КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1114
УДК 004.056

Штонда Роман Михайлович
Начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Зозуля Роман Олександрович
Провідний науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0009-0007-3418-277X
r.zozulia@post.mil.gov.ua

Бокій Олена Володимирівна
Науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0009-0006-3459-5665
olenabokiy1971@gmail.com

УДОСКОНАЛЕННЯ ПАРОЛЬНОЇ ПОЛІТИКИ ТА ВИКОРИСТАННЯ СУЧАСНИХ МЕНЕДЖЕРІВ ПАРОЛІВ ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Анотація. У статті проведено комплексне дослідження актуальних проблем парольної політики в сучасних інформаційно-комунікаційних системах. Обґрунтовано, що в умовах стрімкого розвитку комп'ютерної техніки та зростання обчислювальних можливостей зловмисників традиційні методи автентифікації потребують суттєвого перегляду. Авторами виділено ключові недоліки існуючих підходів, серед яких: використання застарілих алгоритмів хешування, складність впровадження багатофакторної автентифікації на всіх робочих місцях та критичний вплив людського фактору (повторне використання паролів, збереження їх у відкритому вигляді). Окрему увагу приділено аналізу ентропії паролів як основного показника їхньої стійкості до атак методом повного перебору (brute-force). У роботі наведено класифікацію рівнів ентропії відповідно до важливості інформації, що захищається: 40-64 біт для відкритих даних до понад 112-128 біт для об'єктів критичної інфраструктури та інформації з обмеженим доступом. Автори демонструють, що використання сучасних графічних процесорів (наприклад, NVIDIA RTX 4090) дозволяє зловмисникам зламувати слабкі паролі (на базі MD5 або SHA-1) за лічені хвилини, що робить перехід на довгі та складні парольні комбінації життєво необхідним. Доведено, що виконання вимог сучасної парольної політики є практично неможливим для пересічного користувача без використання спеціалізованого програмного забезпечення. У зв'язку з цим детально проаналізовано функціональні можливості та архітектуру безпеки провідних менеджерів паролів: 1Password, Bitwarden та LastPass. Досліджено їхні алгоритми шифрування (AES-256, Argon2id, PBKDF2) та концепцію zero-knowledge, яка гарантує, що доступ до даних має лише власник майстер-пароля. Запропоновано рекомендації щодо вибору оптимальної довжини пароля залежно від використовуваного набору символів для досягнення цільових показників ентропії. Автори підкреслюють, що впровадження автоматизованих інструментів управління паролями у поєднанні з багатофакторною автентифікацією є фундаментальною умовою зміцнення національної безпеки та підвищення кіберстійкості інформаційно-комунікаційних систем державних організацій та установ.

Ключові слова: автентифікація, безпарольні методи автентифікації, довжина пароля, ентропія паролів, менеджер паролів, паролі, парольна політика.

ВСТУП

У сучасному світі розвиток інформаційно-комунікаційних систем (далі – ІКС) та комп'ютерної техніки постійно прискорюється, що призводить до постійного зростання можливостей зловмисників (ворога) і це зумовлює розвиток систем захисту інформації. Одним зі способів захисту є контроль доступу до систем шляхом надання прав та привілеїв при авторизації користувачів у системі. Одним із етапів авторизації є автентифікація, яка в більшості випадків включає в себе надання користувачем знання паролю. У світі згідно з провідними стандартами кіберзахисту впроваджують політики використання паролів. Але різноманітність ІКС, використаних в них програмних і апаратних засобів із різними можливостями контролю дотримання парольної політики призводять до різних можливостей реалізації обмежень паролів. Така різниця в реалізації процесу автентифікації призводить до розмиття обмежень і рекомендацій.

Окремі ІКС мають жорсткі внутрішні вимоги до довжини та складності паролів або правил періодичної зміни, що частково відображає специфіку ризиків у цих ІКС. Але ці підходи іноді суперечать сучасним рекомендаціям щодо користувацького досвіду й ефективності [1].

Постановка проблеми. На сьогодні існує ряд проблем, що пов'язані із парольною політикою:

– застарілі системи та сервіси, де складно впровадити сучасні методи (багатофакторну автентифікацію, сучасні алгоритми хешування, підтримку автозаповнення в менеджерах паролів, що радить зробити NIST SP 800-63B [2]);

– людський фактор, що полягає в повторному використанні паролів, збереження паролів у відкритих нотатках, Excel таблицях, невірна видача імен і паролів, слабка обізнаність персоналу;

– нерівномірне використання багатофакторної автентифікації, що переважно впроваджено в ІКС, але не на всіх автоматизованих робочих місцях (далі – АРМ).

Удосконалення парольної політики дозволить:

– підвищити стійкість ІКС до атак типу "brute force", "credential stuffing" і фішингу;

– інтегрувати сучасні підходи до кібергігієни, що базуються на використанні багатофакторної автентифікації, довгих унікальних паролів і підтримки менеджерів паролів;

– знизити рівень людського фактора, що залишається одним із найуразливіших елементів у ІКС.

Таким чином, вдосконалення парольної політики є необхідною умовою підвищення рівня кіберстійкості, зменшення ймовірності компрометації критичних інформаційних ресурсів і зміцнення національної безпеки загалом.

Аналіз останніх досліджень і публікацій. У статті [3] питання парольної політики розглядається в контексті захисту від хакерських атак типу «brute-force», де наголошується на необхідності використання складних паролів (наприклад, довжиною від 8 символів із використанням літер і цифр) для запобігання повному перебору комбінацій. Також автори підкреслюють важливість захисту облікових даних від фішингу та соціальної інженерії, оскільки викрадення паролів адміністраторів чи керівників надає зловмисникам повний доступ до конфіденційних сховищ даних.

У підручнику [4] парольна політика розглядається як один із базових методів автентифікації користувачів, що ґрунтується на знаннях (паролі або PIN-коді) для перевірки їхньої достовірності при вході в систему. Автори наголошують на важливості

поєднання парольного захисту з технічними засобами, такими як протокол SSL для шифрування фінансової інформації та цифрові підписи для забезпечення цілісності даних.

Мета статті. Метою даної статті є дослідження актуальних проблем парольної політики, аналіз ентропії паролів як міри їхньої стійкості до підбору, а також обґрунтування доцільності впровадження автоматизованих інструментів (менеджерів паролів, таких як 1Password, Bitwarden та LastPass) для мінімізації впливу людського фактора та зміцнення інформаційної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Одним із ключових елементів безпеки інформації та кібербезпеки є управління паролями. Парольна автентифікація, незважаючи на розвиток біометричних та багатофакторних технологій, залишається найпоширенішим способом підтвердження особи користувача в ІКС.

