Муравіцкая А. М. (Мінск)

ТЭРМІНАЛОГІЯ КРЫПТАГРАФІІ: АСАБЛІВАСЦІ ФУНКЦЫЯНАВАННЯ Ў БЕЛАРУСКАЙ МОВЕ

Крыптаграфія (ад грэч. *κρυπτός* – схаваны і *γράφω* – пішу) – навука аб метадах забеспячэння канфідэнцыяльнасці (немагчымасці чытання інфармацыі староннім) і аўтэнтычнасці (цэласнасці і сапраўднасці аўтарства, а таксама немагчымасці адмовы ад аўтарства) інфармацыі.

Першапачаткова крыптаграфія вывучала метады шыфравання інфармацыі – абарачальнага пераўтварэння адкрытага (зыходнага) тэксту на аснове сакрэтнага алгарытму і (або) ключа ў шыфраваны тэкст (шыфратэкст). Традыцыйная крыптаграфія ўтварае раздзел сіметрычных крыптасістэм, у якіх зашыфраванне і расшыфраванне праводзяцца з выкарыстаннем аднаго і таго ж сакрэтнага ключа. Акрамя гэтага раздзелу сучасная крыптаграфія ўключае атрыманне ўтоенай інфармацыі і квантавую крыптаграфію.

Гісторыя крыптаграфіі налічвае каля 4 тыс. гадоў. За асноўны крытэрый перыядызацыі звычайна прымаюць тэхналагічныя характарыстыкі метадаў шыфравання. Першы перыяд (прыблізна з III тыс. да н.э.) характарызуецца панаваннем монаалфавітных шыфраў (асноўны прынцып – замена алфавіту зыходнага тэксту іншым алфавітам праз замену літар іншымі літарамі або сімваламі). Другі перыяд (з IX ст. на Блізкім Усходзе (Ал-Кіндзі) і з XV ст. у Еўропе (Леон Батыста Альберці) да пачатку XX ст.) адзначыўся ўвядзеннем ва ўжытак поліалфавітных шыфраў. Трэці перыяд (з пачатку і да сярэдзіны XX ст.) характарызуецца ўкараненнем электрамеханічных прылад у працу шыфравальшчыкаў. Пры гэтым працягвалася выкарыстанне поліалфавітных шыфраў. Чацвёрты перыяд (з сярэдзіны да 70-х гадоў XX ст.) – перыяд пераходу да матэматычнай крыптаграфіі. У працы Шэнана з'яўляюцца строгія матэматычныя вызначэнні колькасці інфармацыі, перадачы дадзеных, энтрапіі, функцый шыфравання. Абавязковым этапам стварэння шыфраў лічыцца вывучэнне яго ўразлівасці да розных вядомых атак: лінейнаму і дыферэнцыйнаму крыптааналізам. Аднак да 1975 года крыптаграфія заставалася "класічнай", або крыптаграфіяй з сакрэтным ключом.

Сучасны перыяд развіцця крыптаграфіі (з канца 1970-х гадоў па цяперашні час) адрозніваецца ўзнікненнем і развіццём новага накірунку – крыптаграфія з адкрытым ключом. Яе з'яўленне вызначаецца не толькі новымі тэхнічнымі магчымасцямі, але і параўнальна шырокім распаўсюджваннем крыптаграфіі для выкарыстання прыватнымі асобамі (у папярэднія эпохі выкарыстанне крыптаграфіі было выключнай прэрагатывай дзяржавы). Прававое рэгуляванне выкарыстання крыптаграфіі прыватнымі асобамі ў розных краінах моцна адрозніваецца – ад дазволу да поўнай забароны.

Сучасная крыптаграфія ўтварае асобны навуковы напрамак на стыку матэматыкі і інфарматыкі: працы ў гэтай галіне публікуюцца ў навуковых

часопісах, арганізуюцца рэгулярныя канферэнцыі. Практычнае прымяненне крыптаграфіі стала неад'емнай часткай жыцця сучаснага грамадства: яе выкарыстоўваюць у такіх галінах, як электронная камерцыя, электронны дакументаабарот (у тым ліку электронны лічбавы подпіс), тэлекамунікацыі і інш.

Для сучаснай крыптаграфіі характэрна выкарыстанне адкрытых алгарытмаў шыфравання, якія прадугледжваюць выкарыстанне вылічальных сродкаў. Вядома больш за дзясятак праверaных алгарытмаў шыфравання, якія пры выкарыстанні ключа дастатковай даўжыні і карэктнай рэалізацыі алгарытму з'яўляюцца крыптаграфічна ўстойлівымі. Найбольш распаўсюджаныя алгарытмы: сіметрычныя, асіметрычныя і хэш-функцыі. У многіх краінах прыняты нацыянальныя стандарты шыфравання.

У Рэспубліцы Беларусь адкрытая крыптаграфія пачала выкарыстоўвацца з 1991 года спачатку ў банкаўскай сферы, а са стварэннем у 1995 годзе Дзяржаўнага цэнтра бяспекі інфармацыі – і ў іншых сферах [1].

Істотнае пашырэнне прадмета крыптаграфіі і 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.

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 ўтвараюць 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.

У 2012 годзе на ваенным факультэце Белдзяржуніверсітэта адкрылася новая спецыяльнасць "прыкладная крыптаграфія", дзе студэнты-курсанты ў

межах выкладання дысцыпліны “Беларуская мова: прафесійная лексіка” вывучаюць тэрміналагічную лексіку па сваёй спецыяльнасці. Адной з праблем пры выкладанні гэтай дысцыпліны з’яўляецца адсутнасць беларускамоўных падручнікаў і тэрміналагічных слоўнікаў па крыптаграфіі, а таксама недастатковая распрацаванасць дадзенай тэрмінасістэмы як у рускім, так і ў беларускім тэрміназнаўстве. У сваёй працы даводзіцца арыентавацца пераважна на найбольш поўны і вядомы ў рускім тэрміназнаўстве “Словарь криптографических терминов” [2] пад рэдакцыяй Б.А. Пагарэлава і У.М. Сачкова, а таксама на “Словарь основных терминов по криптологии” [3], які параўнальна нядаўна быў выдадзены ў БДУ супрацоўнікамі факультэта прыкладной матэматыкі і інфарматыкі Белдзяржуніверсітэта.

Крыптаграфічная тэрмінасістэма – адна з самых новых і малараспрацаваных “дзялянак” як у беларускім, так і ў рускім тэрміназнаўстве. Таму наперадзе ў мовазнаўцаў і тэрмінолагаў шмат працы ў гэтай галіне, але найперш актуальная задача – стварэнне слоўніка асноўных крыптаграфічных паняццяў і тэрмінаў на беларускай мове.

Літаратура

1. Аператыўна-аналітычны цэнтр пры Прэзідэнце Рэспублікі Беларусь [Электронны рэсурс]. Рэжым доступу: http://oac.gov.by/tzi/cryptography.html (дата доступу: 05.09.2016).
2. Словарь криптографических терминов / Под ред. Б.А. Погорелова, В.Н. Сачкова. – М., 2006. – 94 с.
3. Словарь основных терминов по криптологии / сост.: Ю.С. Харин [и др.]. – Мн., 2013. – 66 с.