БІБЛІЯГРАФІЧНЫЯ СПАСЫЛКІ

1. Гістарычны слоўнік беларускай мовы. Вып. 16. Коржъ-лесничанка / склад. А. М. Булыка [і інш.] ; пад рэд. А. М. Булыкі. Мінск : Белар. навука, 1997. 359 с.

2. Гістарычны слоўнік беларускай мовы. Вып. 29. Пристрастный-ракъ / склад. І. У. Будзько [і інш.] ; пад рэд. А. М. Булыкі. Мінск : Белар. навука, 2009. 484 с.

3. *Дворецкий И. Х.* Латинско-русский словарь. 11-е изд., стереотип. М. : Рус. яз. – Медиа, 2008. 843 с.

4. *Кузнецов С. А.* Большой толковый словарь русского языка / Сост. и гл. ред. С. А. Кузнецов. СПб. : Норинт, 2000. 1536 с.

5. Лингвистический энциклопедический словарь / гл. ред. В. Н. Ярцева. М. : Сов. Энц., 1990. 683 с.

6. *Мохор Валентина.* Эпидемии на территории Беларуси через призму истории 19-го века. URL: https://medvestnik.by/dosug/epidemii-na-territorii-belarusi-cherez-prizmu-istorii-19-go-veka (date of access: 01.07.2025).

7. Национальный корпус русского языка. URL: http://www.ruscorpora.ru (date of access: 01.07.2025).

8. *Романов А. Ю.* Англицизмы и американизмы в русском языке и отношение к ним. СПб. : Изд.-во С.-Птб. ун-та, 2000. 152 с.

9. Тлумачальны слоўнік беларускай літаратурнай мовы : больш за 65 000 слоў / уклад. : І. Л. Капылоў [і інш.] ; пад рэд. І. Л. Капылова. Мінск : Белар. Энцыкл. імя П. Броўкі, 2016. 968 с.

10. Этымалагічны слоўнік беларускай мовы / [В. У. Мартынаў, А. Я. Супрун, Г. А. Цыхун і інш.]. Вып. 1–14. Мінск : Нав. і тэхн., 1978–2017.

11. Online Etymology Dictionary. URL: https://www.etymonline.com (date of access: 01.07.2025).

12. Oxford English Dictionary. URL : https://www.oed.com (date of access: 01.06.2025).

УДК 811.161.3’276.6:51

ТЭРМІНАЛОГІЯ КРЫПТАГРАФІІ ЯК АДЗІН СА СКЛАДНІКАЎ ТЭРМІНАСІСТЭМЫ БЕЛАРУСКАЙ МОВЫ

А. М. Муравіцкая

Беларускі дзяржаўны ўніверсітэт, пр. Незалежнасці, 4, 220030, г. Мінск, Беларусь, almurav@yandex.by

У артыкуле разглядаецца функцыянаванне крыптаграфічнай тэрміналогіі ў дыяхранічным і сінхронным аспектах, вызначаецца месца крыптаграфічнай тэрміналогіі ў тэрмінасістэме беларускай мовы. Шмат увагі надаецца гісторыі і развіццю крыптаграфічных сістэм ад старажытасці і да нашых дзён. Прыводзяцца прыклады сучасных беларускіх крыптаграфічных тэрміналагічных варыянтаў, абрэвіятур і інш.

Ключавыя словы: тэрмін; тэрміналогія; тэрмінасістэма; крыптаграфічная тэрміналогія; тэрміналагічны корпус.

Тэрміналагічны корпус сучаснай беларускай мовы няспынна папаўняецца новымі лексічнымі адзінкамі, развіваецца і ўдасканальваецца. Толькі за апошнія дзесяцігоддзі тэрміналагічная сістэма беларускай мовы ўзбагацілася вялікай колькасцю лексічных адзінак, звязаных з камп'ютарнай сферай, ІТ-тэхналогіямі, палітыкай, эканомікай і інш. сферамі чалавечай дзейнасці. Значнае месца ў гэтай сістэме належыць і крыптаграфічнай тэрміналогіі.