Передові дослідження, які пов’язані із вивченням можливостей зловмисників проводити злам паролів показують, що за допомогою сучасної надпотужної відеокарти GPU NVIDIA GeForce RTX 4090 (яку можна використовувати не лише для ігор чи штучного інтелекту) можливо здійснювати атаки на паролі (brute force, dictionary attack) [5].

На слабких алгоритмах (MD5, SHA-1, SHA-256) RTX 4090 спроможна перебрати весь простір паролів довжиною 8 символів за кілька годин. А при використанні сучасних технологій розподіленого підбору та використання центрів обробки даних час взагалі зменшується до хвилин.

На сучасних алгоритмах (bcrypt, scrypt, Argon2) атаки стають майже нереалістичними, навіть на фермах із десятків відеокарт.

Популярні огляди 2024-2025 років (Hive Systems) підкреслюють, що те, що здавалося “стійким” у 2020-2022 роках, тепер можна зламати значно швидше. Hive Systems опублікували оновлену “Password Table” 2025 року з оцінками часу ентропії паролів для різних сценаріїв. Ці джерела ілюструють швидке зростання практичної здатності ентропії паролів [6].

Пароль (password) – технологічна (секретна) інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до ІКС (автоматизованих систем) або до інформації [7].

В свою чергу ентропія паролів – це міра стійкості пароля до підбору (brute force), яка відображає, скільки інформації містить пароль та наскільки він непередбачуваний (іншими словами – показник того, наскільки важко зламати пароль методом перебору).

Ентропія паролів вимірюється в бітах.

Враховуючи вимоги сучасних стандартів безпеки та передових досліджень, можна розділити ентропію паролів так:

– пароль довжиною від 40 до 64 біт – підходить для захисту облікових записів, в яких обробляється відкрита інформація. Рекомендовано використання таких паролів із застосуванням багатофакторної автентифікації або із суворим обмеженням кількості спроб входу та швидкості запитів під час автентифікації. Якщо виникає підозра на офлайн-витік інформації, необхідно підвищити довжину паролів, щоб вона становила не менше 64 біт [2];

– пароль довжиною від 64 до 80 біт – підходить для захисту внутрішніх сервісів і для захисту облікових записів, в яких обробляється відкрита інформація. 80 біт дає значно кращий запас на випадок офлайн-витоку при середніх можливостях зловмисників [8];

– пароль довжиною від 80 до 96 біт – підходить для захисту ІКС, в яких циркулює конфіденційна та службова інформація. Рекомендовано використання таких паролів із застосуванням багатофакторної автентифікації та виключення можливості їх зберігання у відкритому вигляді [9];

– пароль довжиною від 96 до 128 біт та вище – підходить для захисту інформації з обмеженим доступом та ІКС об'єктів критичної інформаційної інфраструктури або в яких циркулює інформація з обмеженим доступом. Рекомендовано використання таких паролів разом із застосуванням криптографічних ключів. Для таких облікових записів багатофакторна автентифікація, суворі обмеження кількості спроб входу та швидкості запитів під час автентифікації – обов'язкові [10].

Таким чином:

– якщо пароль має 10 символів із чотирма категоріями символів (цифри, малі літери алфавіту, прописні літери алфавіту та неалфавітні символи), він підходить для захисту внутрішніх сервісів і для захисту облікових записів, в яких обробляється відкрита інформація. Такі паролі слід використовувати в АРМ, що не мають доступу до електронних комунікаційних мереж та на яких не обробляється інформація з обмеженим доступом;

– якщо необхідно обробляти конфіденційну інформацію та використовувати ІКС, в яких циркулює службова інформація, тоді паролі в таких АРМ та ІКС повинні бути від 80 до 96 біт відповідно до переліку розподілу складності ентропії паролів, викладеної вище. Необхідно збільшувати кількість символів із чотирма категоріями, а також застосовувати багатофакторну автентифікацію та виключити можливість їх зберігання у відкритому вигляді;

– якщо необхідно обробляти інформацію з обмеженим доступом та використовувати ІКС об'єктів критичної інфраструктури або в яких циркулює інформація з обмеженим доступом, тоді паролі в таких АРМ та ІКС повинні бути від 96 до 128 біт та вище відповідно до переліку розподілу складності ентропії паролів, викладеної вище. Необхідно збільшувати кількість символів із чотирма категоріями, а також використовувати криптографічні ключі, багатофакторну автентифікацію, вводити суворі обмеження кількості спроб входу та швидкості запитів під час автентифікації.

Ентропія паролів показує не просто довжину, а комбінацію довжини й різноманітності символів. Для безпеки варто створювати паролі з ентропією не менше 64 біт (звичайний користувач), а для адміністраторів, обладнання та роботи в самих ІКС – від 112 біт і вище [2].

Для розрахунку ентропії пароля необхідно ввести формулу 1 [11]:

$$H = L \times log_2 S, \quad (1)$$

де, H – ентропія пароля (у бітах);
L – довжина пароля;
S – кількість можливих символів.

Щоб ентропія пароля перевищувала 112 біт, потрібно збільшити довжину пароля, використовувати більший набір символів:

– цифри від 0 до 9;
– малі літери алфавіту від a до z;
– прописні літери алфавіту від A до Z;
– неалфавітні символи !, #, $, = й т. ін.

Враховуючи формулу 1, розробимо таблицю рекомендованих довжин паролів і типів символів для досягнення необхідної ентропії до 131 біт (таблиця 1).

Таблиця 1

Рекомендовані довжини паролів і типів символів для досягнення необхідної ентропії

Довжина пароля	Цифри (10 символів)	Малі літери алфавіту (26 символів)	Малі літери алфавіту та прописні літери алфавіту (52 символи)	Цифри, малі літери алфавіту та прописні літери алфавіту (62 символи)	Цифри, малі літери алфавіту, прописні літери алфавіту та неалфавітні символи (94 символи)
Кількість символів	**Біти**				
6	19.9	28.2	34.2	35.7	39.3
7	23.3	32.9	39.9	41.7	45.9
8	26.6	37.6	45.6	47.6	52.4
9	29.9	42.3	51.3	53.6	59.0
10	33.2	47.0	57.0	59.5	65.6
11	36.5	51.7	62.7	65.5	72.1
12	39.9	56.4	68.4	71.4	78.7
13	43.2	61.1	74.1	77.4	85.2
14	46.5	65.8	79.8	83.4	91.8
15	49.8	70.5	85.5	89.3	98.3
16	53.2	75.2	91.2	95.3	104.9
17	56.5	79.9	96.9	101.2	111.4
18	59.8	84.6	102.6	107.2	118.0
19	63.1	89.3	108.3	113.1	124.5
20	66.4	94.0	114.0	119.1	131.1

На рисунку 1 зображено відповідну лінійну діаграму з маркерами, що демонструє зростання ентропії паролів.

