УДК 004.6 DOI https://doi.org/10.35546/kntu2078-4481.2026.1.34

Е. К. ДОЛЯ
студентка кафедри кібербезпеки інформаційних систем, мереж і технологій
Харківський національний університет імені В. Н. Каразіна
ORCID: 0009-0006-8286-5885

О. Є. ДОЛЯ
кандидат технічних наук, доцент,
доцент кафедри інформаційних управляючих систем
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-0364-988X

НАДІЙНІСТЬ МЕХАНІЗМІВ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ: ВПЛИВ ЛЮДСЬКОГО ФАКТОРА

У статті розглядаються питання надійності парольної автентифікації як одного з найпоширеніших механізмів захисту інформації в сучасних інформаційних системах. Незважаючи на активний розвиток технологій кібербезпеки, паролі залишаються основним засобом автентифікації користувачів, що зумовлює актуальність дослідження проблем, пов'язаних з їх використанням. Особливу увагу приділено впливу людського фактора на рівень захищеності облікових записів, оскільки значна частина інцидентів інформаційної безпеки виникає саме через використання слабких паролів. У роботі було проаналізовано принципи функціонування парольної автентифікації, зокрема поняття складності паролів, роль довжини та різноманітності символів, а також значення хешування паролів під час їх зберігання в інформаційних системах. Окремо розглянуто типові помилки користувачів, серед яких використання простих комбінацій символів, особистої інформації, однакових паролів для різних сервісів та використання коротких паролів. Такі підходи суттєво знижують рівень захисту персональних даних і створюють сприятливі умови для реалізації атак. Практична частина статті ґрунтується на результатах анонімного опитування студентів, проведеного з метою аналізу реальних практик використання паролів і додаткових засобів захисту. В опитуванні досліджено рівень поширеності повторного використання паролів, середню довжину парольних комбінацій, застосування спеціальних символів, обізнаність користувачів щодо хешування паролів, а також використання двоетапної автентифікації та менеджерів паролів. Отримані результати дозволяють зробити висновок про недостатній рівень уваги користувачів до питань інформаційної безпеки, незважаючи на доступність сучасних інструментів захисту. На основі проведеного аналізу сформульовано рекомендації щодо підвищення надійності парольного захисту, зокрема використання унікальних складних паролів, менеджерів паролів та двоетапної (двофакторної) автентифікації.

Ключові слова: *інформаційна безпека, механізми автентифікації, надійність паролів, людський фактор, хешування паролів, двоетапна автентифікація.*

E. K. DOLIA
Student at the Department of Cybersecurity of Information Systems,
Networks and Technologies
V. N. Karazin Kharkiv National University
ORCID: 0009-0006-8286-5885

O. E. DOLIA
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Information Control System
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-0364-988X

RELIABILITY OF AUTHENTICATION MECHANISMS IN INFORMATION SYSTEMS: THE INFLUENCE OF THE HUMAN FACTOR

The article examines the reliability of password authentication as one of the most common mechanisms for protecting information in modern information systems. Despite the active development of cybersecurity technologies, passwords remain the main means of user authentication, which makes it urgent to study the problems associated with their use. Particular attention is paid to the influence of the human factor on the level of account security, since a significant part

of information security incidents arise precisely due to the use of weak passwords. The paper analyzes the principles of functioning of password authentication, in particular the concept of password complexity, the role of length and variety of characters, as well as the importance of hashing passwords when storing them in information systems. Typical user errors are separately considered, including the use of simple combinations of characters, personal information, identical passwords for different services, and the use of short passwords. Such approaches significantly reduce the level of protection of personal data and create favorable conditions for attacks. The practical part of the article is based on the results of an anonymous survey of students conducted to analyze real-world practices of using passwords and additional security measures. The survey investigated the prevalence of password reuse, the average length of password combinations, the use of special characters, users' awareness of password hashing, and the use of two-step authentication and password managers. The results obtained allow us to conclude that users pay insufficient attention to information security issues, despite the availability of modern security tools. Based on the analysis, recommendations were formulated to improve the reliability of password protection, in particular, the use of unique complex passwords, password managers, and two-step (two-factor) authentication.

Key words: *information security, authentication mechanisms, password strength, human factor, password hashing, two-step authentication.*

Постановка проблеми

У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації більшості сфер діяльності людини питання захисту інформації набувають особливої актуальності. Щоденне використання інформаційних систем передбачає необхідність постійної автентифікації користувачів, найпоширенішим засобом якої залишається пароль. Незважаючи на появу новітніх методів біометричної та багатофакторної автентифікації, парольний захист і надалі відіграє ключову роль у забезпеченні доступу до інформаційних ресурсів.

Разом із тим практика показує, що значна кількість інцидентів інформаційної безпеки пов'язана не з недосконалістю технічних засобів захисту, а з людським фактором. Використання слабких, коротких або передбачуваних паролів, повторне застосування одних і тих самих комбінацій для різних сервісів, зберігання паролів у незахищеному вигляді та ігнорування додаткових механізмів захисту створюють серйозні загрози для конфіденційності даних [1-2]. Особливо поширеною залишається практика використання простих паролів на кшталт «123456», «password» або особистої інформації користувача, що суттєво знижує рівень захищеності облікових записів [3-4].

У зв'язку з цим виникає необхідність комплексного дослідження проблеми надійності парольного захисту з урахуванням поведінкових особливостей користувачів. Аналіз реальних практик створення та використання паролів, а також рівня обізнаності щодо сучасних методів інформаційної безпеки дозволяє визначити основні вразливості та сформулювати ефективні рекомендації щодо їх усунення.