Вывучэнне тэрміналогіі крыптаграфіі пачалося параўнальна нядаўна – у апошнія дзесяцігоддзі XX ст., хаця гісторыя крыптаграфіі налічвае прыблізна 4500 гадоў. Гэта быў доўгі шлях развіцця ад так званай наіўнай крыптаграфіі да сучаснай камп'ютарнай крыптаграфіі. І на працягу ўсяго гэтага часу паралельна з развіццём дадзенай навукі развівалася і яе тэрмінасістэма.

На сучасным этапе тэрміналогія крыптаграфіі ўтварае спецыфічны пласт лексікі, які змяшчае аднакампанентныя і шматкампанентныя тэрміны, што ахопліваюць такія раздзелы крыптаграфіі, як атрыманне схаванай інфармацыі, сіметрычныя і асіметрычныя крыптасістэмы, квантавая крыптаграфія, кіраванне ключамі, хэш-функцыі, сістэмы электроннага лічбавага подпісу і інш. Не застаюцца ў баку ад даследчай дзейнасці ў гэтай сферы і навукоўцы нашага ўніверсітэта. У Беларускім дзяржаўным універсітэце праводзяцца навуковыя канферэнцыі, прысвечаныя разнастайным пытанням крыптаграфіі, у тым ліку і пытанням крыптаграфічнай тэрміналогіі. Так, напрыклад, 20–21 кастрычніка 2020 г. у БДУ была праведзена міжнародная навуковая канферэнцыя «Тэарэтычная і прыкладная крыптаграфія» (ТПК–2020), прысвечаная 20-годдзю навукова-даследчага інстытута прыкладных праблем матэматыкі і інфарматыкі. У працы гэтага навуковага форума, арганізаванага ў фармаце відэаканферэнцыі, прынялі ўдзел каля сямідзесяці экспертаў у галіне абароны інфармацыі і інфармацыйнай бяспекі з пяці краін: Беларусі, Расіі, Украіны, Польшы і Італіі. Арганізатарамі канферэнцыі выступілі факультэт прыкладной матэматыкі і інфарматыкі БДУ і навукова-даследчы інстытут прыкладных праблем матэматыкі і інфарматыкі. Праз тры гады (19–20 кастрычніка 2023 г.) у БДУ адбылася II Міжнародная навуковая канферэнцыя «Тэарэтычная і прыкладная крыптаграфія», на якой разглядаліся актуальныя праблемы крыптаграфіі: матэматычныя асновы крыптаграфіі, верагоднасна-статыстычныя метады крыпталогіі, ацэнка надзейнасці крыптаграфічных алгарытмаў і пратаколаў, блокчэйн-сістэмы і інш. напрамкі крыпталогіі. Удзельнікамі канферэнцыі сталі звыш пяцідзесяці экспертаў у галіне абароны інфармацыі і інфармацыйнай бяспекі з Беларусі, Расіі і Казахстана.

У цяперашні час крыптаграфія істотна ўплывае на наша паўсядзённае жыццё. Цяжка ўявіць, як працавалі б без яе інтэрнэт, банкаўскія транзакцыі, электронныя паслугі. Інфармацыя стала звышкаштоўнай, што падштурхоўвае крыптографаў пастаянна ўдасканальваць крыптаграфічныя рашэнні і павышаць бяспеку.

У старажытнасці крыптаграфію выкарыстоўвалі, каб захаваць сакрэтнасць паведамлення. Гэтая задача з'явілася разам з узнікненнем пісьма. Само пісьменства можна ў пэўнай ступені лічыць крыптаграфічнай сістэмай. Свае пасланні спрабавалі шыфраваць яшчэ ў старажытных цывілізацыях: Індыі, Егіпце, Месапатаміі. Каб заблытаць чытача, выкарыстоўвалі метады кадавання і стэнаграфіі, якія толькі ўскосна адносяцца да крыптаграфіі. Шыфраванне звычайна зводзіла-

