УДК **37.091.3:004.056**

Швець Софія Олександрівна
учениця 9Б класу
Ліцей №9 “Гармонія” Оболонського району м. Києва,
м. Київ, Україна
sofiaashvetss@gmail.com

Власенко Юлія Миколаївна
спеціаліст вищої категорії, учитель-методист,
вчитель інформатики та математики
Ліцей №9 “Гармонія” Оболонського району м. Києва,
м. Київ, Україна
yuzefa89school9@gmail.com

ЗАХИСТ ОСОБИСТИХ ДАНИХ КОРИСТУВАЧІВ У ЦИФРОВОМУ СЕРЕДОВИЩІ ЗАСОБАМИ ПАРОЛІВ

Анотація. У статті досліджується проблема захисту особистих даних користувачів у цифровому середовищі і методи підвищення власної безпеки за допомогою надійних паролів. Через зростання кількості кіберзагроз і витоків конфіденційних даних, що часто пов’язані з використанням слабких і повторюваних паролів. У межах дослідження проведено міні-опитування серед 30 учнів щодо створення, зберігання і використання паролів, результати якого показали, що більшість користувачів не зберігає свої паролі надійно і обирає такі паролі, які не є досить захищеними, складними і надійними. У роботі описано розробку власного програмного забезпечення на мові Python для генерації, зберігання та управління паролями, що спрямоване на підвищення рівня захисту облікових записів. Отримані результати підкреслюють необхідність підвищення цифрової грамотності користувачів і впровадження ефективних інструментів кіберзахисту.

Ключові слова: кібербезпека; захист даних; менеджер паролів; генератор паролів.

1. ВСТУП

У сучасному світі кожна людина користується десятками онлайн-сервісів. Щодня ми використовуємо соціальні мережі, електронну пошту, освітні платформи і банківські системи. Щоб отримати доступ до цих сервісів і інформацію, що в них міститься, використовуються облікові записи, основним засобом захисту яких є пароль [1; 2]. Саме він є першою річчю, яка захищає особисті дані користувачів від несанкціонованого доступу.

Проте чим розвинутішими стають технології, тим більше з’являється різних загроз. Хакерські атаки, витоки баз даних державних ресурсів, фішингові сайти і шкідливі програми-віруси стають все більш поширенішими [4; 5]. Більшість таких інцидентів відбувається через використання слабких або однакових паролів для різних сервісів [6]. Значна частина користувачів обирає прості комбінації символів, які легко вгадати, якщо знати їх власника, а також використовує в паролях особисту інформацію, яка є усім відома.

Це дослідження було проведене з метою з’ясувати, як користувачі створюють паролі, які методи захисту використовують і наскільки вони обізнані. Для цього було проведено опитування серед 30 учнів Ліцею, результати якого дозволили проаналізувати рівень цифрової безпеки користувачів власного навчального закладу. Отримані результати показали, що значна частина користувачів надає перевагу простим паролям, які легко запам’ятати, але вони є неймовірно вразливими до атак [7]. Також виявлено,

що досить мала частина респондентів використовує додаткові засоби захисту, такі як менеджери паролів або їх генератори.

Отже, проблема захисту особистих даних залишається як ніколи актуальною, а підвищення цифрової грамотності користувачів є дуже важливою у боротьбі з кіберзлочинністю.

Постановка проблеми. Сучасне інформаційне суспільство зберігає персональні дані у великій кількості онлайн-сервісів. Ненадійні паролі і недостатній рівень обізнаності користувачів щодо видів кіберзагроз можуть призвести до витоку конфіденційної інформації і несанкціонованого доступу до облікових записів, що може привести до жахливих наслідків для їх власника [5].

Аналіз останніх досліджень і публікацій. Проблема захисту даних є однією з основних у сфері кібербезпеки. Одним із найпоширеніших способів злому є брутфорс-атака, яка заключається в автоматичному перебиранні всі можливих комбінацій символів до знаходження правильного пароля. Також фішингові атаки є загрозою для довірливих і неосвічених користувачів, особливо старшого покоління, змушуючи добровільно повідомити свої облікові дані. Сучасні дослідження також приділяють увагу розвитку менеджерів і генераторів паролів, які дозволяють безпечно зберігати складні паролі за допомогою різних методів шифрувань і генерувати нові захищені комбінації [7].

Мета дослідження. Дослідити фактори, що впливають на безпеку паролів та проаналізувати поведінку користувачів під час вибору та використання паролів. Розробити ефективні інструменти для забезпечення надійного захисту особистих даних через створення програми для генерації і зберігання паролів, а також дослідити фактори, що впливають на безпеку паролів.

