УДК 811.111’276.6:004
DOI https://doi.org/10.32782/tps2663-4880/2024.34.1.13

СТРУКТУРНІ ОСОБЛИВОСТІ АНГЛОМОВНИХ ТЕРМІНІВ КІБЕРБЕЗПЕКИ

STRUCTURAL PECULIARITIES OF ENGLISH CYBERSECURITY TERMS

Жовтяк В.А.,
orcid.org/0009-0002-2043-7421
аспірант кафедри англійської мови
Чернівецького національного університету імені Юрія Федьковича

Статтю присвячено дослідженню структурних особливостей англомовної термінології кібербезпеки, опрацьованої на основі термінологічних одиниць, дібраних із сучасних англомовних тлумачних словників. Актуальність теми загострилася із початку повномасштабного вторгнення, коли російські фішингові атаки на бізнесові електронні поштові адреси по всьому світу зросли у рази, залишаючись найпоширенішим кіберзлочином поряд із «вірусом-вимагачем» та витоком персональних даних. В умовах сьогодення лінгвістам варто систематизувати терміни в сфері кібербезпеки. Під кібербезпекою розуміємо попередження ушкодження, захист і відновлення комп’ютерів, електронно-комунікаційних систем та сервісів, дротової та електронної комунікації, включно з інформацією в них, для забезпечення доступу до неї, її цілісності та конфіденційності. Рисами англомовної термінології кібербезпеки є інтеграція в інші сфери, інтернаціональний характер, економія мовних ресурсів, реалізована за допомогою скорочень. Вона відповідає наступним, встановленим до термінів вимогам: дотримання правил і норм певної мови, системність, дефінітивність, незалежність від контексту, точність, стислість, моносемічність, експресивна нейтральність, евфонія. За структурними характеристиками аналізовані терміни кібербезпеки репрезентовано однокомпонентними, двокомпонентними та багатокомпонентними термінами, серед яких перші дві групи представлено приблизно однаковою кількістю одиниць (43 і 40% відповідно), в той час як багатослівних виявилося 17,5%. Серед однослівних термінів переважають похідні, які становлять майже половину прикладів цього виду. Третину однокомпонентних термінів кібербезпеки складають абревіації (34%), а прості за структурою 15% одиниць. Двослівні англомовні терміни кібербезпеки переважно виражені іменниковими словосполученнями зі структурами N+N (14%) та A+N (16%). Багатослівні одиниці в більшості представлено структурами N+N+N(+N) (46, 10,2%). Загалом, досліджувана англомовна термінологія кібербезпеки на 95% побудована на іменниковій основі.

Ключові слова: кібербезпека, термін, вимоги до термінів, структура термінів, кількість компонентів.

The article aims at revealing structural features of the English terminology of cybersecurity on the material of modern English-language explanatory dictionaries. Since the beginning of the full-scale invasion, Russian phishing attacks on business email addresses around the world have increased significantly, remaining the most common cybercrime along with the «ransomware» and personal data leakage. Linguists in the field of cybersecurity should develop professional terms and their definitions by publishing dictionaries and glossaries in this discipline. Cybersecurity means preventing damage, protecting and restoring computers, electronic communication systems and services, wired and electronic communication, including information in them, to ensure access to it, its integrity and confidentiality. The features of the analysed English terminology of cybersecurity are integration into other areas, international character, and saving language resources using abbreviations. It meets the following requirements established for the terms: obeying the rules and norms of a particular language, consistency, definitiveness, independence from the context, accuracy, brevity, monosemic character, neutral expressiveness, and euphony. By the number of components, the analyzed terms of cybersecurity are represented by one-word, two-word and multi-word terms, among which the first two groups are represented by approximately the same number of examples (43 and 40%, respectively), while the latter ones turned out to be much less (17.5%) frequent. Among the one-word terms, derivatives predominate, which make up almost half of the examples of this kind. A third of one-component terms of cybersecurity are abbreviations (34%), while only 15% of them are represented by simple ones. Two-word terms of cybersecurity are mainly expressed by noun phrases with structures N + N (14%) and A + N (16%). Multi-word units are mostly represented by structures N + N + N (+ N) (10.2%). In general, the studied English-language cybersecurity terminology is predominantly (by 95%) built on a nominal basis.

