УДК 004.4:004.6 doi:10.20998/2413-4295.2023.01.07

ПРИКЛАДНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗБЕРІГАННЯ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ

С. О. ЦИБУЛЬНИК*, *, Д. О. ЗУБАРСЬКИЙ, Д. О. ПІВТОРАК

кафедра комп'ютерно-інтегрованих оптичних та навігаційних систем, Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Київ, УКРАЇНА
** e-mail: tsybulnik.s.a@gmail.com*

АНОТАЦІЯ *У сучасному світі персональну інформацію будь-якої людини можна умовно розділити на дві великі категорії: загальна та особлива. Як можна зрозуміти з назви, перша категорія відповідає за той тип даних, які можна знайти у загальному доступі, а саме: прізвище, ім'я, по-батькові, підпис, місце та дата народження, громадянство, сімейний стан, освіта, банківські реквізити, тощо. Подібне різноманіття персональних даних потребує різних методів та автоматизованих засобів зберігання. Сьогодні все частіше приватні та державні установи відмовляються від зберігання інформації у паперовому вигляді. Це пояснюється низьким рівнем безпеки таких сховищ, які можуть постраждати від вогню, води, шкідників, тощо. Показано, що цифрове зберігання інформації дозволяє позбутися подібних проблем. Персональні дані, які зберігаються в електронному вигляді, найчастіше можна відновити навіть при втраті пристрою, з якого здійснювався доступ до них. Одним із основних видів персональної інформації в сучасному суспільстві є дані для входу: логін та пароль. Саме тому було розроблено алгоритмічне та програмне забезпечення автоматизованої системи збереження персональних даних користувача. Дана система має надати можливість користувачу генерувати стійкі до стандартних методів зламу паролі та зберігати їх у базі даних. Розроблення автоматизованої системи проходило з використанням архітектурного шаблону MVC, який є одним з варіантів реалізації багаторівневої архітектурної моделі. Для детального проектування та кодування обрано об'єктно-орієнтовну мову програмування зі статичною строгою типізацією Java. Також прийнято рішення розробити автоматизовану систему у вигляді веб-додатку за допомогою використання фреймворка Spring. У ході процесу розроблення спроектовано локальну базу даних, в якій зберігатимуться персональні дані у вигляді логінів та паролів, які ввів користувач або згенерувала сама система. Розроблено алгоритм генерації стійких до зламу стандартними методами паролів. Також використано алгоритми хешування, як додатковий захист головного пароля від веб-додатку. Створено графічний інтерфейс, який дозволяє користувачу отримати доступ до основних функцій автоматизованої системи.*
Ключові слова: *персональні дані; Spring; менеджер паролів; Java; веб-додаток.*

APPLIED SOFTWARE FOR PERSONAL INFORMATION STORAGE

S. TSYBULNYK*, *, D. ZUBARSKYI, D. PIVTORAK

Department of Computer-Integrated Optical and Navigation Systems, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, UKRAINE

ABSTRACT *In today's world, the personal information of any person can be conventionally divided into two large categories: general and special. As you can understand from the name, the first category is responsible for the type of data that can be found in public access, namely: surname, first name, patronymic, signature, place and date of birth, citizenship, marital status, education, bank details, etc. Such a variety of personal data requires different methods and automated means of storage. Today, private and state institutions increasingly refuse to store information in paper form. This is explained by the low level of security of such storage facilities, which can be affected by fire, water, pests, etc. Information that exists in paper form is very easy to lose, for example, misplaced or lost during movement. It is shown that digital storage of information makes it possible to get rid of such problems. Personal data that is stored electronically can often be recovered even if the device from which it was accessed is lost. One of the main types of personal information in modern society is login data: login and password. That is why the algorithmic and software of the automated system for saving the user's personal data was developed. This system should enable the user to generate passwords resistant to standard hacking methods and store them in the database. The development of the automated system took place using the MVC architectural template, which is one of the options for implementing a multi-level architectural model. For detailed design and coding, an object-oriented Java programming language with static strict typing was chosen. It was also decided to develop an automated system in the form of a web application using the Spring framework. During the development process, a local database was designed, which will store personal data in the form of logins and passwords entered by the user or generated by the system itself. An algorithm for generating hack-resistant passwords has been developed. Hash algorithms are also used as an additional protection of the main password of the web application. A graphical interface has been created that allows the user to access the main functions of the automated system.*
Keywords*: personal data; Spring; password manager; Java; web application.*

