А. М. Муравіцкая
старшы выладчык кафедры беларускага мовазнаўства
Беларускага дзяржаўнага ўніверсітэта

ВАРЫЯНТНАСЦЬ ТЭРМІНАЎ КРЫПТАГРАФІІ

У апошні час варыянтнасць у мове, прызначанай для спецыяльных мэт, асэнсоўваецца лінгвістамі як непазбежная і заканамерная з'ява, выяўляюцца новыя фактары (камунікатыўна-прагматычныя, кагнітыўныя), якія абумоўліваюць з'яўленне і працяглае суіснаванне тэрміналагічных варыянтаў. Тэарэтычныя і прыкладныя аспекты вывучэння варыянтнасці тэрмінаў былі закладзены ў працах К. Я. Авербуха, У. Г. Гака, С. В. Грынёва, У. М. Лейчыка, Ю. У. Слажэнікінай, В. А. Татарынава і іншых вядомых лінгвістаў.

У сучасных даследаваннях ужываюцца розныя намінацыі для абазначэння сінанімічных адносін у тэрміналогіі: сінонімы, дублеты, варыянты. В. А. Татарынаў адзначае, што ў многіх працах па тэрміналогіі з'явы сінаніміі апісваюцца праз паняцце варыянта [4, с. 271]. Аднак некаторыя мовазнаўцы традыцыйна выступаюць супраць з'яў варыянтнасці і дублетнасці ў тэрміналогіі (О. Вюстэр, І. Н. Качан, А. У. Лемаў і інш.). Між іншым сучасныя даследаванні дазваляюць сцвярджаць, што сінанімія – прымета дынамічнага развіцця навукі. На думку В. А. Татарынава, «чым вышэй узровень развіцця навукі, тым сінанімічней мысленне спецыяліста» [4, с. 277]. Лінгвісты адзначаюць, што, з аднаго боку, варыянтнасць тэрміна – гэта спецыфічная рэалізацыя агульнай тэорыі варыянтнасці, якая праяўляецца як цалкам у мове, так і ў асобных яе разнавіднасцях і састаўных элементах [1, с. 73]. З другога боку, сінанімія тэрмінаў адрозніваецца ад сінанімії агульналітаратурных слоў, паколькі сутнасцю тэрміналагічнага вар'іравання з'яўляецца пошук аптымальнага спосабу намінацыі, дакладнага абазначэння пэўнага спецыяльнага паняцця.

Адна з прычын узнікнення тэрміналагічных варыянтаў – імкненне да эканоміі моўных сродкаў. З гэтым звязана з'яўленне абрэвіятур, рознага роду кампазіцый, адсячэнне малаінфарматыўнага або паўтаральнага кампанента, вар'іраванне частак тэрміна. Тэндэнцыя да эканоміі моўных сродкаў выразна прадстаўлена ў крыптаграфічнай тэрмінасістэме. Прывядзём прыклады такіх варыянтаў [2; 3]:

алгарытм праверкі лічбавага подпісу – праверка подпісу;

алгарытм шыфравання асіметрычны – асіметрычнае шыфраванне;

алгарытм шыфравання блочны – блочнае шыфраванне;

алгарытм шыфравання паточны – паточнае шыфраванне;

аналіз крыптаграфічны – крыптааналіз;

метад крыптаграфічнага аналізу – метад крыптааналізу;

параметр крыптаграфічнага пераўтварэння – крыптаграфічны параметр;

пратакол крыптаграфічны – крыптапратакол;

рэжым выпрацоўкі кода аўтэнтычнасці паведамлення – рэжым выпрацоўкі імітаўстаўкі;

сінтэз крыптаграфічны – крыптасінтэз;

сістэма крыптаграфічная – крыптасістэма;

сістэма шыфравання – шыфрсістэма;

стойкасць крыптаграфічная – крыптастойкасць;

стойкасць крыптаграфічная тэарэтычная – стойкасць даказуемая;

тэхніка шыфравальная – шыфртэхніка;

функцыя хэшыравання – хэш-функцыя;

хэш-функцыя крыптаграфічная, якая зададзена ключом – код аўтэнтыфікацыі;

шыфрсістэма з адкрытым ключом – шыфрсістэма асіметрычная;

шыфрсістэма з сакрэтным ключом – шыфрсістэма сіметрычная і інш.

