АСАБЛІВАСЦІ ВЫКАРЫСТАННЯ БЕЛАРУСКАЙ МОВЫ Ў СФЕРЫ АХОВЫ ІНФАРМАЦЫІ

Лукашонак А.К., Ільюшчанка А.І.

Беларускі дзяржаўны ўніверсітэт інфарматыкі і радыёэлектронікі
г. Мінск, Рэспубліка Беларусь

Дапіра Т.П. – выкладчык

У рабоце раскрываюцца паняцці крыптаграфія, шыфратэкст, кадаванне, шыфр Цэзара, ідэнтыфікацыя. Робіцца спроба выкарыстання беларускай мовы ў сістэме забеспячэння прыватнасці. Апісваюцца асаблівасці выкарыстання роднай мовы ў сучаснай крыптаграфіі.

На сённяшні дзень моўная сітуацыя ў Беларусі характарызуецца як білінгвальная. Двухмоўе – гэта адначасовае функцыянаванне ў грамадстве дзвюх моў. У такіх умовах вельмі важным лічым развіваць менавіта нацыянальнукю мову ў сучасных запатрабаваных сферах дзейнасці, а менавіта ў пытаннях інфармацыйных тэхналогій, у галіне абароны інфармацыі, індывідуальнай бяспекі і так далей.

Беларуская мова мае шмат агульных граматычных і лексічных уласцівасцей з іншымі ўсходнеславянскімі мовамі. Разам з тым яна надзеленая асаблівасцямі, дзякуючы якім можа выкарыстоўвацца ў галіне абароны інфармацыі на адным узроўні з іншымі мовамі, а ў нечым і перамагаць над імі.

У працы апісваецца спроба выкарыстаць беларускую мову ў шыфраванні і парольнай абароне.

На працягу ўсёй гісторыі чалавецтва імкнулася схаваць пэўную інфармацыю ад старонніх вачэй. Таму не дзіўна, што з гэтага жадання паўстала цэлая галіна ведаў – крыптаграфія [1]. Крыптаграфія — навука пра метады забеспячэння прыватнасці (немагчымасці чытання інфармацыі староннім) і аўтэнтычнасці (цэласнасці і сапраўднасці аўтарства, а таксама немагчымасці адмовы ад аўтарства) інфармацыі [2].

Інфармацыя, якая перадаецца па канале сувязі і якая падлягае шыфраванню, называецца адкрытым (зыходным) тэкстам (пазначаецца М ад англійскай message), а крыптаграфічна ператвораная інфармацыя называецца шыфратэкстам (пазначаецца С ад англійскай ciphertext). Крыптаграфічнае пераўтварэнне адкрытага тэксту ў шыфратэкст рэалізуецца па пэўным алгарытме. Адпраўнік выконвае крыптаграфічнае пераўтварэнне (шыфраванне) адкрытага тэксту і фарміруе, такім чынам, шыфратэкст, перадаючы яго ў канал сувязі, а атрымальнік выконвае адваротнае крыптаграфічнае пераўтварэнне шыфратэкста (расшыфраванне) у адкрыты тэкст. Сістэма, у якой ажыццяўляецца шыфраванне і расшыфраванне інфармацыі называецца крыптасістэмай або шыфрам [3].

Важным параметрам любога шыфру з'яўляецца ключ — параметр крыптаграфічнага алгарытму, што забяспечвае выбар аднаго пераўтварэння з сукупнасці пераўтварэнняў, магчымых для гэтага алгарытму. У сучаснай крыптаграфіі мяркуецца, што ўся сакрэтнасць крыптаграфічнага алгарытму засяроджана ў ключы, але не ў дэталях самога алгарытму (прынцып Керкгофса) [3].

Варта не блытаць шыфр з кадаваннем — фіксаваным пераўтварэннем інфармацыі з аднаго выгляду ў іншы. У кадаванні адсутнічае паняцце ключа і не дзейнічае прынцып Керкгофса. У цяперашні час кадаванне практычна не ўжываецца для абароны інфармацыі ад несанкцыянаванага доступу, а толькі як абарона ад памылак пры перадачы інфармацыі (перашкодаўстойлівае кадаванне) і ў іншых мэтах, не звязаных з абаронай.

Шыфр можа ўяўляць сабой сукупнасць умоўных знакаў (умоўны алфавіт з лічбаў ці літар альбо алгарытм пераўтварэння звычайных лічбаў і літар).

Для прыкладу выкарыстання беларускай мовы ў шыфраванні мы ўзялі шыфр Цэзара.

Шыфр Цэзара – адна з самых простых і найбольш вядомых крыптасістэм, якая адносіцца да шыфраў падстаноўкі. У гэтай крыптасістэме кожны сімвал адкрытага тэксту замяняецца сімваламі, якія знаходзяцца на некаторым пастаянным ліку пазіцый злева або справа ў алфавіце ад замяняемага сімвала адкрытага тэксту. Лік, які характарызуе колькасць пазіцый зруху налева або направа па алфавіце адносна пазіцыі пераўтваральнага сімвала адкрытага тэксту, з'яўляецца крыптаграфічным ключом і вызначаецца выразам: n-1 (Дзе n – лік знакаў у алфавіце) [4].