Вступ

Велика частина інформації, яка зберігається на пристроях будь-якого користувача, є особистою. Наприклад, медична документація (електронна медична картка з переліком симптомів та діагнозів, рецепти на лікарські засоби, тощо), банківські реквізити, електронні копії документів (паспорт,

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

реєстраційна картка платника податків, документи, які надають право власності на нерухомість, тощо) та довгий список іншої електронної інформації, яку люди хочуть приховати від зловмисників, має залишатися конфіденційним і надійно захищеним. Закон України «Про захист персональних даних» [1] встановлює основний перелік правил, які регулюють порядок оброблення персональних даних людини автоматизованими засобами, забезпечують невтручання в особисте життя та захист її прав і свобод. Отже, закон чітко говорить, що без дозволу людини ніхто не має права отримувати доступ до її персональних даних.

У зв'язку з тим, що кожна людина має фізіологічну, фізичну, культурну та соціальну ідентичність [2] можна розділити всі персональні дані на дві категорії, а саме: особливі та загальні.

Персональна інформація, яка належить до особливої категорії, стосується даних про членство в релігійних, політичних, профспілкових, громадських та інших організаціях, релігійні, політичні та інші переконання людини, статеве життя, етнічне, національне та расове походження, юридичну відповідальність, а також медичні, генетичні, біометричні дані, тощо.

До загальної категорії, як правило, відноситься інформація про підпис, прізвище, ім'я, по-батькові, місце та дату народження, сімейний стан та громадянство, адресу місця проживання, освіту, фінансове становище, банківські реквізити, номер пенсійної справи, тощо.

Зберігання персональних даних може проходити у двох формах: паперовій та цифровій. У наш час все частіше використовується саме друга форма зберігання персональних даних, яка має і переваги, і недоліки [2]. Серед переваг цифрового зберігання варто зазначити можливість локального (використовуючи власні потужності та технічні засоби компанії) або віддаленого (з залученням третьої сторони) розміщення персональних даних та передові технології їх захисту. До недоліків відноситься низький рівень відповідальності компанії, яка надає послуги по зберіганню даних, та шанс втрати персональних даних через вразливості, які присутні в сучасних технологіях [3,4].

При локальному зберіганні даних [5] зловмисники мають використовувати складні методи, які базуються на шкідливому програмному забезпеченні. Це означає, що основним джерелом втрати даних є користувач, якого за допомогою психологічних маніпуляцій примушують встановити прямо (замаскувавши під корисну програму) або приховано (без відома користувача) кейлогер, троянську програму або інші передові засоби викрадення персональних даних. Оскільки пароль, який також є персональними даними, уводиться на пристрої, який знаходиться в офісі компанії і закритий для доступу ззовні, то саме користувач повністю відповідає за його безпеку. Як правило, при такому варіанті зберігання отримати доступ до даних ззовні дуже складно, що є основною перевагою локального зберігання [6].

Зберігання персональної інформації в хмарному сховищі відбувається з залученням компанії, яка має необхідні потужності на віддаленому сервері [7-10]. Дані передаються та зберігаються в зашифрованому вигляді і, навіть у випадку їх викрадення, зловмисники витратять не один місяць на їх розшифровку. При цьому користувач може отримати доступ до своєї персональної інформації з будь-якого пристрою чи гаджету, який має доступ до мережі Інтернет.

Компанія, яка спеціалізується на послугах із хмарного зберігання даних, гарантує, що користувач зможе безпечно синхронізувати всі свої пристрої з серверами компанії. Іншою перевагою є те, що використання хмарного сховища дозволяє відновити всю персональну інформацію, якщо користувач втрачає свій пристрій. Проте, як правило, у рамках ліцензійного договору з користувачем подібні компанії знімають з себе будь-яку фінансову чи юридичну відповідальність за втрату персональних даних, що безперечно є одним з основних недоліків такого методу зберігання. Ризик втрати даних при співпраці з великою та надійною компанією хоч і невеликий, але є, наприклад, у випадку отримання зловмисниками доступу до однієї зі служб, які обслуговують хмарне сховище. Про це свідчать новини останніх років [11,12], які висвітлюють подібні ситуації в передових компаніях світу.

Мета роботи

Невеликі та середні компанії зазвичай не можуть собі дозволити використання локальних сховищ даних через великі фінансові витрати і використовують саме хмарні сховища. На відміну від них, великі компанії надають переваги локальному збереженню даних, всебічній їх охороні (як цифровій, так і фізичній), а також проведенню семінарів з безпеки персональної інформації для своїх працівників.