ся да перастаноўкі і замены сімвалаў. Вучоныя лічаць першым прымяненнем крыптаграфіі выкарыстанне спецыяльных іерогліфаў у старажытным Егіпце. Егіпцяне імкнуліся перасягнуць адзін аднаго ў вынаходлівасці пры перадачы паслання. Перш за ўсё пісцы выкарыстоўвалі больш рэдкія іерогліфы для красамоўства, каб прыцягнуць увагу да сваіх тэкстаў. Прыклады шыфравання можна знайсці і ў старажытнасяміцкай літаратуры. Так, шыфр атбаш, адзін з самых простых, выкарыстоўваўся ў кнізе прарока Іераміі. Паходжанне гэтага слова тлумачыць прынцып дзеяння шыфра – простая падмена літар. Яно было складзена з літар алеф, бэт, таў, шын – чатырох літар старажытнасяміцкага алфавіта – дзвюх першых і дзвюх апошніх. Вядомы і шыфр старажытнай Спарты – скітала (або сцітала). Але скітала – гэта, па сутнасці не шыфр, а прылада – доўгі стрыжань, на які намотвалі стужку з пергамента па спіралі. Шыфраваны тэкст пісалі ў радкі па даўжыні стрыжня, потым размотвалі і перадавалі адрасату. Пасля размотвання тэкст станавіўся нечытальным. Каб расшыфраваць пасланне, адрасату патрэбен быў стрыжань дакладна такога ж дыяметра. Скітала лічыцца самым вядомым старажытным крыптаграфічным прыстасаваннем. Пазней узнік шыфр Цэзара, названы ў гонар яго стваральніка. Прынцып дзеяння шыфра просты: кожная літара зрушвалася па алфавіце ўправа на адну і тую ж колькасць пазіцый. Адрасату патрэбна было толькі ведаць, наколькі – гэта і быў ключ шыфравання. Сам Цэзар выкарыстоўваў зрух на тры сімвалы. Старажытныя прыстасаванні і шыфры больш нагадвалі загадкі, чым метады крыптаграфіі – перыяд прыблізна да XVI ст. яшчэ называюць наіўнай крыптаграфіяй. Да прыкладу, шыфр скітала «ўзламаў» Арыстоцель: замест стрыжня ён узяў конус і намотваў стужку з пасланнем на рознай вышыні, пакуль тэкст не станавіўся чытальным. Выкарыстоўвалі і іншыя спосабы засакрэчвання інфармацыі: адмысловыя дыскі і лінейкі, шыфраванне пры дапамозе кніг і інш.

Гісторыкам вядома аб некалькіх спосабах засакрэчвання пасланняў, якія выкарыстоўвалі ў Візантыі. У асноўным, гэта былі простыя прыёмы: хуткапіс, замена алфавіту, няправільнае напісанне літар, лігатурнае пісьмо. Сустракаліся і складаныя, якія назвалі лічбавым тайнапісам: калі літарам прысвойвалі лічбавае значэнне і шыфравалі тэкст з дапамогай арыфметычных дзеянняў: лічбы раскладвалі на складнікі, дадавалі і аднімалі. У Сярэднявеччы людзі працягвалі выкарыстоўваць монаалфавітныя шыфры, хаця ў некаторых краінах вынаходзілі і іншыя спосабы крыптаграфіі. Але, калі раней шыфравалі ў асноўным ваенныя пасланні, то цяпер сталі засакрэчваць паведамленні дыпламаты, купцы і простыя грамадзяне. Шыфры ўскладняліся па меры распаўсюджвання тэхнікі частотнага крыптааналізу – калі шыфр змаглі разгадаць без ключа, аналізуючы, як часта ў засакрэчаным тэксце сустракаюцца розныя літары. Упершыню гэта тэхналогія з'явілася ў арабскіх краінах. Яе развіццё прывяло да з'яўлення поліалфавітных шыфраў (шыфр простай замены на аснове некалькіх алфавітаў) і шыфраў на аснове замены літар па пэўных правілах. У эпоху Адраджэння былі адкрыты шыфры многаалфавітнай замены, упершыню выкарыстаны метад падвойнага шыфравання. Над разгадкай некаторых тагачасных шыфраў крыптографы разважалі стагоддзямі. Пазней многія з гэтых шыфраў сталі асновай для новых метадаў шыфравання. Крыптаграфія існавала і ў Старажытнай Русі. Літаратуры той эпохі вядома тайнапісанне,

называемае Літарэя. Яна магла быць «простай» і «мудрай». «Простая» нагадвала Тарабарскую грамату, «мудрая» – шыфр простай замены некаторых літар кропкамі, палкамі, кругамі, якія абазначалі разрад ліку.