Аналіз останніх досліджень і публікацій

Проблематика парольної автентифікації та методи захисту облікових записів активно досліджується в працях вітчизняних науковців. Автори Баришев Ю. В., Чайкін М. М., Кохан О. В. [1] зазначають, що використання простих, занадто передбачуваних слів та символьних комбінацій негативно впливають на методи парольної авторизації. Паралельно було запропоновано ознайомитися з методом генерування паролів, що може перетворювати слово, яке б вони в майбутньому використовували для пароля, на набір символів за допомогою мови програмування Java. В іншій роботі, автором Головко Д.Ю. [4] розглянуто те, що є певні поширені паролі, які зламуються найлегше, наприклад: «123456», «password», «111111», «sunshine» та інші. Автор пропонує створювати паролі за допомогою декількох способів: використовувати дитяче слово (згадати слово, яке використовували в дитинстві і додати до нього цифри з символами); робити акроніми з фраз (взяти фразу з цитати/вірша, потім взяти лише першу літеру з кожного слова, записати їх латиницею і додати символи з цифрами); вводити випадкові символи (друкувати випадкові символи) та малювати візуальні ключі на клавіатурі (проводити пальцем по літерах та цифрах в певному порядку).

У багатьох роботах зазначається, що, попри технічний прогрес, людський фактор залишається однією з головних причин порушення інформаційної безпеки. Дослідження показують, що користувачі часто обирають паролі, керуючись зручністю запам'ятовування, а не вимогами безпеки. У своїй статті Коцюк Ю. А. [5] зазначає, що відповідно до статистики багато користувачів відчувають дискомфорт при створенні надійного паролю. З одного боку, занадто прості створені паролі використовувати небезпечно, з іншого боку складні паролі дуже важко запам'ятовувати. Автором було створено список типових помилок користувачів серед яких є використання дати народження та типових паролів, таких як «qwerty», «******» (шість зірочок) тощо. Також авторами Чаплик Т., Гоч П. [6] з'ясовано, що фундаментом для ефективної системи інформаційної безпеки є досвід, компетенції та знання персоналу. Потрібно володіти певним рівнем знань про загрози та деякі принципи безпеки, які визначають ефективність захисту даних користувачів від людського фактора, який наразі є однією з найголовніших причин порушення інформаційної безпеки.

У праці, присвяченій заходам з кібергігієни, зазначається про те, що дуже важливо уникати використання однакових паролів користувачами для різних сервісів [7]. Новохатній Д. Ю. підкреслює те, що надійно створені

паролі є першою лінією захисту від несанкціонованого доступу до облікових записів користувачів. Він рекомендує створювати складні паролі довжиною не менше 12 символів, що містять комбінації великих і малих літер, цифр і спеціальних знаків.

Окремі автори звертають увагу на потребу впровадження двоетапної автентифікації, зважаючи на її високу ефективність у запобіганні зламу. У праці Новохатнього Д. Ю. [7] паралельно звертається увага на двофакторну автентифікацію, яка виконує додатковий рівень захисту паролів, вимагаючи підтвердження особистості користувача під час входу через певний канал, наприклад, за допомогою SMS-коду (одноразового паролю), електронної пошти або спеціального застосунку для автентифікації. Впровадження 2FA підвищує безпеку облікових записів користувачів. Також автори Опірський І., Сікорський Р., Мартинюк Д. [8] вказують на те, що двофакторна автентифікація є засобом забезпечення конфіденційності та цілісності ресурсів у цифровому середовищі. Через велику кількість кіберзагроз і випадків несанкціонованого доступу до облікових записів з'ясовано, що традиційна автентифікація за допомогою пароля вже не може цілком виконувати захисну функцію на належному рівні. Саме тому існує потреба у використанні надійніших засобів автентифікації, проте ефективність двофакторної автентифікації на практиці залежить не лише від технічної реалізації, а й від поведінки самих користувачів.

Також у наукових публікаціях розглядаються методи хешування паролів. В роботі авторів Багрій Р., Бармак О., Манзюк Е. [9] було проведено дослідження схем хешування паролів для підвищення стійкості паролів до різних типів атак. Одним із методів є використання хешування паролів із сіллю, що дозволяє забезпечити більший рівень захисту паролів користувачів, де сіль є випадковим набором символів, який додається до паролю перед його хешуванням. Також у статті висвітлено важливість оновлення та вдосконалення методів хешування та застосування найновіших стандартів безпеки для захисту даних. У роботі автора Тищенко А. А. [10] представлено загальне представлення поняття хешування паролів, яке є одним із найпоширеніших методів зберігання паролів, де паролі перетворюють на випадкові рядки фіксованої довжини за допомогою хеш-функції. Процес хешування є незворотним, неможливо відновити вихідне значення пароля з хешу, що робить його відносно безпечним для зберігання. Втім, атаки методами переборів можуть бути успішними, якщо використовуються слабкі паролі.

Водночас аналіз літературних джерел свідчить про недостатню кількість практичних досліджень, спрямованих на вивчення реальної поведінки користувачів у повсякденному цифровому середовищі. Саме тому поєднання теоретичного аналізу з результатами емпіричного опитування є доцільним та актуальним напрямом дослідження.