Незважаючи на те, який тип сховища персональної інформації обирає користувач, загрози безпеці даних існуватимуть завжди. Саме тому метою даної роботи є розроблення алгоритмічного та програмного забезпечення автоматизованої системи збереження персональних даних користувача, яка дасть йому змогу генерувати стійкі до стандартних методів зламу паролі.

Архітектура автоматизованої системи

Проектування архітектури програмного забезпечення або системи є одним з найважливіших етапів їх життєвого циклу. Правильно побудована модель архітектури надасть необхідну гнучкість, а

також зменшить крихкість при необхідності розширити функціональні можливості.

Існує декілька великих класів архітектури, які можуть використовуватися для рішення одних і тих же завдань. У значній мірі на ефективність обраного класу архітектури впливають потрібні характеристики якості та нефункціональні вимоги, які висуваються до проекту. Враховуючи той факт, що автоматизовану систему збереження персональних даних користувача буде реалізовано у вигляді веб-додатку, прийнято рішення про використання за основу класу закритої багаторівневої (шаруватої) архітектури [13]. У межах кожного класу також існує велике різноманіття можливих моделей архітектури, які забезпечують різний рівень взаємодії її елементів між собою.

Найбільш поширеними в межах багаторівневої архітектури на сьогодні є трьохрівневі моделі MVC, MVP та MVVM [13,14]. Як правило, MVVM використовується для реалізації мобільних додатків, а MVC та MVP – веб-додатків. Проекти програмних систем, в основі яких знаходиться архітектурна модель MVP, відокремлюють програмну логіку від графічного інтерфейсу користувача, що надає ряд переваг у процесі розроблення, наприклад:

- над кожним архітектурним рівнем (модель, вигляд, ведучий) може одночасно працювати окрема команда розробників;
- має високу масштабованість;
- легко забезпечити низьке зчеплення модулів;
- рівень моделі може використовуватись різними рівнями вигляду;
- структура кодової бази є легкою для розуміння;
- забезпечує простоту розширення функціональних можливостей.

Саме тому MVP є однією з найбільш популярних моделей архітектури (архітектурним шаблоном) у сфері веб-програмування. Завдяки широкому колу переваг дана модель була обрана для реалізації при розробленні автоматизованої системи. У загальному випадку запити користувачів обробляються наступним чином:

- веб-браузер клієнта надсилає запит на сторінку ведучого (англ. Presenter), який розміщено на сервері;
- ведучий викликає модель та у відповідь на запит отримує дані, які йому необхідні;
- ведучий через програмний інтерфейс передає отримані дані у вигляд (англ. View);
- вигляд оновлює дані елементів графічного інтерфейсу та надсилає готовий результат назад клієнту для відображення його веб-браузером.

Архітектуру програмного забезпечення, яка відповідає даній моделі, зображено на рис. 1. У відповідності до моделі MVP дана архітектура містить три рівні і чотири шари.

Рівень моделі представлений шаром сховища даних. Він містить базу даних (БД) та низькорівневу програмну логіку (пошук, сортування, збереження, тощо). Також на даному рівні розміщується підсистема роботи з базою даних, яка виступає у ролі посередника між моделлю та ведучим. Вона також забезпечує функції вибору лише необхідної інформації з бази завдяки взаємодії з підсистемами шару сховища даних та передачі цієї інформації на рівень вище. Таким чином забезпечується підвищений рівень безпеки даних, тому що повна копія бази даних ніколи не залишає поточний рівень, а вище передається лише необхідний об'єм інформації.

