Міністерство освіти і науки України
Хмельницький національний університет

АПКН 2019

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК

ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XI всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2019»

14-15 листопада 2019

Том 1
Роботи студентів та молодих вчених Факультету програмування та комп'ютерних і телекомунікаційних систем ХНУ

Хмельницький 2019

Актуальні проблеми комп'ютерних наук. Збірник наукових праць за матеріалами XI всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2019» – Хмельницький: ХНУ, 2019, Т.1. – 248с.

У збірнику наукових праць представлені перспективні практичні розробки аспірантів, магістрів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, прикладної математики й інформатики, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки з сучасних систем пошуку й обробки інформації, САПР та математичного, комп'ютерного і нейромережевого моделювання.

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2019

XI всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

Основні напрямки роботи конференції:

1. Прикладні інформаційні технології.
2. Сучасні системи пошуку, захисту і обробки інформації.
3. Математичне, комп'ютерне і нейромережеве моделювання.
4. САПР, математичні моделі і методи рішення інженерних задач.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

Робочі мови конференції: українська, англійська.

КЕРІВНИЦТВО ОРГКОМІТЕТУ:

СИНЮК О. М.
голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

СОРОКАТИЙ Р. В.
заступник голови оргкомітету, доктор технічних наук, завідувач кафедри Комп'ютерних наук та інформаційних технологій ХНУ, професор

БАРМАК О. В.
заступник голови оргкомітету, доктор технічних наук, професор

СЕКРЕТАРІАТ КОНФЕРЕНЦІЇ:

Мазурець О. В.
секретар конференції, старший викладач каф. КНІТ ХНУ

КОНТАКТНА ІНФОРМАЦІЯ:
e-mail для листування: *apkt.khnu@gmail.com*

ЗМІСТ

УДК 006.4

Сторожук А.І., Багрій Р.О., Скрипник Т.К.

Хмельницький національний університет

ІНФОРМАЦІЙНА СИСТЕМА ГЕНЕРАЦІЇ БЕЗПЕЧНИХ ПАРОЛІВ З АСОЦІАТИВНИМИ ЗВ'ЯЗКАМИ

Розглянуто основні аспекти розробки інформаційної системи для генерації безпечних паролів та проаналізовані способи запам'ятовування паролів, що забезпечували безпечні паролі високої крипто-стійкості з можливістю легкого запам'ятовування. Запропонована інформаційна система забезпечує генерацію паролів високого рівня складності з підбором асоціацій до відповідних символів для легкого запам'ятовування відповідно до заданих умов.

The basic aspects of developing an information system for generating secure passwords are discussed, as well as ways of remembering passwords that provide secure, high-resilience, easy-to-remember passwords. The proposed information system provides the generation of high-complexity passwords with the selection of associations to the appropriate characters for easy memorization according to specified conditions.

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів. Складність створення системи захисту інформації визначається тим, що дані можуть бути викрадені. [1]

Одною з основних проблем захисту інформації є відсутність користування такими простими і елементарними правилами безпеки, як використання надійних і доступних для запам'ятовування паролів.

Проблематика безпечних паролів полягає не тільки в їхній крипто-стійкості як такої. Існує багато алгоритмів, які забезпечують дуже надійні та стійкі до брутфорсу варіанти генерації паролів, але зазвичай вони виглядають складно та являється важкими для запам'ятовування. [2] Внаслідок чого це призводить до частої втрати паролю і відповідно втраті доступу до інформації. Деякі з користувачів у такому випадку використовують менеджері для зберігання паролів, але для них потрібно пароль, що часто призводить не до вирішення проблеми, а лиш ускладнення. [3]

Метою досліджень є розробка інформаційної системи генерації безпечних паролів з асоціативними зв'язками в якості вирішення проблеми доступу та запам'ятовування паролів. Одною з складових якої є

алгоритм генерації, що забезпечує високий рівень захисту конфіденційної інформації і захист від несанкціонованого доступу. Інша складова це метод підбору асоціацій до символів.

На основі даної інформаційної системи необхідно створити програмний додаток для забезпечення генерації безпечних паролів та підбору асоціацій до них.

Також в рамках проведених досліджень було проаналізовано способи запам'ятовування набору даних та символів[4]:

1. Спосіб запам'ятовування за допомогою асоціацій. Це відмінний метод запам'ятовування чисел та символів. За рахунок даної системи знаходиться слово, яке викликає асоціацію з частиною символа і має до них якесь відношення.
2. Спосіб запам'ятовування за допомогою мнемотехніки. Мнемонічний знак – це слово або коротка фраза, яку використовують для того, щоб щось запам'ятати, тому що вона являє собою ключ до іншої інформації.

