Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОД ТА ЗАСІБ ПІДВИЩЕННЯ СТІЙКОСТІ ТЕКСТОВИХ ПАРОЛІВ»

Виконав: студент 2 курсу, групи БС-21М
спеціальності 125 Кібербезпека
_____ А. С. Сухоребра

Керівник: к. т. н., доцент каф. ЗІ
_____ Ю. В. Баришев

Опонент: к. т. н доцент каф. ПЗ
_____ Н. П Бабюк
«22» грудня 2022 р.

Допущено до захисту

Завідувач кафедри ЗІ

д. т. н., проф.

_____ В. А. Лужецький

«22» грудня 2022 р.

Вінниця ВНТУ – 2022 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д. т. н., проф.
_____ В. А. Лужецький
«15» 09 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

1. Тема роботи: «Метод та засіб підвищення стійкості текстових паролів» керівник роботи: Баришев Юрій Володимирович, к. т. н., доцент кафедри ЗІ, затверджені наказом ректора ВНТУ №203 від «14» вересня 2022 р.

2. Строк подання студентом роботи 19 грудня 2022 року.

3. Вихідні дані до роботи:
- формат паролів — текстові;
- розробка метрики для оцінювання стійкості паролів;
- можливість користувачам коригувати рівень збільшення стійкості;
- сумісність засобу з операційними системами: mac, linux, windows.

4. Зміст текстової частини: Вступ. 1. Аналіз процесу автентифікації користувачів на основі текстових паролів. 2. Метод підвищення стійкості текстових паролів. 3. Засіб підвищення стійкості текстових паролів. 4. Тестування та експериментальне дослідження. 5. Економічна частина. Висновки. Список використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: Узагальнена схема роботи процесу генерації захищеного паролю (плакат, А4). Узагальнений алгоритм роботи програми (плакат, А4). Схема роботи алгоритму заміни символів(плакат, А4). Схема роботи алгоритму заміни символів (плакат, А4). Експериментальне оцінювання стійкості паролів (плакат, А4). Теоретична оцінка збільшення стійкості паролю (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	завдання прийняв
1	Баришев Ю. В., к. т. н., доцент каф. ЗІ		
2	Баришев Ю. В., к. т. н., доцент каф. ЗІ		
3	Баришев Ю. В., к. т. н., доцент каф. ЗІ		
4	Баришев Ю. В., к. т. н., доцент каф. ЗІ		
5	Лесько О. Й., к. е. н., проф., завідувач кафедри ЕПВМ		

7. Дата видачі завдання 01.09.2022 року.

КАЛЕНДАРНИЙ ПЛАН

/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	14.09.2022 – 17.09.2022	
2	Аналіз інформаційних джерел за напрямком дослідження, постановка завдання	18.09.2022 – 27.09.2022	
3	Аналіз предметної області	28.09.2022 – 04.10.2022	
4	Постановка задачі	05.10.2022 – 10.10.2022	
5	Розробка алгоритмів та архітектури засобу	11.10.2022 – 02.11.2022	
6	Вибір мови програмування та реалізація розроблених алгоритмів	03.11.2022 – 21.11.2022	
7	Тестування згенерованих текстових паролів та оцінка їх стійкості	22.11.2022 – 24.11.2022	
8	Розробка розділу економічного обгрунтування доцільності розробки	25.11.2022 – 01.12.2022	
9	Оформлення пояснювальної записки	02.12.2022 – 06.12.2022	
10	Попередній захист та доопрацювання МКР	07.12.2022 - 08.12.2022	
11	Перевірка магістерської роботи на наявність плагіату	09.12.2022 – 10.12.200	
12	Представлення МКР до захисту, рецензування	11.12.2022 – 21.12.2022	
13	Захист МКР	22.12.2022 – 23.12.2022	

Студент _____ (підпис) А. С. Сухоребра

Керівник роботи _____ (підпис) Ю. В. Баришев

АНОТАЦІЯ

УДК 004.056

Сухоребра А.С. Метод та засіб підвищення стійкості текстових паролів. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2022. 86 с.

Бібліогр.:34 назв; рис.: 22; табл.: 16.

Магістерська кваліфікаційна робота присвячена розробці методу та засобу покращення текстового паролю. Було проаналізовано види парольної автентифікації і встановлені напрями покращення стійкості паролю. У роботі наведено аналіз предметної області, можливості автентифікації, сучасні вимоги та методи парольної автентифікації. Розроблено математичний опис процесу покращення тестового паролю. Було розроблено та протестовано програмний засіб, який дозволив протестувати розроблений метод. Оцінено витрати на розробку та обґрунтовано економічну доцільність використання засобу

Ключові слова: пароль, автентифікація, клавіатура, система безпеки, кібербезпека.

ABSTRACT

Sukhorebra A. S. Method and tool of increasing the stability of text passwords. Master's thesis on specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2022. 86. p.

Bibliography: 34 titles; Fig.: 22.; tab.: 16.

The master's thesis is devoted to the analysis of password authentication and establishing directions for improving password strength. The work provides an analysis of the subject area, authentication possibilities, modern requirements and methods of password authentication. Development costs are estimated in the economic section.

Keywords: password, authentication, keyboard, security system, cyber security.

ЗМІСТ

ВСТУП

Комп'ютери, мережі, Інтернет є невід'ємною частиною повсякденного життя людей. Економіка планети стає все більш залежною від інформаційних технологій. Особливо гостро це почало відчуватись з появою пандемії COVID-19 [1]. Сьогодні мережа кожної компанії має доступ до Інтернету, це створює великі проблеми з безпекою, оскільки для злому комп'ютера не потрібен фізичний доступ.

Одним з основних факторів, які визначають стан захищеності тієї чи іншої системи інформаційної інфраструктури, є ефективність роботи системи управління та надання доступу користувачам і захисту інформації, що там зберігається. Для запобігання істотного матеріального та нематеріального збитку потрібні серйозні міри захист секретної та цінної інформації від несанкціонованого доступу. Головним завданням у проблемі захисту інформації в інформаційних системах від забороненого доступу є завдання розмежування функціональних повноважень. Задача спрямована на запобігання можливості зловмисника зчитувати або модифікувати інформацію, що зберігається.

Стандартна автентифікація за паролем – це найпростіша форма автентифікації, з якою всі знайомі. Вона передбачає, що користувач вводить своє ім'я користувача разом із секретним кодом або фразою-паролем, що дозволяє йому отримати доступ до мережі, облікового запису або застосунку.

Внаслідок поширеності парольної автентифікації також існує відбувається й поширення засобів для автоматизованого підбору паролів. Водночас паролі, створені на основі послідовності випадкових чисел, є складними для запам'ятовування, тому користувачі нехтують правилами кібергігієни, наприклад, записуючи паролі на стікери та розклеюючи їх до моніторів [2]. Часто це з’ясовується під час аудиту безпеки [3]. Саме тому актуально розробити метод та програмний засіб, які дозволятимуть користувачам вводити прості і легкі для

запам'ятовування слова чи словосполучення та будувати на їх основі стійкі паролі.

Об’єктом дослідження є процес автентифікації користувачів інформаційних систем.

Предметом є метод і засоби підвищення стійкості паролю.

Мета магістерської кваліфікаційної роботи підвищити стійкість зрозумілих для користувачів текстових паролів.

Для досягнення мети необхідно розв’язати такі задачі:

– проаналізувати стандартні методи парольної автентифікації;

– проаналізувати особливості використання парольної автентифікації;

– проаналізувати сучасні вимоги до паролів та можливості алгоритмів автентифікації;

– розробити метод покращення стійкості текстових паролів;

– формалізувати модель оцінювання стійкості покращених паролів;

– розробити програмний засіб, шо реалізує запропонований метод;

– виконати тестування розробленого програмного засобу.

Наукова новизна магістерської роботи полягає в тому, що: удосконалено метод генерування текстових паролів, що відрізняється від відомих тим, що на основі парольної фрази користувача відбувається внесення замін символів та випадкових символів, що дозволяє досягти більшої стійкості зрозумілих для користувачів текстових паролів.

Практична цінність роботи: засіб підвищення стійкості текстових паролів.

Результати магістерської кваліфікаційної роботи доповідались на таких конференціях: XLIX Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії [3], L Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії [4], XLVII Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії [5] .

1 АНАЛІЗ ПРОЦЕСУ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ НА ОСНОВІ ТЕКСТОВИХ ПАРОЛІВ

1.1 Аналіз методів автентифікації користувачів

Одним з основних факторів, що визначають стан захищеності тієї чи іншої системи інформаційної інфраструктури, є ефективність роботи системи управління та надання доступу користувачам та захисту інформації, що там зберігається. Для запобігання істотного матеріального та нематеріального втрат потрібні серйозні міри захист секретної та цінної інформації від несанкціонованого доступу. Головним завданням проблеми захисту інформації в інформаційних системах від забороненого доступу є завдання розмежування функціональних повноважень. Завдання спрямоване на запобігання можливості зловмисника зчитувати чи модифікувати інформацію, що зберігається. Дії щодо захисту інформації від несанкціонованого доступу включають [6] :

– недопущення злодія до ІС, засноване на засобах розпізнавання користувача;

– створення спеціального забезпечення для захисту інформації;

– використання спеціальних засобів захисту інформації від несанкці-онованого доступу

– В результаті аналізу виявлено такі основні засоби забезпечення захисту інформації від несанкціонованого доступу [6]:

– законодавчі, організаційні та морально-етичні засоби;

– фізичні та інженерно-технічні засоби;

Законодавчі, організаційні та морально-етичні засоби мають низьку стійкість без підтримки фізичних, технічних та програмних засобів. Також виявлено, що вони володіють високою залежністю від суб'єктивних факторів, наприклад, від загальної організації роботи на підприємстві або в організації [7].

Виявленими недоліками фізичних та інженерно-технічних засобів є висока вартість, необхідність регулярного контролю та проведення регламентованих робіт, можливість подачі помилкових небезпек.

Виявлені переваги апаратних та програмних засобів: надійність, незалежність від суб'єктивних факторів, здатність до модифікації та розвитку, універсальність. Виявлено такі недоліки, які виявляються у різних видах даних засобів: висока вартість, залежність від типу обладнання, недостатня гнучкість[8].

Одним із напрямків застосування програмно-апаратних засобів є системи контролю та управління доступом. Для успішного функціонування системи контролю та управління доступом до ІС необхідно вирішення двох завдань: Зробити неможливим обхід системи управління та розмежування доступу. Гарантувати ідентифікацію користувача, який здійснює вхід до системи. Зазначені завдання виконуються шляхом проведення наступних процесів контролю та управління доступом, що застосовуються до користувача:

– ідентифікацію, тобто, надання суб'єктам індивідуального та унікального доступу.

– автентифікацію, тобто підтвердження автентичності ідентифікації суб'єкта з метою доказу того, що суб'єкт є саме тим, ким він представився. Таким чином зроблено висновок про те, що забезпечення інформаційної безпеки ключової системи залежить від якості функціонування процесів автентифікації та ідентифікації користувачів[8].

Організації та підприємства наразі як ніколи залежать від надійної роботи своїх інформаційних систем, які стали ключем до їх успіху та ефективності. У той час як залежність від інформаційних систем, яка постійно зростає, створює нагальну потребу збирати інформацію та робити її доступною, поширення комп’ютерних технологій також створило можливості для недоброзичливців порушувати цілісність і валідність інформаційних систем [9].

Незважаючи на широке використання паролів, мало уваги приділено характеристикам їх фактичного використання паролів. Паролі забезпечують першу лінію захисту від несанкціонованого доступу до комп’ютера та особистої інформації. Чим надійніший пароль, тим більш захищеним буде комп’ютер від хакерів і зловмисного програмного забезпечення.

Як було зазначено раніше, виділяють такі методи автентифікації користувачів [10]:

– знання певної інформації, наприклад, пароль, PIN-код, особисту інформацію;

– наявність чого-небудь – фізичний предмет, наприклад, мобільний телефон чи карта;

– біометричні дані, такі як відбитки пальців, сканування сітківки ока, геометрії обличчя.

Автентифікація за паролем – це найпростіша форма автентифікації. Вона передбачає, що користувач вводить своє ім'я разом із секретним кодом або фразою-паролем, що дозволяє йому отримати доступ до мережі, облікового запису або застосунку. Теоретично, якщо пароль зберігається в секреті та безпеці, несанкціонованого доступу можна буде запобігти. Кіберзлочинці використовують програми, які пробують тисячі потенційних паролів, що дозволяє отримати доступ при спробі ввести правильний пароль. Автентифікація, найчастіше, відбувається на основі особистих даних, таких як: пароль, PIN-код, особиста інформація тощо.

Біометрична автентифікація стає все більш популярною, оскільки вона зазвичай використовується на смартфонах, а також деяких ноутбуках. Вона спирається на фізичні характеристики користувача щодо його ідентифікації. Наприклад, біометрична автентифікація може використовувати відбитки пальців, сканування сітківки або райдужної оболонки, а також розпізнавання обличчя та голосу. Це високонадійна форма аутентифікації, оскільки немає двох з однаковими фізичними характеристиками. Біометрична автентифікація - це ефективний спосіб точно дізнатися, хто входить до системи.

Ще однією її перевагою є те, що користувачам не потрібно мати картку, ключ або мобільний телефон. Їм навіть не обов'язково пам'ятати свій пароль. Однак варто відзначити, що біометричні системи безпечніші в парі з паролем.

На жаль, біометричні системи мають недоліки. По-перше, вони дуже коштовні в установці та вимагають спеціального обладнання, такого як

сканери сітківки ока або зчитувачі відбитків пальців. Є також побоювання щодо конфіденційності біометричних систем. Деякі користувачі відмовляються від можливості поділитись своєю біометричною інформацією з компанією. Таким чином, системи біометричної автентифікації найбільш поширені в середовищах, що потребують найвищого рівня безпеки, таких як сектори розвідки та оборони.

Перелічені методи базуються на використанні різних даних для автентифікації, так званих факторів. За кількістю факторів методи автентифікації поділяються на такі [11]:

- однофакторна автентифікація – використовується лише один раунд автентифікації під час якого користувач надає один із SYK, SYH, SYA факторів, як підтвердження своєї автентичності;

- багатофакторна автентифікація – цьому типі автентифікації необхідно автентифікуватуся кілька разів, надаючі різні фактори.

В останні роки було розроблено широкий спектр методів автентифікації, включаючи двофакторну аутентифікацію, біометрію, CAPTCHA та багато інших. Двофакторна автентифікація (2FA) або форма багатофакторної автентифікації базується на паролях для створення більш стійкого рішення безпеки. Вона вимагає, щоб користувач автентифікував себе за допомогою того, що його відомо, та того, що він має. Банкомати були однією з перших систем, що використовують двофакторну автентифікацію [12], тому що вони вимагають як вставки дебетової картки, так і PIN-коду.

За типом факторів автентифікація поділяється на:

– Автентифікація на основі пароля : у цьому типі автентифікації використовується тільки пароль, додаткова автентифікація не потрібна. Підтвердження відбувається за допомогою спеціальних символів, альфа-цифр і багатьох інших. Крім того, вони можуть бути комбінацією літер футів тощо.

– Біометрична автентифікація : цей тип використовується державними та приватними організаціями, допомагає їм легко автентифікувати будь-якого

користувача. Такий спосіб поділений на декілька типів: сканер очей, відбиток пальця, сканер виразу обличчя.

– Автентифікація на основі токенів : тут створюється токен доступу на основі введених даних. Після того, як вказуються зазначені облікові дані, формується зашифрований токен, який має зазначений термін дії.

Для комп'ютерної безпеки цей метод зазвичай вимагає, щоб користувач ввів своє ім'я користувача, пароль та одноразовий код, який буде відправлено на фізичний пристрій. Код може бути надісланий на мобільний телефон за допомогою текстового повідомлення або може бути згенеровано за допомогою мобільного додатка.

Двофакторна автентифікація — чудовий варіант для MSP (managed service provider) та інших підприємств, оскільки вона додає додатковий рівень безпеки, який хакерам буде складно зламати. Навіть якби хакер зміг вгадати пароль, ймовірність того, що він, одночасно з цим, отримає доступ і до одноразового коду, відправленого на пристрій - низька.

Не в усіх випадках можна покладатися на мобільні телефони, натомість можливо використовувати систему автентифікації за допомогою токенів. Вони використовують спеціальний фізичний пристрій забезпечення двофакторної аутентифікації. Це може бути ключ, який вставляється в USB-порт мобільного пристрою, або, можливо, смарт-карта з радіочастотною ідентифікацією або чіп зв'язку ближнього радіусу дії.