Формулювання мети дослідження

Метою даного дослідження є аналіз надійності парольної автентифікації в сучасних інформаційних системах з урахуванням впливу людського фактора, а також визначення рівня обізнаності користувачів щодо основних принципів створення безпечних паролів і використання додаткових механізмів захисту.

Для досягнення поставленої мети в роботі передбачено розв'язання таких завдань:

– дослідити принципи функціонування парольної автентифікації;
– проаналізувати типові помилки користувачів при створенні та використанні паролів;
– оцінити рівень використання двоетапної автентифікації та менеджерів паролів;
– узагальнити результати опитування та сформулювати практичні рекомендації щодо підвищення рівня інформаційної безпеки.

Викладення основного матеріалу дослідження

Парольна автентифікація є одним із найпоширеніших механізмів контролю доступу до інформаційних ресурсів [11]. Її популярність зумовлена відносною простотою реалізації, універсальністю та звичністю для користувачів. Пароль виступає секретною інформацією, знання якої підтверджує право користувача на доступ до певної системи або сервісу.

Процес парольної автентифікації передбачає кілька основних етапів. Під час реєстрації користувач створює пароль, який не зберігається у відкритому вигляді, а проходить процедуру криптографічного перетворення – хешування. Хеш-функція перетворює пароль у фіксований набір символів. Під час кожної спроби входу введений пароль хешується, а отримане значення порівнюється зі збереженим набором символів у системі [12].

Надійність пароля визначається сукупністю кількох характеристик, серед яких ключовими є довжина, складність та унікальність. Чим більша довжина пароля, тим більший простір можливих комбінацій, що суттєво підвищує стійкість до атак повного перебору. Використання комбінації великих і малих літер, цифр та спеціальних символів додатково ускладнює процес зламу [7].

Унікальність пароля означає його використання лише для одного сервісу. Повторне застосування одного і того самого пароля значно підвищує ризики, оскільки компрометація одного облікового запису може призвести до втрати доступу до кількох ресурсів одночасно [7]. Саме ця проблема є однією з найпоширеніших у практиці користувачів.

Парольний захист є об'єктом різноманітних атак. Найпоширенішими є атаки повного перебору, при яких система послідовно перевіряє всі можливі комбінації символів [13]. Ефективність таких атак значною мірою залежить від довжини та складності пароля. Не менш поширеними є словникові атаки, які ґрунтуються на використанні баз

даних найпопулярніших паролів [14]. Саме тому комбінації на кшталт «123456», «password» або імен користувачів залишаються вкрай небезпечними.

Людський фактор є одним із ключових аспектів, що впливають на ефективність парольного захисту. Більшість користувачів схильні обирати прості та легко запам'ятовувані паролі, нехтуючи рекомендаціями з безпеки. Це пояснюється як низьким рівнем обізнаності, так і прагненням мінімізувати зусилля під час роботи з інформаційними системами [5].

Одним із найбільш ефективних способів підвищення рівня захисту облікових записів є впровадження двоетапної автентифікації. Цей механізм передбачає використання додаткового фактору підтвердження особи, наприклад одноразового коду, що надсилається на мобільний пристрій або генерується спеціальним застосунком [7-8]. Навіть у разі компрометації пароля наявність другого фактору значно знижує ймовірність несанкціонованого доступу. Однак результати досліджень свідчать про те, що користувачі не завжди активно використовують двоетапну автентифікацію через незручність або недостатнє розуміння її переваг.

Менеджери паролів є програмними засобами, призначеними для безпечного зберігання та генерації складних унікальних паролів [3]. Вони дозволяють зменшити когнітивне навантаження на користувачів і водночас підвищити загальний рівень інформаційної безпеки. Використання таких засобів є одним із рекомендованих підходів у сучасних системах захисту інформації.

Отже, аналіз теоретичних аспектів парольної автентифікації підтверджує, що ефективність захисту значною мірою залежить від поєднання технічних рішень і відповідальної поведінки користувачів. Саме тому доцільним є доповнення теоретичного аналізу практичним дослідженням, спрямованим на оцінку реальних підходів до використання паролів, що буде розглянуто в наступному підрозділі.

Практична частина: аналіз результатів опитування

З метою дослідження реальних практик використання парольної автентифікації та рівня обізнаності користувачів щодо засобів захисту облікових записів було проведено анонімне опитування. Опитування здійснювалося дистанційно за допомогою онлайн-інструментів і не передбачало збору персональних даних або реальних паролів респондентів. У дослідженні взяли участь 28 осіб, серед яких основну частину становили студенти.

Анкетування охоплювало десять запитань, спрямованих на виявлення підходів користувачів до створення та використання паролів, частоти їх зміни, застосування додаткових механізмів захисту, а також рівня обізнаності у сфері інформаційної безпеки. Отримані результати подано у вигляді діаграм, що дозволяє наочно проаналізувати основні тенденції.

Питання та результати опитування:

Питання 1. Частота використання одного пароля

Респондентам було запропоновано оцінити, як часто вони використовують один і той самий пароль для кількох сервісів. Отримані результати подано у вигляді відсоткового співвідношення: 42,9 % – часто, 35,7 % – інколи, 14,3 % – ніколи та 7,1 % відповідно рідко (рис. 1).