Отже на основі аналізу способів запам'ятовування набору даних та символів можна зробити висновок, що додаток повинен бути безкоштовним, простим і водночас зручним у користуванні, мати надійну систему, а згенерований пароль має бути легкий для запам'ятовування.

Враховуючи зазначені вимоги розроблено інформаційну систему (ІС), що дає можливість виконувати основні функції системи генерації безпечного пароля та забезпечує підбір асоціації до нього (рис.1).

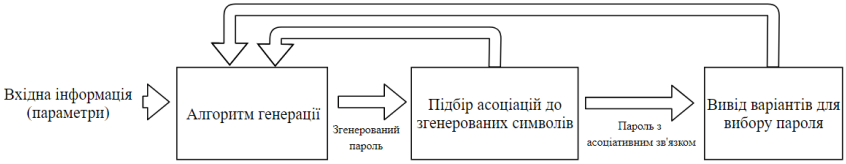

Рисунок 1 – Схема роботи інформаційної системи

Робота інформаційної системи проходить у декілька етапів. На кожному етапі виконується послідовність роботи інформаційної системи генерації безпечних паролів починаючи від ініціалізації генератора до генерації пароля.

На етапі «Алгоритм генерації» вхідна інформація служить джерелом ентропії і реалізує алгоритм на виході якого отримуємо згенерований пароль.

На етапі «Підбір асоціацій до згенерованих символів» до згенерованого паролю підбирається асоціативні слова з бази відповідно до кожного символу. Також включає можливість повернення до

попереднього етапу, якщо користувача не влаштовує згенерований пароль.

На етапі «Вивід варіантів для вибору пароля» згенерований пароль з відібраними асоціативними словами, що були отримані на попередньому етапі виводяться у вікні з можливістю копіювання, або повернення до попереднього етапу.

Однією з основних части інформаційної системи є модуль генерації безпечних паролів, схема алгоритму роботи якого показано на рисунку 2.

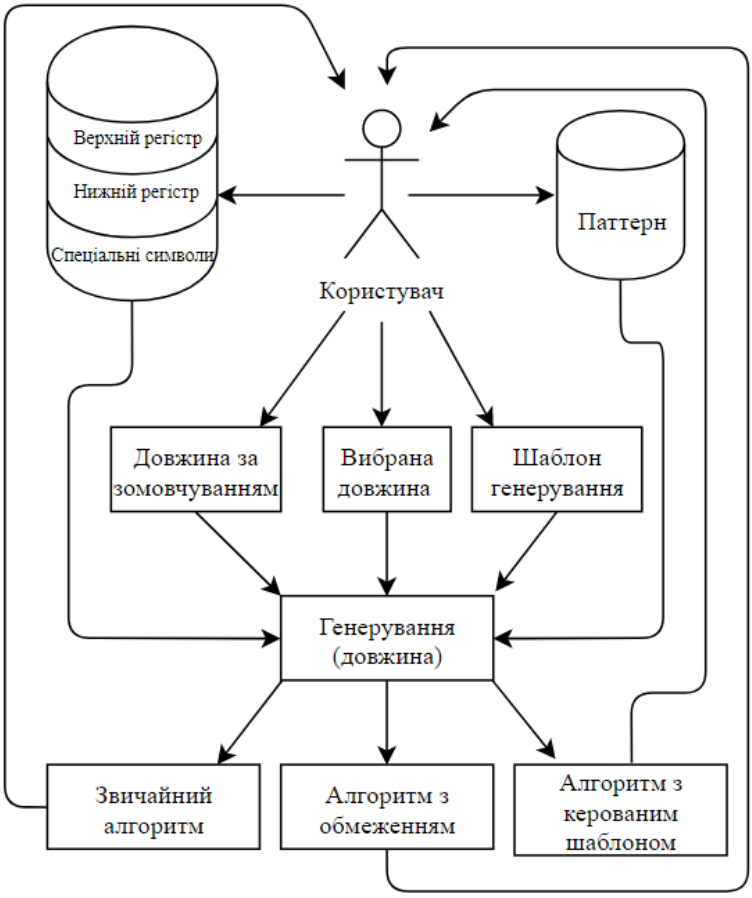

Рисунок 2 – Схема роботи алгоритму генератора паролів

При запуску генератора у користувача є можливість вибрати умови генерації – верхній регістр, нижній регістр та спеціальні символи. Також вказати, або генерувати довжину за замовчуванням (8 символів). Незалежно від здійсненного вибору користувачем система генерації підходить до кінцевого етапу своєї роботи, при якому використовуючи існуючі алгоритми генерації, з досить великою долею ентропії відбувається перетворювання рядка даної довжини в випадковий набір символів та чисел, що відповідає заданим умовам.