Для забезпечення безпеки системи токенів дуже важливо, щоб фізичний пристрій автентифікації (тобто електронний ключ або смарт-картка) не потрапили до чужих рук. Системи на основі токенів, як правило, дорожчі, ніж інші методи автентифікації за паролем, тому що вони вимагають придбання спеціального обладнання, однак вони більш безпечні.

Оцінка методів автентифікації користувача на основі зручності використання, безпеки та можливості розгортання.

Кожен метод автентифікації користувача зазвичай можна оцінити за такими трьома ключовими параметрами:

Зручність використання: наскільки природним і безпроблемним для кінцевого користувача є використання цієї автентифікації?

Безпека визначає**:** наскільки важко зловмиснику обійти автентифікацію

Можливість розгортання: наскільки легко розгортати для всіх користувачів на різних платформах, пристроях, у регіонах тощо? Важливим фактором є те, чи є сценарій використання B2C чи B2E, тобто чи є кінцевий користувач споживачем чи працівником.

Також існує три категорії методів автентифікації користувачів:

Щось, що знає (something you know - SYK) - секрет, наприклад, пароль або секретне запитання. Зазвичай їх найлегше розгорнути на всіх пристроях і платформах, але вони не будуть безпечними, оскільки є легкою мішенню для фішингу та інших хакерів [13] .

Щось, чим володіє (something you have – SYH) – зазвичай певний пристрій, наприклад ключ, сумісний з FIDO. Зазвичай вони захищені від фішингу та інших зломів, оскільки закритий ключ ніколи не залишає пристрій автентифікації. Однак вони схильні до фізичних крадіжок і непрості у використанні в сценаріях B2C, оскільки споживач зазвичай не має спеціальних пристроїв автентифікації.

Щось, що характеризує (something you are - SYA): це в основному біометричні методи, такі як відбиток пальця або розпізнавання обличчя. Зазвичай вони найбільш природні для використання для кінцевих користувачів, але дуже сильно залежать від основного пристрою чи платформи.

Порівняння основних методів парольної автентифікації таких як: Apple Face [14], Розпізнавання обличчя [15], Розпізнавання відбитків пальців [16], FIDO 2 U2F [17], FIDO 2 [18], SMS OTP [19], OATH OTP [20], Паролі, Секретні питання, Особиста інформація, Email OTP» наведена у таблиці 1.1

Таблиця 1.1. Основні методи автентифікації користувачів

Методи автентифікації	Категорія	Зручність використання	Безпека	Можливість розгортання	Стислий опис
Apple Face ID	SYA	Висока	Висока	Низька	Безпечний і простий у використанні, але корисний лише на деяких пристроях Apple, не надто сумісний між програмами. наприклад ще не підтримує такий стандарт, як FIDO2, ще навіть не підтримується на Macbook.
Розпізнавання обличчя	SYA	Висока	Середня	Низка	Загальне розпізнавання обличчя – непостійна безпека, сильно залежить від апаратного та програмного забезпечення пристрою. наприклад Безпека розпізнавання обличчя Android значною мірою залежить від марки пристрою.
Розпізнавання відбитків пальців	SYA	Середня	Середня	Низка	Загалом безпечніше та зручніше розгортати, ніж розпізнавання обличчя, з кожним роком стає все зручніше. Практично всі смартфони мають досить пристойний сканер відбитків пальців.
FIDO 2 U2F	SYH	Середня	Середня	Низка	Означається лише як сильний другий фактор, залежить від сумісних пристроїв, таких як Yubikey, тому широко використовується у випадках використання B2E, але не може використовуватися в B2C.

Продовження табл.1.1

Методи автентифікації	Категорія	Зручність використання	Безпека	Можливість розгортання	Стислий опис
FIDO 2	SYH	Середня	Висока	Низка	Використовує біометричні автентифікатори та намагається зробити їх сумісними на різних пристроях, працюючи з усіма користувачами.
SMS OTP	SYH	Низка	Середня	Висока	Не дуже безпечний, оскільки схильний до атаки обміну SIM-картою, але активно використовується як другий фактор у сценаріях B2C, оскільки кожен користувач має смартфон.
OATH OTP (токени)	SYH	Низка	Висока	Середня	Досить безпечно, але потребує програми Authenticator, і користувач має знати, як її налаштувати.
Паролі	SYK	Низька	Низька	Середня	Найбільш поширений через історію та можливість розгортання.
Секретні питання	SYK	Середня	Низька	Середня	Достатньо поширений, але слабший за паролі, оскільки особиста інформація багатьох користувачів - загальнодоступна
Особиста інформація	SYK	Середня	Низька	Висока	Не рекомендується до використання, найменш безпечний метод з наведених
Email OTP	SYK	Низька	Середня	Середня	Метод для сценаріїв B2C, як і SMS, не залежить від іншого пристрою, але значною мірою покладається на ефективність і безпеку служби електронної пошти користувача.

Наведені стандартні методи парольної автентифікації, згідно до таблиці обрання одного методу автентифікації не буде доцільним рішенням. Варто обирати декілька методів, базуючись на кінцевому призначенні.

1.2 Аналіз сучасних вимог до паролів

Найкращі методи роботи з паролями змінилися за останнє десятиліття, але багато компаній та користувачів застрягли у використанні застарілих рекомендацій. Нижче наведено передові методи роботи з паролями для організацій на сьогоднішній день відповідно до рекомендацій NIST [21]:

– Необхідно використовувати автономні або інтегровані інструменти перевірки паролів, щоб перевірити якість пароля, замість того, щоб покладатися на складні буквено-цифрові символи та символи.

– Дозволена довжина пароля повинна бути принаймні 64 символами, а не обмежена 8-10 символами.

– Треба робити регулярну зміну наявних паролів

– Використання запитань-підказок для відновлення пароля, неприйнятно, оскільки соціальні мережі та відсутність конфіденційності даних допомагають хакерам легко знаходити відповіді.

– Використання менеджерів паролів, це добра практика, дозвольте копіювати та вставляти дані в поля введення.

– Багатофакторна автентифікація (MFA), щоб додати ще один рівень захисту шляхом підтвердження входу.

Окрім стандартизованих NIST рекомендацій, які були розроблені на основі їх аудиту [3], за останній час більшість компаній запровадили те, що вони вважають основними критеріями паролів. Зазвичай мають критерії такі:

– складні паролі повинні складатися з алфавітних (великих і малих) і цифрових символів на додаток до спеціальних символів і подібних символів;

– необхідно регулярно змінювати паролі.

– нові паролі, повинні бути такими, що раніше не використовувалися.

Ці вказівки настільки широко прийняті, що вони визначені в стандарті безпеки даних індустрії платіжних карток (PCI DSS) [22]. Але, як і у випадку з усіма зрілими технологічними політиками, важливо час від часу відступати й оцінювати, чи вони все ще мають сенс у нашому середовищі, що розвивається. Потрібно відмовитися від деяких найкращих практик щодо паролів, які використовуються протягом десятиліть, і застосувати нові норми до практик керування паролями.

Національний інститут стандартів і технологій (NIST) опублікував переглянуті рекомендації щодо цифрової ідентифікації, у яких описано, що на сьогоднішній день вважаються передовими методами використання паролів. Оновлені практичні поради щодо керування паролями згідно NIST:

– Реєстрація та підтвердження особи
– Автентифікація та керування життєвим циклом цифрової ідентифікації

Нижче наведені деякі з найпоширеніших найкращих практик щодо паролів, згідно з останніми рекомендаціями.

Здається, завжди необхідно було вибирати паролі, які містять різні цифри, великі та малі літери та спеціальні символи, щоб зробити пароль складним. Однак NIST заявив, що це не призводить до створення надійніших паролів, і така практика повинна бути замінена більш динамічною підтримкою вибору пароля.

1.3 Аналіз методів та засобів генерування паролів

NIST рекомендує організаціям підтримувати користувачів у виборі кращих паролів, перевіряючи вибрані паролі на відомі слабкі паролі та витік даних про порушення. Якщо не можливо виконувати перевірку пароля під час того, як користувачі створюють або змінюють свої паролі, обов’язково забезпечте регулярну перевірку надійності пароля. Наявність таких інструментів, як HashCat [23] і подібних інструментів перевірки паролів, робить перевірку якості підбору пароля досить легкою.

Також можна побачити, що деякі постачальники інтегрують таку функціональність у свої продукти. Microsoft, наприклад, додала позначку «Ризикований вхід» для користувачів, які входять у свій Azure Active Directory за допомогою витоку облікових даних [24]. Необхідно шукати нові функції в системі керування обліковими записами користувачів, оскільки деякі інші постачальники починають інтегрувати цю функцію.

Довгий час зустрічалось те, що пароль міг бути не коротшим або довшим за 8-10 символів. Це можна побачити в деяких великих організаціях у всьому світі, безсумнівно, через обмеження застарілих систем. NIST чітко рекомендує довжину пароля. Це означає, що паролі повинні бути дозволені щонайменше з 64 символів. Довші фрази переважають над коротшими безглуздими паролями, коли йдеться про безпеку, а також їх легше запам’ятати. Легше було б легше запам’ятати щось на зразок *AllCarsAreBeautifull* порівняно з чимось на зразок *a@dcla98pL*.

NIST відмовився від широко поширеної практики регулярної зміни пароля на випадок, якщо хакери отримають інформацію без відома користувача. Аргументом проти цієї практики є властивість людини вибирати послідовність або шаблон пароля, щоб полегшити навантаження із запам’ятовування паролів. Отже, якщо мати тенденцію додавати число або інший додатковий символ у кінці свого поточного пароля кожного разу, коли необхідно змінити пароль це буде створювати слабкий пароль.

Популярна тенденція відновлення забутих паролів полягає в тому, що користувачі можуть скидати паролі, якщо вони успішно відповідають на запитання підказки. Якість запитань-підказок часто може залишати бажати кращого. Низький рівень ентропії в поєднанні з усіма особистими даними, які зараз поширюються в соціальних мережах, послаблює використання підказок паролів.

NIST радить припинити використання запитань-підказок як засобу, щоб допомогти користувачам відновити доступ до облікового запису. Більш просунутою формою захисту пароля є багатофакторна автентифікація. Apple

використовує його, і багато інших організацій також пропонують його. Цей метод без пароля, який використовується для входу в систему, дозволяє ідентифікувати когось за обличчям, сіткою ока, рукою або відбитками пальців, серцебиттям, голосом, місцем розташування, часом і цифровим сертифікатом, апаратним маркером USB тощо. Додаткові рівні захисту знижують ризик злому.

Наразі деякі сайти не дозволяють користувачам вставляти свої паролі в поля форми, тим самим порушуючи автоматичне використання менеджерів паролів.

Слід заохочувати та підтримувати використання менеджерів паролів, гарантуючи, що користувачі можуть вставляти паролі в поля для введення даних. Менеджери паролів (також звані сховищами паролів) генерують, синхронізують, створюють резервні копії та зберігають паролі на кількох програмах і пристроях. Усе це робиться в зашифрованому вигляді для потужної додаткової безпеки.

Проблема з генеруванням випадкового, незламного пароля полягає в тому, що такі паролі важко запам’ятати. Якщо вводити лише символи без асоціацій - це справді випадкова мода — тоді, імовірно, такий пароль буде так само важко запам’ятати, як комусь зламати. Тож має сенс використовувати, здавалося б, випадковий пароль, який майже неможливо розпізнати для злому програмного забезпечення, але який буде знайомим і асоціативним. Нижче наведені відомі методи генерації паролю.

Експерт із безпеки Брюс Шнайєр ще в 2008 році запропонував метод пароля, який він рекомендує досі [25]. Це працює так: необхідно взяти речення та перетворіть його на пароль. Речення може бути будь-яким, або особистим, або таким що запам’ятається. Необхідно взяти слова з речення, потім скоротити і скомбінувати їх унікальними способами, щоб створити пароль, наприклад: W8!ICr8Smth = (Wait I create sometheing) «Почекайте! Я створю що-небудь!»

Методи запам’ятовування та мнемонічні пристрої можуть допомогти запам’ятати незламний пароль. Принаймні таку теорію висунули комп’ютерні вчені Університету Карнегі-Меллона, які пропонують використовувати метод «Людина-Дія-Об’єкт» (ЛДО) для створення та зберігання незламних паролів.

ЛДО здобув популярність завдяки бестселеру Джошуа Фоера «Місячна хода з Ейнштейном» [26]. Метод виглядає так:

Необхідно обрати зображення цікавого місця, наприклад, гора Рашмор та обрати фотографію знайомої або відомої людини, наприклад - гурт Nirvana та уявити якусь випадкову дію разом із випадковим об’єктом (Nirvana керує формою для желе на горі Рашмор).

ЛДО метод запам'ятовування має когнітивні переваги – мозок краще запам’ятовує візуальні, спільні підказки та дивовижні, незвичайні сценарії. Коли створюються та запом’ятовується кілька історій ЛДО, то їх можна використовувати для створення паролів.

1.4 Постановка задачі

Як показав наведений аналіз є багато різних способів, методів та рекомендації до створення стійкого та надійного паролю. Метою роботи є підвищення стійкості зрозумілих для користувачів текстових паролів, з урахуванням наведеної інформації, а саме: стандартні методи та особливості використання парольної автентифікації, сучасні вимоги до паролів та можливості алгоритмів автентифікації. На основі проведеного аналізу буде розроблено програму для підвищення стійкості паролів, яка буде враховувати і включати у себе сучасні правила та рекомендації до парольної автентифікації.

1.5 Висновки до розділу

У першому розділі магістерської кваліфікаційної роботи були розглянуті та проаналізовані особливості використання, сучасні вимоги до паролів, також розглянуто алгоритми автентифікації. При аналізі літератури та написанні розділу було визначено актуальність теми, та висунутих тез.

2 МЕТОД ПІДВИЩЕННЯ СТІЙКОСТІ ТЕКСТОВИХ ПАРОЛІВ

2.1 Математичний опис процесу генерування паролю

Для виконання математичного опису процесу генерування паролю використано принцип синтезу цифрових автоматів [27]. Необхідно, щоб кожному елементу з отриманих множин відповідав бодай один структурний елемент схеми. Представлено процес генерування паролю у вигляді, операційного автомату, що має такі складові:

OA={DI, DO,S,Y,X}, де:

DI – множина вхідних даних;

DO – множина вихідних даних;

S – множина проміжних даних;

Y – множина виконуваних операцій;

X – множина логічних умов.

Відповідно до автоматного представлення, визначено множини для перетворення фрази від користувача у захищений пароль:

DI={T,P,D};

DO={O};

S ={S, S_G,S_Z,S_B,S_m};

Y ={G, Z, B};

X ={a};

де:

T – фраза від користувача, яка буде основою для подальших перетворень, та складання кінцевого словника, який міститиме варіанти покращеного паролю;

P – імовірність заміни, яка може задаватися користувачем для регулювання ступеню зміни паролю;

O – варіанти покращеного паролю. Множина змінених фраз від користувача передбачена для вибору необхідного словосполучення;

S – початковий стан;

S_G – визначення необхідності заміни чи додавання нового символу та основі прийнятого рішення генеруванням псевдовипадкового числа;

S_Z – заміна символами, з використанням таблиці замін a, на позиціях визначених генератором псевдовипадкових чисел;

S_N – фраза від користувача в поєднанні з символьними вставками;

S_B – фраза від користувача в поєднанні з символьними вставками та великими літерами;

S_m – фраза від користувача в поєднанні з символьними вставками та малими літерами

a – таблиця замін.

Загальна схема процесу генерування захищеного паролю представлена на рис. 2.1

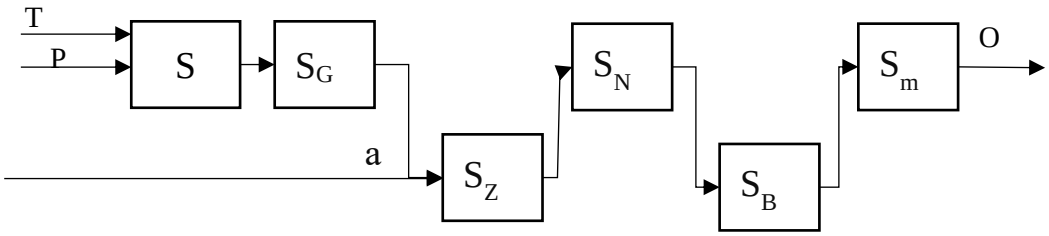


Рисунок 2.1 – Узагальнена схема роботи процесу генерації захищеного паролю

Тепер можна переходити до узагальненого опису методу генерації стійкого текстового паролю.

