УДК 004.056

**О. В. Кохан**

# АЛГОРИТМ ПІДСИЛЕННЯ ПАРОЛЯ

Вінницький національний технічний університет

***Анотація***

*Проаналізовано відомі методи автентифікації. Розглянуто важливість генерування якісного пароля на основі ключового слова користувача. Запропоновано алгоритм підвищення стійкості паролів, які задаються користувачем і є зручними для запам'ятовування.*

**Ключові слова:** генерування паролів, стійкий пароль, автентифікація, авторизація

***Abstract***

*Known authentication methods are analyzed. The importance of generating a quality password based on the user 's keyword is considered. An algorithm for user-defined and easy-to-remember passwords strengthening was proposed.*

**Keywords:** password generation, persistent password, authentication, authorization.

## Вступ

Одним з найпростіших та найпоширеніших методів автентифікації є автентифікація на основі знання певного секрету - пароля. Проте даний метод може бути доволі просто зламаний методом підбору пароля за спеціальними словниками чи навіть грубим методом перебору символів-літер. Наразі проблема генерування стійких паролів, що будуть зрозумілими і запам'ятовуватимуться користувачу, є особливо актуальним, оскільки кожен користувач має велику кількість облікових записів, інформація яких потребує захисту. Тому виникає необхідність створення методу підсилення паролів, що дозволить покращити рівень захисту даних користувачів.

Метою є покращення стійкості пароля без суттєвої втрати його легкості до запам'ятовування користувачем.

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати найпоширеніші методи автентифікації;
- визначити вимоги до стійкості паролів;
- обрати підхід до перетворення зрозумілих слів у стійкий пароль.

## Аналіз методів автентифікації

Для підтвердження належності даному користувачеві відповідного ідентифікатора можна використовувати будь-яку іншу секретну інформацію, яка повинна бути доступна лише йому, або унікально його характеризувати. Це визначається факторами автентифікації – вид інформації, що надає користувач системі при автентифікації (табл. 1) [1, 2].

Для перевірки справжності користувача в системах найчастіше використовують пароль як фактор автентифікації, де секретний ключ вводиться з клавіатури. Оскільки такий спосіб є зручним і простим в реалізації, то в системах, які використовують декілька факторів автентифікації, пароль зустрічається майже завжди як один з факторів автентифікації [1, 3].

Таблиця 1.1 – Класифікація факторів автентифікації

| Клас факторів автентифікації | Приклади параметрів, які використовуються як фактор автентифікації |
|---|---|
| На основі володінням секретної інформації | Пароль чи парольна фраза,<br>PIN-код (Personal Identification Number) |
| На основі володіння чим-небудь | Фізичний ключ,<br>Карта з магнітною стрічкою,<br>OTP-токен генерації паролю,<br>Параметри використовуваного обчислювального пристрою |
| На основі біометричних характеристик | Відбиток пальця,<br>Тембр голосу,<br>Сітківка ока. |

Для систем із різним ступенем захисту використовують постійні, умовно-постійні та тимчасові паролі для забезпечення більшого захисту. Чим більше символів має пароль, тим більш стійким він є (важче піддається підбору та іншим типам атак). Також не менш важливим фактором являється набір символів пароля [4]. Більш різноманітні і непередбачувані символи дозволять зробити пароль стійкішим.

Порте, чим більше різноманітних символів та цифр використовувати в парольному слові, тим важче запам’ятати його. Тому багато користувачів обирають більш прості та передбачувані паролі (рис. 1) [5].

| | |
|---|---|
| 1. 123456 | 13. 123321 |
| 2. 123456789 | 14. 666666 |
| 3. qwerty | 15. 18atcskd2w |
| 4. 12345678 | 16. 7777777 |
| 5. 111111 | 17. 1q2w3e4r |
| 6. 1234567890 | 18. 654321 |
| 7. 1234567 | 19. 555555 |
| 8. password | 20. 3rjs1la7qe |
| 9. 123123 | 21. google |
| 10. 987654321 | 22. 1q2w3e4r5t |
| 11. qweryuiop | 23. 123qwe |
| 12. mynoob | 24. zxcvbnm |

Рисунок 1 - Список популярних паролів світу

Також до популярних паролів відносять: ім’я та прізвище, дата народження, імена дітей чи домашніх тварин, слова зі словників [1, 5]. Очевидно, що використання таких паролів є недоцільним для захисту інформації, яка має певну цінність [2, 3, 6]. З іншого боку паролі, які можна вважати стійкими – незручні для користувачів, а тому спричиняють проблеми, пов’язані з їх втратою [6], що особливо актуально у зв’язку з необхідністю їх періодичного оновлення [1, 3].