Key words: cyber security, term, term requirements, term structure, number of components.

Постановка проблеми. Актуальним сьогодні постає питання вивчення сфери кібербезпеки, оскільки повномасштабне російське вторгнення в Україну спричинило виникнення нових видів шахрайства, спрямованих на усі сфери онлайн послуг. Убезпечення комп’ютерних систем і додатків є метою кібербезпеки як нової міждисциплінарної галузі знань, яка вимагає особливого різнобічного вивчення її термінології. Це завдання викликано потребою часу, оскільки розвиток цієї сфери відбувається зі стрімкою швидкістю. Завдяки своїй суспільній значущості сфера кібербезпеки стала одним з пріоритетних об’єктів державної діяльності й об’єктом лінгвістичних наукових досліджень, адже експертам у цій сфері необхідно володіти високим рівнем англійської фахової мови, яка є цільовою у світовому кіберпросторі.

Аналіз останніх досліджень і публікацій. На підставі аналізу сучасних вітчизняних та зарубіжних публікацій виявлено, що проблематика кібербезпеки розглядається у наукових

працях А.В. Басова [2], Р.В. Лук'янчука [6] та В.С. Черновола [9], питання її дефініції проаналізовано у статтях О.А. Баранова [1], С. Вдовенка, Ю. Даника, С. Фараона [4], Т.М. Ботвина [3], А. Йохансен [13] та *Англо-українському словнику термінів з інформаційних технологій та кібербезпеки* під ред. А.Я. Гладун [5]. Проте, залишається низка нерозкритих питань щодо значення, структури, походження та особливостей функціонування термінології кібербезпеки в сучасному англійськомовному дискурсі.

Постановка завдання. Метою статті є вивчення структури термінів кібербезпеки в англійській мові, дібраних із сучасних англомовних тлумачних словників. Реалізація поставленої мети передбачає розв'язання таких завдань: запропонувати дефініцію терміну «кібербезпека», описати лінгвальні ознаки до англомовної термінології кібербезпеки, проаналізувати структуру термінів за кількістю компонентів і частиномовним принципом.

Виклад основного матеріалу. За останніми даними Національного індексу кібербезпеки (National Cyber Security Index) від квітня 2024 р. до п'ятірки країн-світових лідерів у сфері кібербезпекі належить Польща (90,83), Естонія (85,83), Україна (80,83), Латвія (79,17) та Великобританія (75,00).. Значну роль у розвитку кібербезпеки України відіграла допомога Великобританії, яка для захисту критичної інфраструктури країни від російських атак започаткувала у 2022 р. «Українську кібер програму» (*Ukraine Cyber Programme*), виділивши на неї пакет допомоги у розмірі 6,36 млн фунтів стерлінгів. Варто зазначити, що за інформацією цього ж джерела, з початку повномасштабного вторгнення російські фішингові (*phishing*) атаки на бізнесові електронні поштові адреси в Європі та США зросли у 8 разів, залишаючись найпоширенішим кіберзлочином поряд із «вірусом-вимагачем» (*ransomware*) та витоком персональних даних (*personal data breaches*) [12].

На противагу списку найбільш захищених країн у сфері кібербезпеки, було створено індекс країн за поширеністю кіберзлочинів (*Cybercrime Index*) [15]. Очолює цю статистику країна-агресор, за нею слідують Україна, Китай, США, Нігерія, Румунія та Великобританія.

Отже, лінгвістам в сфері кібербезпеки варто вести двосторонній англо-український діалог з фахівцями та експертами під час розробки фахових термінів та їх визначень та укладати термінологічні словники та глосарії.

Надамо варіанти визначення терміну «кібербезпека», який широко використовується в законодавстві та щоденному житті в контексті захисту критичної інфраструктури України від кіберзагроз.

На думку О.А. Баранова, під дефініцією терміну «кібербезпека» необхідно розуміти «деякий стан комп'ютерних та цифрових систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в таких інформаційних системах» [1].

У Законі «Про основні засади забезпечення кібербезпеки України» термін «кібербезпека» вживається в наступному значенні: «Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [8].

«Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [там само].