2.2 Узагальнений опис методу генерації паролів

Аналіз показав, що метод парольної авторизації є зручним та широко використовується в системах перевірки прав користувача. Однак такий метод передбачає наявність певних характеристик, які наводились у першому розділі роботи. Однією з головних таких характеристик є стійкість пароля та його зручність у використанні. Наявність спеціальних символів, літер різного

регістру, цифр; покращує стійкість паролів та водночас стає важчим запам’ятовування таких ключових слів. Тому пропонується метод генерування паролів, що дозволить поєднати ці дві властивості та надасть змогу користувачам на основі слова, яке б вони воліли використовувати як пароль, отримувати варіанти більш стійких паролів. Опис метода умовно поділяється на наступні кроки:

Крок 1. Користувач вводить слово або словосполучення, яке є бажаною для нього основою формування паролю.

Крок 2. Генерується псевдовипадкове число rand_n, яке масштабується відповідно до значень ймовірності. Якщо вказано символи які входять до таблиць змін – виконується замін згідно таблиць

Крок 3. Після виконання кроку 2 формується словник який містить у собі n-варіантів сгенерованних паролів, з яких можно обрати тої, що підійде найбільше.

Крок 4. Якщо кроки 2 та 3 були виконані для кожного символу, введеного користувачем, то виконання алгоритму завершується, інакше відбувається перехід до наступного символу і перехід до кроку 2.

Як видно з узагальненого опису методу, його важливим елементом є генерування псевдовипадкових послідовностей. Зокрема такі ключові особливості методу як виконання замін та додавання символів повністю покладачються на коректність його реалізації. Таким чином показники якості методу залежать від показників якості генератора. Саме тому доцільно визначити вимоги до методів генерування псевдовипадкових послідовностей чисел, виходячи із особливостей запропонованого узагальненого опису методу, та проаналізувати можливі шляхи реалізації відповідно до цих вимог.

2.3 Обґрунтування вибору способу генерування псевдовипадкових чисел

Генератори та їх реалізації в бібліотеках підпрограм повинні задовольняти низку вимог.

Вимога 1. Статистична стійкість. Значення на виході генератора мають бути рівномірно розподілені, а кореляція відсутня. Іншими словами, всі значення під послідовністю фіксованої довжини повинні мати ту саму ймовірність появи в послідовності, що видається генератором.

Вимога 2. Довгий період. Період генератора має бути досить великим, щоб не бути вичерпаним протягом місяців комп'ютерного часу. Чисельний експеримент на суперкомп'ютері може задіяти 109 випадкових чисел в секунду протягом багатьох годин, тому 1013-1016 випадкових чисел можуть робити внесок у результат обчислювального експерименту.

Вимога 3. Змінний діапазон чисел. Для цілих чисел існує рівномірний вибір із діапазону. Для послідовностей існує рівномірний вибір випадкового елемента, функція для створення випадкової перестановки списку на місці та функція для випадкової вибірки без заміни.

Вимога 4. Рівномірність розподілу. Існує ряд методів, які задовільняють критеріям перевірки «випадковості» побудови таких чисел з розподілом близьким до рівномірного (хоча ці числа взаємозалежні). Зазвичай використовують деяке рекурентне співвідношення. Це значить, що кожне наступне число $\alpha k+1$ утворюють із попереднього αk (або групи попередніх чисел), використовуючи деякий алгоритм, який використовує арифметичні та логічні операції.

Вимога 5. Обчислювальна простота. Алгоритм, який, який прийняв на вході число N, дозволяє або не підтвердити припущення складності числа, або точно стверджувати його простоту. У другому випадку він називається справжнім тестом простоти. Отже, тест простоти є лише гіпотезу у тому, що й алгоритм не підтвердив припущення складності числа N, це число може бути простим з певною ймовірністю. Це визначення має на увазі меншу впевненість відповідно до результату перевірки справжньому стану речей, ніж справжнє випробування на простоту, яке дає математично підтверджений результат.

Безпека деяких алгоритмів шифрування залежить від стійкості генератора випадкових чисел завдяки якому формується ключ або послідовність біт. Шифри з досконалою стійкістю потребують повністю випадкового ключа такої ж

довжини, як і вихідний ключ. Проте у більшості випадків, насправді випадкові послідовності біт необхідної довжини не доступні. Тому були наведені вимоги для генераторів псевдовипадкових послідовностей. Такі послідовності можуть справляти враження випадкових, але отримані вони в результаті роботи детермінованого алгоритму.

У роботі буде використовуватися бібліотека random із мови програмування Python [29]. Майже всі функції модуля залежать від базової функції random(), яка рівномірно генерує випадкове число з плаваючою точкою в напіввідкритому діапазоні [0.0, 1.0). Python використовує Mersenne Twister як основний генератор. Він створює 53-розрядні числа з плаваючою точністю та має період 2**19937-1. Базова реалізація в C є одночасно швидкою та потокобезпечною. Mersenne Twister є одним із найбільш протестованих генераторів випадкових чисел [30]. Однак, будучи повністю детермінованим, він не підходить для всіх цілей і зовсім непридатний для криптографічних цілей. Функції, які надає цей модуль, насправді є зв’язаними методами прихованого екземпляра класу random.Random. Також є можливість створити власні екземпляри Random, щоб отримати генератори, які не мають спільного стану.

Якщо проводити генерацію чисел у діапазоні [0-100] при використанні рекурентного співвідношення, кожне наступне число αk+1 утворюють із попереднього αk (або групи попередніх чисел), отримується можливість досягнення рівномірного закону розподілу, що в свою чергу, дозволить зробити коректні заміни символів. Для формування псевдовипадкових чисел в комп'ютері може використовуватися алгоритмічний спосіб. При цьому способі випадкові числа формуються за допомогою спеціальних програм.

Переваги методу:

– в даний час пропонується досить генераторів, що генерують випадкові числа, перевірених практикою і, отже, не потребують особливих перевірках;

– можна багаторазово відтворити одну і ту ж послідовність;

– в пам'яті комп'ютера зберігається тільки програма генератора, що займає, як правило, малий обсяг;

– алгоритмічний датчик може бути реалізований і апаратно, за рахунок чого істотно скорочується час формування випадкового числа і в цілому час моделювання.

Недоліки:

– на формування випадкового числа при програмної реалізації генератора потрібні витрати машинного часу;

– будь-алгоритмічний генератор може згенерувати обмежену кількість неповторюваних чисел.

Наразі, практично скрізь застосовуються алгоритмічні генератори випадкових чисел. Створення високопродуктивних комп'ютерів істотно знижує роль першого недоліку (витрати машинного часу). Другий недолік усувається використанням в одній моделі декількох генераторів випадкових чисел.

Алгоритмічні генератори не забезпечують отримання теоретично «чистої» випадковості чисел, так як їх формування йде за математичними законами.

Внаслідок цього рано чи пізно послідовність випадкових чисел стане повторюватися або виродиться. Отже, починаючи з деякого елемента послідовності, всі наступні числа дорівнюватимуть нулю.

Тому алгоритмічні генератори називають генераторами псевдовипадкових чисел, що володіють:

– статистичними властивостями випадкових чисел, які визначаються шляхом їх перевірки спеціальними тестами;

– періодичністю, тобто повторюваністю через певні проміжки часу.

Якість алгоритмічного генератора оцінюється тим, наскільки повно він задовольняє таким вимогам:

– закон розподілу формуються чисел повинен бути рівномірним ;

– числа повинні бути статистично незалежними;

– числа в послідовності не повинні повторюватися;

– формування чисел повинно займати мінімальний машинний час і мінімальний обсяг пам'яті.

Оскільки метод Mersenne Twister володіє цими перевагами, тому для задач магістерської кваліфікаційної роботи доцільно використати цей алгоритмічний генератор.

2.4 Розробка таблиці замін

Більшість відомих генераторів паролів не враховують українську мову. Адже кирилиця вже давно підтримується багатьма системами та сервісами.

Проблема не так у самому факті відсутності української мови, як у зменшенні кількості різних комбінацій. Наприклад, перебір пароля, що складається лише з цифр, займатиме 10 (кількість символів у паролі). Відповідно, якщо пароль складається з цифр і малих англійських літер, то перебір займатиме (10 + 26) (кількість символів у паролі), що дещо суттєвіше. Наприклад, перебір тризначного пароля з цифр складатиметься з 1000 комбінацій, а перебір пароля з цифр та малих англійських літер складатиметься з 36^3 комбінацій.

Таким чином, виняток 66 українських літер (малі + великі) сильно звужує область перебору. Наприклад, той самий тризначний пароль лише з українських літер (малі + великі) складається 66^3 комбінацій.

Необхідно враховувати, що більшість програм для підбору пароля просто не розраховані на українську мову, а якщо і розраховані, то рідко використовуються для перебору українських літер. Отже наявність навіть однієї української літери зробить безглуздим їх застосування. Звичайно, це не означає, що українська абетка надасть абсолютну безпеку. В даному випадку українська мова сильно збільшує складність для того хто атакує, а не робить пароль абсолютно безпечним.

Для перевірки складності паролів зазвичай використовують спеціальні контролери паролів. Контролер паролів дозволяє перевірити вразливість паролів. Контролер здійснює спроби злому пароля за такою методикою:

1.Перевірка використання як пароль вхідного імені користувача, його ініціалів і їх комбінацій.

2.Перевірка використання як пароль слів з різних словників:

– чоловічі і жіночі імена;

– назви країн і міст;

– імена персонажів мультфільмів, кінофільмів;

– спортивні терміни (назви спортивних команд, імена спортсменів, спортивний жаргон і тому подібне);

– числа (цифрами і прописом);

– рядки букв і цифр (наприклад, AA, AAA, AAAA);

– біблійні імена і назви;

– біологічні терміни;

– жаргони і лайливі слова;

– послідовність символів у порядку їх розташування на клавіатурі (наприклад, QWERTY, ASDF, ZXCVBN і так далі);

– імена комп'ютерів;

– персонажі і місця події з творів Шекспіра;

– іноземні слова, що часто вживаються;

– назви астероїдів.

3. Перевірка різних перестановок слів з такими параметрами:

– заміною першої букви на прописну;

– заміною всіх букв на прописні;

– інверсією всього слова;

– заміною букви «О» на цифру «0» і навпаки (цифру «1» на букву «l» і так далі);

– перетворенням слів на множину.

4. Перевірка різних перестановок слів

– заміна однієї рядкової букви на прописну (наприклад, michel-miChel і тому подібне – близько 400 000 слів);

– заміна двох рядкових букв на прописні (близько 1 500 000 слів);

– заміна трьох рядкових букв на прописні і так далі.

5. Для іноземних користувачів перевірка слів на мові користувача.

6. Перевірка пар слів.

Для реалізації засобу підвищення стійкості паролів потрібно обрати такі шляхи, які дозволять протистояти згаданій вище атаці. На вхід скрипту подаються слова, цифри, символи або словосполучення, на основі яких буде генеруватися пароль. Для вводу у скрипті запроваджено змінні в яких визначаємо які символи доступні для використання. Фраза, яку вводить користувач має такі обмеження щодо алфавіту, які накладаються особливістю клавіатур:

- цифри – від 0 до 9 та символів з клавіатури, що можна ввести з («!№;%:?*()&\»);

- великих\маленьких літер англійської мови (a-z/A-Z).

Використання української розкладки клавіатури для введення паролю не розглядається, оскільки, як було показано вище, це несуттєво збільшить стійкість і ускладнить введення та запам’ятовування користувачам. Крім того, низка застосунків не передбачає можливість введення літер поза латинською абеткою.

Основою для таблиці замін є інтуїтивно зрозумілі взаємозалежності між символами. Найбільш поширеними є уподобання знаку @ букві a, 0 – букві o, $ - англійській букві s, і на цифру 1. Також було додано нетривіальну, але зрозумілу взаємозаміну для словосполучення ‘and’ та логічним ‘але’. Цифри 3, 5, 7 – замінені на власні поєднання з кнопкою Shift на українській розкладці клавіатури. Розроблені заміни представлені в табл.2.1

Таблиця 2.1 – Таблиця замін

Оригінальний символ	Символ для заміни
s	$
and	&
a	@
o	0
i	1
3	#
5	%
7	?
8	*
0	_

Після розробки таблиці замін можна переходити до програмної реалізації алгоритму.

2.5 Висновок до розділу

У розділу було розроблено математичний опис процесу генерування паролю. За основу було взято принцип синтезу цифрових автоматів. Описано вхідні, вихідні дані та стани автомату. Наведено схему його роботи. Це дозволило формалізувати постановку задачі та визначити основні параметри цього процесу, що дозволило в подальшому визначити ті параметри, які можна змінювати для досягнення поставленої мети.

Запропоновано узагальнений опис методу генерації паролів, який представлено у вигляді покрокового алгоритму. Було встановлено наступні вимоги генераторів псевдовипадкових чисел: статистична стійкість, довгий період, змінний діапазон чисел, рівномірність розподілу та обчислювальна простота. На основі цих вимог було обрано генератор, що реалізується бібліотекою random із мови програмування Python. Перевагою є рівномірне генерування випадкових чисел. Було розроблено таблиці замін, які дозволять підвищити стійкість паролю.

3 ЗАСІБ ПІДВИЩЕННЯ СТІЙКОСТІ ТЕКСТОВИХ ПАРОЛІВ

3.1 Обґрунтування вибору мови програмування

Python — це популярна мова програмування загального призначення, яку можна використовувати для різноманітних програм [31]. Вона включає високорівневі структури даних, динамічні типи, динамічне зв’язування та багато інших функцій, які роблять його таким же корисним як для розробки складних програм, так і для сценаріїв або «склеюючого коду», який з’єднує компоненти разом. Завдяки повсюдному поширенню та здатності працювати майже на будь-якій системній архітектурі, Python є універсальною мовою, яку можна знайти в різних програмах.

Також в п’ятірку найпопулярніших мов входить C++. Беззаперечними перевагами якого є швидкість виконання коду, керування пам’яттю, об’єктно-орієнтовні парадигми програмування, стандартизовані бібліотеки, масштабованість та можливість низькорівневого керування. Завдяки ним ця мова набула широкого застосування в розробці ігор, операційних систем, баз даних, IoT пристроях, додатках, які пов’язані з фінансовою діяльність та медичними закладами [31].

Також популярність не поступається Java. Головними її перевагами є [31]:

- простота:
- об’єктно-орієнтовність;
- кросплатформеність;
- портативність;
- користування пам’яттю;
- підтримка багатопоточності;

Результати порівняльного аналізу наведено у таблиці 3.1.

Таблиця 3.1 — Порівняльна характеристика мов програмування

	C++	Java	Python
Продуктивність	Висока, через особливості компілювання коду	Низька, оскільки є JDK	Середня, через наявність CPython інтерпритатора
Підтримка безкоштовних інструментів розгортання Backend	-	+	+
Кросплатформеність	-	+	+
Сфера застосування	Розробка ігор IoT Сервіси пов'язані з медициною та фінансами	Web-розробка, Мобільні застосунки, Big Data, Програми для відлагодження коду	Машинне навчання, Штучний інтелект, Інженерія даних, Web-розробка Скрипти автоматизації
Можливість керування пам'яттю	+	-	+

На основі проведеного аналізу було обрано мову Python, оскільки вона дозволяє розгортати Backend, що важливо для можливості використання запропонованого засобу, як бібліотеки для розширення веб-серверів та інтеграції її до веб-застосунків. Водночас Python на відміну від Java, яка також дозволяє розгортати Backend, має вищу продуктивність та можливість керування пам'яттю.

3.2 Узагальнений алгоритм роботи програми

На початку роботи імпортується модуль random – який рівномірно генерує випадкове число з плаваючою точкою в напіввідкритому діапазоні [0.0, 1.0). З'являється можливість створити власні екземпляри Random, щоб отримати генератори, які не мають спільного стану. Клас Random також може бути підкласом, якщо планується використовувати інший базовий генератор.

Після імпорту random визначаються основні змінні:

– uppercase_letters;

– lowercase_letters;

– digits;

– symbols;

Кожна змінна містить у собі набір символів:

- uppercase_letters - великі літери з діапазону (A-Z);
- lowercase_letters – містить у собі метод який трансформує літери з uppercase_letters в нижній регістр;
- digits – містять цифри від 0 до 9;
- symbols – містить усі символи які доступні для вводу з клавіатури.

Також необхідно оголосити змінну для таблиці замін, цією змінною буде – SECURE.

Вона включає для себе набір змінних для заміни. Ця таблиця дуже легко масштабується необхідно лише додати необхідну пару (значення/значення) для наступних замін.

Для збереження у собі результати усіх змін паролів вводиться змінна list.

Функція securePass приймає один аргумент password – який є основою паролю яку вказує користувач.

Змінна securePass проходить по циклу, і надалі пароль змінюється згідно таблиці замін, a\b – служать парою для замін, після замін пароль додається до словника методом append і потрапляє до наступної функції.