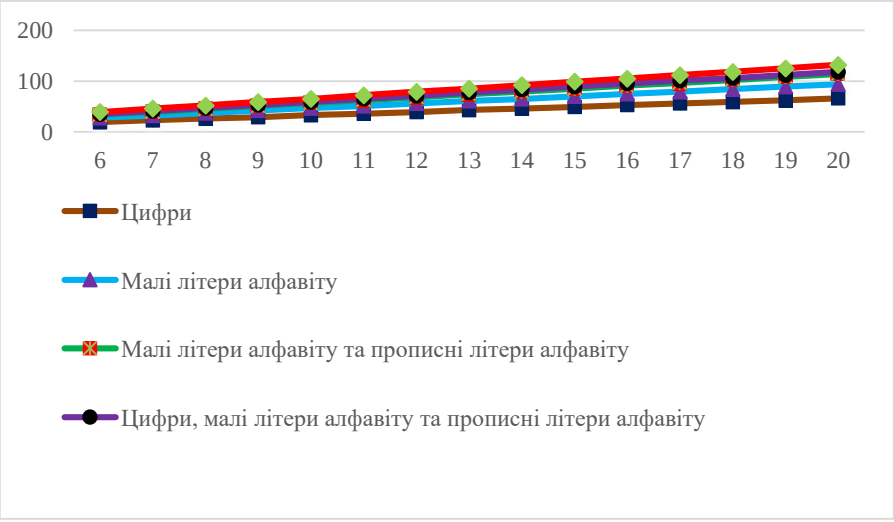

Рис. 1. Зростання ентропії паролів

Враховуючи вимоги до довжини та складності паролів, користувачу буде важко використовувати такі паролі при недопущенні використання словникових послідовностей, тому доцільним буде використовувати автоматизовані інструменти (менеджери паролів) для допомоги у виборі надійних паролів.

Менеджери паролів дозволяють користувачам створювати, зберігати та автоматично вводити складні паролі, мінімізуючи ризик використання слабких або повторюваних комбінацій. Вони також забезпечують захист від фішингових атак, синхронізують дані між пристроями та пропонують додаткові функції, такі як генерація паролів чи перевірка їхньої безпеки.

Державна служба спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ України) рекомендує надавати перевагу наступним програмним рішенням (менеджерам паролів): 1Password, Bitwarden, LastPass, KeePass [12].

Розглянемо їхні функціональні можливості, рівень безпеки (використовувані алгоритми шифрування, архітектуру).

Менеджер паролів 1Password – це програмне рішення, розроблене компанією AgileBits (тепер 1Password), призначене для безпечного зберігання, управління та використання конфіденційних даних, таких як паролі, дані кредитних карток, захищені нотатки та паролі для розробки. Його основна мета – забезпечити користувачам зручний і безпечний спосіб створення складних унікальних паролів, їх зберігання та автоматичне введення в онлайн-сервіси, програми чи корпоративні системи. 1Password допомагає уникнути використання слабких або повторюваних паролів, мінімізуючи ризики компрометації облікових записів, і водночас спрощує доступ до сервісів завдяки інтеграції з браузерами, додатками та платформами [13].

Менеджер паролів 1Password пропонує широкий набір функцій, які забезпечують зручність, безпеку та гнучкість для користувачів.

Основні можливості цього менеджера паролів включають:

– генерацію паролів. Функція дозволяє створювати складні, унікальні паролі із заданими параметрами (довжина, використання цифр, малих літер алфавіту, прописних літер алфавіту та неалфавітних символів);

– безпечне зберігання даних. Функція дозволяє зберігати паролі, захищені нотатки, ліцензії на програмне забезпечення, SSH-ключі та інші чутливі дані у зашифрованому вигляді;

– автозаповнення. Функція дозволяє автоматичне введення логінів, паролів та інших даних на вебсайтах і в додатках через розширення для браузерів (Chrome, Firefox, Safari, Edge) або мобільні додатки;

– хмарну синхронізацію. Функція дозволяє здійснювати синхронізацію зашифрованих даних між кінцевими пристроями через хмарні сервери 1Password;

– функцію моніторингу безпеки облікових даних (Watchtower). Функція дозволяє: сканувати паролі на предмет слабкості, повторного використання чи компрометації внаслідок витоків даних; попереджати про незахищені вебсайти (наприклад, ті, що використовують HTTP замість HTTPS); встановлювати нагадування про закінчення терміну дії паролів або документів;

– двофакторну автентифікацію. Функція дозволяє здійснювати інтеграцію з двофакторною автентифікацією, включаючи підтримку кодів Time-based One-Time Password (далі – TOTP) для додаткового захисту облікових записів;

– безпечний обмін. Функція надає можливість ділитися паролями чи іншими даними через зашифровані посилання або в межах командних акаунтів;

– функцію тимчасового приховування сховищ даних (Travel Mode). Увімкнувши цю функцію, є можливість залишити лише ті сховища, які позначені як безпечні (наприклад, паролі до менш критичних сервісів). Усі інші дані будуть тимчасово видалені, але залишаться на серверах менеджера паролів 1Password. Після вимкнення функції дані автоматично відновлюються через синхронізацію;

– командні та сімейні функції. Функція дозволяє забезпечити управління доступом для команди чи членів сім'ї, включаючи розподіл прав і створення окремих сховищ (vaults) для різних груп даних;

– інтеграцію для розробників. Функція дозволяє зберігати API-ключі, токени і паролі, а також інтеграцію з інструментами CI/CD через 1Password CLI та Secrets Automation;

– можливість працювати на різних операційних системах, пристроях і платформах. Функція дозволяє використовувати менеджер паролів на різних типах пристроїв (комп'ютер, ноутбук, планшет, смартфон) і операційних системах (Windows, macOS, Linux, iOS, Android) без втрати основних функцій або необхідності адаптації даних.

Менеджер паролів 1Password використовує передові технології шифрування та архітектуру нульового знання (zero-knowledge), щоб забезпечити максимальний захист даних користувачів.