Да пачатку Першай сусветнай вайны крыптаграфію ўжо лічылі паўнавартасным баявым інструментам у ЗША, Расіі, Англіі, Германіі і інш. краінах. Дзяржавы перахоплівалі засакрэчаныя паведамленні, а крыптааналітыкі разбуралі сакрэтныя палітычныя планы. Так, расшыфроўка перахопленай тэлеграмы нямецкага пасла Артура Цымермана падштурхнула ЗША ўступіць у вайну на баку Антанты.

Падчас Другой сусветнай вайны буйныя дзяржавы выкарыстоўвалі электрамеханічныя шыфратары. Шыфры прылад у той час лічыліся няўскрывальнымі. Самі прылады былі ротарнымі, як, напрыклад, шыфравальная машына «Энігма». З яе дапамогай паведамленні шыфравала армія Германіі і яе саюзнікі, пры дапамозе М-209 – армія ЗША. У СССР выраблялі абодва тыпы прылад. Самымі ўстойлівымі да ўзлому лічыліся коды, якія стварала «Энігма». Прынцып працы быў такі: пры кожным націску на клавішу правы ротар зрушваўся на адну пазіцыю, а пры пэўных умовах зрушваліся і іншыя ротары. Рух ротараў кожны раз прыводзіў да розных крыптаграфічных пераўтварэнняў. Аднак мала хто ведае пра савецкую шыфравальную тэхніку 1940–1950-х гг., напрыклад пра машыну «Фіялка», якая не была ўзламана і з'яўлялася засакрэчанай да нядаўняга часу [3].

Сучасная крыптаграфія ўтварае асобны навуковы напрамак на стыку матэматыкі і інфарматыкі. Практычнае прымяненне крыптаграфіі стала неад'емнай часткай жыцця сучаснага грамадства: яе выкарыстоўваюць у такіх галінах, як электронная камерцыя, электронны дакументазварот (у тым ліку электронны лічбавы подпіс), тэлекамунікацыі і інш. Істотнае пашырэнне прадмета крыптаграфіі, кола даследчыкаў і карыстальнікаў прывяло да з'яўлення вялікай колькасці новых паняццяў і тэрмінаў, што выкарыстоўваюцца ў навуковых публікацыях і нарматыўных прававых дакументах. У выніку некаторыя тэрміны ў розных крыніцах сталі трактавацца па-рознаму. Сустракаецца шмат варыянтаў пры перакладзе з англійскай мовы аднаго і таго ж тэрміна. Па сутнасці на сучасным этапе працягваецца выпрацоўка і фарміраванне адзінай крыптаграфічнай тэрміналогіі.

Як ужо адзначалася вышэй, адна з асаблівасцей крыптаграфічнай тэрмінасістэмы – гэта цесная сувязь з матэматычнай тэрміналогіяй. Значная колькасць матэматычных тэрмінаў актыўна выкарыстоўваецца ў крыптаграфічнай тэрміналогіі, напрыклад: *лацінскі квадрат*, *дыскрэтны лагарыфм у канечнай групе*, *рэгістр зруху*, *сістэма ўраўненняў з перакручанымі правымі часткамі*, *часовая складанасць алгарытму*, *хэш-функцыя*, *аднабаковая хэш-функцыя*, *група кропак эліптычнай крывой* і інш. Акрамя таго неабходна адзначыць, што шматлікія крыптаграфічныя тэрміны паходзяць непасрэдна ад вядомых матэматычных тэрмінаў. Найбольш шматлікай з'яўляецца група тэрмінаў, якія ўтварыліся ад матэматычнага тэрміна *дыскрэтная функцыя.* Большасць гэтых тэрмінаў прысвечана тлумачэнню крыптаграфічных уласцівасцей дыскрэтных функцый: *афіннае прыбліжэнне*, *бент-функцыя*, *забарона функцыі*, *група інерцыі функцыі*, *лавінны крытэрый*, *карэляцыйна-імуннае адлюстраванне*, *збалансаваная функцыя*, *эластычная функцыя* і інш. Другую значную групу ўтва-