Принцип роботи функції lower полягає в отриманні паролю з функції securePass, після чого методом join приєднуємо до отриманої комбінації символи нижнього регістру, після чого, отриманий результат додається до словника і все записується до змінної pass2 яка потрапляє до наступної функції.

Функція upper працює аналогічно до функції lower, але додає символи верхнього регістру, а результат передає до кінцевого словника, де зберігаються усі паролі.

Алгоритм не має обмежень на кількість символів, які вводить користувач. Заміна кожного символу буде відбуватися у циклі, кількість повторів якого залежить від довжини введеного слова, де визначатиметься чи буде замінена літера на символ з таблиці замін. Кожен результат заміни буде потрапляти до словника який призначено для зберігання усіх паролів, з моменту вводу. Тобто до початку проходу паролю до циклів, перший пароль записується у словник,

наступний пароль, після першого циклу, також додається у словник. Користувачу повинно бути доступною можливість побачити усі метаморфози з паролем від вводу – до кінцевого вигляду, і обрати той, який здається йому найбільш зручним. Алгоритм підвищення стійкості паролів продемонстровано на рисунку 3.1.

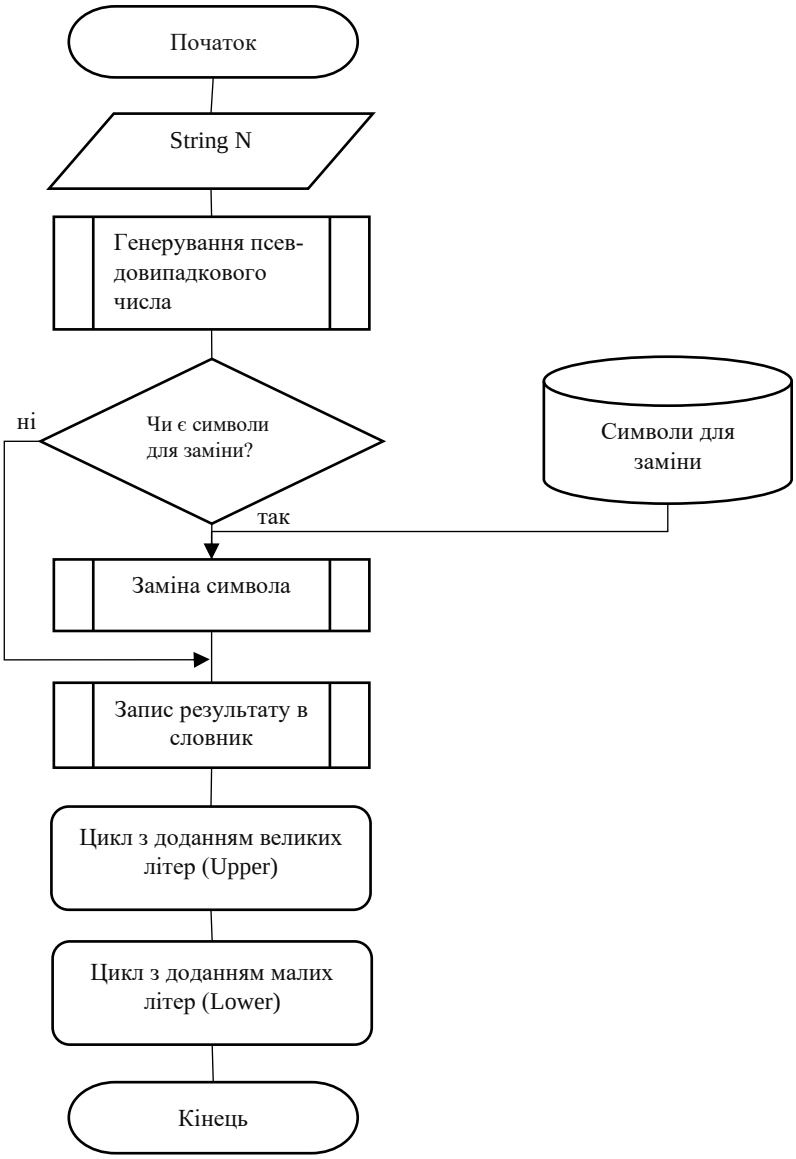


Рисунок 3.1 – Узагальнений алгоритм роботи програми

Оскільки, розроблено загальний алгоритм роботи програми, тепер слід описати роботу ключових процесів.

3.3 Реалізація замін

Для реалізації таблиці замін використовується змінна SECURE в яку додаються необхідні пари (значення літери або символу для котрого буде використана заміна та значення літери або символу яке буде використано для заміни).

У коді це виглядає таким чином, як це показано на рис. 3.2.

```
SECURE = (('s', '$'), ('and', '&'), ('a', '@'), ('o', '0'), ('i', '1'), ('3', '#'), ('5', '%'), ('7', '?'), ('8', '*'),
          ('0', '_'))
```

Рисунок 3.2 – Вигляд змінної SECURE, що представляє собою таблицю замін

Таблиця замін у мові програмування Python – легко реалізується і дуже просто масштабується, тому є можливість розширювати таблицю скільки завгодно без втрат оптимізації і продуктивності. Схема роботи алгоритму представлена на рис.3.3

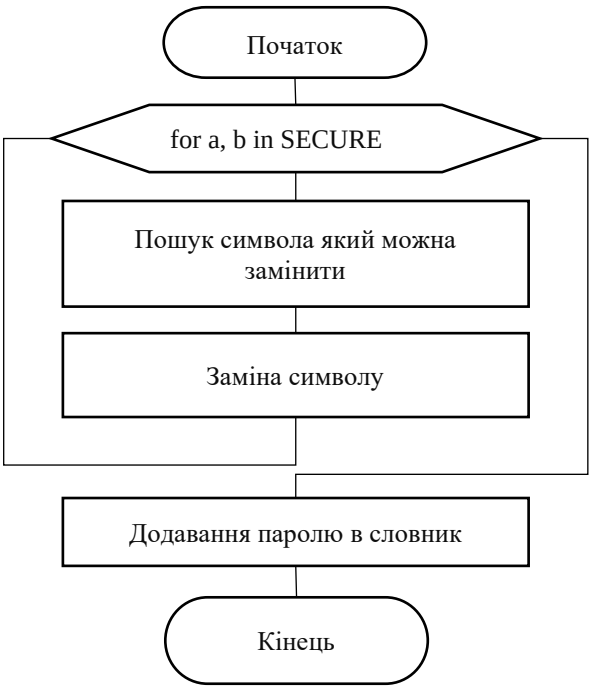


Рисунок 3.3 – Схема роботи алгоритму заміни символів

Тепер можна описати реалізацію вставки символів до покращеного текстового паролю.

3.4 Реалізація вставки символів

В основу функції вставки символів, що доступні для вводу з клавіатури, взяти змінну symbols.

Перед цим обчислюється кількість символів для вставки: довжина паролю, введеного користувачем, множиться на імовірність замін, яку теж вводить користувач. Остання представлена в коді змінною probability.

Функція symbols_s приймає на вхід пароль зі змінами та вставленими великими та малими буквами pass3 та кількість символів, що необхідно додати length. Схема роботи алгоритму представлена на рис. 3.4

Рисунок 3.4 – Схема роботи алгоритму реалізації вставки символів

Після розробки всіх необхідних алгоритмів їх слід протестувати на відповідність поставленим вимогам.

3.5 Теоретична оцінка стійкості паролів

На сьогоднішній день перспективними видаються дві методики проведення ефективної та досить надійної запобіжної перевірки паролів. Одна з них будується на основі використання марківської моделі генерування паролів. На рис. 3.5 показано спрощену версію такої моделі. Ця модель задає мову, алфавіт якої складається з трьох символів [32]. Стан системи в будь-який момент ідентифікується останнім вибраним символом. Коефіцієнти переходів з одного стану до іншого задаються ймовірностями слідування одних символів за іншими.

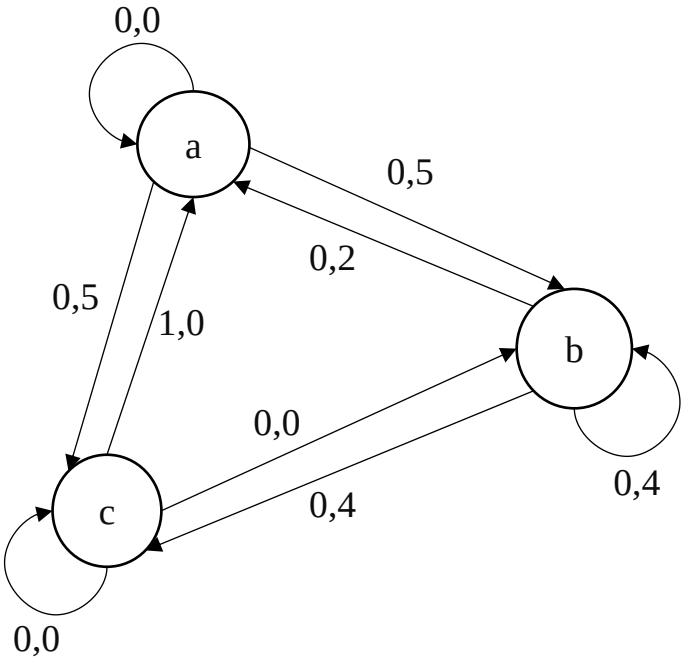


Рисунок 3.5 – Марківська модель першого порядку

Наприклад, ймовірність того, що наступною літерою буде b за умови, що поточною є літера a, в такому разі дорівнює 0,5. Розрахунок представлено у формулах 4.1, 4,2.

M=(3, {a,b,c}, T, 1), де (4.1)

$$T=\begin{bmatrix}0,0 & 0,5 & 0,5\\ 0,2 & 0,4 & 0,4\\ 1,0 & 0,0 & 0,0\end{bmatrix} \quad (4.2)$$

Загалом марківська модель задається чотирма значеннями{т, А, Т, де т позначає число станів моделі, А - простір станів, Т - матрицю ймовірностей переходів, а К - порядок моделі. Для моделі порядку К ймовірності переходу до того чи іншого символу алфавіту залежить від значень до попередніх символів.

Інший підхід передбачає використання оцінок стійкості паролі на основі математичного апарату комбінаторики.

Паролі, які створюють користувачі належать до алфавіту, який складається з англійських великих на малих букв, в поєднанні з 10 цифрами. В сумі виходить абетка з 62 символів.

Для введення з клавіатури доступно 24 спецсимвола: (), [],{},\,/ та інше. Тепер алфавіт для створення паролю збільшився до 86 символів. Розрахунки кількості всіх можливих комбінацій паролів відповідно до розміру алфавіту, та зростання їх кількості у відсотковому відношенні, представлено в табл.3.2.

Таблиця 3.2 – Порівняльна характеристика кількості всіх можливих комбінацій та їх процентне співвідношення

Довжина паролю, симв.	Кількість можливих комбінацій (алфавіт з 62 символів)	Кількість можливих комбінацій (алфавіт з 86 символів)	Зростання кількості комбінацій, %
1	62	86	138,71%
2	3844	7396	192,40%
3	238328	636056	266,88%
4	14776336	54700816	370,19%
5	916132832	4704270176	513,49%
6	56800235584	4,04567E+11	712,26%
7	3,52161E+12	3,47928E+13	987,98%
8	2,1834E+14	2,99218E+15	1370,42%
9	1,35371E+16	2,57327E+17	1900,91%
10	8,39299E+17	2,21302E+19	2636,74%
11	5,20366E+19	1,90319E+21	3657,42%
12	3,22627E+21	1,63675E+23	5073,19%

Як видно з порівняльної характеристики наглядно видно, що збільшення алфавіту та довжини пароля призводить до збільшення кількості комбінацій в 1,5 рази.

3.6 Висновки до розділу

У розділі було обгрунтовано вибір мови програмування для реалізації описаних алгоритмів. Було обрано Python з огляду на його зручність в розгортанні Backend. Це розширює можливості використання розробленої програми в якості розширення веб-серверів або інтеграції до веб-застосунків. В порівнянні з мовою програмування Java, яка також дозволяє розгортати Backend, Python має вищу продуктивність та можливість керування пам’яттю.

Було розроблено загальний алгоритм роботи майбутнього додатку. На основі проведеної розробки було визначено його ключові функції. Для кожної з них розроблені схеми роботи.

Функція , що реалізує заміни базується на таблиці замін, розробленій раніше. Такий прийом допоможе збільшити стійкість текстового пароля, причому роблячи його зрозумілим та легшим для запам’ятовування користувачем.

Функція, що реалізує вставку символів в основі своїй має значення яке є добутком довжини пароля та імовірності. Це передбачено для керування користувачем складністю текстового паролю.

4 ТЕСТУВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

4.1 Тестування коректності роботи програмного засобу

Як було зазначено вище, у користувача є можливість керувати складністю паролю. Це пояснюється тим, що вони можуть бути застосовані до різних застосунків, як для банкінгу так і для онлайн – кінотеатру. На рисунку 4.1 представлено приклад роботи програми для генерування текстового паролю з імовірністю вставок 15%.

```
Enter Your Password: master
Enter the probability for password:15
ma$ter
ma$teruA
ma$teruA?).{;'
ma$ter
ma$terdN
ma$terdN/@_'{!
m@$ter
m@$terfX
m@$terfX\@!-?$
m@$ter
m@$terzK
m@$terzK_@$}[;
m@$ter
m@$terpY
m@$terpY;({.+@
m@$ter
m@$terdX
m@$terdX_@% (&
m@$ter
m@$teraE
m@$teraE'/#%[$
m@$ter
m@$terkS
m@$terkS./ \)*
m@$ter
m@$terlI
m@$terlI{?]*%.
m@$ter
```

Рисунок 4.1 – Приклад масиву згенерованих паролів текстових паролів з ймовірністю вставок 0,15

Довжина парольної фрази master 6 букв, введена імовірність 15%. Добутком цих двох значень є 0,9, яке округлюється до 1. Слід зазначити допустиме відхилення, оскільки вибірка букв невелика, то значення заміни в середньому буде 1. Наприклад, паролі m@$ternU? , m@$terK& та m@$terJ+ мають один доданий символ в кінці, а m@$terdL\\ – два.

Для кращого розуміння було введено довший пароль та більшу імовірність вставок (рис.4.2):

```
Enter Your Password: password
Enter the probability for password:50
pa$$word
pa$$wordaZ
pa$$wordaZ@{*]?)&%
pa$$word
pa$$wordlP
pa$$wordlP} ?%;@_.
p@$$word
p@$$wordbQ
p@$$wordbQ[#_*/(;@
p@$$w0rd
p@$$w0rddE
p@$$w0rddE'.${ }%!
p@$$w0rd
p@$$w0rdtE
p@$$w0rdtE[#.$%?-;
p@$$w0rd
p@$$w0rdhE
p@$$w0rdhE_\)/$&#[
p@$$w0rd
p@$$w0rdvS
p@$$w0rdvS?-{!,* .
p@$$w0rd
p@$$w0rdlO
p@$$w0rdlO(@{)\*}]
p@$$w0rd
p@$$w0rdgT
p@$$w0rdgT]-['@?){
p@$$w_rd
```

Рисунок 4.2 – Приклад масиву згенерованих паролів текстових паролів з імовірністю вставок 0,5

Довжина паролю password 8 букв, введена імовірність 50%. В результаті середнім числом вставок має бути 4 символи.