Оскільки зручні парольні фрази легко зламуються вищезгаданими методами, то виникає необхідність розробки алгоритму, що дозволить підсилити парольне слово користувача, яке легко запам’ятовується. Внаслідок цього буде отримано більш стійкий до атак перебору пароль дружній до користувача.

## Результати дослідження

Щоб поєднати дві характеристики, а саме – легкість в запам’ятовуванні та надійність, пропонується алгоритм генерування паролів (рис. 2).

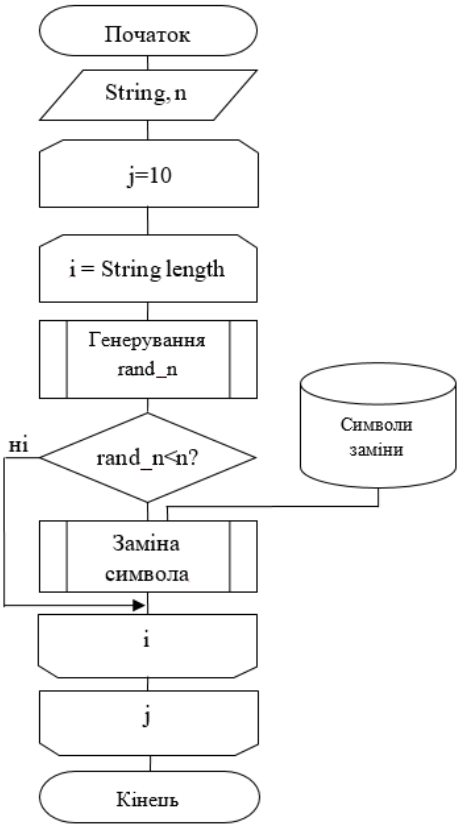


Рисунок 2 - Алгоритм роботи блоку генерування паролів

На вхід подаються дані, що вводилися користувачем, а саме ключове слово, з якого буде генеруватися пароль, та відсоток заміни символів у парольній фразі. Заміна кожного символу буде відбуватися у циклі, кількість повторів якого залежить від довжини введеного слова, де визначатиметься чи буде замінена літера на символ. Для більшої варіативності паролів до літер підібрано декілька символів, які візуально схожі на відповідну літеру та легко вводяться з клавіатури.

## Висновки

Аналіз методів автентифікації показав, що існує багато можливостей підтвердження ідентифікатора, проте найпопулярнішим є парольний. Проте, вони мають недолік, пов'язаний зі складністю запам'ятовування стійких паролів, що обумовлює порушення найкращих практик щодо організації політик безпеки стосовно паролів. Саме тому запропоновано алгоритм, який дозволить забезпечити компроміс між стійкістю пароля та зручністю його запам'ятовування.

Надалі планується провести дослідження внаслідок якого буде відібрано варіанти заміни символів, які будуть найзручнішими для користувачів з точки зору комфорту запам'ятовування.

## СПИСОК ВИКОИСТАНОЇ ЛІТЕРАТУРИ

1. Афанасьев А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов // А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, 2012. 550 с.

2. Баришев Ю. В., Каплун В. А. Метод автентифікації віддалених користувачів для мережевих сервісів. *Інформаційні технологій та комп'ютерна інженерія*. 2014. №2. С. 13-17.

3. Y. Baryshev, V. Kaplun, K. Neuimina. Discretional model and method of distributed information resources access control. *Scientific Works of Vinnytsia National Technical University*. 2017. №2. 8 p. URL: https://works.vntu.edu.ua/index.php/works/article/download/504/505 (accessed 09.11.2020)

4. Парольна защита. Инструкция по организации [Електронний ресурс]. URL: https://compnote.ru/otdelit/instruktsiya-po-organizatsii-parolnoy-zashhityi/ (дата звернення 01.12.2020)

5. Найпопулярніші паролі в світі. Чи Ви користуєтесь одним з них? [Електронний ресурс]. URL: https://www.trans.eu/ua/blog/transportna-haluz/najpopuljarnishi-paroli-v-sviti-chi-vi-koristuetes-odnim-z-nih/ (дата звернення 01.12.2020).

6. Кохан О. В., Баришев Ю. В.. Засіб генерування стійкого пароля. *XLIX науково-технічної конференції підрозділів ВНТУ*: матеріали доповідей (18-29 травня 2020). Вінниця, 2020. 3 с. URL: https://publish.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/9390/7674 (дата звернення 01.12.2020).

***Кохан Олександр Володимирович*** - студент групи БС-20б, факультет інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail : sasha.kohan98@gmail.com
Науковий керівник - ***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, email: yuriy.baryshev@vntu.edu.ua

***Alexander Kohan*** - student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University: sasha.kohan98@gmail.com
Scientific supervisor – ***Yurii Baryshev*** – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, email: yuriy.baryshev@vntu.edu.ua