

РОЛЯ БЕЛАРУСКАГА АЛФАВІТА ВА ЎСТОЙЛІВАСЦІ ПАРОЛЬНОЙ АХОВЫ

Асадчы І.В., Ягораў В.А.

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

Пятрова Н.Я. – к.філал.н., дацэнт

У артыкуле даследуецца ўплыў выкарыстання спецыфічных сімвалаў беларускага алфавіта на эфектыўнасць паролнай аховы. Асабліва ўвага надаецца літары «ў» і яе патэнцыялу для павышэння трываласці пароляў.

У сучасным свеце, дзе людзі актыўна выкарыстоўваюць інтэрнэт для зносін і фінансавых аперацый, ахова інфармацыі, персанальных даных, кібербяспека і т. п. становяцца ключавымі аспектамі. Увечка інфармацыі можа прывесці да сур'ёзных праблем як для дзяржавы, так і для кожнага яе жыхара, уключаючы як страту інфармацыі, так і сродкаў. Таму важна ведаць, як эфектыўна ахоўваць персанальныя даныя ад патэнцыйных пагроз.

Пароль, таксама ключ бяспекі, – умоўнае слова або выпадковы набор знакаў, што складаецца з літар, лічбаў і іншых сімвалаў і прызначаны для пацвярджэння асобы або паўнамоцтваў. Палітыка пароляў – гэта пэўны комплекс правіл, асноўная мэта якіх заключаецца ў матывацыі карыстальнікаў да выкарыстання надзейных пароляў і правільнага абыходжання з імі. Яна можа быць як рэкамендацый, так і патрабаваннем [1]. Аднак многія сервісы строга абмяжоўваюць выкарыстаныя сімвалы пры стварэнні пароля, а таксама яго максімальную даўжыню, што негатыўна адбіваецца на яго надзейнасці. Сучасныя сервісы найчасцей прад'яўляюць наступныя патрабаванні да пароляў: даўжыня не менш за 8 знакаў, наяўнасць літар верхняга і ніжняга рэгістраў, выкарыстанне лічбаў і спецыяльных знакаў. Разам з тым, часам бывае недастаткова такога набору сімвалаў, як засцерагчы ад небяспекі свой акаўнт ці персанальную інфармацыю.

Асноўныя віды атак для атрымання пароля парушальнікам – гэта фішынг і BruteForce, ці метады грубай сілы. Асаблівасць фішынг-атакі ў тым, што карыстальнік сам уводзіць пароль на падрабленых сайтах пад уплывам маніпуляцый з боку парушальніка. Таму пры фішынгу не мае значэння, наколькі пароль надзейны [2]. Метады грубай сілы, або BruteForce, заключаецца ў простым пераброўванні ўсіх магчымых камбінацый пароля. У адрозненне ад фішыngu, BruteForce не патрабуе неасцярожных дзеянняў карыстальніка, таму пра надзейнасць пароля трэба паклапаціцца загадзя [3].

Беларускае пісьмо – літарна-гукавое. Яно ўключае сістэму графічных знакаў (літары, пунктуацыю), з дапамогай якіх дакладна перадаецца гукавы склад кожнага слова нашай мовы. Сукупнасць літар, размешчаных у традыцыйна ўстаноўленым парадку, называецца алфавітам. У беларускім алфавіце 32 літары: 10 літар для абазначэння галосных гукаў і 21 літара для перадачы зычных гукаў [4, с. 66]. Беларускі алфавіт спрадвечу меў шмат адметных асаблівасцей, але да

нашых дзён захаваліся такія спецыфічныя літары (у параўнанні з рускай мовай), як «ў» (у нескладовае), «і», знак апострафа. Пры неабходнасці абазначыць націск у друкаваных дакументах часта вылучаюць націскны галосны верхнім рэгістрам. Усе гэтыя асаблівасці можна выкарыстоўваць для стварэння трывалых, але простых для запамінання пароляў.

У будучым, з развіццём тэхналогій, такіх як, напрыклад, квантавыя камп'ютары, якія могуць значна паскорыць перабор пароляў, выкарыстанне нацыянальных алфавітаў усіх сусветнаведомых сучасных моў можа стаць яшчэ больш пашыранай з'явай у кібербяспецы. Мы лічым, што беларуская мова, дзякуючы сваёй унікальнасці, можа стаць адным з ключавых элементаў у стварэнні больш трывалых сістэм аўтэнтафікацыі.