Результат роботи програми при введенні довгого паролю та великого відсотку замін представлений на рис. 4.3. Слід зазначити, що при введених даних текстовий паролю збільшиться майже вдвічі. Довжина паролю 12 символів, а замін – 90%, добутком цих значень є число, яке округлюється до 11.

```
Enter Your Password: university
Enter the probability for password:90
univer$ity
univer$itycA
univer$itycA,!%]-\'+*&
univer$ity
univer$ityqT
univer$ityqT(-[},/'? .
univer$ity
univer$itydF
univer$itydF?!#%_)*${-
univer$ity
univer$itylY
univer$itylY']?_*[()}%
un1ver$1ty
un1ver$1tybQ
un1ver$1tybQ(.*_)/#'%&
un1ver$1ty
un1ver$1tykA
un1ver$1tykA%]$+&/\*#)
un1ver$1ty
un1ver$1tydL
un1ver$1tydL *,+#!($.;
un1ver$1ty
un1ver$1tyvG
un1ver$1tyvG#(+;[$&]?}
un1ver$1ty
un1ver$1tyiV
un1ver$1tyiV@_$*% {/]-
un1ver$1ty
```

Рисунок 4.3 – Приклад масиву згенерованих паролів текстових паролів з 90-відсотковою імовірністю замін

Також було передбачено заборони введення занадто коротких паролів, менше 5 символів, інакше ні імовірність замін, ні вставки не будуть дієвими. Приклад роботи програми наведено на рис. 4.4

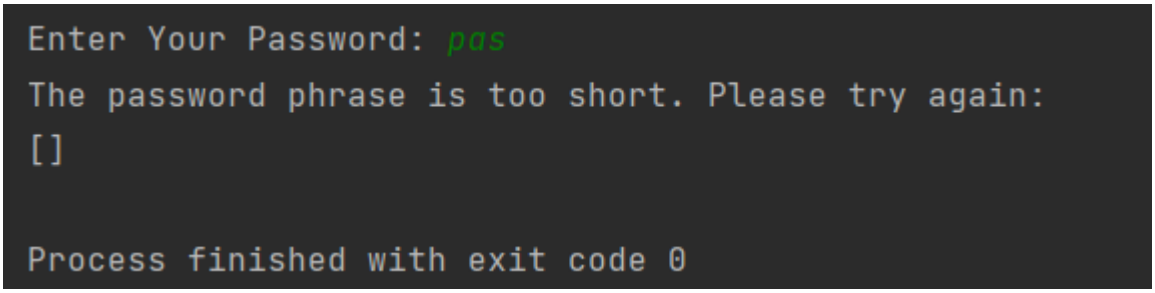


Рисунок 4.4 – Вигляд відповіді програми на спробу користувача ввести пароль нижче порогового значення

Після генерування паролів, необхідно впевнитися, що їх стійкість підвищилася.

4.2 Оцінка стійкості текстового паролю

Для оцінки стійкості було обрано ресурс 2ip.io/ua/passcheck/.

На рис.4.5 зображено пароль, який вводить користувач для подальшої зміни, та приблизний час його зламу.

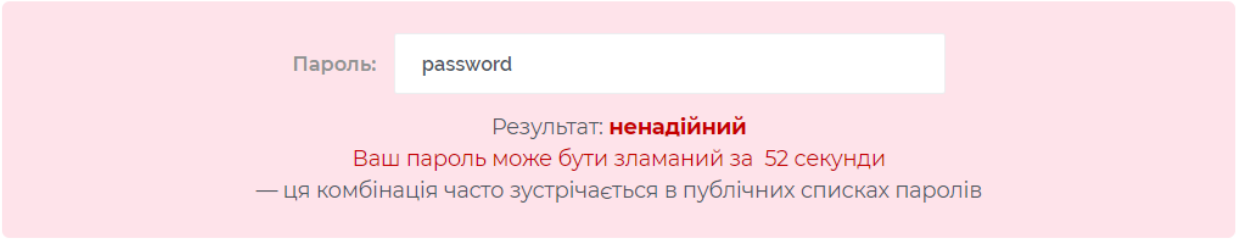


Рисунок 4.5 – Стійкість початкового паролю

Також слід використати сервіс haveibeenpwned.com. Він перевіряє паролі та електронні пошти на предмет компрометації: чи не був пароль користувача викрадений чи зламаний? На основі більше десятка списків вже викритих паролів haveibeenpwned.com проводить свої пошуки. На рис. 4.6 зображено результат перевірки початкової фрази.

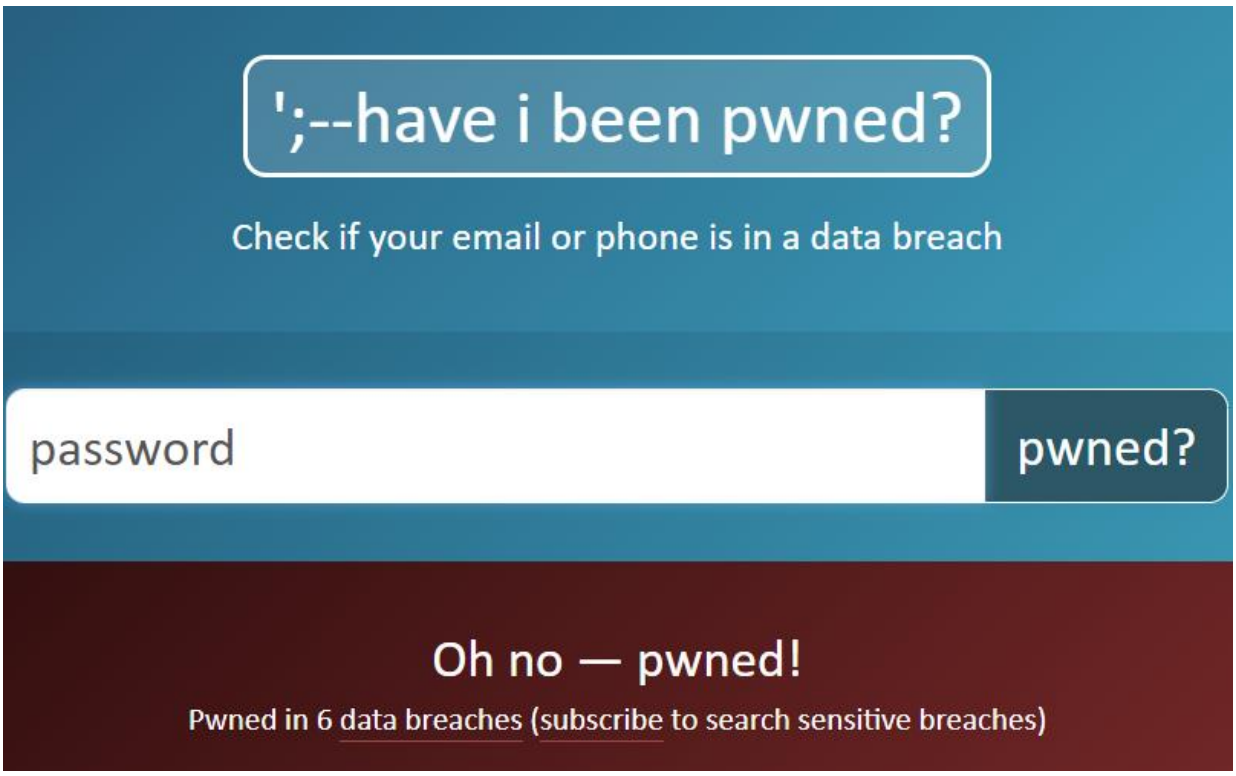


Рисунок 4.6 – Перевірка фрази на наявність в базах зламаних паролях

Потім перевіряємо стійкість паролю з мінімальними змінами: а на @, s на $, о на 0 (рис.4.7). Стійкість збільшилася, але фразу все ще легко зламати.

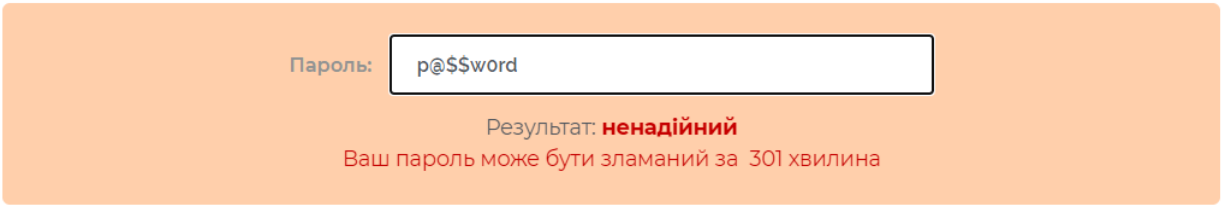


Рисунок 4.7 – Стійкість паролю з мінімальними замінами

Виконаємо аналогічну перевірку для пароля з замінами (рис.4.8). Оскільки password та його найближчі аналоги: p@$$word та p@$$w0rd також є найбільш популярними, тому не дивно що haveibeenpwned.com знайшов його в своїх базах. Вони можуть бути використані злочинцями для створення власних словників паролів. На основі них можуть виконуватися атаки грубого підбору та словників. Слід зазначити, що в «переліки» зловмисників входять не тільки відомі паролі, а й їх можливі модифікації.

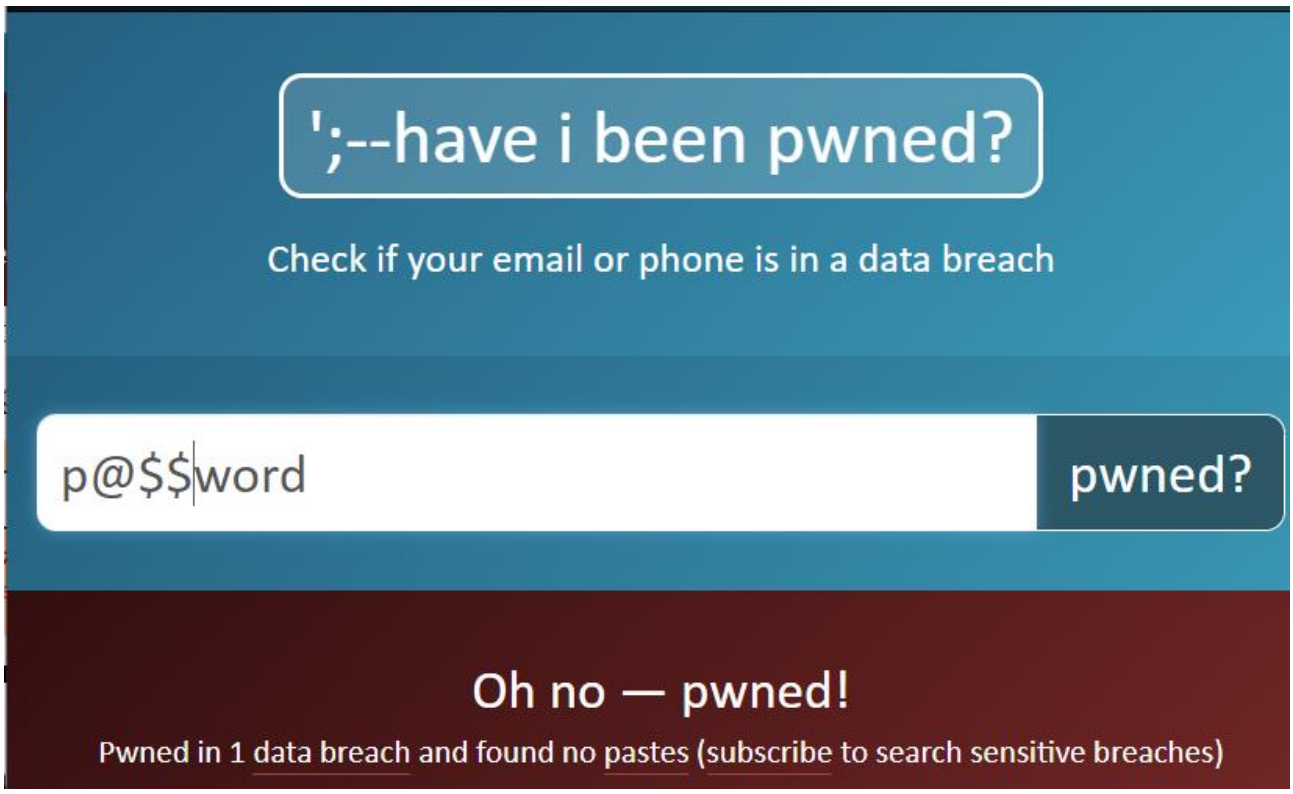


Рисунок 4.8 – Перевірка паролю з мінімальними замінами на наявність в публічних базах

Опісля буде перевірено стійкість паролю разом із замінами та вставками (рис. 4.9). Згідно сервісу p@$$wordrQ все ще ненадійний, але час його зламу виріс до 8173 днів. Цей результат може бути прийнятний, оскільки згідно парольних політик на підприємствах пароль може змінювати в інтервалі від одного місяця до одного року.

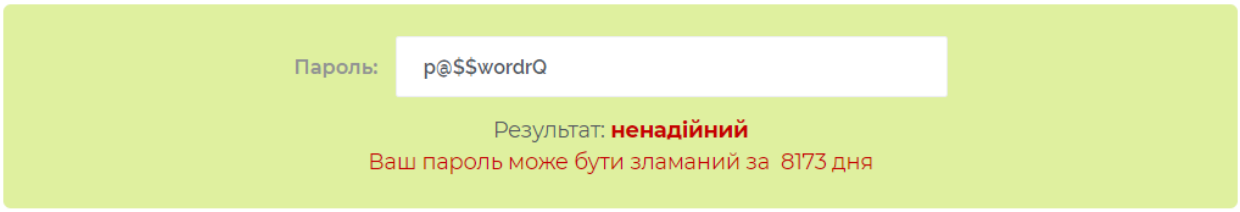


Рисунок 4.9 – Стійкість паролю, включаючи заміни та вставлення

Перевірено ще цей пароль на наявність в публічних базах (рис.4.10). Як видно з рисунку – нічого не знайдено. З цього можна зробити висновок, що незначні вставки можуть зменшити імовірність компротентації коистувацього

паролю. Оскільки, haveibeenpwned.com не знайшов збігів, то при подальших модифікаціях парольної фрази перевірки не будуть виконуватися.

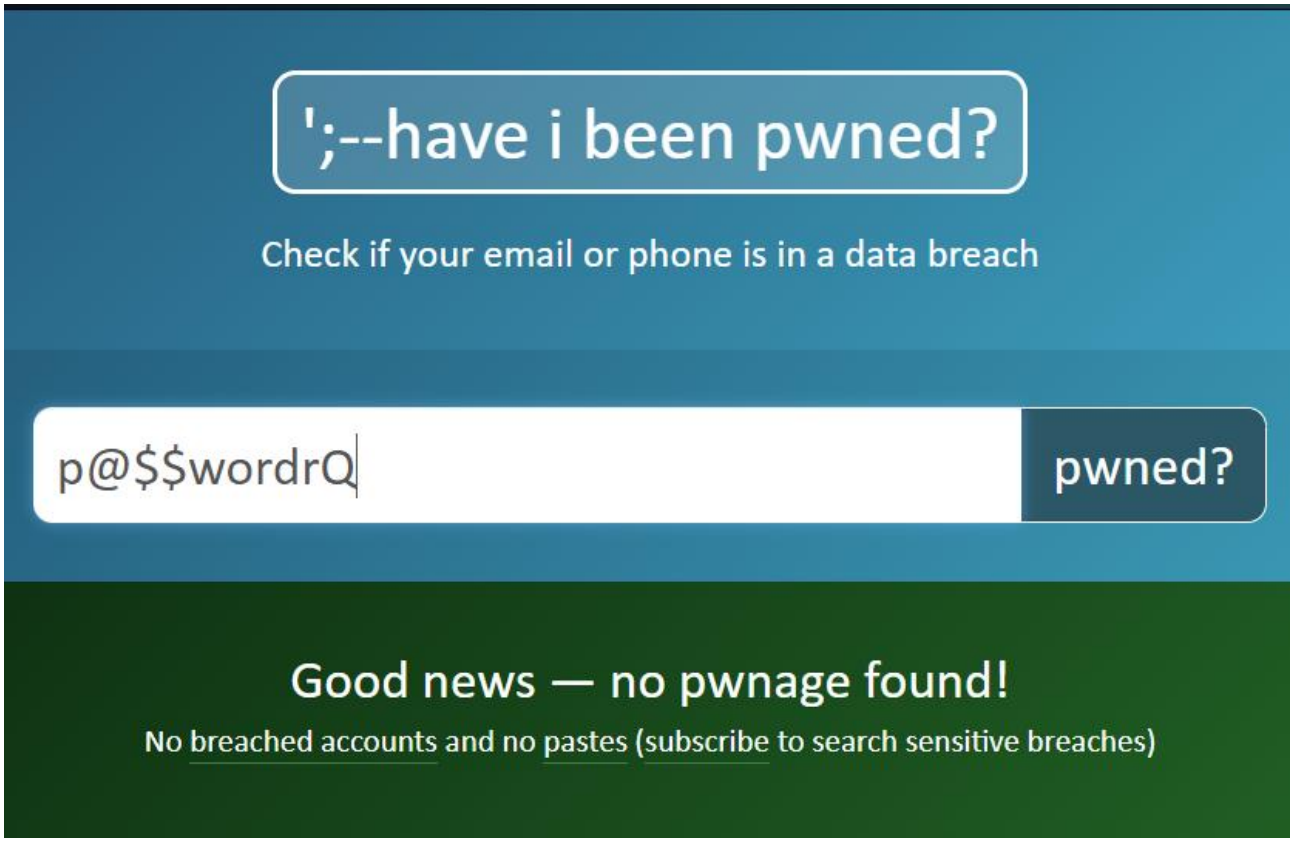


Рисунок 4.10 – Перевірка паролю, включаючи заміни та вставлення, щодо наявності в публічних базах

Перевірено ще декілька згенерованих комбінацій на надійність.