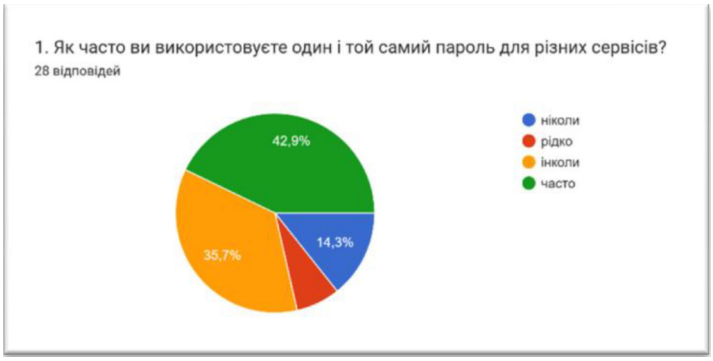

Рис. 1. Розподіл відповідей респондентів щодо використання одного пароля

Аналіз відповідей свідчить, що більшість опитаних часто використовують однакові паролі, що є ризикованою практикою з точки зору кібербезпеки. Для захисту фахівці з кібербезпеки рекомендують використовувати унікальні складні паролі для кожного ресурсу [15].

Питання 2. Середня довжина паролів

Питання було спрямоване на визначення середньої довжини паролів, які використовують респонденти. Варіанти відповідей включали кілька діапазонів довжини паролів. Отримані результати подано у вигляді відсоткового співвідношення: 50 % опитуваних використовують 9–12 символів, 28,6 % використовують 6–8 символів, 17,9 % використовують більше 12 символів і 3,5 % відповідно використовують до 6 символів (рис. 2).

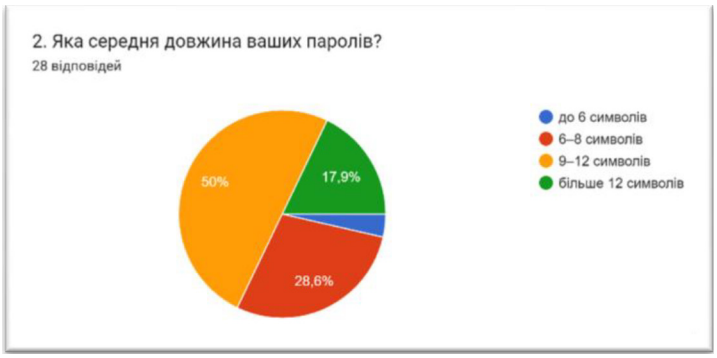

Рис. 2. Середня довжина паролів, що використовуються респондентами

З отриманих даних видно, що більшість опитаних (50 %) використовують паролі довжиною 9–12 символів і 17,9 % опитаних респондентів використовують паролі довжиною більше 12 символів. Довгі паролі надійніші, тому пароль має складатися принаймні з 12–14 символів [7].

Питання 3. Використання різних типів символів у паролях

У межах даного питання було досліджено, які типи символів переважають у паролях користувачів: лише літери, літери з цифрами або комбінація літер, цифр та спеціальних символів. Результати опитування відображено на рисунку: 53,6 % опитаних використовують літери, цифри та спеціальні символи, 32,1 % використовують літери та цифри, 10,7 % лише літери і 3,6 % випадково згенеровані паролі (рис. 3).

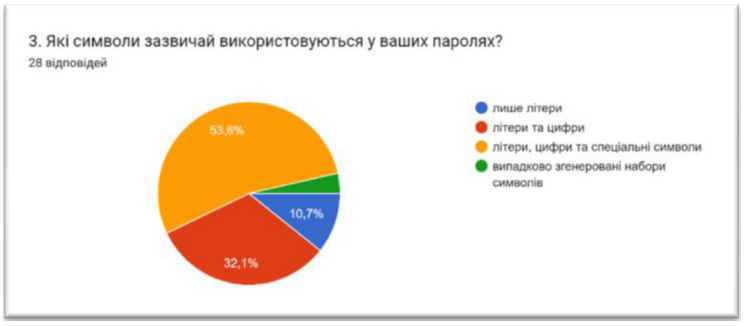

Рис. 3. Типи символів, що використовуються у паролях

Отримані результати демонструють, що більшість опитаних (53,6 %) використовують комбінації літер, цифр та спеціальних символів, що є правильним. Випадкові паролі можуть забезпечувати максимальну складність при мінімальній довжині.

Питання 4. Використання власної інформації у паролях

Метою даного питання було з'ясування, чи використовують респонденти власну інформацію під час створення нового паролю для облікового запису. Отримані результати подано у вигляді відсоткового співвідношення: 46,4 % опитаних не використовують і 32,1 % інколи (рис. 4).

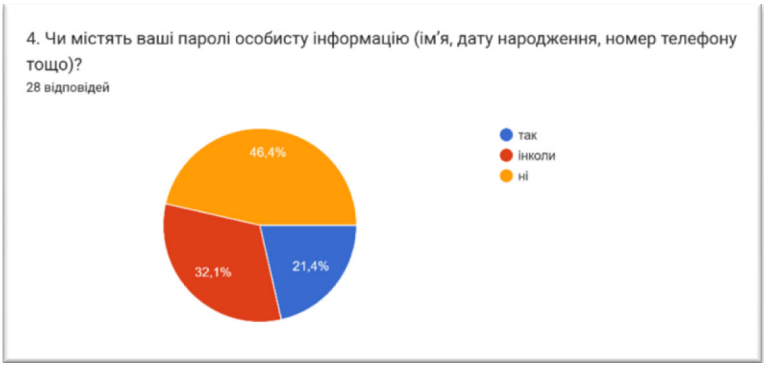

Рис. 4. Використання особистої інформації у паролях

З отриманих даних видно, що більшість опитаних не використовують особисту інформацію для створення паролів, проте певна частка опитаних іноді використовують.