2. МЕТОДИКА ДОСЛІДЖЕННЯ

Під час підготовки дослідження було проаналізовано сучасні підходи до забезпечення кібербезпеки, зокрема методи створення та захисту паролів, а також виявлено основні проблеми, пов’язані з використанням слабких і повторюваних паролів [2; 4]. Саме дослідження базується на онлайн-опитуванні (Google Forms), у якому взяв участь учні Ліцею №9 м. Києва. Окремим етапом стала практична реалізація отриманих результатів, у межах якої було розроблено власне програмне забезпечення для генерації, зберігання та контролю паролів [3].

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

3.1. Аналіз опитування

Для розуміння психології вибору паролів було проведене онлайн-опитування за допомогою сервісу Google Forms. Анкета складалася з 9 питань, які можна поділити на 4 категорії: створення паролів, безпечне використання паролів, ускладнення паролів, збереження паролів. У кожному питанні 3-4 варіанти відповідей, 4 питання надають можливість дописати свою відповідь.

Як показали результати опитування (Рис. 1), зазвичай користувачі обирають прості паролі, які легко придумати і запам’ятати, не захищають свою особисту інформацію складними комбінаціями і обирають зручність. Такі дії можуть призвести до неприємних наслідків, як, наприклад, витік даних у відкритий доступ. 64.5% використовують однакові паролі для сайтів, менша частина з них лише додає декілька символів до вже існуючого пароля, що не є методом створення нового пароля. Знаючи один пароль користувача, хакер може легко зрозуміти, як людина створює свої паролі, додати до

кілька нових символів і отримати доступ до тієї інформації, доступ до якої був засекречений іншим паролем.

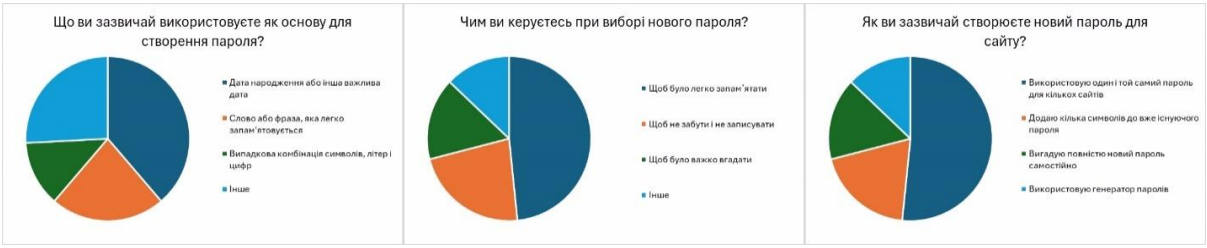

Рис. 1. Результати опитування (категорія «Створення паролів»)

Підбиваючи підсумки опитування з другої категорії (Рис. 2), зазвичай користувачі нехтують своє безпекою і до більшості сайтів використовують однаковий нескладний пароль. Якщо зловмисник захоче отримати доступ до особистої інформації, то він не зіткнеться з жодними проблемами. Паролі слід змінювати раз в 3 місяці або в півроку, адже існують сайти, де зібрані злиті паролі користувачів. Вони допомагають перевірити, чи є пароль у вільному доступі, але також надають змогу хакерам отримати всю інформацію з сайтів, де використовується один і той же обліковий запис.

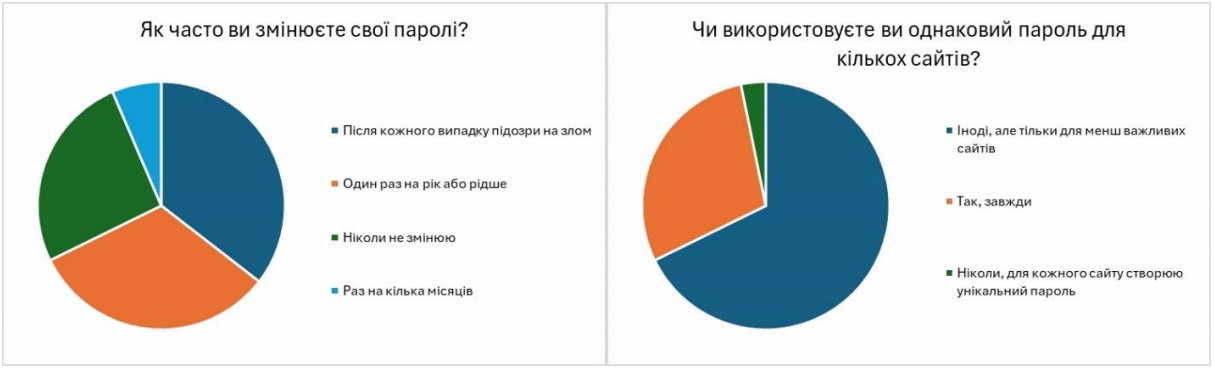

Рис. 2. Результати опитування (категорія «Безпечне використання паролів»)

У категорії «Ускладнення паролів» (Рис. 3) користувачі показали досить високий рівень піклування про свою інтернет-безпеку: більша частина використовує спеціальні символи, які значно ускладнюють угадування пароля і застосовує автоматичні генератори паролів, у яких є алгоритм створення складного пароля. На жаль, є відсоток користувачів, що не знають що таке автоматичні генератори паролів або не довіряють таким інструментам, але ніколи не пізно почати піклуватися про свою безпеку і ускладнювати свої паролі.