На рисунку 4.11 зображено час зламу паролю, який дуже схожий на попередній. Різниця між ними в заміненії буві о на 0 та доданих 2 буквах в кінці.

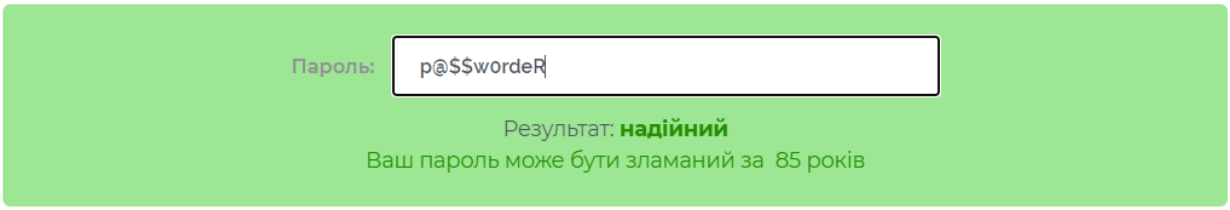


Рисунок 4.11 – Стійкість паролю з додатковою заміною та вставками

На рисунку 4.12 зображено результат аналізу стійкості паролю, які відповідає сучасним вимогам.

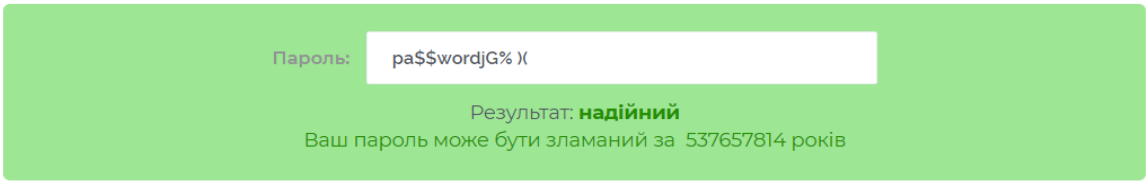


Рисунок 4.12 – Стійкість текстового паролю, який відповідає всім сучасним вимогам

Для глибшого дослідження було використано нетривіальний пароль – Mistolinia та інший сервіс з перевірки стійкості текстових паролів – whatismyip.com/password-strength-test/(рис.4.13).

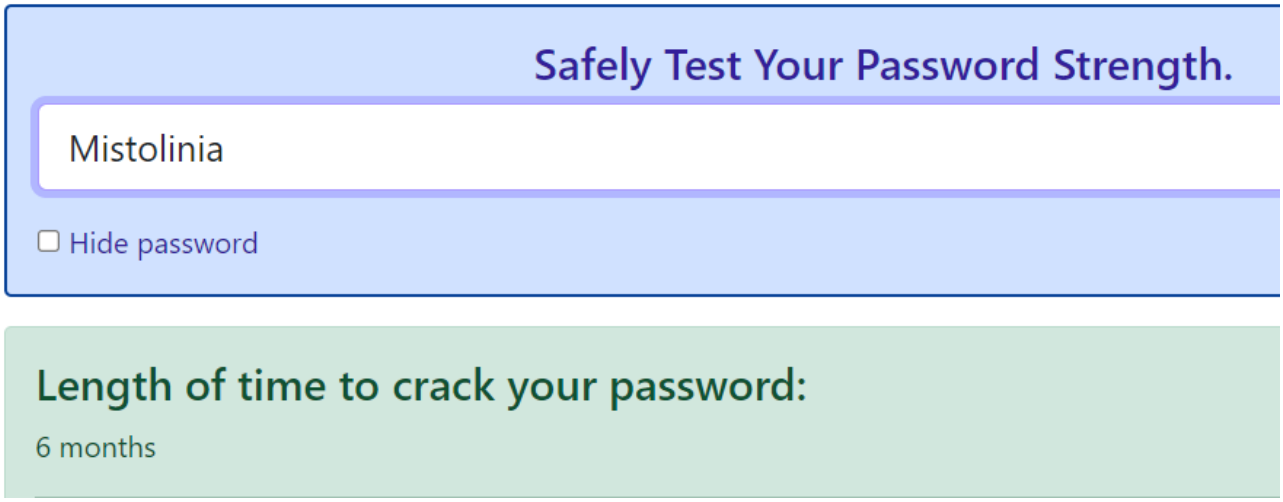


Рисунок 4.13 – Перевірка стійкості паролю в початковому вигляді

Аналогічно паролю password та його найближчим аналогам, проведено перевірку, використовуючи сервіс haveibeenpwned.com (рис. 4.14).

Оскільки нічого не було знайдено, можна зробити висновок що маловідомі назви в складі текстового паролю мають більшу стійкість до перебору та зламу. Проведено ще декілька досліджень стійкості, використовуючи сервіс whatismyip.com, для цього введемо паролі з меншою (рис. 4.15) та більшою кількістю вставок (рис. 4.16)

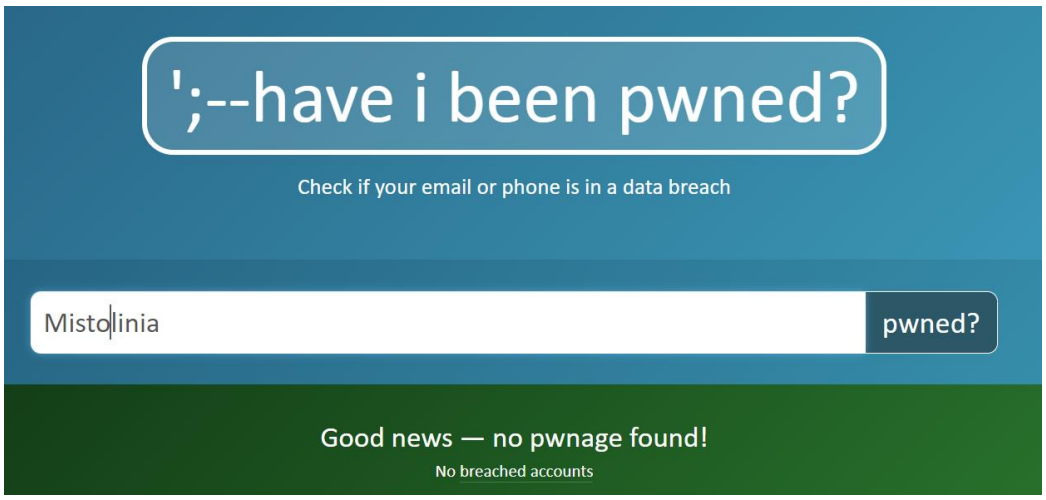


Рисунок 4.14 – Перевірка нетривіального паролю на можливість компроментації, шляхом використання публічних баз

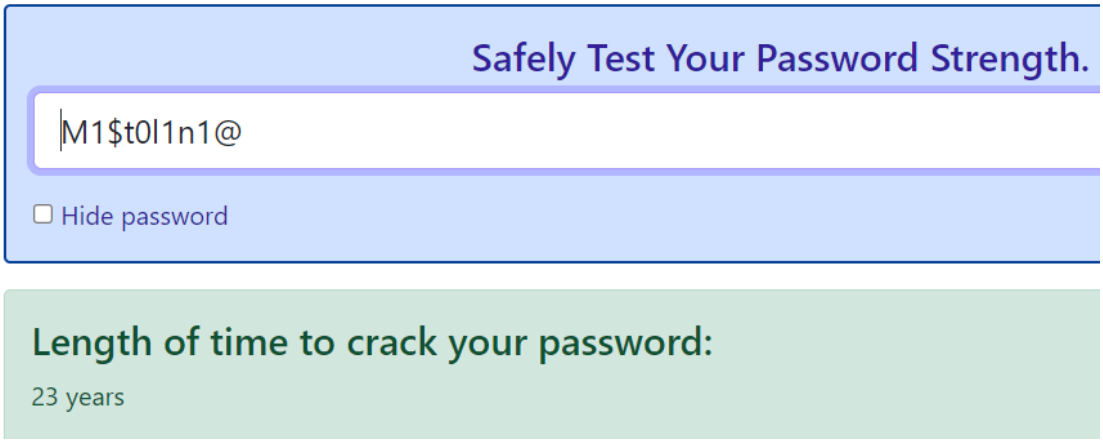


Рисунок 4.15 – Стійкість паролю зі замінами та вставкою

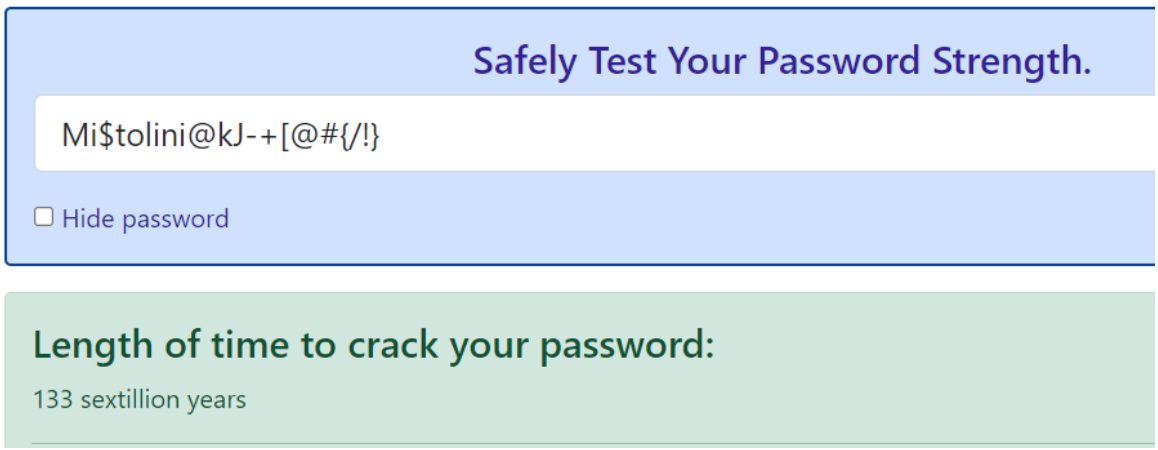


Рисунок 4.16 – Стійкість паролю з замінами та додатковими вставками

В таблиці 4.1 наведено попарну порівняльну характеристику стійкості паролів

Таблиця 4.1 – Порівняльна характеристика стійкості текстових паролів

Пароль	Оцінка стійкості 2ip.io, роки.	Оцінка стійкості whatismyip.com, роки	Наявність в базі haveibeenpwned.com
Everest12	0,15	0,11	-
Evere$t12cK	6810	2000	-
Okkotsu	$8{,}1 \times 10^{-6}$	$3{,}8 \times 10^{-6}$	-
Okkot$uxG	0,3	0,08	-
Rosenrot	0,00044	0,0001	+
R0$enr0tiQ	85	23	-
LinkinPark2000	98314382	39×10^{6}	+
L1nk1nP@rk2000vH	22313782400325	39×10^{18}	-

На основі розробленої таблиці можна сформувати такий перелік рекомендацій для створення захищеного паролю:

– довжина понад вісім символів;

– він не містить поширених поєднань букв і слів;

– не містить символів, що повторюються або йдуть один за одним (0000, 1111, 12345678, QWERTY, abc123, йцукен, привіт, пароль і т.д);

– він не містить імені, прізвища, дати народження та інших персональних даних користувача;

– він не містить імені, прізвища або дати народження батьків, дітей, чоловіка або дружини користувача та інших персональних даних;

– такого слова немає в англійській мові, українській, і бажано - в інших мовах теж;

– він містить спеціальні символи, цифри, великі та малі літери;

– він використовується тільки для одного сервісу;

– не зберігається на смартфоні користувача або в нотатках ноутбука;

– його немає у базі haveibeenpwned.com;

– його не знають рідні, кохані, колеги користувача;

– пароль істотно відрізняється від минулого пароля, що використовувався на цьому ж сервісі.

Після тестування програми та оцінки стійкості згенерованих паролів можна розрахувати економічну складову.

4.3 Висновки до розділу

Розроблену програму було протестовано.

Було показано результати генерації паролів при різних вхідних даних: фраза, її довжина та імовірність заміни.

Рекомендованим варіантом є середня довжина паролю, від 6 до 10 літер, та імовірність в межах 40 – 60 %. Такі паролі є легко запам’ятовуваними для користувача та мають достатню стійкість. Причому фразу, яка стане основою для майбутого паролю, слід обирати з обережністю. На основі проведених досліджень можна стверджувати: не слід використовувати персональні дані, загально відомі назви та назви, які можеа дізнатися, використавши соціальну інженерію. Наприклад: місце подорожей, улюблений гурт, свій перший концерт та інше.

При збільшенні одного з показників збільшується як розмір паролю так і його стійкість. При цьому запам’ятовуваність дещо зменшується. Такі паролі можна використовувати для банкінгу або для облікових записів в соціальних мережах.

Для оцінки стійкості згенерованих текстових паролів було обрано сервіс 2ip.io/ua/passcheck/ та whatismyip.com. Для перевірки на наявність паролю в публічних базах було використано haveibeenpwned.com.

5 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність результатів виконаної роботи.

Магістерська кваліфікаційна робота «Метод та засіб підвищення стійкості текстових паролів» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок (або рішення про виведення науково-технічної розробки на ринок може бути прийнято у процесі проведення самої роботи), тобто коли відбувається так звана комерціалізація науково-технічної розробки. Цей напрямок є пріоритетним, оскільки результатами розробки можуть користуватися інші споживачі, отримуючи при цьому певний економічний ефект. Але для цього потрібно знайти потенційного інвестора, який би взявся за реалізацію цього проекту і переконати його в економічній доцільності такого кроку.

Для наведеного випадку мають бути виконані такі етапи робіт:

1) проведено комерційний аудит науково-технічної розробки, тобто встановлення її науково-технічного рівня та комерційного потенціалу;

2) розраховано витрати на здійснення науково-технічної розробки;

3) розрахована економічна ефективність науково-технічної розробки у випадку її впровадження і комерціалізації потенційним інвестором і проведено обґрунтування економічної доцільності комерціалізації потенційним інвестором.

5.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Метод та засіб підвищення стійкості текстових паролів» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 5.1 [32]:

Таблиця 5.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає

Продовження табл.5.1

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовують ся у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки зведено до таблиці 5.2.

Таблиця 5.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	4	4	4
2. Ринкові переваги (наявність аналогів)	2	2	3
3. Ринкові переваги (ціна продукту)	4	4	3
4. Ринкові переваги (технічні властивості)	3	3	2
5. Ринкові переваги (експлуатаційні витрати)	2	2	2
6. Ринкові перспективи (розмір ринку)	2	2	2
7. Ринкові перспективи (конкуренція)	3	2	3
8. Практична здійсненність (наявність фахівців)	5	5	5
9. Практична здійсненність (наявність фінансів)	3	4	3
10. Практична здійсненність (необхідність нових матеріалів)	4	5	5
11. Практична здійсненність (термін реалізації)	4	4	4
12. Практична здійсненність (розробка документів)	4	3	4
Сума балів	40	40	40
Середньоарифметична сума балів $СБ_c$	40,0		

За результатами розрахунків, наведених в таблиці 5.2, можна зробити висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використано рекомендації, наведені в табл. 5.3 [32].

Таблиця 5.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Метод та засіб підвищення стійкості текстових паролів» становить 40,0 бала, що, відповідно до таблиці 4.3, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вище середнього).

5.2 Розрахунок узагальненого коефіцієнта якості розробки

Окрім комерційного аудиту розробки доцільно також розглянути технічний рівень якості розробки, розглянувши її основні технічні показники. Ці показники по-різному впливають на загальну якість проектної розробки.

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення розраховується за формулою [33]:

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i \quad , \tag{5.1}$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

α_i – коефіцієнт, який враховує питому вагу *і-го* технічного показника в загальній якості розробки. Коефіцієнт α_i визначається експертним шляхом і при цьому має виконуватись умова $\sum_{i=1}^{k} \alpha_i = 1$;

β_i – відносне значення *і-го* технічного показника якості нової розробки.

Відносні значення β_i для різних випадків розраховано за такими формулами: для показників, зростання яких вказує на підвищення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{нi}}{I_{ai}} \quad , \tag{5.2}$$

де $I_{нi}$ та $I_{на}$ – чисельні значення конкретного *і*-го технічного показника якості відповідно для нової розробки та аналога;

Для показників, зростання яких вказує на погіршення в лінійній залежності якості нової розробки:

$$\beta_i = \frac{I_{ai}}{I_{нi}} \quad ; \tag{5.3}$$

Використовуючи наведені залежності можемо проаналізувати та порівняти техніко-економічні характеристики аналогу та розробки на основі отриманих наявних та проектних показників, а результати порівняння зведемо до таблиці 5.4.