Для шыфравання інфармацыі неабходна мець, акрамя адкрытага тэксту, яшчэ і алфавіт. Для гэтага шыфру мы карысталіся беларускім алфавітам. Кожная літара алфавіта адпавядае яе парадкаваму нумару, а апостраф мае нумар трыццаць тры.

Зашыфруем паведамленне, у якасці якога выкарыстаем першыя радкі верша Якуба Коласа:

“Люблю я прыволле
Шырокіх палёў,
Зялёнае мора
Ржаных каласоў.”

Выкарыстоўваючы ключ роўны пятнаццаці, атрымаем шыфратэкст:

“ылпыл м я’ірюыыу
зі’ющце яоыўг
хмыўьоу эю’о
’фоыіх шоыоаг”

Размаўляючы пра бяспеку інфармацыі, якая знаходзіцца ў тэлефоне, камп’ютары ці ў іншых прыладах, неабходна таксама ведаць і разумець, што такое ідэнтыфікацыя і якія тыпы ідэнтыфікатараў ёсць на сённяшні дзень.

Ідэнтыфікацыя – працэс прысваення ўнікальнай (непаўторнай) прыкметы (ідэнтыфікатара) суб'екту доступу, па якім ён будзе пазнаны [5].

Віды ідэнтыфікатараў:

1. Ідэнтыфікатар можа быць запісаны на пэўнае прыстасаванне, якое гарантуе супрацьдзеянне пагрозе захаванасці ідэнтыфікатара. Прыкладам могуць быць спецыялізаваныя прыстасаванні, што забяспечваюць захаванасць інфармацыі і якія падключаюцца да персанальнага камп’ютара праз раздым USB.

2. У якасці ідэнтыфікатара могуць выкарыстоўвацца біяметрычныя характарыстыкі чалавека (паводніцкія і фізіялагічныя).

3. Ідэнтыфікатар, які вядомы толькі суб'екту доступу. Такі падыход мяркуе, што ідэнтыфікатар неабходна запомніць. Прыкладам з'яўляецца пароль.

Пароль часта выкарыстоўваюць у інфармацыйных сістэмах. Гэта абумоўлена наступнымі перавагамі:

- выбраць яго можа сам суб’ект інфармацыйнай сістэмы;
- пры кампраметацыі яго можна досыць лёгка змяніць;
- складанасць і кошт сістэмы невысокія.

Часцей за ўсё паролі напісаны з выкарыстаннем рускага ці англійскага алфавітаў, а паролі на беларускай мове выкарыстоўвае меншасць людзей. Але трэба звярнуць увагу: паролі на беларускай мове з прычыны яе асаблівасцей будуць мець большую ўстойлівасць і надзейнасць.

Так, напрыклад, на падбор пароля на рускай мове "пьедестал" - па дадзеных сайта 2ip.ru, спатрэбіцца 193 хвіліны, а на падбор пароля "п'едэстал" па-беларуску спатрэбіцца 53 гадзіны.

Адбываецца гэта праз наяўнасць ў беларускай мове такога надрадковага знака, як апостраф. Ён з'яўляецца спецыяльным сімвалам [6]. Прыкладамі іх з'яўляюцца : $, #, @,!, %, ^, &, *, (,). Дастасаванне ў алфавіт гэтых сімвалаў значна павялічвае час падбору пароля.

Такім чынам, у сферы абароны інфармацыі беларуская мова мае свае асаблівасці і перавагі, можа выкарыстоўвацца ў абароне інфармацыі на адным узроўні з рускай і англійскай мовамі. На сённяшні дзень

беларускую мову актыўна выкарыстоўвае моладзь, таму нам, студэнтам тэхнічнага ўніверсітэта, хочацца выкарыстоўваць яе ў цікавай і вельмі распаўсюджанай галіне аховы інфармацыі.

Спіс выкарыстаных крыніц:

1. Крыптаграфія. Што гэта такое? [Электронны рэсурс]. – Рэжым доступу: https://be.atomiyme.com/%D0%BA%D1%80%D1%8B%D0%BF%D1%82%D0%B0%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F-%D1%88%D1%82%D0%BE-%D0%B3%D1%8D%D1%82%D0%B0-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D0%B0%D1%81%D0%BD%D0%BE%D0%B2%D1%8B/ – Дата доступу: 08.04.2022.

2. Крыптаграфія [Электронны рэсурс]. – Рэжым доступу: https://www.wiki.be-by.nina.az/%D0%9A%D1%80%D1%8B%D0%BF%D1%82%D0%B0%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F – Дата доступу: 04.04.2022.

3. Шыфр [Электронны рэсурс]. – Рэжым доступу: https://be.wikipedia.org/wiki/%D0%A8%D1%8B%D1%84%D1%80 – Дата доступу: 04.04.2022.

4. Борботько, Т.В. Шифрование и расшифрование информации с использованием шифра Цезаря: пособие / Т. В. Борботько [и др.]. – Минск: БГУИР, 2021. – 8 с.

5. Борботько, Т.В Противодействие утечке конфиденциальной информации. Лабораторный практикум: пособие / Т. В. Борботько [и др.]. – Минск: БГУИР, 2018. – 188 с.

6. Какие специальные символы в пароле? [Электронны рэсурс]. – Рэжым доступу: https://rsbset.ru/kakie-spetsialnye-simvoly-v-parole/#i – Дата доступу: 08.04.2022.