Менеджер паролів 1Password застосовує комбінацію алгоритмів шифрування для захисту даних, а саме:

– AES-256-GCM. Використовується для шифрування всіх даних у сховищах (vaults). Цей алгоритм шифрування з автентифікованим шифруванням (Galois/Counter Mode) забезпечує конфіденційність і цілісність даних;

– PBKDF2-HMAC-SHA256. Застосовується для створення криптографічного ключа з головного пароля та секретного ключа (Secret Key). Використовує тисячі ітерацій (зазвичай 100 000+), щоб ускладнити атаки brute-force;

– Secret Key. Унікальний 128-бітний ключ, який генерується для кожного облікового запису та комбінується з головним паролем для створення повного ключа шифрування. Цей ключ додає додатковий рівень захисту, оскільки навіть у разі компрометації головного пароля дані залишаються захищеними;

– RSA-2048. Використовується для шифрування обміну даними між пристроями та серверами під час синхронізації;

– Secure Remote Password. Протокол для безпечної автентифікації, який забезпечує захист головного пароля під час входу в систему, не передаючи його на сервер.

Менеджер паролів 1Password побудований на основі архітектури нульового знання, що гарантує, що ні розробники 1Password, ні будь-які сторонні особи не мають доступу до зашифрованих даних користувача.

Ключові аспекти архітектури:

– локальне шифрування. Усі дані шифруються на пристрої користувача перед відправленням на сервери. Сервери зберігають лише зашифровані дані, які неможливо розшифрувати без головного пароля та секретного ключа;

– головний пароль і секретний ключ. Доступ до даних можливий лише за наявності головного пароля (відомого лише користувачу) та секретного ключа (зберігається локально або в акаунті користувача). Менеджер паролів не зберігає ці дані на своїх серверах;

– хмарна синхронізація. Зашифровані дані передаються через захищені TLS-з'єднання (TLS 1.2/1.3) до серверів менеджера паролів, які розміщені на інфраструктурі Amazon Web Services (AWS) із суворим контролем доступу;

– локальне зберігання (опціонально). Менеджер паролів підтримує локальні сховища без хмарної синхронізації, що дозволяє користувачам зберігати дані лише на службових пристроях;

– двофакторна автентифікація. Хоча головний пароль і секретний ключ є основними засобами захисту, менеджер паролів підтримує двофакторну автентифікацію (TOTP або апаратні ключі, такі як YubiKey) для додаткового захисту облікового запису;

– захист від атак. Менеджер паролів використовує захист від атак типу brute-force, а також моніторинг безпеки через Watchtower для виявлення витоків даних.

Менеджер паролів 1Password є одним із провідних менеджерів паролів завдяки своїм розширеним функціональним можливостям, високому рівню безпеки та підтримці широкого спектра платформ. Використання надійних алгоритмів шифрування (AES-256-GCM, PBKDF2-HMAC-SHA256, RSA-2048) і архітектури нульового знання (zero-knowledge) робить його ефективним інструментом для захисту конфіденційних даних. Функції, такі як Watchtower, Travel Mode та підтримка розробників, роблять цей менеджер паролів універсальним рішенням для індивідуальних і корпоративних користувачів, які прагнуть поєднати безпеку із зручністю.

Менеджер паролів Bitwarden – це програмне рішення із відкритим вихідним кодом, призначене для безпечного зберігання, генерації та керування паролями, нотатками та іншими даними. Він підтримує як приватних користувачів, так і юридичні організації (установи), дозволяючи синхронізувати дані між пристроями, забезпечувати колаборацію в командах та відповідати регуляторним стандартам (наприклад, GDPR, HIPAA, SOC 2). Основна мета його використання полягає у спрощенні процесу створення сильних паролів і захисті від крадіжок даних, використовуючи end-to-end шифрування, де навіть компанія розробник не має доступу до ваших даних (zero-knowledge) [14].

Менеджер паролів Bitwarden пропонує широкий набір функцій, які забезпечують зручність, безпеку та гнучкість для користувачів.

Основні можливості цього менеджера паролів включають:

– генерацію та автозаповнення паролів. Функція дозволяє автоматичну генерацію сильних паролів (з урахуванням складності) та автозаповнення форм на вебсайтах і в додатках. Забезпечує підтримку безпарольної автентифікації (passkeys);

– зберігання даних. Функція дозволяє використовувати зашифроване сховище (vault) для паролів, нотаток, ідентифікаційних даних тощо. Забезпечує необмежене зберігання в безкоштовній версії;

– синхронізацію. Функція дозволяє здійснювати синхронізацію даних між необмеженою кількістю пристроїв (веб, десктоп: Windows, macOS, Linux; мобільні: iOS, Android; розширення для браузерів: Chrome, Firefox, Safari, Edge тощо);

– спільний доступ. Функція дозволяє здійснювати обмін паролями в організаціях (установах), Send – для тимчасового обміну зашифрованими текстами та файлами з наступними опціями: термін дії, ліміт доступу, пароль;

– адміністрування. Функція дозволяє здійснювати централізоване керування доступом, політиками, звітами про безпеку, забезпечує інтеграцію з Singke Sign-On (далі – SSO), API, SIEM-інструментами;

– імпорт та експорт. Функція дозволяє здійснювати легкий імпорт з інших менеджерів або браузерів, експорт у зашифрованому вигляді;

– самостійний хостинг. Функція реалізує можливість розгортання сервера менеджера паролів Bitwarden на власній інфраструктурі (локально або в приватній хмарі), замість використання його хмарних серверів;

– додаткові інструменти. Функція включає генератор паролів для створення складних паролів, перевірку на витоки даних для виявлення скомпрометованих паролів та підтримку двофакторної автентифікації через TOTP, e-mail або апаратні ключі. Також за допомогою даної функції є можливість забезпечити біометричну автентифікацію для швидкого доступу на мобільних кінцевих пристроях і браузерах.

Менеджер паролів Bitwarden забезпечує високий рівень безпеки завдяки zero-knowledge архітектурі, end-to-end шифруванню та регулярним аудитам. Дані шифруються локально на пристрої перед відправкою на сервери, і тільки користувач може їх розшифрувати. Сервіс відповідає стандартам ISO 27001,

SOC 2 Type 2, SOC 3, GDPR, CCPA, HIPAA. Щорічні аудити від незалежних фірм (наприклад, через HackerOne) та відкритий код дозволяють громадський огляд.