раюць тэрміны *тэорыі верагоднасцей і матэматычнай статыстыкі.* Тут цэнтральнае месца належыць паняццям *сапраўднай выпадковасці* і *псеўдавыпадковасці*: *псеўдавыпадковая паслядоўнасць*, *сапраўдная выпадковая паслядоўнасць*, *выпадковая ідэальная паслядоўнасць*, *энтрапія* і інш. [2, с. 3–66]. У сучаснасці крыптаграфічная тэрмінасістэма працягвае няспынна ўдасканальвацца і развівацца, аб чым сведчыць наяўнасць тэрміналагічных варыянтаў, напрыклад: *алгарытм шыфравання асіметрычны – асіметрычнае шыфраванне*; *алгарытм шыфравання блочны – блочнае шыфраванне*; *алгарытм шыфравання паточны – паточнае шыфраванне*; *аналіз крыптаграфічны – крыптааналіз*; *метад аналізу крыптаграфічнага – метад крыптааналізу*; *параметр крыптаграфічнага пераўтварэння – крыптаграфічны параметр*; *пратакол крыптаграфічны – крыптапратакол*; *сістэма шыфравання – шыфрсістэма*; *стойкасць крыптаграфічная – крыптастойкасць*; *тэхніка шыфравальная – шыфртэхніка*; *функцыя хэшыравання – хэш-функцыя*; *сінтэз крыптаграфічны – крыптасінтэз*; *сістэма крыптаграфічная – крыптасістэма*; *алгарытм праверкі подпісу лічбавага – праверка подпісу*; *хэш-функцыя крыптаграфічная, якая зададзена ключом – код аўтэнтыфікацыі*; *рэжым выпрацоўкі кода аўтэнтычнасці паведамлення – рэжым выпрацоўкі імітаўстаўкі*; *стойкасць крыптаграфічная тэарэтычная – стойкасць даказуемая*; *шыфрсістэма з адкрытым ключом – шыфрсістэма асіметрычная*; *шыфрсістэма з сакрэтным ключом – шыфрсістэма сіметрычная* і інш. [2, с. 3–66].

Крыптаграфічная тэрмінасістэма змяшчае шэраг тэрміналагічных адзінак, якія маюць два і больш варыянты: *алгарытм крыптаграфічны – крыптаалгарытм*, *алгарытм крыптаграфічнага пераўтварэння*, *крыптаграфічнае пераўтварэнне*, *крыптапераўтварэнне*; *апаратура лінейнага шыфравання – апаратура засакрэчвання*, *засакрэчвальная апаратура сувязі (ЗАС)*; *паведамленне зашыфраванае – паведамленне шыфраванае*, *шыфртэкст*; *сістэма крыптаграфічная – крыптасістэма*, *крыптаграфічная сістэма абароны інфармацыі*; *сродкі праграмныя – праграмнае забеспячэнне*, *праграмныя сродкі*; *пратакол аўтэнтыфікацыі абанентаў – аўтэнтыфікацыя абанента (карыстальніка)*, *пратакол ідэнтыфікацыі*; *пратакол ідэнтыфікацыі ўзаемнай – аўтэнтыфікацыя ўзаемная*, *пратакол ідэнтыфікацыі*; *пратакол ідэнтыфікацыі аднабаковай – аўтэнтыфікацыя аднабаковая*, *пратакол ідэнтыфікацыі*; *размежаванне доступу – функцыя-сэрвіс размежавання доступу*, *сістэма размежавання доступу; падзел сакрэту – схема падзелу сакрэту*, *пратакол падзелу сакрэту* і інш. [2, с. 3–66].