Виходячи з аналізу схеми роботи модуля генерації за допомогою алгоритму, стає зрозуміло, що він виконує свою ціль та включає в себе всі поставлені умови.

Для інформаційної системи генерації безпечних паролів був створений модуль підбору асоціацій до символів, що має наступний алгоритм роботи (рис. 3).

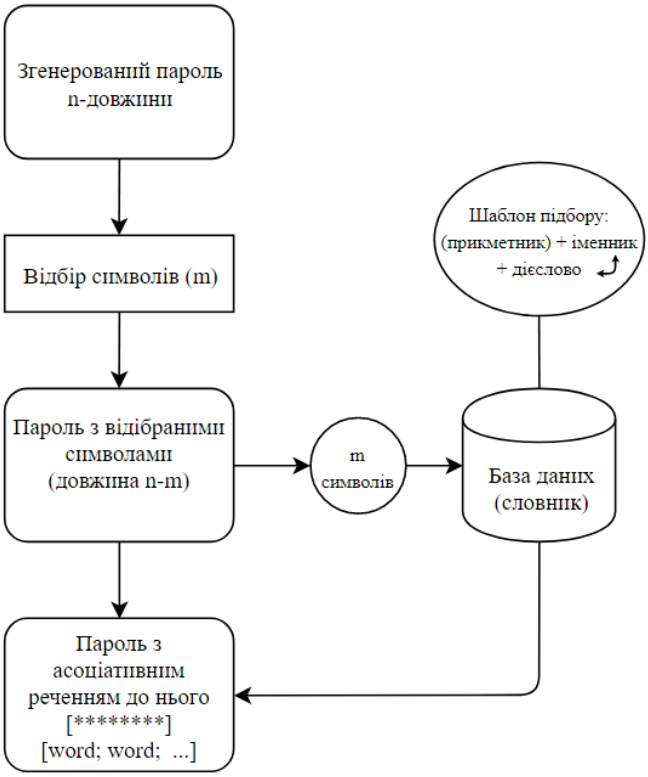

Рисунок 3 – Схема роботи модуля підбору асоціацій

Згенерований пароль довільної довжини проходить етап «відбору символів» для можливості підбирати для допустимих символів асоціативні слова (де "m" – кількість допустимих символів, а "n" – загальна кількість символів), після чого наступає етап в якому «пароль з відібраними символами» дає запит в «Базу даних» для отримання асоціативних слів до "m" символів. Та також передає в кінцевий етап згенерований пароль в чистому вигляді. Коли база даних(словник) отримує запит відбираються потрібні слова і будуються за «шаблоном підбору» (рис. 3) та відправляють результат на кінцевий етап в якому вони виводяться разом з паролем в вікні і пропонують представлений варіант для запам'ятовування.

Отже, інформаційна система підбору асоціацій до згенерованих символів для легкого запам'ятовування дозволить отримувати криптостійкі паролі з словами-підказками для ефективного використання. Це дозволить задіяти додаток в різних сферах для підвищення інформаційної безпеки даних. Основними перевагами розробленої інформаційної системи для генерації паролів є:

- можливість користуватися додатком, без активного з'єднання з Інтернетом;
- локальна генерація, що забезпечує максимальну конфіденційність;
- наявність функції для легкого запам'ятовування за рахунок асоціацій.

Інформаційні системі буде доступно розширення функціоналу генератора, за рахунок доповненням нових функціональних можливостей таких як вибір алгоритму генерації.

Перелік посилань

1. Криптографічний захист інформації [Електронний ресурс]. – Режим доступу: http://www.znanius.com/3851.html
2. PassGAN: A Deep Learning Approach for Password Guessing [Електронний ресурс]. – Режим доступу: https://arxiv.org/pdf/1709.00440.pdf
3. Генераторы паролей: какие существуют и насколько безопасно их использовать [Електронний ресурс]. – Режим доступу: https://vc.ru/services/48217-generatory-paroley-kakie-sushchestvuyut-i-naskolko-bezopasno-ih-ispolzovatGLEED2D
4. Generating Memorable Mnemonic Encodings of Numbers [Електронний ресурс]. – Режим доступу: https://arxiv.org/pdf/1705.02700.pdf