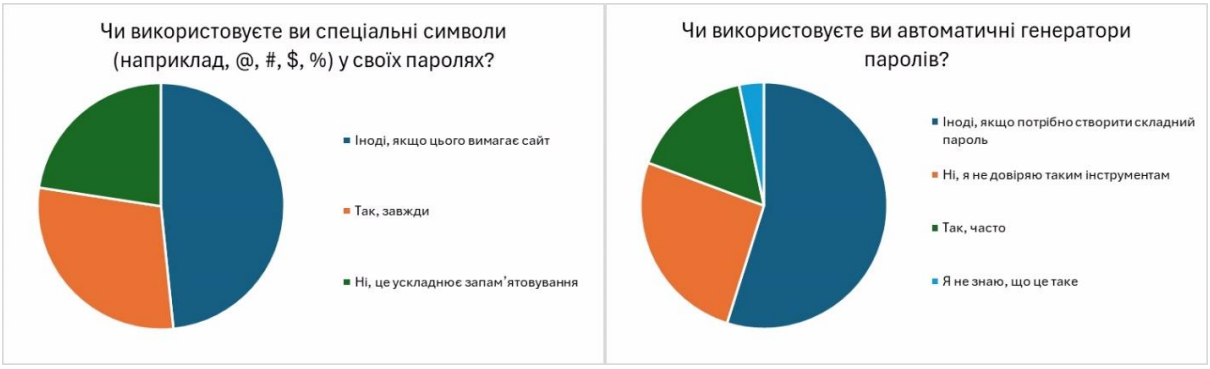

Рис. 3. Результати опитування (категорія «Ускладнення паролів»)

Зовсім малий відсоток учнів використовує менеджери паролів і обирає їх запам'ятовування або записування на фізичні носії (Рис. 4). Це не є неправильним, але запам'ятати велику кількість складних комбінацій людина не може фізично. Записування паролів на окремий файл не є безпечним, адже через хакерські програми злодії можуть отримати віддалений доступ до пристроїв користувачів, а записування паролів на блокнот може бути небезпечним у разі постійної роботи з людьми, які можуть піддивитися паролі і використати їх.

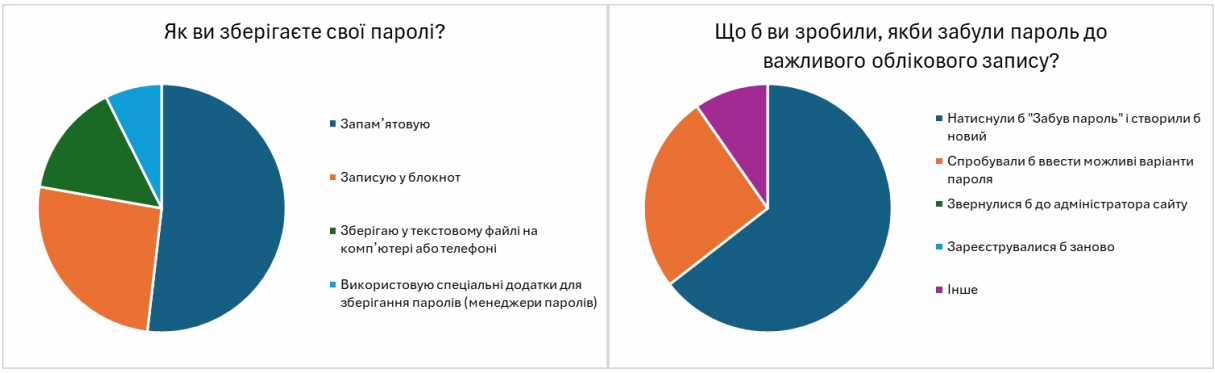

Рис. 4. Результати опитування (категорія «Збереження паролів»)

Після проведення опитування та аналізу отриманих результатів було встановлено, що значна частина користувачів нехтує базовими правилами кібербезпеки: використовує однакові паролі для різних сервісів, створює прості комбінації та не застосовує спеціалізовані засоби для їх збереження. Це свідчить про необхідність створення зручних та ефективних інструментів для підвищення рівня захисту персональних даних.