Менеджер паролів Bitwarden застосовує комбінацію алгоритмів шифрування для захисту даних, а саме:

– AES-256-CBC. Основний симетричний алгоритм для шифрування захищеного сховища (стандарт, затверджений урядом Сполучених Штатів Америки (далі – США) для найвищого рівня секретної інформації). Доповнено HMAC-SHA256 для перевірки цілісності та захисту від маніпуляцій;

– Password-Based Key Derivation Function 2 (далі – PBKDF2) (SHA-256). Функція похідності ключів (Key Derivation Function (далі – KDF) з 600 000 ітерацій (за замовчуванням) для генерації майстер-ключа з майстер-пароля та e-mail. Сіль (salt) додається для захисту від brute-force;

– Argon2id. Гібридна функція похідності ключів (KDF), що комбінує Argon2d і Argon2i, забезпечуючи стійкість до атак грубої сили (brute-force) і побічних каналів шляхом використання великого обміну пам’яті та обчислень.

У цьому менеджері паролів вона генерує безпечний майстер-ключ із пароля;

– HMAC-based Key Derivation Function. Розширення майстер-ключа до 512-біт для забезпечення симетричного шифрування;

– Elliptic Curve Digital Signature Algorithm (AES256). Алгоритм цифрового підпису на основі еліптичних кривих, що застосовується для генерації та перевірки безпарольної автентифікації (passkeys), забезпечуючи безпечну безпарольну автентифікацію;

– асиметричне шифрування. Асиметричне шифрування в цьому менеджері паролів засноване на алгоритмах RSA або Elliptic Curve Cryptography, використовується для безпечного обміну даними, зокрема в функціях організації (установи) та аварійного доступу (emergency access). Воно забезпечує шифрування даних публічним ключем і розшифрування приватним ключем, гарантуючи конфіденційність і безпеку передачі;

– Cryptographically Secure Pseudo-Random Number Generator. Використовується для створення криптографічно стійких ключів та ініціалізаційних векторів (IV), забезпечуючи високу випадковість і безпеку;

– FIPS 140. Сумісні бібліотеки гарантують відповідність стандартам безпеки для криптографічних операцій, підвищуючи надійність шифрування.

Ключові аспекти архітектури:

– Zero-knowledge модель. Забезпечує, що всі дані користувача шифруються локально на пристрої за допомогою AES-256 перед відправкою на сервери, і лише користувач із майстер-паролем може їх розшифрувати.

– Це гарантує те, що противник, зловмисники, які отримали доступ до серверів, та навіть розробники менеджера паролів Bitwarden не можуть отримати доступ до незашифрованих даних;

– комунікація. В менеджері паролів Bitwarden комунікація захищена за допомогою HTTPS із TLS, що запобігає атакам типу “людина посередині” (MitM-атак), забезпечуючи безпечну передачу даних. Після 9 невдалих спроб входу активується автоматизований тест (Completely Automated Public Turing test to tell Computers and Humans Apart), а мінімальна довжина майстер-пароля в 12 символів підвищує стійкість до brute-force атак;

– Self-hosting. Менеджер паролів Bitwarden дозволяє розгорнути сервер на власній інфраструктурі (з використанням NGINX, віртуальних приватних мереж, міжмережевих екранів), забезпечуючи повний контроль над даними без їх передачі на зовнішні сервери. Це гарантує, що всі дані залишаються в межах мережі, підвищуючи конфіденційність і відповідність регуляторним вимогам;

– захист від атак. Менеджер паролів Bitwarden забезпечує захист від атак завдяки двофакторній автентифікації, перевірці на витоки паролів, регулярній ротації ключів і хешуванню з унікальним випадковим рядком даних (salt) для підвищення безпеки. Відкритий код на GitHub дозволяє перевіряти безпеку та надійність реалізації.

Менеджер паролів Bitwarden характеризується як потужний і доступний менеджер паролів, пропонуючи безкоштовну версію (преміум-версія доступна від 10 доларів США на рік) з необмеженим зберіганням і синхронізацією, відкритий код для аудиту безпеки та опцію selt-hosting, що робить його ідеальним для користувачів. Він також вважається одним із найбезпечніших менеджерів паролів завдяки прозорості та відсутності прихованого доступу.

Менеджер паролів LastPass – це програмне рішення і захищене сховище (vault), призначене для спрощення цифрового життя користувачів та підприємців. Він допомагає створювати, зберігати та автоматично заповнювати сильні унікальні паролі, забезпечуючи безпечний доступ до акаунтів на всіх кінцевих пристроях. Основна мета – усунути ризик повторного використання слабких паролів, мінімізуючи загрози для особистої та корпоративної безпеки, з акцентом на зручність для користувачів, організацій (установ) [15].

Менеджер паролів LastPass пропонує широкий набір функцій, які забезпечують зручність, безпеку та гнучкість для користувачів.

Основні можливості цього менеджера паролів включають:

– автозаповнення (Autofill). Функція дозволяє автоматично заповнювати логіни, паролі та дані форм на вебсайтах і в додатках для швидкого доступу без ручного введення;

– генерацію та зберігання паролів. Функція дозволяє створювати складні, унікальні паролі та зберігати їх у захищеному сховищі (vault), яке вміщує не лише паролі, а й дані Wi-Fi-профілів, адрес, документів, податкових форм та інших конфіденційних файлів;

– спільний доступ і керування. Функція дозволяє ділитися паролями з родиною, колегами чи партнерами через персональні або спільні сховища з налаштованими правами доступу (наприклад, тимчасовий доступ чи обмеження);

– синхронізацію пристроїв. Функція дозволяє здійснювати автоматичну синхронізацію даних між всіма пристроями (комп'ютери, смартфони, планшети) для забезпечення безперервного доступу;

– додаткові інструменти. До додаткових інструментів включається моніторинг SaaS-додатків, захист від фішингу, моніторинг даркнету (для виявлення витоків даних), єдиний вхід (SSO), двофакторна аутентифікація та панелі для моніторингу безпеки.

Менеджер паролів LastPass забезпечує високий рівень безпеки завдяки zero-knowledge архітектурі та сучасним криптографічним методам, що робить його одним із лідерів у галузі менеджерів паролів.

Менеджер паролів LastPass використовує алгоритм шифрування AES-256 для даних у сховищі та функцію похідної Password-Based Key Derivation Function 2 (PBKDF2) з SHA-256 для захисту майстер-пароля, роблячи його стійким до атак, таких як brute-force або rainbow table атаки. Майстер-пароль не зберігається у відкритому вигляді на серверах – він обробляється локально на кінцевому пристрої користувача.