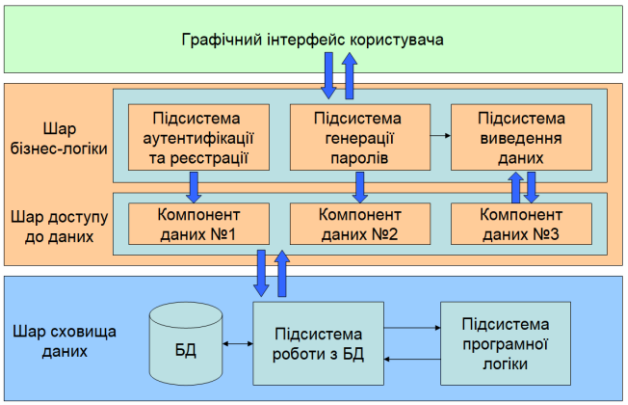

Рис. 1 – Архітектура автоматизованої системи

Рівень ведучого представлений двома шарами: бізнес-логіки та доступу до даних. Бізнес-логіка представлена трьома основними підсистемами, які реалізують набір бізнес-правил або вимоги до програмного забезпечення автоматизованої системи збереження персональних даних користувача. На даному етапі розроблення реалізовано три підсистеми: аутентифікації та реєстрації (відповідає за акаунти користувачів), генерації паролів (відповідає за створення випадкових паролів), виведення даних (відповідає за взаємозв'язок рівнів моделі та ведучого з рівнем вигляду, тобто графічним інтерфейсом користувача). Останні дві підсистеми також мають спільні взаємозв'язки для визначення параметрів паролю, які обрав користувач, наприклад, довжина, спеціальні символи, тощо.

Шар доступу до даних має три компонента, які взаємодіють з низькорівневою підсистемою роботи з базою даних. Як видно з рис. 1, перші два компоненти передають дані, пов'язані з областю своєї відповідальності, в односторонньому напрямку від відповідної підсистеми шару бізнес-логіки до підсистеми роботи з базою даних. Третій компонент даних веде взаємодію в двосторонньому напрямку як з нижнім рівнем, так і з сусіднім шаром бізнес-логіки.

Рівень вигляду представлений графічним інтерфейсом, який дає користувачу спрощений доступ до функціональних можливостей автоматизованої системи у вигляді набору полів для введення та виведення даних. Програмний інтерфейс даного рівня взаємодіє з усіма підсистемами рівня ведучого, але назад отримує інформацію тільки з підсистеми

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

виведення даних. Основна задача цього програмного інтерфейсу полягає у поєднанні отриманої інформації з відповідними полями графічного інтерфейсу користувача завдяки використанню певного набору контрактів.

Алгоритми та функціональні можливості

У відповідності до зображеної на рис. 1 архітектури було реалізовано ряд функціональних можливостей. У першу чергу був створений графічний інтерфейс користувача, який дає йому змогу проводити основні операції з автоматизованою системою. Для її використання користувачу спочатку треба пройти реєстрацію або, якщо його профіль вже міститься в базі даних, здійснити вхід, використовуючи свій логін та майстер-пароль. Реєстрація створює новий персональний кабінет та зберігає початкові персональні дані користувача, а аутентифікація дає змогу отримати доступ до вже існуючого. Вікно персонального кабінету користувача зображено на рис. 2.

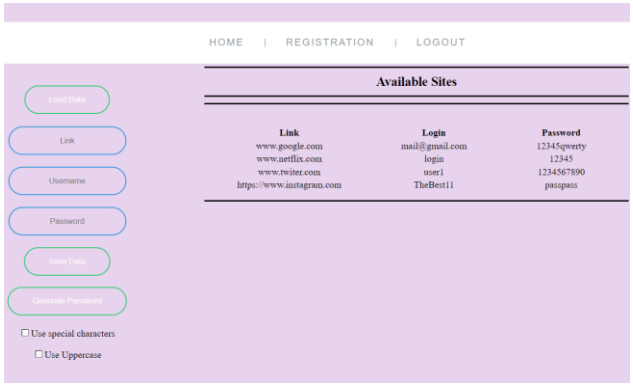

Рис. 2 – Персональний кабінет користувача

Комбінація логіна та пароля – це той вид персональних даних, які має захистити (зберегти) розроблене програмне забезпечення. Як видно з рис. 2, серед наявних функціональних можливостей автоматизованої системи збереження персональних даних користувача є генерація пароля. Таким чином, користувач має можливість автоматизовано створити новий пароль з наступними характеристиками:

- довжина від 3 до 50 символів;
- використання спеціальних символів, наприклад, №, ?, !, *, %, тощо;
- використання літер у верхньому регістрі;
- використання лише цифр.

Останній варіант генерування класичного цифрового пароля має найнижчий рівень безпеки (найменш стійкий до зламування). Але у розробленому програмному забезпеченні реалізовано алгоритм створення графічного пароля, який використовується деякими додатками, обраної довжини на основі квадратної матриці з неповторюваних цифр. Також користувач має змогу обрати координати початкового елементу матриці та напрямок збільшення нумерації. Така числова інтерпретація графічного паролю буде завжди починатися з цифри «1», перед якою буде розміщено спеціальний код, що є підказкою користувачу про зроблений раніше вибір.