За визначенням, поданим у глосарії ресурс-центру комп'ютерної безпеки Національного Інституту Стандартів та Технологій (National Institute of Standards and Technology), кібербезпека – це попередження ушкодження, захист і відновлення комп'ютерів, електронно-комунікаційних систем, електронно-комунікаційних сервісів, дротової та електронної комунікації, включно з інформацією в них, для забезпечення доступу до неї, її цілісності, конфіденційності та невідмовності (переклад наш) [11].

Словник *Cambridge Dictionary* подає таку дефініцію кібербезпеки : *«things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet»* [10].

Як і будь-якій іншій термінології, термінології кібербезпеки притаманні наступні риси:

1) інтеграція, що трапляється завдяки тому, що кібербезпека є ключовою ланкою в таких сферах, як бізнес (*personal information breach*), банківська справа, освіта (*identity theft*), тощо;

2) інтернаціональний характер, що відбувається завдяки термінам зі схожим написанням і значенням у принаймні трьох неспоріднених мовах (наприклад, *cache, domain, host, hub, spam*);

3) економія мовних ресурсів, реалізована за допомогою скорочення: *URL – Uniform Resource Locator, POP 3 – Post Office Protocol, Version 3*.

Аналіз термінологічних одиниць дозволив нам погодитися з визначеннями А.С. Д'якова та Т.Р. Кияка:

1. Термін повинен відповідати правилам і нормам певної мови (наприклад, англ. *cipher* запозичено з лат. *cifra* за певними правилам транслітерації в англійській мові, для яких не є характерним голосний *-a* в кінці слова).

2. Термін повинен бути систематичним. Наприклад, термін *Trojan Horse* відноситься до терміносистеми Cybersecurity, де означає тип комп'ютерного вірусу, однак в літературі та історії відноситься до напівміфічного періоду троянської війни та винаходу хитромудрого Одисея.

3. Термін характеризується дефінітивністю, тобто, кожен термін має окреме чітке визначення, наприклад: *Applet – Java programs, an application program that uses the client's web browser to provide a user interface* [7].

4. Термін характеризується незалежністю від контексту, наприклад: *network mapping* завжди означає «мережне картографування».

5. Термін має бути точним, хоча в субмовах трапляються багато численні «хибно орієнтовні» одиниці, наприклад, *hub* – концентратор, а не хаб.

6. Термін повинен бути стислим і коротким, хоча ця вимога інколи суперечить вимозі точності терміна, наприклад, *bit, browser, cookie, filter,* легко сприймаються, чого не скажеш про такі терміни як *Internet Control Message Protocol, Layer 2 Forwarding Protocol, Open shortest path first, etc*.

7. Термін має бути моносемантичним. Так *spam* означає лише "*electronic junk mail or junk newsgroup postings"*.

8. Явище синонімії є мало характерним для досліджуваної термінології.

9. Терміни мають бути експресивно нейтральними.

10. Термін повинен бути милозвучним (евфонічним), тому не слід створювати терміни із діалектизмів, жаргонізмів або варваризмів [7].

Матеріалом нашого дослідження є 451 термін кібербезпеки, вибраний нами з онлайн-глосарію *Glossary of Cyber Security Terms* [11].

Розглянемо їхні структурні та словотворчі особливості. Спочатку проаналізуємо їх за кількістю компонентів.

Нами було виокремлено 192 однослівних терміни (42,6%), 180 двослівних (39,9%) та 79 багатослівних (17,5%), останні містять 3 і більше компонентів.

Серед однослівних переважають іменникові, які становлять 106 прикладів (*worm, zombies, gateway*), 16 є формою дієслова-герундієм (*windowing, fuzzing*), 3 – дієсловами (*ramper, gethostbyname*), 65 однослівних термінів представлено абревіатурами (*WHOIS, ARPANET, BIND*).

Вартим уваги, однак малочисельними (3, 0,6%), виявилися терміни-телескопізми, утворені шляхом усічення їх складових:

– *syslog* – system logging;

– *vishing* – voice phishing;

– *windump* – Windows dumping.

Двослівні терміни представлено іменниками зі структурою:

• N+N (64, 14,2%), наприклад: *activity monitors, access matrix, bastion host, block cipher, buffer overflow, covert channels, data custodian, dictionary attack, fragment offset, hijack attack, ingress filtering, internet standard, jump bag, link state, program infector, proxy server*, тощо.