Ключові аспекти архітектури менеджера паролів LastPass полягають у застосуванні моделі Zero-knowledge – означає, що всі дані шифруються та хешуються на кінцевому пристрої користувача перед відправкою на сервери LastPass, тому компанія не має доступу до паролів, нотаток чи критичної інформації. Додатково впроваджено нову інфраструктуру безпеки на базі хмарної платформи з високою доступністю.

Менеджер паролів LastPass у 2025 році лишається популярним менеджером паролів, що забезпечує баланс між функціональністю, доступністю та безпекою, з перевагами на кшталт безкоштовного плану з необмеженим зберіганням, автозаповненням форм, моніторингом даркнету та інструментами спільного доступу. Оновлена інфраструктура з zero-knowledge архітектурою, алгоритмом шифрування AES-256, PBKDF2 з SHA-256, сертифікацією ISO 27701 та командами моніторингу загроз (як TIME та POST) свідчить про зусилля щодо відновлення довіри після інцидентів 2022 року, хоча минулі проблеми все ще викликають обережність і нижчі оцінки.

Менеджер паролів KeePass – це безкоштовне, відкрите, легке і зручне у використанні програмне рішення. Його основна мета полягає в допомозі користувачам безпечно керувати численними паролями, зберігаючи їх в одній базі даних, зашифрованій за допомогою сучасних алгоритмів шифрування, таких як AES-256, ChaCha20 і Twofish. Для доступу до бази потрібно запам'ятати лише один головний ключ. Менеджер паролів KeePass є відкритим програмним рішенням, що дозволяє перевірити його вихідний код на коректність реалізації функцій безпеки [16].

Менеджер паролів KeePass пропонує широкий набір функцій, які забезпечують зручність, безпеку та гнучкість для користувачів.

Основні можливості цього менеджера паролів включають:

– сильну безпеку. Функція дозволяє підтримує AES (Rijndael), ChaCha20 і Twofish для шифрування баз даних паролів. Шифрує всю базу даних, включаючи імена користувачів, нотатки тощо. Використовує SHA-256 для хешування компонентів основного ключа. Захищає від атак за допомогою функцій похідного ключа (AES-KDF, Argon2 тощо). Шифрує паролі в оперативній пам'яті під час роботи. Використовує захищені потоки в пам'яті для завантаження внутрішнього XML-формату (у версії 2.x).

Має безпекові елементи керування редагуванням паролів, стійкі до проникнення противника та зловмисників. Включає в своєму складі опцію для запобігання певним знімкам екрану. Показує діалог основного ключа на захищеному робочому столі;

– кілька ключів користувача. Функція дозволяє використовувати один основний пароль для розшифрування всієї бази. Підтримує файли ключів для посилення безпеки, які можна носити на портативних (змінних) носіях. Дозволяє комбінувати основний пароль і файл ключа. У версії 2.x може блокувати базу до поточного облікового запису Windows;

– портативність, відсутність встановлення і доступність. Функція забезпечує портативність (працює на Windows без встановлення, може бути перенесений на USB-накопичувач). Пропонує пакети для встановлення з ярликами в меню Start і на робочому столі. Не зберігає жодної інформації в системі, не залишає слідів після видалення. Порти доступні для інших систем, як Android, iOS тощо. Оптимізує інтерфейс для користувачів (у версії 2.x);

– експорт у формати TXT, HTML, XML і CSV. Дана функція дозволяє експортувати список паролів у формати TXT, HTML, XML і CSV. XML-формат легко використовується в інших додатках. HTML-формат використовує CSS для форматування. CSV-формат сумісний з іншими менеджерами паролів і таблицями. Підтримує додаткові формати через плагіни;

– імпорт із багатьох форматів файлів. Функція дозволяє імпортувати CSV-формат із різних менеджерів, як от Password Keeper. Імпортує дані з текстового файлу TXT-формату, який експортується з програми CodeWalletPro. Імпортує текстові файли TXT-формату з Password Safe v2. У версії 2.x підтримується понад 35 форматів. Додаткові формати підтримуються через відповідні плагіни;

– легке перенесення бази даних. Функція дозволяє легко переносити між кінцевими пристроями базу паролів, яка складається з одного файлу;

– підтримку груп паролів. Функція дозволяє створювати, модифікувати та видаляти групи для сортування паролів;

– поля часу та вкладення записів. Функція дозволяє підтримувати поля часу (час створення, час останньої модифікації, час останнього доступу та термін дії). Дозволяє вкладати файли до записів паролів. Версія 2.x включає внутрішній редактор для тексту, зображень і документів без експорту;

– Auto-Type, глобальна гаряча клавіша Auto-Type та Drag&Drop. Функція дозволяє мінімізувати та вводити інформацію з вибраного запису в діалоги та вебформи із кастомними послідовностями. Має глобальну гарячу клавішу для роботи у фоні. Всі поля (назва, ім’я користувача, пароль, URL, нотатки) можна перетягувати в інші вікна;

– інтуїтивну та безпечну обробку буфера обміну Windows. Функція дозволяє копіювати значення полів у буфер подвійним кліком. Автоматично очищує буфер через заданий час після копіювання пароля;

– пошук та сортування. Функція дозволяє шукати конкретні записи в базах, а також сортувати групи паролів кліком на заголовки стовпців;

– підтримку багатомовності. Функція дозволяє здійснювати переклад на інші мови. Доступно понад 45 мов;

– генератор випадкових паролів. Функція дозволяє генерувати сильні випадкові паролі з кастомними наборами символів і відповідною довжиною;

– архітектуру плагінів. Функція дозволяє підтримувати плагіни для розширення функцій, включаючи додаткові методи імпорту та експорту;

– відкритого коду. Функція дозволяє безкоштовний повний доступ до вихідного коду. Запобігає бекдорам, дозволяє компіляцію та перевірку безпеки користувачів.

Менеджер паролів KeePass забезпечує високий рівень безпеки завдяки сучасним криптографічним стандартам та архітектурі, орієнтованій на конфіденційність і стійкість до атак. Файли баз даних шифруються повністю, включаючи паролі, імена користувачів, URL, нотатки тощо.

Підтримуються наступні алгоритми шифрування:

– менеджер паролів KeePass версії 1.x: Advanced Encryption Standard (AES/Rijndael) з розміром ключа 256 біт (стандарт NIST FIPS 197); Twofish з розміром ключа 256 біт;

– менеджер паролів KeePass версії 2.x: AES/Rijndael (256 біт, NIST FIPS 197); ChaCha20 (256 біт, RFC 8439). Додаткові алгоритми, як Twofish, Serpent і GOST, через плагіни.