Будь-який згенерований пароль, а також майстер-пароль від персонального кабінету користувача, перед зберіганням у базу даних проходить етап шифрування за наступним алгоритмом:

1) Генерується новий пароль (або береться майстер-пароль під час реєстрації користувача).

2) Останній символ запам'ятовується та видаляється з паролю.

3) Виконується хеш-перетворення паролю.

4) Кожен символ отриманого хешу зміщується на певну кількість символів алфавіту, яка залежить від символу з пункту 2).

5) Виконується додаткове хеш-перетворення.

Як правило, зламування хешу проходить в декілька разів швидше, ніж зламування грубою силою (наприклад, багатократний перебір варіантів). Але хешування персональних даних забезпечує додатковий захист у процесі їх передавання від клієнта до сервера або бази даних. Якщо зловмисник контролює один чи декілька проміжних сервісів, він не зможе відразу отримати доступ до персональних даних користувача, тому що йому ще треба буде витратити час на зламування хешу.

З іншого боку, методи, які базуються на безпосередньому зламуванні паролю, проявляють себе по-різному. На початку 21-го століття уявлення надійних паролів базувалося на використанні «хакерських» слів, в яких частина літер замінювалася на цифри. Рис. 3 ілюструє два різних підходи до створення паролю: «хакерський» та «простий». Розглянемо їх особливості окремо.

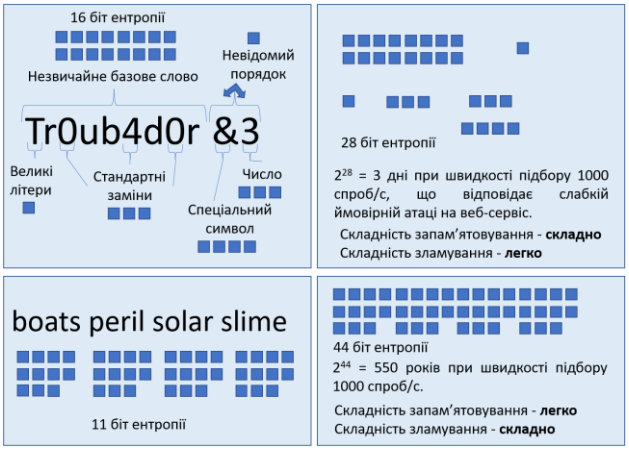

Рис. 3 – Ілюстрація складності зламування деяких паролів

«Хакерський» підхід зображено в першому рядку рис. 3. Як було сказано вище, його основною

особливістю є те, що за основу паролю обирається якесь нестандартне слово і деякі літери в ньому замінюються на цифри. Ці заміни є стандартними, наприклад, літера «О» у будь-якому регістрі замінюється цифрою «0», тому вони вносять по 1 біту ентропії в загальну складність паролю. Окрім базового слова у паролі можуть бути також присутні додаткові символи, які також вносять свій вклад у загальну складність паролю. У наведеному на рис. 3 прикладі складність «хакерського» паролю становить приблизно (розрахунок окремих елементів проводився наближено для демонстрації лише загальної тенденції) 28 біт ентропії. Такий пароль при 1000 спробах підбору в секунду зловмисник може зламати за 3 дні. Отже, складність злому такого паролю є низькою, а складність запам'ятовування – високою через наявність верхнього регістру та додаткових символів. Подібні паролі сьогодні все ще використовуються в деяких додатках.

«Простий» підхід зображено в другому рядку рис. 3. Він полягає у комбінації декількох (у наведеному прикладі чотирьох) звичайних/простих/стандартних не пов'язаних між собою логічними зв'язками слів, кожне з яких записане в одному і тому ж регістрі, складається з п'яти літер і вносить по 11 біт ентропії в загальну складність паролю. Загальна складність подібного паролю складає приблизно 44 біт ентропії. На відміну від попереднього випадку при 1000 спробах підбору в секунду зловмисник зможе зламати такий пароль за 550 років. Запам'ятати такий пароль легше завдяки візуальному їх відтворенню на спільній картині у свідомості користувача (рис. 4) або завдяки музикальній чи рифмованій аналогії. Отже, складність зламування такого паролю є високою, а складність запам'ятовування – низькою, незважаючи на значно більшу кількість символів.