Таблиця 5.4 – Порівняння основних параметрів розробки та аналога.

Показники (параметри)	Одиниця вимірю-вання	Аналог	Проектований пристрій	Відношення параметрів нової розробки до аналога	Питома вага показника
Порівняльна швидкість кодування інормації	бал	9	9,8	1,09	0,2
Надійність роботи	%	90	96	1,07	0,25
Рівень захищеності даних	%	90	97	1,07	0,3
Дружність інтерфейсу	бал	7,5	9	1,2	0,1
Співвідношення ресурс/продуктивність	бал	5	8	1,75	0,15

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення складе:

$$B_н = \sum_{i=1}^{k} \alpha_i \times \beta_i = 1{,}09 \cdot 0{,}2 + 1{,}07 \cdot 0{,}25 + 1{,}07 \cdot 0{,}3 + 1{,}2 \cdot 0{,}1 + 1{,}75 \cdot 0{,}15 = 1{,}19.$$

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,19 рази.

5.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Метод та засіб підвищення стійкості текстових паролів», під час планування, обліку і калькулювання собівартості науково-дослідної роботи згруповано за відповідними статтями.

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп,

науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [34]:

$$З_о = \sum_{i=1}^{k} \frac{М_{пі} \cdot t_i}{Т_р}, \quad (5.4)$$

де k – кількість посад дослідників залучених до процесу досліджень;

$М_{пі}$ – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

$Т_р$ – середнє число робочих днів в місяці, $Т_р$=24 дні.

$$З_о = 16200{,}00 \cdot 24 / 24 = 16200{,}00 \ грн.$$

Проведені розрахунки зведемо до таблиці (табл. 5.5).

Таблиця 5.5 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	16200,00	675,00	24	16200,00
Інженер-розробник програмного забезпечення	16100,00	670,83	24	16100,00
Технік	6810,00	283,75	12	3405,00
Всього				35705,00

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Метод та засіб підвищення стійкості текстових паролів» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} С_i \cdot t_i, \quad (5.5)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (5.6)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду;

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 24 дн;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}65 / (24 \cdot 8) = 63{,}34 \text{ грн.}$$

$$З_{p1} = 63{,}34 \cdot 8{,}00 = 506{,}69 \text{ грн.}$$

Тепер буде розраховано витрати на основну заробітну плату для працівників(табл.5.6)

Таблиця 5.6 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Підготовка обладнання для розробки програмного забезпечення	8,00	2	1,10	63,34	506,69

Продовження табл. 5.6

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Підготовка робочого місця розробника програмного забезпечення	4,00	3	1,35	77,73	310,92
Інсталяція програмного забезпечення	5,35	5	1,70	97,88	523,67
Налагодження програмних блоків	2,10	4	1,50	86,37	181,37
Всього					1522,65

Додаткову заробітну плату розраховано як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (5.7)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (35705,00 + 1522,65) · 11 / 100% = 4095,04 грн.

Нарахування на заробітну плату дослідників та робітників розраховано як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (5.8)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (35705,00 + 1522,65 + 4095,04) · 22 / 100% = 9090,99 грн.

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Метод та засіб підвищення стійкості текстових паролів».

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj} , \quad (5.9)$$

де H_j – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

B_j – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

$M_1 = 3,0 \cdot 221,00 \cdot 1,1 - 0 \cdot 0 = 729,30$ *грн.*

Проведені розрахунки зведено до таблиці 5.7.

Таблиця 5.7 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір офісний Mondi A4 80 г/м Smart Line OFFICE білий	221,00	3,0	-	-	729,30
Папір офісний кольоровий Spectra Color A4 80 г/м 10 кольорів по 10 аркушів Rainbow різнокольоровий	79,00	3,0	-	-	260,70
Набір настільний 4-410 15 предметів	267,00	4,0	-	-	1174,80
Набір настільний 7015 - 08 SCHOLZ	364,00	2,0	-	-	800,80

Продовження табл.5.7

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Тонер IPM HP LJ P1005/1006/1505/CANON LBP-3010/3020 (TSH87B) black	523,00	2,0	-	-	1150,60
Диск оптичний CD-RW	22,00	3,0	-	-	72,60
USB флеш накопичувач Transcend 16Gb JetFlash 700 (TS64GJF700)	119,00	1,0	-	-	130,90
Всього					4319,70

Витрати на комплектуючі *($К_в$)*, які використовуються при проведенні НДР на тему «Метод та засіб підвищення стійкості текстових паролів» відсутні.

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення. Витрати за статтею «Спецустаткування» відсутні.

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховано за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \quad , \qquad (5.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.і}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

$К_і$ – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($К_і$ = *1,10…1,12);*

k – кількість найменувань програмних засобів.

$В_{прг} = 100,00 \cdot 1 \cdot 1,11 = 111,00$ *грн.*

Отримані результати зведено до таблиці (табл. 5.8):

Таблиця 5.8 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Середовище розробки: pycharm	1	100,00	111,00
Всього			111,00

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховано з використанням прямолінійного методу амортизації за формулою:

$$А_{обл} = \frac{Ц_б}{Т_в} \cdot \frac{t_{вик}}{12}, \quad (5.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$Т_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$$А_{обл} = (42699,00 \cdot 1) / (2 \cdot 12) = 1779,13 \text{ грн.}$$

Проведені розрахунки зведено до таблиці (табл. 5.9).

Таблиця 5.9 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
ноутбук Hp Omen 15-en0044ur AMD Ryzen 5 /	42699,00	2	1	1779,13

Продовження табл.5.9

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Робоче місце інженера-розробника ПЗ	8750,00	5	1	145,83
Пристрої передачі даних	6540,00	2	1	272,50
Пристрій виводу інформації	6732,00	5	1	112,20
Оргтехніка	8250,00	4	1	171,88
Приміщення лабораторії	742000,00	25	1	2473,33
ОС Windows 10	8370,00	2	1	348,75
Прикладний пакет Microsoft Office 2016	7825,00	2	1	326,04
Всього				5629,66

Витрати на силову електроенергію (B_e) розраховано за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{впі}}{\eta_i}, \quad (5.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e = 6,20$ грн;

$K_{впі}$ – коефіцієнт, що враховує використання потужності, $K_{впі} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,03 \cdot 160,0 \cdot 6,20 \cdot 0,95 / 0,97 = 29,76$ *грн.*

Проведені розрахунки зведено до таблиці 5.10.

Таблиця 5.10 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
ноутбук Hp Omen 15-en0044ur AMD Ryzen 5 / Ryzen 5 Pro 4600H 3.0ГГц ядер: 6 Об'єм ОЗУ: 16 Гб Тип памяті: DDR4	0,03	160,0	29,76

Продовження табл.5.10

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Робоче місце інженера-розробника ПЗ	0,15	160,0	148,80
Пристрої передачі даних	0,01	160,0	9,92
Пристрій виводу інформації	0,50	10,0	31,00
Оргтехніка	0,62	2,5	9,61
Інше	0,10	50,0	31,00
Всього			260,09

До статті «Службові відрядження» дослідної роботи на тему «Метод та засіб підвищення стійкості текстових паролів» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов'язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховано як 20 – 25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{H_{св}}{100\%}, \quad (5.13)$$

де $H_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 0%.

$B_{св} = (35705,00 + 1522,65) \cdot 0 / 100\% = 0,00$ *грн.*

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховано як 30 – 45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{H_{сп}}{100\%}, \quad (5.14)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 0%.

$B_{сп} = (35705,00 + 1522,65) \cdot 0 / 100\% = 0,00$ *грн.*

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховано як 50 – 100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.15)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів} = 50\%$.

$I_в = (35705,00 + 1522,65) \cdot 50 / 100\% = 18613,83$ *грн.*

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховано як 100 – 150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.16)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв} = 115\%$.

$В_{нзв} = (35705,00 + 1522,65) \cdot 115 / 100\% = 42811,80$ *грн.*

Витрати на проведення науково-дослідної роботи на тему «Метод та засіб підвищення стійкості текстових паролів» розраховано як суму всіх попередніх статей витрат за формулою:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (5.17)$$

$В_{заг}$*= 35705,00 +1522,65 +4095,04 +9090,99 +4319,70 +0,00 +0,00 + 111,00 + 5629,66 +260,09 +0,00 +0,00 +18613,83 +42811,80 = 122159,77 грн.*

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховано за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (5.17)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, прийнято η=0,9.

$$ЗВ = 122159,77 / 0,9 = 135733,07 \text{ грн.}$$

Тепер можна розрахувати економічну ефективність науково-технічної розробки.

5.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Метод та засіб підвищення стійкості текстових паролів» передбачають комерціалізацію протягом 4-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик (табл.5.11);

Таблиця 5.11 – Таблиця збільшення споживачів кожного року

Показник	1-й рік	2-й рік	3-й рік	4-й рік
Збільшення кількості споживачів, осіб	2000	5000	10000	7000

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 25000 осіб;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 250,00 грн;

$\pm\Delta Ц_o$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 20,25 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 4-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховується за формулою:

$$\Delta П_i = (\pm\Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (5.18)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2022 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0{,}8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо ρ =40%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2022 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1$ = (20,25·25000,00+270,25·2000)·0,83·0,4·(1-0,18/100%)=284967,22 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2$ = (20,25·25000,00+270,25·7000)·0,83·0,4·(1-0,18/100%)=652831,52 грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3 =$(20,25·25000,00+270,25·17000)·0,83·0,4·(1-0,18/100%)=1388560,12 грн.

Збільшення чистого прибутку 4-го року:

$\Delta П_4 =$(20,25·25000,00+270,25·24000)·0,83·0,4·(1-0,18/100%)=1903570,14 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (5.20)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ=0,24;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$ПП =$284967,22/(1+0,24)^1+652831,52/(1+0,24)^2+1388560,12/(1+0,24)^3+
+1903570,14/(1+0,24)^4=229812,27+424578,25+728282,09+805159,91=
=2187832,53 грн.

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \qquad (5.21)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 135733,07 грн.

$PV = k_{інв} \cdot ЗВ$ = 2 · 135733,07 = 271466,14 грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \tag{5.22}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 2187832,53 грн;

PV – теперішня вартість початкових інвестицій, 271466,14 грн.

$E_{абс} = ПП - PV$ = 2187832,53 - 271466,14 = 1916366,39 грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{5.23}$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 1916366,39 грн;

PV – теперішня вартість початкових інвестицій, 271466,14 грн;

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+1916366,39/271466,14)^{1/4}= 0,68.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (5.24)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2022 році в Україні d =0,1;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,27.

$\tau_{мін}$ = 0,1+0,27 = 0,37 < 0,68 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Метод та засіб підвищення стійкості текстових паролів» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \quad (5.25)$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 0,68 = 1,46 р.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

5.5 Висновки до розділу

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Метод та засіб підвищення стійкості текстових паролів» становить 40,0 бала, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вище середнього).

При оцінюванні за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,19 рази.

При оцінюванні рівня конкурентоспроможності, згідно узагальненого коефіцієнту конкурентоспроможності розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 4 рази.

Також термін окупності становить 1,46 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Метод та засіб підвищення стійкості текстових паролів».

ВИСНОВКИ

Магістерська кваліфікаційна робота присвячена аналізу парольної автентифікації і встановленню напрямів для покращення стійкості паролю.

У першому розділі магістерської кваліфікаційної роботи були розглянуті та проаналізовані особливості використання, сучасні вимоги до паролів, також розглянуто алгоритми автентифікації. Було обрано автентифікацію за паролем, оскільки вона найбільш поширена як самостійний вид так і в складі MFA. Було визначено 3 пункти за якими визначається зручність способу парольної автентифікації: зручність використання, безпека та можливість розгортання. На їх основі була зроблена порівняльна характеристика, яка показала сильні і слабкі сторони кожної з них. При аналізі літератури та написанні розділу було визначено актуальність теми, та висунутих тез

Було здійснено постановку задачі дослідження. Аналіз джерел показав лише одну роботу, в якій намагались вирішити цю задачу, але оскільки в ній було реалізовано лише перший крок, то викладені в ній ідеї потребують удосконалення.

Потім було розроблено математичний опис процесу генерування паролю в основі якого лежить принцип синтезу цифрових автоматів. Це дасть можливість визначити вхідні, вихідні дані та стани автомату, що сприйятиме подальшій розробці алгоритмів.

Запропоновано узагальнений опис методу генерації паролів, який представлено у вигляді покрокового алгоритму. Встановлено наступні вимоги генераторів псевдовипадкових чисел: статистична стійкість, довгий період, змінний діапазон чисел, рівномірність розподілу та обчислювальна простота. На основі них обрано генератор, що реалізується бібліотекою random із мови програмування Python, перевагою є рівномірість генерування випадкових чисел. Згідно до поставлених вимог розроблено таблиці замін, які дозволять підвищити стійкість паролю.

Було обгрунтовано вибір мови програмування для реалізації описаних алгоритмів. Python було вибрано з огляду на його зручність в розгортанні Backend та можливості керування пам’яттю. Після цього розроблено загальний алгоритм роботи майбутнього додатку. На основі проведеної розробки було визначено його ключові функції. Для кожної з них розроблені схеми роботи.

Розроблену програму було протестовано та оцінено стійкість згенерованих текстових паролів. Показано результати генерації паролів при різних вхідних даних: фраза, її довжина та імовірність заміни.

Для оцінки стійкості згенерованих текстових паролів було обрано сервіс 2ip.io/ua/passcheck/та whatismyip.com, перевірка на наявність в публічних базах – haveibeenpwned.com.

Економічні розрахунки даної магістерської роботи склало 40,0 бали, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вище середнього).

При оцінюванні за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,19 рази.

При оцінюванні рівня конкурентоспроможності, згідно узагальненого коефіцієнту конкурентоспроможності розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 4 рази.

Також термін окупності становить 1,46 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sh. Riley. Password Security : What Users Know and What They Actually Do. 2006. Vol 7, No 1, pp 2833-2836. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.597.5846&rep=rep1&type=pdf. (accessed 14.09.2022)
2. K. Parker. A very weak and widespread password is written on a sticker / st. June 29, 2020. URL: https://securenetworkers.com/a-very-weak-and-wide-spread-password-is-written-on-a-sticker-st/ (accessed 14.09.2022)
3. Сухоребра А. С., Войтович О. В. Роль кібераудиту в сучасних IT-технологіях: збірник тез та доповідей XLIX Науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії (м.Вінниця, 30 березня 2020 р.) 2 с. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/9063 (дата звернення: 15.09.2022)
4. Сухоребра А. С. Методика аудиту відповідно до NIST SP 800-53: збірник тез та доповідей L Науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії (м.Вінниця, 4 березня 2021 р) Вінниця, 2021. 2 с. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2021/paper/view/1195 (дата звернення: 15.09.2022)
5. Сухоребра А. С., Коломієць А.А. Математика та криптографія: збірник тез та доповідей XLVII Науково-технічої конференції факультету інформаційних технологій та комп'ютерної інженерії (м.Вінниця, 14 безерня 2018 р) Вінниця, 2018.
6. About Face ID advanced technology. Apple Support. URL: https://support.apple.com/en-us/HT208108 (accessed 20.09.2022)
7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Загальна частина: Постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: https://www.kmu.gov.ua/npas/32791826 (дата звернення: 06.09.2022).
8. Захист інформації в комп’ютерних системах : підручник / Гапак О. М та ін. Ужгород: ДВНЗ «УжНУ», 2021. 184 с.
9. Коршун Н. В., Літвінчук І. С., Корчомний Р. О., Борисов І. В. Розробка рекомендацій щодо мінімізації ризиків зломів облікових записів на основі аналізу найпоширеніших методів злому. 2021. №4 (21). С 161 – 170. URL: https://elibrary.kubg.edu.ua/id/eprint/38750/1/N_Korshun_I_Litvinchuk_R_Korchomnyi_I_Borysov_CEST_12.pdf (дата звернення 02.10.2022)
10. Password Authentication: Avoiding 4 Common Vulnerabilities. July 27, 2020. URL: https://swoopnow.com/password-authentication (accessed 12.10.2022)
11. Vissarion Yfantis. Smart Card Authentication. Raise Your Security Levels to a Higher Standard. July 16, 2019. URL:

https://www.parallels.com/blogs/ras/smart-card-authentication (accessed 13.10.2022)
12. Which password authentication method works best for businesses? URL: https://www.passportalmsp.com/blog/which-password-authentication-method-works-best-businesses (accessed 14.10.200)
13. Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees. July 13, 2021 URL: https://www.gao.gov/products/gao-21-105309/ (accessed: 15.10.2022).
14. Two-factor authentication for Apple ID. URL: https://support.apple.com/en-us/HT204915 (accessed: 16.10.2022)
15. J. M. Stewart. Multi-Step Authentication and Why You Should Use It. Global Knowledge. Expert Reference Series of White Papers. Global Knowledge Training LLC, 2013. 13 p. URL: https://d12vzecr6ihe4p.cloudfront.net/media/965986/wp-multi-step-authentication-and-why-you-should-use-it.pdf (accessed: 17.10.2022)
16. A.Saleh, A.Bahaa and A. Wahdan. Fingerprint Recognition. Advanced Biometric Technologies. 2011. №205. pp. 201-204.
17. FIDO Alliance - Open Authentication Standards More Secure than Passwords. URL: https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/FIDO-U2F-COMPLETE-v1.2-ps-20170411.pdf (accessed: 18.10.2022).
18. FIDO Authentication. A Passwordless Vision. URL: https://fidoalliance.org/fido2/ (accessed: 20.10.2022).
19. Alharbi, E., & Alghazzawi, D. Two Factor Authentication Framework Using OTP-SMS Based on Blockchain. Transactions on Machine Learning and Artificial Intelligence. 2019. Vol 7, No 3, pp. 17–27. URL: https://journals.scholarpublishing.org/index.php/TMLAI/article/view/6524 (accessed : 02.11.2022).
20. NetIQ Identity and Access Management (IAM). CyberRes. URL: https://www.microfocus.com/en-us/cyberres/identity-access-management (accessed: 04.11.2022).
21. NIST Special Publication 800-63-3. Digital Identity Guidelines, 2017 (upd. 2020). 464 p. URL: https://pages.nist.gov/800-63-3/sp800-63-3.html (accessed : 06.11.2022).
22. Payment Card Industry Data Security Standard. Requirements and Testing Procedures. Version 4.0 .2022. 360 p. URL: https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf (accessed: 08.11.2022).
23. Hashkat. URL: https://hashcat.net/hashcat/ (accessed: 08.11.2022).
24. What is Azure Active Directory? September 15, 2022. URL: https://learn.microsoft.com/uk-ua/azure/active-directory/fundamentals/active-directory-whatis (accessed: 10.11.2022)