Для крыптаграфічнай тэрмінасістэмы характэрна наяўнасць тэрмінаў-абрэвіятур. Сярод іх пераважаюць абрэвіятуры іншамоўнага паходжання (часцей з англійскай мовы), якія не перакладаюцца і падаюцца на пісьме лацінскай графікай. Як правіла, ім адпавядае тэрміналагічнае словазлучэнне:

AES (advanced encryption standard) – стандарт шыфравання;

CRL (certificate revocation list) – спісадазваныхсертыфікатаў;

DES (data encryption standard) – стандартшыфравання;

DSS (digital signature standard) – стандартлічбавагаподпісу;

EDI (electronic data interchange) – сістэмаабменудадзеныміэлектронная;

EES (escrowed encryption standard) – стандартшыфраванняз дэпаніраваннемключоў;

EFT (electronic funds transfer) – сістэмапераводусродкаўграшовыхэлектронная;

KEK (key enciphering key) – ключшыфраванняключоў;

LFSR (linear feedback shift register) – рэгістрзрухузлінейнайзваротнайсувяззю;

OCSP (online certificate status protocol) – пратаколправеркістатусасертыфікатаанлайнавы;

OWHF (one-way hash function) – хэш-функцыяаднабаковая;

PKI (public key infrastructure) – інфраструктураадкрытыхключоў;

*SHS (secure hash standard) – стандартфункцыіхэшыраванняі*інш.

Параўнальнанядаўнаўкрыптаграфічнайтэрмінасістэместаліўжываццабеларускамоўныяабрэвіятуры: *СКАДС – сродкікрыптаграфічныяабароныдзяржаўныхсакрэтаў*;*СКАІ – сродкікрыптаграфічныяабароныінфармацыі*;*ЭЛП – подпісэлектроннылічбавы*іінш.

Наяўнасцьварыянтаўтэрмінаўсведчыцьпраняпоўнуюсфарміраванасць тэрмінасістэмы.

Прычымсяродкрыптаграфічныхтэрмінаўсустракаеццашматтэрміналагічны хадзінак, якіямаюцьдваі большварыянты:

алгарытмкрыптаграфічны – крыптаалгарытм,алгарытмкрыптаграфічнагапераўтварэння,крыптаграфічнаепераўтварэнне,крыптапераўтварэнне;

апаратура лінейнага шыфравання – апаратура засакрэчвання, засакрэчвальная апаратура сувязі (ЗАС);

паведамленне зашыфраванае – паведамленне шыфраванае, шыфртэкст;

падзел сакрэта – схема падзелу сакрэта, пратакол падзелу сакрэта;

пратакол аўтэнтыфікацыі абанентаў – аўтэнтыфікацыя абанента (карыстальніка), пратакол ідэнтыфікацыі;

пратакол ідэнтыфікацыі аднабаковай – аўтэнтыфікацыя аднабаковая, пратакол ідэнтыфікацыі;

пратакол ідэнтыфікацыі ўзаемнай – аўтэнтыфікацыя ўзаемная, пратакол ідэнтыфікацыі;

размежаванне доступу – функцыя-сэрвіс размежавання доступу,сістэма размежавання доступу;

сістэма крыптаграфічная – крыптасістэма, крыптаграфічная сістэма абароны інфармацыі;

сродкі праграмныя – праграмнае забеспячэнне, праграмныя сродкі, сродкі праграмнага забеспячэння;

функцыя крыптаграфічная – пераўтварэнне крыптаграфічнае, крыптапераўтварэнне і інш.

Такім чынам, на сучасным этапе працягваецца выпрацоўка і фарміраванне крыптаграфічнай тэрміналогіі. Наяўнасць даволі значнай колькасці варыянтаў сярод тэрміналагічных адзінак крыптаграфіі сведчыць пра дынамічнае і эвалюцыйнае развіццё дадзенай часткі беларускай навуковай тэрмінасістэмы.

Літаратура

1. Лейчик, В. М. Терминоведение : Предмет, методы, структура / В. М. Лейчик. – М. : Либроком, 2014. – 264 с.

2. Словарь криптографических терминов / Под ред. Б. А. Погорелова, В. Н. Сачкова. – М. : МЦНМО, 2006. — 94 с.

3. Словарь основных терминов по криптологии / Сост. : Ю. С. Харин [и др.]. – Минск : БГУ, 2014. – 94 с.

4. Татаринов, В. А. Теория терминоведения : В 3 т. – Т. 1. Теория термина : история и современное состояние / В. А. Татаринов. – М. : Московский лицей, 1996. – 312 с.

В. У. Пахірка
старшы выкладчык кафедры гуманітарных дысцыплін
Мінскага інавацыйнага ўніверсітэта

ФРАЗЕАЎТВАРАЛЬНАЯ АКТЫЎНАСЦЬ ГЕРМАНІЗМАЎ У ФАЛЬКЛОРНА-ДЫЯЛЕКТНЫХ ЗАПІСАХ XIX СТ.

Словы нямецкага паходжання ўтвараюць вялікі пласт запазычанай лексікі ў беларускай мове, што тлумачыцца, у першую чаргу, старажытнасцю беларуска-нямецкіх моўных кантактаў. Яшчэ ў старабеларускі перыяд германізмы пачынаюць адаптавацца да фанетычных, марфалагічных і сінтаксічных нормаў, уваходзіць у склад фразеалагічных зваротаў, прыказак і прымавак.

Гэты працэс працягваецца і падчас станаўлення сучаснай літаратурнай мовы (XIX – пачатак XX ст.). Прааналізаваць