Рис. 4 – Приклад візуальних аналогій паролю

Наведений приклад дає лише наближене уявлення складності безпосереднього зламування паролю. На рис. 5 та рис. 6 наведено уточнений розрахунок часу зламування паролів різної довжини, які складаються з комбінації звичайних, простих чи стандартних слів без урахування зміни регістру окремих символів та без використання цифр чи спеціальних символів.

Загальна кількість слів для генерування 9800		Середній час зламування, спроб/с	
Кількість слів у паролі	Кількість можливих комбінацій слів	100 мільйонів (маленька розподілена система)	1 мільйон (один комп'ютер)
2	96 мільйонів	Моментально	1 хвилина
3	943 мільярди	1 година	5 днів
4	9 квадрильйонів	1 рік	1 століття
5	90 квінтильйонів	144 століття	-
6	889 секстильйонів	-	-
7	8 октильйонів	-	-

Рис. 5 – Порівняння часу зламування паролів різної довжини

Загальна кількість слів для генерування 9800		Середній час зламування, спроб/с	
Кількість слів у паролі	Кількість можливих комбінацій слів	100 мільярдів (велика розподілена система)	1 мільярд (суперкомп'ютер)
2	96 мільйонів	Моментально	Моментально
3	943 мільярди	5 секунд	8 хвилин
4	9 квадрильйонів	13 годин	2 місяця
5	90 квінтильйонів	14 років	14 століть
6	889 секстильйонів	14 століть	-
7	8 октильйонів	-	-

Рис. 6 – Порівняння часу зламування паролів різної довжини

На рис. 5 та рис. 6 не вказано ще одну категорію систем – 1 трильйон спроб/с. Подібний рівень є недоступним для більшості зловмисників, тому у загальному порівнянні не розглядається. Такі системи сьогодні можуть існувати, наприклад, у спецслужб наддержав або у злочинних організацій, які інфікували та об'єднали в єдину мережу тисячі звичайних персональних комп'ютерів по всьому світу. Варто розуміти, що наведені на рисунках дані є теоретично найгіршим варіантом для зловмисників. У реальності правильна комбінація слів може бути підібрана мінімум в 2-3 рази швидше.

Також з рис. 5 та рис. 6 можна зробити висновок, що зламати пароль, який складається з 5 слів можуть вищеназвані зловмисники, пароль з 6 слів – організації з дуже великим бюджетом, наприклад, спецслужби або великі приватні компанії, які спеціалізуються на кібербезпеці. Паролі з 7 слів і більше на сьогоднішній день неможливо зламати за адекватний часовий проміжок навіть перерахованим вище категоріям. Отже, можна зробити висновок, що за складність підбору паролю в першу чергу відповідає його довжина. Інші елементи (наприклад, спеціальні символи, цифри, тощо) лише сильно ускладнюють можливість запам'ятовування і не вносять значних покращень у безпеку.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Саме тому в розробленій автоматизованій системі реалізовано алгоритм генерації паролів, які складаються з декількох слів (на вибір користувача). Також для забезпечення вимог деяких веб-сайтів та додатків є можливість включення в згенерований пароль спеціальних символів, цифр та зміни регістру окремих елементів (кількість обирається користувачем), тому що, наприклад, ПриватБанк обмежує довжину паролю користувача лише 15 символами і вимагає наявності хоча б цифр. Це значно погіршує безпеку паролю, але у користувача немає можливості обійти подібні обмеження з боку тих, хто надає необхідні послуги.

На даному етапі процесу розроблення в програмі доступний тільки словник англійської мови з кількістю слів близько 3000. У майбутньому необхідно розширити базу англійських слів та додати декілька найбільш поширених в Європі мов. Також планується удосконалити графічний інтерфейс користувача та функціональні можливості автоматизованої системи зберігання персональної інформації шляхом розширення списку категорій персональних даних, які може зберігати система.

Висновки

Сьогодні кожна людина декілька разів на день користується своєю персональною інформацією, яка при потраплянні в чужі руки може призвести до негативних для людини наслідків різного рівня серйозності. Саме тому збереження персональних даних користувачів електронних пристроїв є дуже актуальною задачею. У даній роботі частково вирішити дану задачу запропоновано шляхом використання автоматизованої системи зберігання персональної інформації користувача (логінів та паролів) у вигляді веб-додатку.

