202
Organic Search Engine Optimization	203
Orkut	203
Orphan File	204
Outsourced Product Development	204
Pasta Theory	205
Patch	206
Pay Per Click	206
Personal Digital Assistant	207
PHP: Hypertext Preprocessor 3.0	207
Pierre Salinger Syndrome	208
Pipe	208
Planking	208
Private Automatic Branch Exchange	209
Proof of work	209
Protocol Stack	210
Q-learning	211
QR code phishing (quishing)	211
Quadtree	211
Quantization	212
Quantization Error	212
Quantum Internet	212
Query Plan Monitoring	212

Radio Frequency Identification (RFID)	213
Radio Frequency Identification Tag (RFID tag)	213
Rational Rose	213
Record	214
Region of Interest (ROI)	214
Registered Jack-11 (RJ-11)	214
Registered jack-45 (RJ45)	215
Release management	215
Remote Desktop	215
Route Control	216
Router	216
RSA Identification Verification for Health Care	216
RTP Control Protocol (RTCP)	216
Scrum	217
Self-join (Inner Join)	217
Simple IT Infrastructure Definition	217
Single Inline Memory Module (SIMM)	218
Smartphone	218
Software Development Kit (SDK)	218
Software Modem	219
Software Switch	219
Sound Card	219
Sprite Effects	220
SQL injection	220
Steganography	220
Strongly typed	220
Superkey	220
Suspend Mode	221
Tablet	221
Telecommunications	221
Temporal Key Integrity Protocol (TKIP)	222
Terminal Node Controller (TNC)	222
The Green Grid	223
The Institute of Electrical and Electronic Engineers (IEEE)	223
Third Generation Wireless	223
Three Easily Defined Operating System Components	224
Three-finger Salute	224
Time Division Multiplexing (TDM)	225
Time-domain Reflectometry (TDR)	225
To boot up	225
Transact-SQL (T-SQL)	226
Transport Right	226
Trust Anchor	226
Two-phase Commit	226

Ubuntu	227
Unified Process (UP)	227
Unique Constraint	227
Universal Plug and Play (UPnP)	228
Universally Unique Identifier (UUID)	228
Unlocked Cellphone	228
“Update” Statement	229
Usability	229
User acceptance testing (UAT)	229
Variable	230
Vector Graphics Rendering	230
Video Graphics Array (VGA) Connector	230
Video on Demand (VoD)	230
Virtual Data Room (VDR)	231
Virtual Memory (VM)	231
Virtual Network Computing (VNC)	231
Virtualization Stack	232
VMware	232
Voice over Internet Protocol (VoIP) Trunk Gateway	232
Voice over Internet Protocol Caller Identification (VoIP caller ID)	233
Vulcan Nerve Pinch	233
Wallpaper	234
Watchdog Timer (WDT)	234
Wavelength Division Multiplexing (WDM)	234
Web Development	234
Web-based training (WBT)	235
Wiki	235
Windows Internet Naming Service (WINS)	235
Word Processor	235
Workaround	236
X.509 Certificate	236
XaaS – Anything as a Service	236
XaaS Provider	237
XAI – Explainable Artificial Intelligence	237
XDR – Extended Detection and Response	237
XDR Detection	237
XDR Platform	238
XDR Response	238
X-IDS – Explainable Intrusion Detection System	238
XML – eXtensible Markup Language	239
XOR – Exclusive OR	239
XPC – Cross-Process Communication	239
XSS – Cross-Site Scripting	239
XSS Attack Vector	240

XSS Filter	240
Y2K Bug – Year 2000 Bug	240
YAGNI – You Aren’t Gonna Need It	241
YAML – YAML Ain't Markup Language	241
YANG – Yet Another Next Generation	241
YARA – Yet Another Recursive Acronym	241
YARN – Yet Another Resource Negotiator	242
Yellow Card Alert	242
Yellow Card Protocol	242
Yellow Dog Attack	243
Yellow Hat Hacker	243
Yellow PowerShell Warning	243
Yellow Team	243
Yield	244
Yield Curve Risk	244
Yield Management	244
Yottabyte	244
Yottacon	245
YouTube API	245
Y-Path	245
YubiKey	245
Zero Fill	246
Zero Hour Attack	246
Zero Knowledge Proof (ZKP)	246
Zero Trust Architecture	246
Zero-Day Vulnerability	247
Zigbee	247
Zigbee Security	247
Zip Bomb	248
ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)	248
Zombie (in cybersecurity context)	248
Zombie Network (Botnet)	248
Zombie Process	249
Zone Transfer	249
Zone-Based Firewall	249
Zone-based Firewall	249

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.