Питання 5. Частота зміни паролю

У межах даного питання було досліджено, як часто користувачі змінюють свої паролі: регулярно, лише у разі підозри на злам, практично ніколи і коли забувають пароль. Результати опитування відображено на рисунку: 50 % змінюють лише у разі підозри на злам, 21,4 % практично ніколи, 14,3 % коли забувають пароль і 14,3 % раз на кілька місяців (рис. 5).

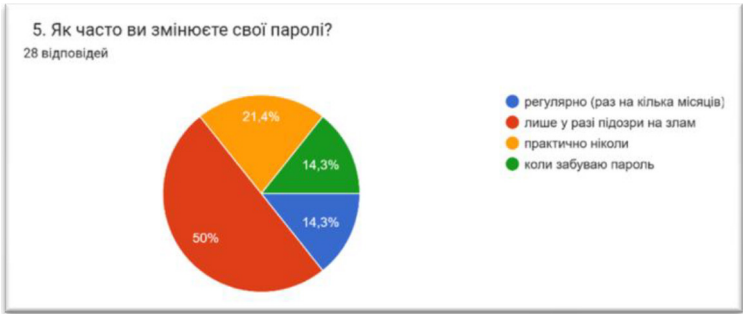

Рис. 5. Аналіз частоти зміни паролю

Отримані результати демонструють, що більшість опитаних змінюють свої паролі лише у разі підозри на злам, інші 14,3 % змінюють регулярно раз на кілька місяців.

Питання 6. Використання двоетапної (двофакторної) автентифікації

Метою даного питання було з'ясування, чи використовують респонденти двоетапну (двофакторну) автентифікацію для захисту облікового запису: так, ні або взагалі не знають що це. Отримані результати подано у вигляді відсоткового співвідношення (рис. 6).

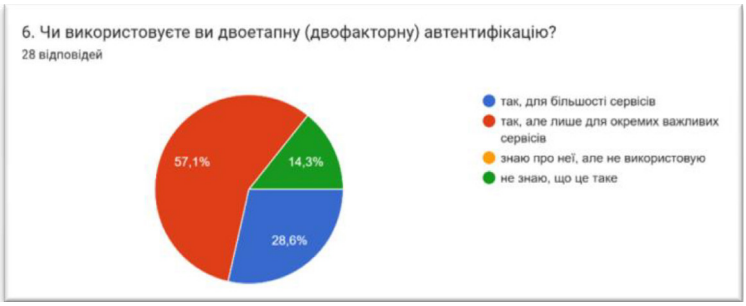

Рис. 6. Аналіз використання двоетапної (двофакторної) автентифікації

З отриманих даних видно, що більшість опитаних (57,1 %) використовують двофакторну автентифікацію для окремих важливих сервісів й інша частка респондентів (28,6 %) використовують для більшості сервісів. 14,3 % опитаних не знають про двофакторну автентифікацію, проте вона потрібна для додаткового захисту облікових записів.

Питання 7. Спосіб двоетапної автентифікації, який використовується

Питання було спрямоване на визначення способів двоетапної автентифікації, які використовують респонденти. Варіанти відповідей включали кілька варіантів: SMS-код; мобільний застосунок; апаратний ключ або не використовують. Отримані результати подано у вигляді відсоткового співвідношення (рис. 7).

Рис. 7. Способи двоетапної автентифікації, що використовуються респондентами

З отриманих даних видно, що більшість опитаних використовують мобільний застосунок для двоетапної автентифікації, 17,9 % використовують SMS-код і 10,7 % використовують апаратний ключ.

Питання 8. Хешування паролів

Респондентам було поставлено питання, чи знають вони, що таке хешування паролів із трьома варіантами відповіді: так, розумію принцип; чув, але не знаю що це; не знаю. Отримані результати подано у вигляді відсоткового співвідношення (рис. 8).

Рис. 8. Аналіз результатів щодо хешування паролів

Аналіз відповідей свідчить, що лише 35,7 % респондентів цілком розуміють що таке хешування паролів. Інші 64,3 % не повною мірою або взагалі не знають, що таке хешування паролів. Прості паролі (наприклад, «123456») мають відомі хеші. Чим складніший пароль, тим важче зловмисникам підібрати його хеш.

Питання 9. Використання менеджерів паролів

Метою даного питання було з'ясування, чи використовують респонденти менеджери паролів для запам'ятовування паролів: так, постійно; пробував(ла), але не використовую; знаю про них, але не довіряю; не знаю, що це. Отримані результати подано у вигляді відсоткового співвідношення (рис. 9).

Рис. 9. Використання респондентами

З отриманих даних видно, що більшість (42,9 %) постійно використовують менеджери паролів, інші 21,4 % пробували, але не використовують, і 25 % взагалі не знають про менеджери паролів. Використовувати менеджери паролів дуже зручно, бо не потрібно запам'ятовувати всі свої паролі. Паролі потім при вході на сайт підставляються автоматично, тому користувачам не потрібно вводити їх щоразу під час входу.

Питання 10. Оцінка рівня власної обізнаності у питаннях інформаційної безпеки

Питання було спрямоване на визначення оцінки рівня власної обізнаності у питаннях інформаційної безпеки респондентами. Варіанти відповідей включали кілька варіантів: високий, середній та низький. Отримані результати подано у вигляді відсоткового співвідношення (рис. 10).