Для крыптаграфічнай тэрмінасістэмы характэрна наяўнасць тэрмінаў-абрэвіятур. Сярод іх пераважаюць іншамоўныя (часцей з англійскай мовы): *PKI (public key infrastructure) – інфраструктура адкрытых ключоў*; *KEK (key enciphering key) – ключ шыфравання ключоў*; *OCSP (online certificate status protocol) – пратакол праверкі статуса сертыфіката анлайнавы*; *LFSR (linear feedback shift register) – рэгістр зруху з лінейнай зваротнай сувяззю*; *CRL (certificate revocation list) – спіс адазваных сертыфікатаў*; *EDI (electronic data interchange) – сістэма абмену данымі электронная*; *EFT (electronic funds transfer) – сістэма пераводу сродкаў грашовых электронная*; *DSS (digital signature standard) – стандарт лічбавага подпісу*; *SHS (secure hash standard) –*

стандарт функцыі хэшыравання; *AES (advanced encryption standard) – стандарт шыфравання; DES (data encryption standard) – стандарт шыфравання*; *EES (escrowed encryption standard) – стандарт шыфравання з дэпаніраваннем ключоў*; *OWHF (one-way hash function) – хэш-функцыя аднабаковая* і інш. [1, с. 15–91]. Параўнальна нядаўна сталі ўжывацца ў крыптаграфічнай тэрмінасістэме беларускамоўныя абрэвіятуры: *СКАДС – сродкі крыптаграфічныя абароны дзяржаўных сакрэтаў*; *СКАІ – сродкі крыптаграфічныя абароны інфармацыі*; *ЭЛП – подпіс электронны лічбавы* і інш.

Крыптаграфія – адна з самых старажытных навук – прайшла доўгі шлях у сваім развіцці, яе гісторыя налічвае амаль 4500 гадоў. На працягу гэтага часу паралельна складвалася і развівалася яе тэрмінасістэма. На сучасным этапе крыптаграфія з'яўляецца адным з самых запатрабаваных напрамкаў, а крыптаграфічная тэрмінасістэма стала крыніцай папаўнення і ўзбагачэння новымі лексічнымі адзінкамі тэрміналагічнага корпуса беларускай мовы, адным з яе істотных складнікаў.

БІБЛІЯГРАФІЧНЫЯ СПАСЫЛКІ

1. Словарь криптографических терминов / под ред. Б. А. Погорелова, В. Н. Сачкова. М. : МЦНМО, 2006. 94 с.

2. Словарь основных терминов по криптологии / сост. : Ю. С. Харин [и др.]. Минск : БГУ, 2013. 66 с.

3. От манускриптов до шифровальных машин: история криптографии. URL: https://naked-science.ru/article/sci/ot-manuskriptov-do-shifro (date of access: 26.06.2025).

УДК 811.161.3'373

ПРЭЦЭДЭНТНАЯ ЛЕКСЕМА «СЛОВА» Ў МАСТАЦКАЙ СПАДЧЫНЕ ЯКУБА КОЛАСА

Ю. В. Назаранка

Беларускі дзяржаўны ўніверсітэт, пр. Незалежнасці, 4, 220030, г. Мінск, Беларусь, julijanazarenko@mail.ru

Аналізуецца антэцэдэнтная дэфініцыя прэцэдэнтнай лексемы «слова» ў мастацкай спадчыне класіка беларускай літаратуры Якуба Коласа на матэрыяле выслоўяў, выбраных з 12-томнага збору твораў, даследуецца яе канцэптуальна-прагматычнае значэнне і актуальнасць у пазакантэкставым выкарыстанні. Сцвярджаецца моўнарытарычная каштоўнасць аўтарскіх выслоўяў у паўсядзённым маўленні праз іх трапнасць, дарэчнасць, выразнасць, а таксама бясспрэчная карысць для ўзбагачэння лексікону.

***Ключавыя словы*:** прэцэдэнтная лексема; антэцэдэнтная дэфініцыя; выслоўе; дыскурс; мастацкі тэкст; кантэкст.