Для розроблення автоматизованої системи було спроектовано закриту багаторівневу архітектуру на базі моделі (шаблону) MVP. Реалізовано графічний інтерфейс, який є найвищим рівнем і дає доступ користувачу до основних функціональних можливостей. Реалізовано ряд підсистем, які дають змогу виконувати реєстрацію/аутентифікацію користувача, генерування, шифрування та зберігання паролів, а також іншої персональної інформації. Показано, що для генерування надійних паролів є важливою в першу чергу їх довжина. Розроблено та апробовано алгоритм подвійного хеш-перетворення паролів (у тому числі майстер-пароля) для підвищення їх стійкості до зламу.

У майбутньому планується розширити функціональні можливості розробленої автоматизованої системи зберігання персональних даних користувача. По-перше, необхідно додати німецьку, французьку та польську мови в базу для генерування паролів. По-друге, необхідно розширити базу наявних слів англійської мови. По-третє, потрібно провести дослідження нових методів генерації стійких до зламу паролів, наприклад, комбінацію слів кирилицею, але написаних відповідними символами англійської розкладки клавіатури.

Список літератури

1. LAW OF UKRAINE On Personal Data Protection. URL: https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text (дата звернення 05.10.2022).
2. Belen-Saglam R., Nurse J., Hodges D. Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*. 2022. Vol. 66. P. 103163 doi:10.1016/j.jisa.2022.103163.
3. Liu X. Research on consumers' personal information security and perception based on digital twins and Internet of Things. *Sustainable Energy Technologies and Assessments*. 2022. Vol. 53. Part C. P. 102706. doi:10.1016/j.seta.2022.102706.
4. Chua H., Ooi J., Herbland A. The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security*. 2021. Vol. 110. P. 102453. doi:10.1016/j.cose.2021.102453.
5. Raskin M. Protocols with constant local storage and unreliable communication. *Theoretical Computer Science*. 2023. Vol. 940. Part A. P. 269-282. doi:10.1016/j.tcs.2022.11.006.
6. O'Reilly J. *Network Storage Tools and Technologies for Storing Your Company's Data*. Elsevier Science & Technology, 2016, 280 p.
7. Widjaja A. E., Chen J. V., Sukoco B. M., Ha Q.-A. Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study. *Computers in Human Behavior*. 2019. Vol. 91. P. 167-185. doi:10.1016/j.chb.2018.09.034.
8. Zhao Y., Chang J. Certificateless public auditing scheme with designated verifier and privacy-preserving property in cloud storage. *Computer Networks*. 2022. Vol. 216. P. 109270. doi:10.1016/j.comnet.2022.109270.
9. Li L., Liu J. SecACS: Enabling lightweight secure auditable cloud storage with data dynamics. *Journal of Information Security and Applications*. 2020. Vol. 54. P. 102545. doi:10.1016/j.jisa.2020.102545.
10. Doukas N., Markovskyi O., Bardis N. Hash function design for cloud storage data auditing. *Theoretical Computer Science*. 2019. Vol. 800. P. 42-51. doi:10.1016/j.tcs.2019.10.015.
11. 533 million Facebook users' phone numbers and personal data have been leaked online. URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (дата звернення 01.02.2023).
12. The Social Media Sites That Have Lost The Most User Data. URL: https://businessplus.ie/tech/social-media-lost-user-data/ (дата звернення 01.02.2023).
13. Цибульник С. О., Барандич К. С. *Технології розроблення програмного забезпечення. Частина 1. Життєвий цикл програмного забезпечення. Підручник* [Електронний ресурс]: підручник для здобувачів ступеня бакалавра за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології». Київ: КПІ ім. Ігоря Сікорського, 2022, 270 с.
14. Цибульник С. О., Бідник Д. С., Півторак Д. О. Розроблення автоматизованої бібліографічної системи.

Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях. – Харків: НТУ «ХПІ». 2022. №2 (12). С. 54-60. doi:10.20998/2413-4295.2022.02.08.