Блокові шифри використовуються в режимі Cipher Block Chaining (CBC) для приховування шаблонів простого тексту. Вектор ініціалізації (IV) генерується випадково при кожному збереженні, дозволяючи створювати унікальні зашифровані копії. Автентичність і цілісність даних забезпечуються хешем SHA-256 (у версії 1.x – простого тексту; у версії 2.x – HMAC-SHA-256 шифротексту за схемою Encrypt-then-MAC).

Хешування ключа та функції похідного ключа. Компоненти основного ключа (пароль, файл ключа, ключ Windows чи плагін) стискаються SHA-256 (NIST FIPS 180-4) до 256-бітного ключа. Для генерації ключа шифрування застосовується функція похідного ключа, що ускладнює атаки.

Менеджер паролів KeePass використовує спеціальні методи для захисту головного пароля, а саме:

– AES-KDF (доступно в версії 1.x і версії 2.x). Використовує багаторазові обчислення AES для створення безпечного ключа. На операційних системах Windows застосовується технологія CNG/BCrypt для швидкої роботи;

– Argon2 (доступно лише на версії 2.x). Він ускладнює атаки за допомогою спеціалізованих пристроїв (GPU/ASIC), оскільки потребує багато пам’яті. Існує два варіанти – Argon2d та Argon2id. Argon2d ліпше захищає від атак через графічні процесори. Argon2id додає захист від атак через сторонні канали. Для звичайних користувачів рекомендується Argon2d.

Загальна архітектура.

Менеджер паролів KeePass є портативним, безслідним додатком з відкритим кодом, що дозволяє проведення аудиту. Він шифрує дані в пам’яті, захищає від програм або апаратних пристроїв, які записують натискання клавіш на кінцевому пристрої (захищений десктоп, Auto-Type), блокує буфер обміну та підтримує комбіновані ключі. Не залишає слідів в системі, портативний для USB. Плагіни розширюють безпеку без компрометації ядра.

Загалом менеджер паролів KeePass вважається одним із найбезпечніших менеджерів паролів завдяки стійкості до brute-force, відсутності телеметрії та повному шифруванню.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

До складу паролів має входити не менше ніж 12 символів (великих, малих літер, цифр і спеціальних символів), що включає принаймні по одному символу кожного регістру.

Заборонено використовувати стандартні паролі виробників комунікаційного обладнання, які можна знайти у відкритому доступі (admin, cisco тощо), та паролі, що мають у своєму складі:

– послідовність символів у алфавітному порядку або порядку розміщення на клавіатурі (наприклад abcdeEFGhi, qwerTYUiop тощо);

– словникові слова, сленгові вирази, скорочення, у тому числі набрані в іншомовній клавіатурній розкладці (наприклад Ruchka, Waib, Kjusy (Логін), P@ssw0rd тощо);

– послідовність із трьох і більше символів, що повторюються (uuuu@Yu240, 15htVA2222Lf тощо);

– послідовність символів утворених із доступної інформації про користувача (прізвище, ім’я, телефон, тощо);

– шаблонних паролів (наприклад, Company123!).

Примусова зміна паролів повинна здійснюватися щонайменше щоквартально.

При зміні паролів повинні змінюватись принаймні 50 % символів. З метою коректного та вірного введення паролів доцільно використовувати менеджери паролів.

Менеджер паролів 1Password є оптимальним для enterprise з централізованим управлінням, інтеграцією SSO, Active Directory і доступним (інтуїтивним) інтерфейсом користувача. Рекомендується для використання у великих організаціях (установах).

Менеджер паролів Bitwarden найбільше підходить для гібридних сценаріїв та децентралізованого управління завдяки self-host, має відкритий код та доступний для користувачів.

Менеджер паролів LastPass підходить для невеликих організацій та установ з фокусом на SIEN, SSO, але слід враховувати події, що відбувались в 2022–2024 роках, однак оновлення 2025 року значно покращили цей менеджер паролів.

Менеджер паролів KeePass (версії 1.x та версії 2.x) є бюджетним рішенням для користувачів або малих організацій (установ) із децентралізованим управлінням. Слід пам’ятати, що безкоштовна версія підходить для користувачів, а не для організацій (установ), навіть малих.

Подальшими дослідженнями є:

– проведення практичного тестування паролів 1Password, Bitwarden, LastPass, KeePass;

– проведення дослідження щодо вибору та впровадження безпечного менеджера паролів, з урахуванням необхідності централізованого (децентралізованого) управління.

Боремося з кібертерором разом! Разом до перемоги! Слава Україні!

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shtonda, R., Palamarchuk, S., Bokii, O., Tereshchenko, T., & Chernysh, Y. (2025). Comprehensive methodology for evaluating functional capabilities of antivirus software. *Cybersecurity: Education, Science, Technique*, *4*(28), 375–384. https://doi.org/10.28925/2663-4023.2025.28.813

2. National Institute of Standards and Technology. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf
3. Skladannyi, P. M., et al. (2025). GDPR methods for ensuring data storage security against leaks and threats. *Telecommunication and Information Technologies, 2*, 59–76. https://doi.org/10.31673/2412-4338.2025.027860
4. Buriachok, V. L., Anosov, A. O., Semko, V. V., Sokolov, V. Y., & Skladannyi, P. M. (2019). *Technologies for ensuring network infrastructure security.* Kyiv: Borys Grinchenko Kyiv University.
5. Chick3nman. (n.d.). *Hashcat v6.2.6 benchmark on the Nvidia RTX 4090.* https://gist.github.com/Chick3nman/32e662a5bb63bc4f51b847bb422222fd
6. Liu, Z. (n.d.). Nvidia's flagship gaming GPU can crack complex passwords in under an hour. *Tom's Hardware.* https://www.tomshardware.com/pc-components/gpus/nvidias-flagship-gaming-gpu-can-crack-complex-passwords-in-under-an-hour
7. State Service of Special Communications and Information Protection of Ukraine. (1999). *ND TZI 1.1-003-99: Terminology in the field of information protection in computer systems against unauthorized access.*
8. OWASP Foundation. (n.d.). *Password storage cheat sheet.* https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html
9. ArXiv. (n.d.). *Evaluating Argon2 adoption and effectiveness in real-world software.* https://arxiv.org/html/2504.17121
10. Internet Engineering Task Force. (2021). *RFC 9106: Argon2 memory-hard function for password hashing and proof-of-work applications.* https://datatracker.ietf.org/doc/rfc9106/
11. Shtonda, R. M. (2025). The impact of password length on entropy according to modern standards. In *Global trends in science and education: Proceedings of the IX International scientific and practical conference* (pp. 238–241). https://sci-conf.com.ua/ix-mizhnarodna-naukovo-praktichna-konferentsiya-global-trends-in-science-and-education-22-24-09-2025-kiyiv-ukrayina-arhiv/
12. State Service of Special Communications and Information Protection of Ukraine. (n.d.). *What are password managers and how do they work?* https://cip.gov.ua/ua/faqs/sho-take-menedzheri-paroliv-yak-voni-pracyuyut
13. 1Password. (n.d.). *Password manager & extended access management.* https://1password.com/
14. Bitwarden. (n.d.). *Password manager for business, enterprise & personal use.* https://bitwarden.com/
15. LastPass. (n.d.). *Password manager & vault application.* https://www.lastpass.com/password-manager
16. Tucha.ua. (n.d.). *How to use KeePass easily.* https://tucha.ua/uk/blog/instructions/yak-lehko-korystuvatysya-keepass