З отриманих даних видно, що більшість респондентів (42,9 %) оцінюють свій рівень обізнаності як середній. 39,3 % вважають свій рівень високим. Найменша частка опитаних (17,9 %) має низький рівень обізнаності. Бути обізнаним в питаннях інформаційної безпеки важливо, щоб захистити себе від втрати важливої інформації та перебоїв у роботі.

Таким чином, результати проведеного опитування дозволяють сформувати комплексне уявлення про сучасні підходи користувачів до парольної автентифікації та створюють підґрунтя для подальшого формулювання практичних рекомендацій щодо підвищення рівня інформаційної безпеки.

Рис. 10. Рівень обізнаності у питаннях інформаційної безпеки

Висновки

У ході проведеного дослідження було розглянуто проблему надійності парольної автентифікації в сучасних інформаційних системах з урахуванням впливу людського фактора. Встановлено, що, незважаючи на розвиток новітніх технологій захисту інформації, паролі й надалі залишаються основним засобом автентифікації користувачів, а отже, відіграють ключову роль у забезпеченні безпеки облікових записів та персональних даних.

Аналіз теоретичних аспектів показав, що ефективність парольного захисту значною мірою залежить від таких характеристик пароля, як довжина, складність та унікальність. Використання коротких і передбачуваних комбінацій символів, а також повторне застосування одного й того самого пароля для різних сервісів істотно підвищує ймовірність несанкціонованого доступу. Окрему увагу було приділено ролі хешування паролів і застосуванню додаткових механізмів захисту, які дозволяють зменшити ризики компрометації навіть у разі витоку даних.

Результати практичної частини дослідження, що ґрунтувалися на анонімному опитуванні користувачів, підтвердили наявність суттєвих проблем у сфері використання парольної автентифікації. Отримані дані свідчать про те, що значна частина користувачів не дотримується базових рекомендацій з інформаційної безпеки, зокрема використовує повторювані або недостатньо складні паролі, рідко здійснює їх зміну та не завжди застосовує двоетапну автентифікацію. Це вказує на вирішальний вплив людського фактора на загальний рівень захищеності інформаційних систем.

Водночас результати опитування дозволили оцінити рівень обізнаності користувачів щодо сучасних засобів захисту, таких як менеджери паролів і двоетапна автентифікація. Незважаючи на доступність цих інструментів, їх використання залишається недостатньо поширеним, що свідчить про необхідність підвищення рівня цифрової грамотності та формування відповідального ставлення до питань інформаційної безпеки.

Таким чином, проведене дослідження підтверджує актуальність проблеми надійності парольного захисту та доцільність поєднання технічних рішень із освітніми та організаційними заходами. Отримані результати можуть бути використані в навчальному процесі, а також слугувати підґрунтям для розробки практичних рекомендацій щодо підвищення рівня інформаційної безпеки користувачів у сучасному цифровому середовищі.

Список використаної літератури

1. Баришев Ю. В., Чайкін М. М., Кохан О. В. Метод та засіб підвищення стійкості зрозумілих користувачам текстових паролів. Наукові праці Вінницького національного технічного університету. 2022. № 2. С. 1–8. DOI: https://doi.org/10.31649/2307-5376-2022-2-1-8

2. Габрильчук А. В., Сусукайло В. А., Курій Є. О., Василишин С. І. Дослідження кібератак з використанням машинного навчання на системи управління інформаційною безпекою. Науковий журнал «Комп'ютерні системи та мережі». 2025. Вип. 7, № 1. С. 68 – 78. DOI: https://doi.org/10.23939/csn2025.01.068

3. Чуєва А. О. Паролі як критичний фактор уразливості в кібербезпеці. *Free and Open Source Software* : матеріали XVI-ої Міжнародної науково-практичної конференції, 13–14 лютого 2025 р. Харків : ХНЕУ ім. С. Кузнеця, 2025. С. 87–89. URL: https://repository.hneu.edu.ua/bitstream/123456789/35624/3/foss-2025-theses.pdf (дата звернення: 24.01.2026).

4. Головко Д. Ю. Безпека в цифровому просторі : електронний навчальний курс. Біла Церква : БІНПО ДЗВО «УМО» НАПН України, 2024. 54 с. URL: https://lib.iitta.gov.ua/id/eprint/739432/ (дата звернення: 24.01.2026).

5. Коцюк Ю. А. Роль людського чинника у питаннях захисту інформаційних систем. Наукові записки Національного університету «Острозька академія». Серія: Психологія і педагогіка. 2012. Вип. 20. С. 128–138. URL: https://eprints.oa.edu.ua/id/eprint/1419/1/NZ_Vyp_20.pdf#page=128

6. Чаплик Т., Гоч П. Інтеграція інтелектуального капіталу в стратегію інформаційної безпеки підприємств: виклики та перспективи. Дослідження та інновації. 2025. Том 1 № 1 (4). С. 47–54. URL: https://rni.com.ua/index.php/ri/article/view/47

7. Новохатній Д. Ю. Виконання заходів з кібергігієни (кібербезпеки) при використанні електронних пристроїв та програмних застосунків. *Матеріали Всеукраїнської науково-практичної конференції* (м. Київ, 2025 р.). Київ : ДУІКТ, 2025. С. 275–278. URL: https://duikt.edu.ua/uploads/p_2779_46212583.pdf.