References (transliterated)

1. LAW OF UKRAINE On Personal Data Protection. Available at: https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text (accessed 05.10.2022).
2. Belen-Saglam R., Nurse J., Hodges D. Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, 2022, vol. 66, pp. 103163, doi:10.1016/j.jisa.2022.103163.
3. Liu X. Research on consumers' personal information security and perception based on digital twins and Internet of Things. *Sustainable Energy Technologies and Assessments*, 2022, vol. 53, Part C, pp. 102706, doi:10.1016/j.seta.2022.102706.
4. Chua H., Ooi J., Herbland A. The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security*, 2021, vol. 110, pp. 102453, doi:10.1016/j.cose.2021.102453.
5. Raskin M. Protocols with constant local storage and unreliable communication. *Theoretical Computer Science*, 2023, vol. 940, Part A, pp. 269-282, doi:10.1016/j.tcs.2022.11.006.
6. O'Reilly J. *Network Storage Tools and Technologies for Storing Your Company's Data*. Elsevier Science & Technology, 2016, 280 p.
7. Widjaja A. E., Chen J. V., Sukoco B. M., Ha Q.-A. Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study. *Computers in Human Behavior*, 2019, vol. 91, pp. 167-185, doi:10.1016/j.chb.2018.09.034.
8. Zhao Y., Chang J. Certificateless public auditing scheme with designated verifier and privacy-preserving property in cloud storage. *Computer Networks*, 2022, vol. 216, pp. 109270, doi:10.1016/j.comnet.2022.109270.
9. Li L., Liu J. SecACS: Enabling lightweight secure auditable cloud storage with data dynamics. *Journal of Information Security and Applications*, 2020, vol. 54, pp. 102545, doi:10.1016/j.jisa.2020.102545.
10. Doukas N., Markovskyi O., Bardis N. Hash function design for cloud storage data auditing. *Theoretical Computer Science*, 2019, vol. 800, pp. 42-51, doi:10.1016/j.tcs.2019.10.015.
11. 533 million Facebook users' phone numbers and personal data have been leaked online. Available at: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (accessed 01.02.2023).
12. The Social Media Sites That Have Lost The Most User Data. Available at: https://businessplus.ie/tech/social-media-lost-user-data/ (accessed 01.02.2023).
13. Tsybulnyk S. O., Barandych K. S. Tekhnolohii rozroblennia prohramnoho zabezpechennia. Chastyna 1. Zhyttievyi tsykl prohramnoho zabezpechennia. Pidruchnyk [Elektronnyi resurs]: pidruchnyk dlia zdobuvachiv stupenia bakalavra za spetsialnistiu 151 «Avtomatyzatsiia ta komp'iuterno-intehrovani tekhnolohii». Kyiv. KPI im. Ihoria Sikorskoho, 2022, 270 p.
14. Tsybulnyk S., Bidnyk D., Pivtorak D. Development of an automated bibliographic system. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2022, no. 2(12), pp. 54-60, doi:10.20998/2413-4295.2022.02.08.

Відомості про авторів (About authors)

Цибульник Сергій Олексійович – кандидат технічних наук, доцент, КПІ ім. Ігоря Сікорського, доцент кафедри комп'ютерно-інтегрованих оптичних та навігаційних систем; м. Київ, Україна; ORCID: 0000-0002-4462-0936; e-mail: tsybulnik.s.a@gmail.com.

Tsybulnyk Serhii – Candidate of Technical Sciences (Ph. D.), Docent, Associate Professor, Department of Computer-Integrated Optical and Navigation Systems, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine; ORCID: 0000-0002-4462-0936; e-mail: tsybulnik.s.a@gmail.com.

Зубарський Дмитро Олександрович – студент кафедри комп'ютерно-інтегрованих оптичних та навігаційних систем; м. Київ, Україна.

Zubarskyi Dmytro – student, Department of Computer-Integrated Optical and Navigation Systems, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine.

Півторак Діана Олександрівна – кандидат технічних наук, доцент, КПІ ім. Ігоря Сікорського, доцент кафедри комп'ютерно-інтегрованих оптичних та навігаційних систем; м. Київ, Україна; ORCID: 0000-0003-3708-5610.

Pivtorak Diana – Candidate of Technical Sciences (Ph. D.), Docent, Associate Professor, Department of Computer-Integrated Optical and Navigation Systems, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine; ORCID: 0000-0003-3708-5610.

Будь ласка, посилайтесь на цю статтю наступним чином:

Цибульник С. О., Зубарський Д. О., Півторак Д. О. Прикладне програмне забезпечення для зберігання персональної інформації. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2023. № 1 (15). С. 53-59. doi:10.20998/2413-4295.2023.01.07.

Please cite this article as:

Tsybulnyk S., Zubarskyi D., Pivtorak D. Applied software for personal information storage. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2023, no. 1(15), pp. 53-59, doi:10.20998/2413-4295.2023.01.07.

Надійшла (received) 25.02.2023
Received 16.03.2023