Звернем увагу, што надзейнасць і трываласць пароля характарызуецца энтрапіяй (H, яго нявызначанасцю), якая залежыць ад даўжыні пароля і ёмістасці слоўніка (колькасці ўсіх магчымых сімвалаў). Менавіта таму камбінацыя тыпу «Ubs6fvTln*vf» і просты для запамінання пароль «Domovionok1!» маюць аднолькавае значэнне энтрапіі. Розніца паміж гэтымі паролямі ў тым, што першы немагчыма лёгка запомніць без запісу. Калі запісаць пароль у памяць камп'ютара або на папярковы носбіт, узнікае рызыка яго крадзяжу. Таму асацыятыўныя паролі на аснове канкрэтных выразаў і словазлучэнняў з'яўляюцца больш практычнымі для выкарыстання. Матэматычнае выражэнне энтрапіі можна запісаць так:

дзе L – даўжыня пароля, A – ёмістасць алфавіта (колькасць усіх магчымых сімвалаў, што выкарыстоўваюцца ў паролях)[5].

На аснове гэтай формулы працуюць сайты, якія дапамагаюць разлічыць час, неабходны для падбору такога пароля метадам BruteForce. Разгледзім паролі, што складаюцца з 8 знакаў, але выкарыстоўваюць розныя алфавіты. Для праверкі хуткасці падбору мы выкарысталі сайт HowSecureIsYourPassword[6]. Вынікі прадстаўлены ў Табліцы 1.

Табліца 1 – Хуткасць падбору пароля ў залежнасці ад ёмістасці алфавіта.

Пароль	Час
Snow2024	6.67 хвілін
Cner2024	16 дзён
CnerŲ024	3 месяцы

Для BruteForce самым папулярным інструментам з'яўляецца HashCat. Гэта праграма здольна правяраць дзясяткі тысяч пароляў у секунду, выкарыстоўваючы графічны працэсар камп'ютара. Аднак у базавай версіі наладак HashCat адсутнічаюць кірылічныя сімвалы, у тым ліку і «ў нескладовае»[7]. Таму, на нашу думку, пароль становіцца немагчымым падбраць без ручнога дадання гэтых сімвалаў у слоўнік. Разам з тым, нам уяўляецца, штобеларускія словы і словазлучэнні для запамінання носбітамі прасцейшыя, чым словы і словазлучэнні на замежнай, напрыклад, англійскай мове, таму знікае неабходнасць запісваць пароль для запамінання. Таксама важна падкрэсліць адсутнасць падрыхтаваных спісаў пароляў з выкарыстаннем слоў на беларускай мове. Менавіта таму такі пароль можна лічыць трывалым.

Такім чынам, выкарыстанне беларускай мовы ў інфармацыйных тэхналогіях не губляе сваёй актуальнасці, а некаторыя яе спецыфічныя рысы можна эфектыўна выкарыстаць у кібербяспецы, паколькі ўжыванне, напрыклад, беларукалітары «ў» у паролі значна павялічвае яго надзейнасць.

Спіс выкарыстаных крыніц:

1. Технологии защиты компьютерной информации [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/tehnologii-zaschity-kompyuternoy-informatsii>. – Дата доступа: 13.03.2025.
2. Спам и фишинг [Электронный ресурс]. – Режим доступа: <https://www.kaspersky.ru/resource-center/threats/spam-phishing>. – Дата доступа: 13.03.2025.
3. Брутфорс-атака: определение, примеры, защита [Электронный ресурс]. – Режим доступа: <https://www.kaspersky.ru/resource-center/definitions/brute-force-attack>. – Дата доступа: 13.03.2025.
4. Беларуская мова (прафесійная лексіка): вучэбна-метадычны дапаможнік для студэнтаў БНТУ ў 4 ч. Ч. 1. Беларуская мова: агульныя звесткі, паходжанне і развіццё, функцыянальныя стылі / Л. А. Гіруцкая [і інш.]. – Мінск: БНТУ, 2005. – 289 с.
5. Сложность пароля [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Сложность_пароля. – Дата доступа: 13.03.2025.
6. HowSecure is Your Password? [Электронный ресурс]. – Режим доступа: <https://www.passwordmonster.com/>. – Дата доступа: 13.03.2025.
7. MaskAttack [Электронный ресурс]. – Режим доступа: https://hashcat.net/wiki/doku.php?id=mask_attack. – Дата доступа: 13.03.2025.