25. Bruce Schneier. Passwords are not broken, but how we choose them sure is . The Guardian. 2008. URL: https://www.theguardian.com/technology/2008/nov/13/internet-passwords (accessed: 12.11.2022)
26. Дж. Фойер. Місячне прогулянка з Ейнштейном - Мистецтво та наука про все пам’ятати. Нью-Йорк. 2020. 304 с.
27. Заплотинський Б.А. Основи інформаційної безпеки: конспект лекцій. Одеса:КІІВіП, 2017.128 с.
28. Глушков В. М. Синтез цифровых автоматов. Москва: Физматгиз, 1962. 476 с.
29. "Случайные" числа в Python – random, randint и randrange. URL: https://younglinux.info/python/random (дата звернення 20.11.2022)
30. Matsumoto, M., Nishimura, T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. 1998. URL: http://www.math.sci.hiroshima-u.ac.jp/m-mat/MT/ARTICLES/mt.pdf (accessed 01.12.2022)
31. Найпопулярніші мови програмування 2022 року: рейтинги TIOBE, GitHub і не тільки. URL: https://dev.ua/news/movy-prohramuvannia-2022-reiting (дата звернення 08.12.2022)
32. Столлингс В. Основы защиты сетей. Приложения и стандарты. Киев: Вильямс, 2002. 434 с.
33. Кавецький В. В., Козловський В. О., Причепа І. В. Економічне обґрунтування інноваційних рішень: практикум. Вінниця: ВНТУ, 2016. 113 с.
34. Козловський В. О., Лесько О. Й., Кавецький В. В. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт. Вінниця: ВНТУ, 2021 р. 42 с.

ДОДАТОК А

Код програми

```
import random
uppercase_letters =
"ABCDEFGHIJKLMNOPQRSTUVWXYZ
"
lowercase_letters =
uppercase_letters.lower()
digits = "0123456789"
symbols = ",./;'[]{}()*&%$#@!\\?-
+_ "
SECURE = (('s', '$'), ('and', '&'), ('a',
'@'), ('o', '0'), ('i', '1'), ('3', '#'), ('5', '%'), ('7',
'?'), ('8', '*'),
          ('0', '_'))
list = []
def securePass(password):
   for a, b in SECURE:
 password = password.replace(" ", "")
password = password.replace(a, b)
      list.append(password)
      lower(password)
def lower(lw):
   a =
".join(random.sample(lowercase_letters, 1))
   pass2 = lw + a
   upper(pass2)
def upper(up):
   a =
".join(random.sample(uppercase_letters, 1))
   pass3 = up + a
   list.append(pass3)
   symbols_s(pass3)
def symbols_s(pass3):
   a =
".join(random.sample(symbols, lenght))
   pass4 = pass3 + a
   list.append(pass4)
passwd = input("Enter Your
Password: ")
probability = input("Enter the
probability for password:")
pr1 = int (probability)
pr2 = pr1 / 100
lenght = len (passwd)
lenght = round (lenght * pr2)
securePass(passwd.strip())

print(list)
```

ДОДАТОК Б.

Акт перевірки на плагіат

Назва роботи: Метод та засіб підвищення стійкості текстових паролів

Автор роботи: Сухоребра Ангеліна Сергіївна

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 88,5%. Схожість – 11,5%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Каплун В. А.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Сухоребра А.С.
(підпис) (прізвище, ініціали)

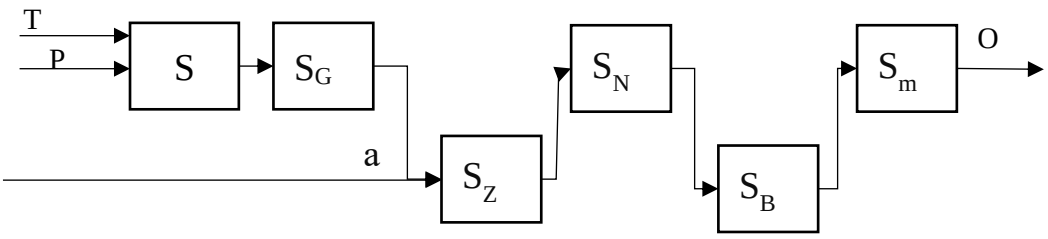
Керівник роботи _____ Барлачев Ю.В.
(підпис) (прізвище, ініціали)

ІЛЮСТРАТИВНА ЧАСТИНА

МЕТОД ТА ЗАСІБ ПІДВИЩЕННЯ СТІЙКОСТІ ТЕКСТОВИХ ПАРОЛІВ

(Назва магістерської кваліфікаційної роботи)

Узагальнена схема роботи процесу генерації захищеного паролю



Узагальнений алгоритм роботи програми

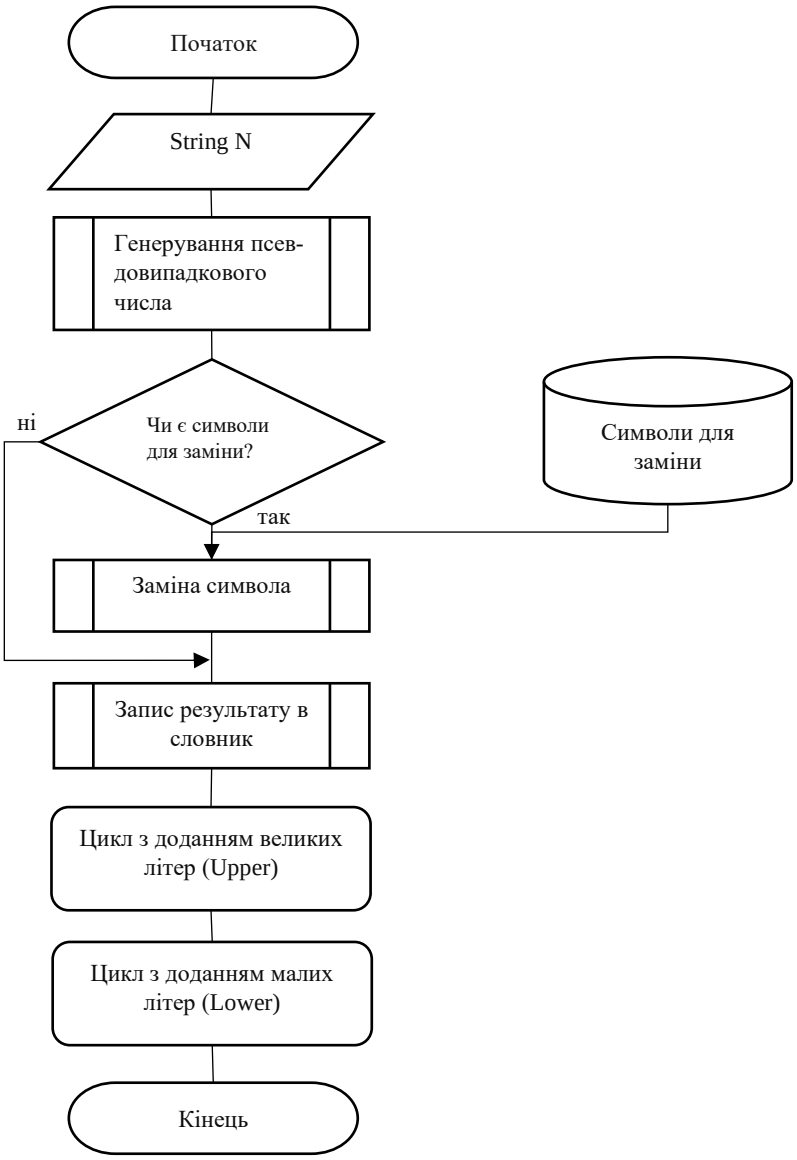


Схема роботи алгоритму заміни символів

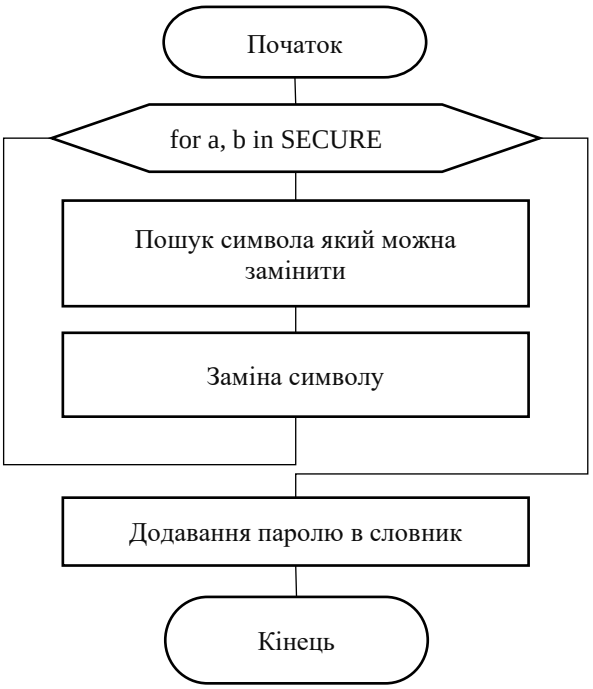
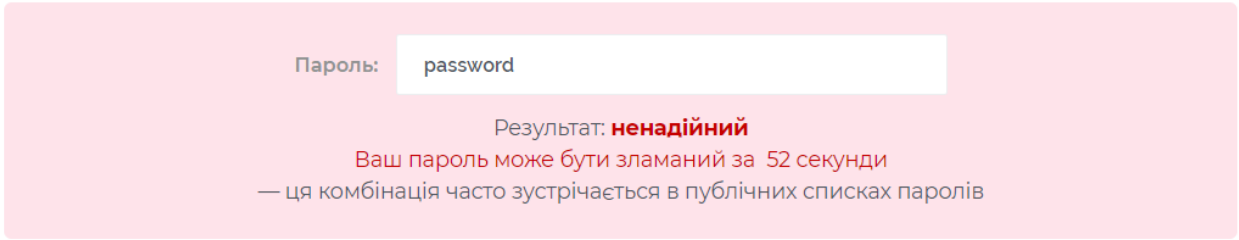
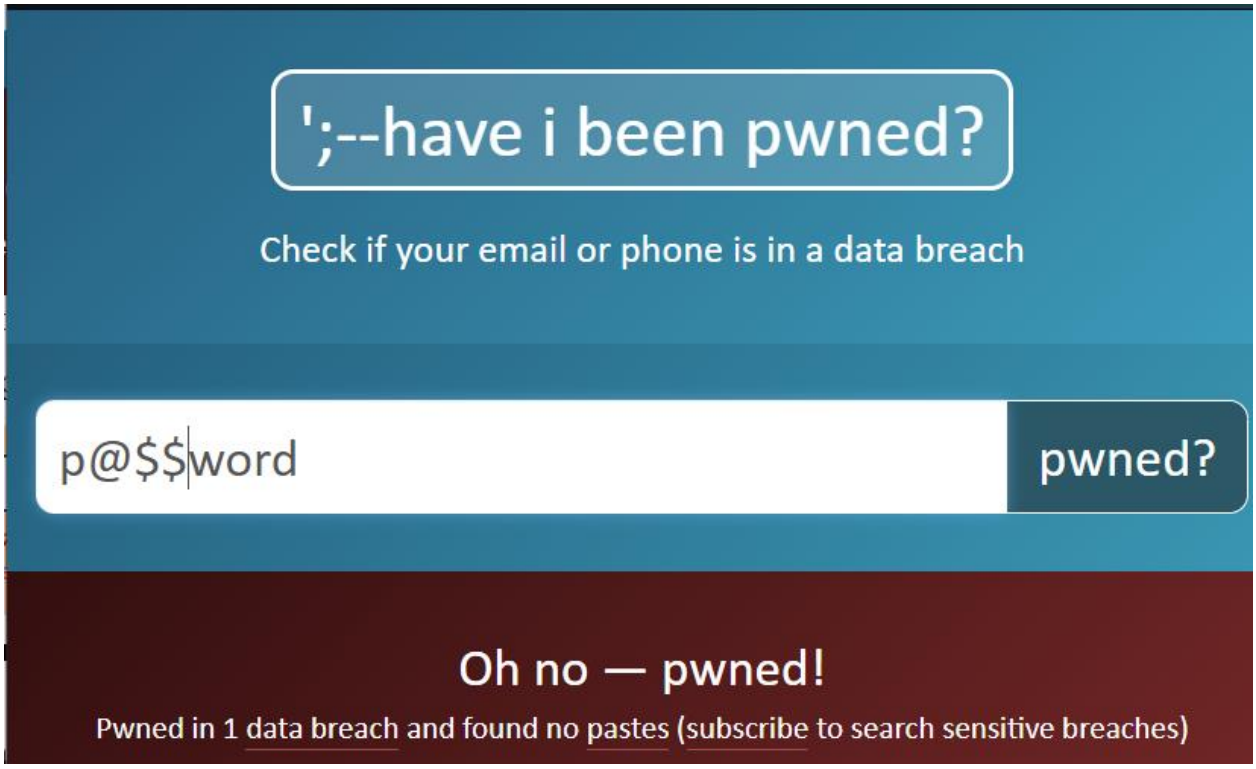
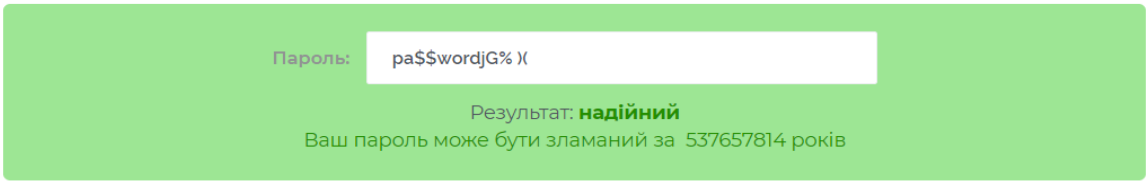


Схема роботи алгоритму заміни символів

Експериментальне оцінювання стійкості паролів







Теоретична оцінка збільшення стійкості паролю

Довжина паролю, симв.	Кількість можливих комбінацій (алфавіт з 62 символів)	Кількість можливих комбінацій (алфавіт з 86 символів)	Зростання кількості комбінацій, %
1	62	86	138,71%
2	3844	7396	192,40%
3	238328	636056	266,88%
4	14776336	54700816	370,19%
5	916132832	4704270176	513,49%
6	56800235584	4,04567E+11	712,26%
7	3,52161E+12	3,47928E+13	987,98%
8	2,1834E+14	2,99218E+15	1370,42%
9	1,35371E+16	2,57327E+17	1900,91%
10	8,39299E+17	2,21302E+19	2636,74%
11	5,20366E+19	1,90319E+21	3657,42%
12	3,22627E+21	1,63675E+23	5073,19%