3.2. Розробка програмного забезпечення

У зв'язку з цим у межах дослідження було розроблено власне програмне забезпечення (менеджер паролів) на основі мови програмування Python [3]. Основною метою програми є підвищення рівня захисту персональних даних шляхом використання складних випадкових паролів, які важко підібрати за допомогою автоматичних атак. Програма має простий і зрозумілий інтерфейс (Рис. 5), що дозволяє користувачу швидко виконувати основні операції. Є можливість зберігати існуючі паролі (збережені в базі як ім'я сервісу, логін і відповідний пароль), генерувати випадкові паролі, що відповідають умовам надійності, зберігати облікові дані, переглядати і редагувати збережену раніше інформацію.

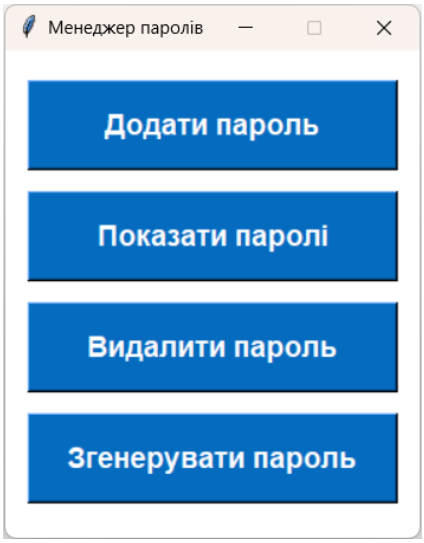

Рис. 5. Інтерфейс програми

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У процесі дослідження були проаналізовані основні методи злому паролів. Це дозволило визначити важливість застосування надійних паролів і засобів їхнього зберігання. Дослідження показало, що надійні паролі повинні бути довгими, випадковими, містити комбінацію літер різного регістру, цифр і спеціальних символів. Використання однакових паролів для різних облікових записів значно підвищує ризик їх злому.

На основі опитування, що провела серед учнів Ліцею №9 «Гармонія» виявлено, що користувачі часто обирають легкі для запам'ятовування паролі, не використовуючи генерацію паролів та менеджери зберігання. Досліджуючи тему, було проаналізовано популярні сервіси генерації паролів і менеджери паролів. На основі порівняльної характеристики визначено їхні переваги та недоліки, що допомогло сформувати вимоги до створення власного програмного продукту.

У майбутньому доцільно продовжити дослідження цієї теми, розширивши вибірку респондентів, включивши різні вікові групи. Перспективними напрямами подальших досліджень можуть стати підвищення ефективності менеджерів паролів, дослідження використання багатофакторної автентифікації, розробка програмних інструментів для автоматичного створення та зберігання надійних паролів.

Такі дослідження допоможуть підвищити рівень цифрової безпеки користувачів та сприятимуть більш відповідальному ставленню до захисту особистих даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. Київ, 2018. С. 112-131.
2. Коваленко О. В., *Основи кібербезпеки*. Київ: КПІ ім. Ігоря Сікорського, 2021.
3. Костюченко А.О. Основи програмування мовою Python: навчальний посібник. Чернігів: ФОП Баликіна С.М., 2020. 180 с.
4. Петренко С. О., *Кібербезпека в інформаційному суспільстві*. Київ: Наукова думка, 2019.
5. Шелест М. Ю., *Інформаційна безпека та захист даних*. Харків: ХНУРЕ, 2020.
6. Bonneau J., The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. IEEE Symposium on Security and Privacy, 2012. URL: https://doi.org/10.1109/SP.2012.49

7. Gaw S., Felten E., Password Management Strategies for Online Accounts. SOUPS, 2006. URL: https://doi.org/10.1145/1143120.1143127

Матеріал надійшов до редакції 03.04.2026 р.

PROTECTION OF USERS' PERSONAL DATA IN THE DIGITAL ENVIRONMENT BY MEANS OF PASSWORDS

Shvets Sofiia Oleksandrivna
9-B Grade Student
Lyceum No. 9 "Harmonia" of Obolonskyi District, Kyiv
Kyiv, Ukraine
sofiaashvetss@gmail.com

Vlasenko Yuliia Mykolaivna
Top Category Specialist, Methodologist Teacher,
Teacher of Computer Science and Mathematics
Lyceum No. 9 "Harmonia" of Obolonskyi District, Kyiv
Kyiv, Ukraine
yuzefa89school9@gmail.com

Abstract. The article examines the problem of protecting users' personal data in the digital environment and methods of improving personal security through the use of strong passwords. The relevance of the study is обусловлена the growing number of cyber threats and data breaches, which are often associated with the use of weak and reused passwords. As part of the research, a mini-survey was conducted among 30 students regarding the creation, storage, and use of passwords. The results showed that most users do not store their passwords securely and tend to choose passwords that are not sufficiently strong, complex, or reliable. The paper also describes the development of proprietary software in Python for password generation, storage, and management, aimed at enhancing account security. The obtained results emphasize the need to improve users' digital literacy and to implement effective cybersecurity tools.

Keywords: cybersecurity, password, data protection, password manager, password generator.