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Roman Shtonda
Head of Research Department
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID: 0000-0001-5986-0847
roman.shtonda@viti.edu.ua

Roman Zozulia
Leading Researcher
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID: 0009-0007-3418-277X
r.zozulia@post.mil.gov.ua

Olena Bokii
Research Scientist
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID: 0009-0006-3459-5665
olenabokiy1971@gmail.com

IMPROVING PASSWORD POLICY AND USING MODERN PASSWORD MANAGERS TO ENHANCE CYBER RESILIENCE OF INFORMATION AND COMMUNICATION SYSTEMS

Abstract. The article presents a comprehensive study of current password policy issues in modern information and communication systems. It is substantiated that in the face of rapid computer technology development and the growing computing capabilities of cyber adversaries, traditional authentication methods require a significant overhaul. The authors identify key shortcomings of existing approaches, including the use of outdated hashing algorithms, the complexity of implementing multi-factor authentication (MFA) across all workstations, and the critical impact of the human factor (password reuse, storing credentials in plaintext). Particular attention is paid to the analysis of password entropy as the primary indicator of resistance to brute-force attacks. The paper provides a classification of entropy levels based on the sensitivity of the protected information: from 40-64 bits for public data to over 112-128 bits for critical infrastructure objects and restricted access information. The authors demonstrate that the use of modern graphics processing units (e.g., NVIDIA RTX 4090) allows attackers to crack weak passwords (based on MD5 or SHA-1) in mere minutes, making the transition to long and complex password combinations vital for security. It is proven that meeting the requirements of modern password policies is practically impossible for the average user without the use of specialized software. In this regard, the functional capabilities and security architecture of leading password managers – 1Password, Bitwarden, and LastPass – are analyzed in detail. Their encryption algorithms (AES-256, Argon2id, PBKDF2) and the "zero-knowledge" concept, which guarantees that only the master password holder can access the data, are thoroughly examined. The article proposes recommendations for selecting the optimal password length depending on the character set used to achieve target entropy indicators. The authors emphasize that the implementation of automated password management tools combined with multi-factor authentication is a fundamental condition for strengthening national security and increasing the cyber resilience of information and communication systems of state organizations and institutions.

Keywords: authentication, passwordless authentication methods, password length, password entropy, password manager, passwords, password policy.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shtonda, R., Palamarchuk, S., Bokii, O., Tereshchenko, T., & Chernysh, Y. (2025). Comprehensive methodology for evaluating functional capabilities of antivirus software. *Cybersecurity: Education, Science, Technique*, *4*(28), 375–384. https://doi.org/10.28925/2663-4023.2025.28.813

2. National Institute of Standards and Technology. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf
3. Skladannyi, P. M., et al. (2025). GDPR methods for ensuring data storage security against leaks and threats. *Telecommunication and Information Technologies, 2*, 59–76. https://doi.org/10.31673/2412-4338.2025.027860
4. Buriachok, V. L., Anosov, A. O., Semko, V. V., Sokolov, V. Y., & Skladannyi, P. M. (2019). *Technologies for ensuring network infrastructure security.* Kyiv: Borys Grinchenko Kyiv University.
5. Chick3nman. (n.d.). *Hashcat v6.2.6 benchmark on the Nvidia RTX 4090.* https://gist.github.com/Chick3nman/32e662a5bb63bc4f51b847bb422222fd
6. Liu, Z. (n.d.). Nvidia's flagship gaming GPU can crack complex passwords in under an hour. *Tom's Hardware.* https://www.tomshardware.com/pc-components/gpus/nvidias-flagship-gaming-gpu-can-crack-complex-passwords-in-under-an-hour
7. State Service of Special Communications and Information Protection of Ukraine. (1999). *ND TZI 1.1-003-99: Terminology in the field of information protection in computer systems against unauthorized access.*
8. OWASP Foundation. (n.d.). *Password storage cheat sheet.* https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html
9. ArXiv. (n.d.). *Evaluating Argon2 adoption and effectiveness in real-world software.* https://arxiv.org/html/2504.17121
10. Internet Engineering Task Force. (2021). *RFC 9106: Argon2 memory-hard function for password hashing and proof-of-work applications.* https://datatracker.ietf.org/doc/rfc9106/
11. Shtonda, R. M. (2025). The impact of password length on entropy according to modern standards. In *Global trends in science and education: Proceedings of the IX International scientific and practical conference* (pp. 238–241). https://sci-conf.com.ua/ix-mizhnarodna-naukovo-praktichna-konferentsiya-global-trends-in-science-and-education-22-24-09-2025-kiyiv-ukrayina-arhiv/
12. State Service of Special Communications and Information Protection of Ukraine. (n.d.). *What are password managers and how do they work?* https://cip.gov.ua/ua/faqs/sho-take-menedzheri-paroliv-yak-voni-pracyuyut
13. 1Password. (n.d.). *Password manager & extended access management.* https://1password.com/
14. Bitwarden. (n.d.). *Password manager for business, enterprise & personal use.* https://bitwarden.com/
15. LastPass. (n.d.). *Password manager & vault application.* https://www.lastpass.com/password-manager
16. Tucha.ua. (n.d.). *How to use KeePass easily.* https://tucha.ua/uk/blog/instructions/yak-lehko-korystuvatysya-keepass

Отримано редакцією журналу / Received: 16.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 26.03.26