• Num+N (1, 0,2%): *zero day*;

• A+N (74, 16,4%): *active content, blue team, brute force, competitive intelligence, cryptographic algorithm, digital certificate, due care, dynamic library, ephemeral port, full duplex, hybrid attack,* тощо;

• N+Abbr (1, 0,2%): *standard ACLs*;

• N+Ger: (20, 4,4%): *cache cramming, cloud computing, data mining, domain hijacking, dumpster diving, egress filtering, password cracking, radiation monitoring, stack mashing,* тощо.

• Abbr+N (12, 2,7%): *BIND*, *CGI, HTTP proxy, IP address, IP flood, MAC address, RPC scans, SQL injection, SYN flood, TCP dump, UDP scan,* тощо;

• Абревіації у двокомпонентних термінах кібербезпеки поєднуються з герундієм, прикметником та дієприкметником минулого часу (participle II):

• Abbr+Ger (3, 0,6%): IP forwarding, IP spoofing, TCP fingerprinting

• A+Abbr (2, 0,4%): *reflexive ACLS*, *triple DES;*

• P2+Abbr (2, 0,4%): *extended ACLs, host-based ID*.

• A+Ger (3, 0,6%): *social engineering, private addressing, static routing*.

Багатослівні терміни представлені переважно іменниками з наступними структурами:

• N+N+N(+N) (46, 10,2%): *access control service, boot record infector, business continuity plan, call admission control, cyclic redundancy check, data encryption standard, disaster recovery plan, fault line attacks, fragment overlap attack, hypertext transfer protocol*, *internet control message protocol,* тощо;

1. N pr N (4, 0,9%): *denial of service, measures of effectiveness,* тощо;

2. N+A+N (1, 0,2%): *world wide web*;

3. (N+)P2+N(+N) (17, 3,8%): *list based access control, packet switched network, role based access control, split horizon, switched network, token based access control, wired equivalent privacy*, тощо;

4. (N)+P1+N(+N) (5, 1,1%): *layer tunnelling protocol, routing information protocol, spanning port*, тощо;

5. Abbr+A +N (3, 0,6%): *TCP full/half open scan;*

6. N to V (1, 0,2%)*: time to live*

Також зафіксовано 1 дієслівну термінологізовану фразу: *open shortest path first*.

Проілюструємо отримані дані на рисунку 1.

Як видно з рисунку 1, у досліджуваній термінології переважають однокомпонентні терміни, на 12 термінів менше представлено двокомпонентними одиницями, багатокомпонентні терміни становлять найменшу частку.

Розглянемо однослівні терміни кібербезпеки за способом словотворення. За цим принципом проаналізовані лексичні одиниці поділяємо на прості, похідні, складені, абревіатури та телескопізми.

Серед однослівних термінів-іменників ми виділили 28 простих терміни (6,2%), наприклад: *bot, byte, bit, cell, cron, frame, hop, host, patch, port, root, smurf, spam, switch, worm,* тощо.

Іменники-деривати репрезентовано 66 термінами (14%). З них утворені афіксальним шляхом становлять 22 одиниці (4,9%) (***a**vail**ability, bio**metr**ics, col**lis**ion, con**fid**entiality, counter**meas**ure, crypt**analys**is, def**ace**ment, dis**rup**tion, en**crypt**ion, in**cid**ent, non-re**pud**iation, recon**naiss**ance,* etc). За допомогою префіксації було утворено лише 9 термінів (***hyper**link**, inter**net**, inter**rupt**, intra**net**, mal**ware, **over**load, **pre**amble, etc)* (2%), суфіксації – 35 (7,8%) (*filt**er**, fragm**entation**, ident**ity**, oct**et**, parti**tions**, regist**ry**, rout**er**, safe**ty**, seg**ment**, signa**ture,** sniff**er**, stegano**graph**y, topo**logy**, us**er,** etc*). Тобто найбільше похідних іменників у досліджуваній англомовній термінології кібербезпеки було утворено за допомогою суфіксації.

Складені однослівні іменники мають структуру NN (12 іменників, 2,7%) і AN (3, 0,6%). Прикладами для цієї групи можуть слугувати наступні терміни: *bandwidth, checksum, crimeware, honeymonkey, netmask, ransomware, traceroute, backdoor, smartcard,* тощо.

