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

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.