8. Опірський І., Сікорський Р., Мартинюк Д. Аналіз ефективності двофакторної автентифікації та людського фактора у кібербезпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Том 4 № 28. С. 413–434. DOI: https://doi.org/10.28925/2663-4023.2025.28.853

9. Багрій Р., Бармак О., Манзюк Е. Підвищення стійкості паролів у веб-системах за допомогою вдосконалених схем хешування. Вісник Хмельницького національного університету. Серія: Технічні науки. 2024, Том 331 № 1. С. 48–51. DOI: https://doi.org/10.31891/2307-5732-2024-331-6

10. Тищенко А. А. Дослідження методів зберігання паролів і надання рекомендацій для підвищення безпеки особистих даних. *Free and Open Source Software*: матеріали XV-ої Міжнар. наук.-практ. конф. (Харків, 13–14 лют. 2024 р.). Харків : ХНЕУ ім. С. Кузнеця, 2024. С. 136–138. URL: https://repository.hneu.edu.ua/bitstream/123456789/31827/3/foss-2024-theses.pdf

11. Журавель Ю. І., Лісовський Б. В. Аналіз моделей та алгоритмів автентифікації на основі біометричних даних. Сучасний захист інформації. 2025, Вип. 2. С. 51-58. DOI: https://doi.org/10.31673/2409-7292.2025.022701

12. Розломій І.О. Методи підсилення хеш-функції паролю при авторизації користувачів. Вісник Хмельницького національного університету. 2020. № 1. С. 225-229. URL: https://journals.khnu.km.ua/vestnik/?p=1076

13. Бондаренко І. О., Скидан Т. М. Атака «BRUTE FORCE» та способи підвищення стійкості шифрів. *Матеріали LIII науково-технічної конференції підрозділів ВНТУ* (Вінниця, 20–22 березня 2024 р.). Вінниця : ВНТУ, 2024. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2024/paper/view/20656

14. Товкун Ю. І. Аналіз стійкості паролів з використанням AI-генерованих атак. Вісник Херсонського національного технічного університету. 2025, Том 2 № 1(92). С. 230-233. DOI: https://doi.org/10.35546/kntu2078-4481.2025.1.2.31

15. Журавлюк В. В., Барна О. В. Безпека в соціальних мережах: загрози, ризики та способи захисту. *Сучасні цифрові технології та інноваційні методики навчання: досвід, тенденції, перспективи* : матеріали XV Міжнародної науково-практичної інтернет-конференції (м. Тернопіль, 10 квітня, 2025 р.). Тернопіль : ТНПУ ім. В. Гнатюка, 2025. С. 202–205. URL: http://dspace.tnpu.edu.ua/handle/123456789/36143

References

1. Baryshev Yu. V., Chaikin M. M., Kokhan O. V. (2022) Metod ta zasib pidvyshchennya stiykosti zrozumilykh korystuvacham tekstovykh paroliv [Method and means of increasing the stability of user-understandable text passwords]. Naukovi pratsi Vinnyts′koho natsional′noho tekhnichnoho universytetu [Scientific works of Vinnytsia National Technical University] (electronic journal), vol. 2, pp. 1–8. Retrieved from: https://doi.org/10.31649/2307-5376-2022-2-1-8 [in Ukrainian].

2. Habrylchuk A. V., Susukailo V. A., Kurii E. O., Vasylyshyn S. I. (2025) Doslidzhennya kiberatak z vykorystannyam mashynnoho navchannya na systemy upravlinnya informatsiynoyu bezpekoyu [Analysis of Cyber Attacks Using Machine Learning on the Information Security Management Systems]. Naukovyy zhurnal “Komp’yuterni systemy ta merezhi” [Scientific journal “Computer Systems and Networks”] (electronic journal), vol. 7, no. 1, pp. 68–78. Retrieved from: https://doi.org/10.23939/csn2025.01.068 [in Ukrainian].

3. Chueva A. O. (2025) Paroli yak krytychnyy faktor urazlyvosti v kiberbezpetsi [Passwords as a critical vulnerability factor in cybersecurity]. Proceedings of the XVIth International Scientific and Practical Conference “Free and Open Source Software” (Ukraine, Kharkiv, February 13–14, 2025), Kharkiv: Simon Kuznets Kharkiv National University of Economics, pp. 87-89. Retrieved from: https://repository.hneu.edu.ua/bitstream/123456789/35624/3/foss-2025-theses.pdf [in Ukrainian].

4. Golovko D. Yu. (2024) Bezpeka v tsyfrovomu prostori: elektronnyy navchal′nyy kurs [Security in the digital space: electronic training course]. Bila Tserkva: BINPO DZVO “UMO”. Retrieved from: https://lib.iitta.gov.ua/id/eprint/739432/ [in Ukrainian].

5. Kotsyuk Y. A. (2012) Rol′ lyuds′koho chynnyka u pytannyakh zakhystu informatsiynykh system [The role of the human factor in issues of information systems protection]. Naukovi zapysky Natsional′noho universytetu Ostroz’ka akademiya. Seriya: Psykholohiya i pedahohika [Scientific notes of the National University of Ostroh Academy. Series: Psychology and Pedagogy] (electronic journal), no. 20, pp. 128-138. Retrieved from: https://eprints.oa.edu.ua/id/eprint/1419/1/NZ_Vyp_20.pdf#page=128 [in Ukrainian].