Абревіатури становлять 65 одиниць (14,4%): *ISO, ITU-T, NAT, OSI, SHA1, SOCKS, TCP, IP, WHOIS,* тощо;

Однослівні терміни-дієслова представлені єдиним прикладом (1, 0,2%): *to tamper*. Також зафіксовано однослівні віддієслівні терміни-фрази/команди (2, 0,4%): *gethostbyaddr, gethostbyname.*

Типовим явищем у досліджуваному матеріалі (16, 3,5%) виявилися також однослівні терміни, виражені герундієм, похідним від дієслова: *auditing*, *flooding, fuzzing, hardening, patching, phishing, scavenging, smishing, stealthing, trunking, windowing,* тощо.

Зобразимо отримані дані на рисунку.

Із рисунку 2 видно, що у досліджуваній термінології переважають похідні однослівні іменники, які разом становлять близько половини (43%) аналізованих однослівних термінів кібербезпеки. Абревіації представляють майже третю їх частину (34%). Прості терміни складають 15% цієї групи термінів. Найменше використано складених іменників (6%) та телескопізмів (2%).

Узагальнення кількості аналізованих термінів кібербезпеки за частиномовним принципом представлено на рисунку 3.

Із рисунку 3 видно, що іменники та їх словосполучення становлять 428 одиниць або 95%