6. Chaplyk T., Goch P. (2025) Intehratsiya intelektual′noho kapitalu v stratehiyu informatsiynoyi bezpeky pidpryyemstv: vyklyky ta perspektyvy [Integration of intellectual capital into the information security strategy of enterprises: challenges and prospects]. Doslidzhennya ta innovatsiyi [Research and Innovations] (electronic journal), vol. 1, no. 4, pp. 47–54. Retrieved from: https://rni.com.ua/index.php/ri/article/view/47 [in Ukrainian].

7. Novokhatniy D.Yu. (2025) Vykonannya zakhodiv z kiberhihiyeny (kiberbezpeky) pry vykorystanni elektronnykh prystroyiv ta prohramnykh zastosunkiv [Implementation of cyber hygiene (cyber security) measures when using electronic devices and software applications]. Proceedings of the All-Ukrainian Scientific and Practical Conference (Ukraine, Kyiv, February 27, 2025), Kyiv: Educational and Scientific Institute of Cybersecurity and Information Protection DUICT, pp. 275–278. Retrieved from: https://duikt.edu.ua/uploads/p_2779_46212583.pdf [in Ukrainian].

8. Opirskyy I., Sikorskyi R., Martyniuk D. (2025) Analiz efektyvnosti dvofaktornoyi avtentyfikatsiyi ta lyuds′koho faktora u kiberbezpetsi [Analysis of the effectiveness of two-factor authentication and the human factor in cybersecurity]. Elektronne fakhove naukove vydannya "Kiberbezpeka: osvita, nauka, tekhnika" [Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"] (electronic journal), vol. 4, no. 28, pp. 413–434. Retrieved from: https://doi.org/10.28925/2663-4023.2025.28.853 [in Ukrainian].

9. Bahrii R., Barmak O., Manziuk E. (2024) Pidvyshchennya stiykosti paroliv u veb-systemakh za dopomohoyu vdoskonalenykh skhem kheshuvannya [Improving the resistance of passwords in web systems using advanced hashing schemes]. Visnyk Khmel′nyts′koho natsional′noho universytetu. Seriya: Tekhnichni nauky [Herald of Khmelnytskyi National University. Technical sciences] (electronic journal), vol. 331, no. 1, pp. 48–51. Retrieved from: https://doi.org/10.31891/2307-5732-2024-331-6 [in Ukrainian].

10. Tyshchenko A. A. (2024) Doslidzhennya metodiv zberihannya paroliv i nadannya rekomendatsiy dlya pidvyshchennya bezpeky osobystykh danykh [Research on password storage methods and recommendations for improving personal data security]. Proceedings of the 15th International Scientific and Practical Conference "Free and Open Source Software" (Ukraine, Kharkiv, February 13–14, 2024), Kharkiv: Simon Kuznets Kharkiv National University of Economics, p. 144. Retrieved from: https://repository.hneu.edu.ua/bitstream/123456789/31827/3/foss-2024-theses.pdf

11. Zhuravel Y. I., Lisovsky B. V. (2025) Analiz modeley ta alhorytmiv avtentyfikatsiyi na osnovi biometrychnykh danykh [Analysis of authentication models and algorithms based on biometric data]. Suchasnyy zakhyst informatsiyi [Modern information security] (electronic journal), vol. 2, no. 62, pp. 51-58. Retrieved from: https://doi.org/10.31673/2409-7292.2025.022701 [in Ukrainian].

12. Rozlomiy I. O. (2020) Metody pidsylennya khesh-funktsiyi parolyu pry avtoryzatsiyi korystuvachiv [Methods of increasing the password hash function at user authorization]. Visnyk Khmel′nyts'koho natsional′noho universytetu [Bulletin of Khmelnytsky National University] (electronic journal), vol. 1, no. 281, pp. 225–229. Retrieved from: https://journals.khnu.km.ua/vestnik/?p=1076 [in Ukrainian].

13. Bondarenko I. O., Skydan T. M. (2024) Ataka "BRUTE FORCE" ta sposoby pidvyshchennya stiykosti shyfriv [«BRUTE FORCE» attack and methods of increasing the stability of ciphers]. Proceedings of the LIII scientific and technical conference of VNTU divisions (Ukraine, Vinnytsia, March 20-22, 2024), Vinnytsia: Vinnytsia National Technical University, pp. ???. Retrieved from: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2024/paper/view/20656 [in Ukrainian].

14. Tovkun Yu. I. (2025) Analiz stiykosti paroliv z vykorystannyam AI-henerovanykh atak [Analysis of password resistance to AI-generated attacks]. Visnyk Khersons′koho natsional′noho tekhnichnoho universytetu [Visnyk of Kherson National Technical University] (electronic journal), vol. 2, no. 92, pp. 230–233. Retrieved from: https://doi.org/10.35546/kntu2078-4481.2025.1.2.31 [in Ukrainian].

15. Zhuravlyuk V. V., Barna O. V. (2025) Bezpeka v sotsial′nykh merezhakh: zahrozy, ryzyky ta sposoby zakhystu [Security in social networks: threats, risks and methods of protection]. Proceedings of the XV International Scientific and Practical Internet Conference (Ukraine, Ternopil, April 10, 2025), Ternopil: Ternopil Volodymyr Hnatiuk National Pedagogical University, pp. 202–205. Retrieved from: http://dspace.tnpu.edu.ua/handle/123456789/36143 [in Ukrainian].

Дата першого надходження статті до видання: 20.01.2026
Дата прийняття статті до друку після рецензування: 23.02.2026
Дата публікації (оприлюднення) статті: 30.04.2026