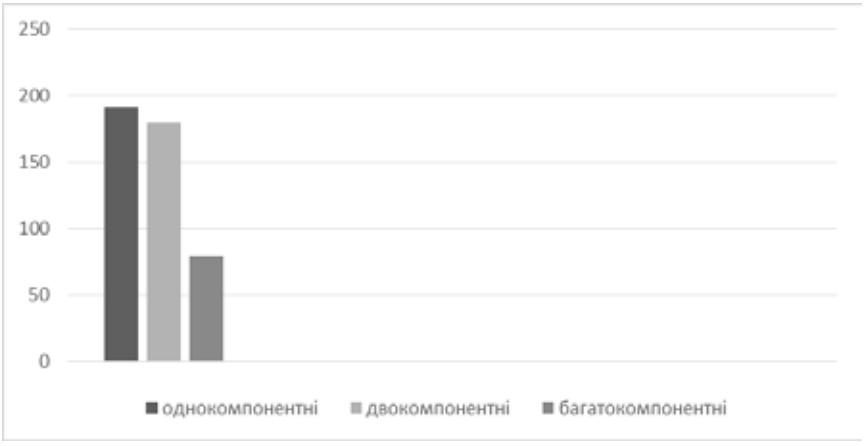

Рис. 1. Класифікація англомовних термінів кібербезпеки за кількістю компонентів

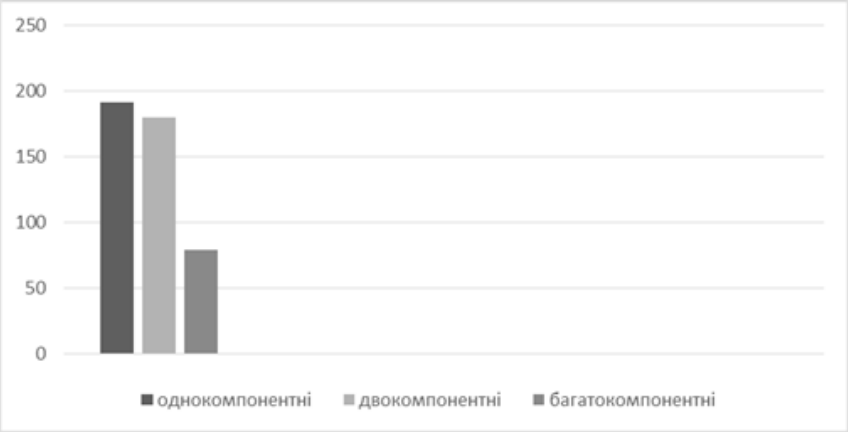

Рис. 2. Структура однослівних англомовних термінів кібербезпеки

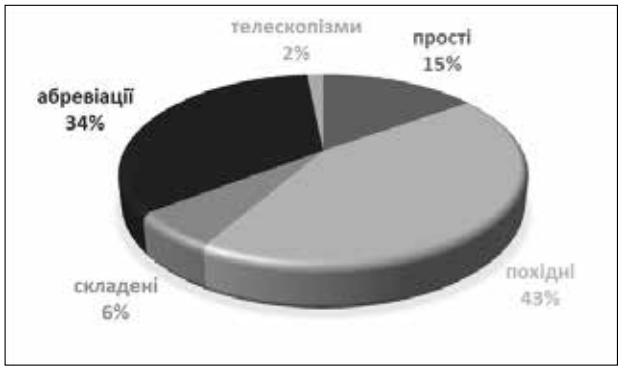

Рис. 3. Структура англомовних термінів кібербезпеки за частинами мови

досліджуваної англомовної термінології кібербезпеки. Таким чином, можемо стверджувати, що аналізована термінологія в більшості має іменникове підґрунтя, оскільки однією з основних функцій терміна є номінативна. Дії, окрім дієслів, представлено герундієм та його поєднанням із іншими частинами мови, переважно іменником.

Висновки. В результаті проведеного дослідження ми виявили, що досліджувані терміни кібербезпеки представлено однослівними, двослівними та багатослівними термінами, серед яких перші дві групи представлено приблизно однаковою кількістю прикладів (43 і 40% відповідно), в той час як багатослівних виявилося значно менше (17,5%). Серед однослівних термінів переважають похідні, які становлять майже половину прикладів цього виду. Третину однокомпонентних термінів кібербезпеки складають абревіації (34%), в той час як простими представлено лише 15% із них. Загалом, досліджувана англомовна термінологія кібербезпеки майже повністю (95%) побудована на іменниковій основі.

Перспективу подальших розвідок вбачаємо в аналізі функційних особливостей термінів кібербезпеки у дискурсі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 54–62. URL: http://ippi.org.ua/sites/default/files/ 14boavpk.pdf

2. Басов А. В. Забезпечення громадської безпеки: поняття та зміст. *Адміністративне право і процес*. 2012. № 2 (2). URL: http://applaw.knu.ua/index.php/arkhiv-nomeriv/2-2-2012/item/52-zabezpechennya-hromadskoyi-bezpekyponyattya-ta-zmist-basov-a-v1

3. Ботвин Т. М. Щодо англомовної термінологічної системи сектору кібербезпеки України в умовах воєнного стану: аналіз дефініцій. *Вчені записки ТНУ імені В. І. Вернадського*. *Серія: Філологія. Журналістика.* Том 33 (72). № 6. Ч. 1. 2022. С. 90–94.

4. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *Комп'ютерні науки та кібербезпека*, 2019, (1), 18–30. https://doi.org/10.26565/2519-2310-2019-1-02

5. Гладун А.Я. Англо-український словник термінів з інформаційних технологій та кібербезпеки / А.Я. Гладун, О.О. Пучков, І.Ю. Субач, К.О. Хала. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 380 с.

6. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник НАДУ*: зб. наук. праць. 2015. Вип. 3. С. 110–116.

7. Основи термінотворення: Семантичний та соціолінгвістичний аспекти / Д'яков А.С., Кияк Т.Р., Куделько З.Б. Київ. КМ Academia. 2000. 218 с.

8. Про основні засади забезпечення кібербезпеки України. Протокол. Юридичний інтернет ресурс. URL: Стаття 1. Визначення термінів – Про основні засади забезпечення кібербезпеки України – Закони України | Protocol

9. Черновол В.С. Кібербезпека як різновид публічної безпеки. *Актуальні проблеми адміністративно-правового забезпечення діяльності Національної поліції*. Харків, 2017. С. 72–74.

10. Cambridge Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/cybersecurity

11. Glossary of Cyber Security Terms. URL: https://csrc.nist.gov/glossary/term/cybersecurity

12. Griffiths Ch. The latest 2024 Cyber Crime statistics. AAG IT Support. URL: aag-it.com

13. Johansen A.G. What is cyber security? What you need to know? *NORTON.LifeLock*. 28.04.2022. URL: https://us.norton.com/ blog/ malware/what-is-cybersecurity-what-you-need-toknow#

14. Schatz D., Bashroush R., Wall J. Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*. 2017, 12 (2). DOI: https://doi.org/ 10.15394/jdfsl.2017.1476

15. World-first “Cybercrime Index” ranks countries by cybercrime threat level. World-first “Cybercrime Index” ranks countries by cybercrime threat level | University of Oxford