УДК 004.056:342.6
DOI https://doi.org/10.32782/2524-0374/2025-6/81

ЗАГАЛЬНІ ПІДХОДИ ДО СТВОРЕННЯ СТІЙКИХ ПАРОЛІВ КОРИСТУВАЧАМИ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

A COMPLEX APPROACH TO CREATING STRONG PASSWORDS FOR SPECIAL PURPOSE INFORMATION SYSTEMS MIA AND NATIONAL POLICE OF UKRAINE

Кудінов В.А., к.ф.-м.н., доцент,
завідувач кафедри інформаційних технологій
Національна академія внутрішніх справ
ORCID ID: 0000-0002-5299-0590

Корнейко О.В., к.т.н., професор,
професор кафедри інформаційних технологій
Національна академія внутрішніх справ
ORCID ID: 0000-0002-1882-9680

Пакриш О.Є., к.т.н., доцент,
доцент кафедри інформаційних технологій
Національна академія внутрішніх справ
ORCID ID: 0000-0002-6420-5246

Актуальність статті полягає в тому, що протягом останнього часу в системі Міністерства внутрішніх справ України з метою цифровій трансформації та інформаційно-аналітичного забезпечення Міністерства внутрішніх справ України та державних органів, що находяться у сфері його управління, вживаються дієві заходи щодо створення та впровадження різноманітних інформаційних систем спеціального призначення. У статті пропонується комплексний підхід до створення стійких паролів для інформаційних систем спеціального призначення Міністерства внутрішніх справ та Національної поліції України. На основі аналізу 25 літературних джерел автори визначили та проаналізували 20 основних вимог до створення надійних паролів. Безумовне дотримання користувачами інформаційних систем зазначених вимог забезпечить високий рівень стійкості парольного захисту від злому та практично уникне незаконного використання злочинцями прав доступу поліцейських до своїх відомчих інформаційних ресурсів. Запропоновано комплексний підхід щодо створення стійких паролів користувачів інформаційних систем спеціального призначення Міністерства внутрішніх справ України та Національної поліції України. Вважаємо, що безумовне дотримання користувачами цих інформаційних систем зазначених вимог дозволить забезпечити високий рівень стійкості парольного захисту до перебору та майже уникнути неправомірне використання зловмисниками правами доступу поліцейських до їх відомчих інформаційних ресурсів. На даний час немає єдиного підходу щодо формату створення паролів в системах авторизації різних інформаційних системах спеціального призначення Міністерства внутрішніх справ України та Національної поліції України, тому, на нашу думку, єдиний формат створення паролів в цих системах необхідно розробляти з урахуванням запропонованого нами комплексного підходу та відповідних рекомендацій з тестування паролів. Подальші дослідження будуть спрямовані на вивчення особливостей створення та використання стійких паролів користувачів конкретних інформаційних систем спеціального призначення Міністерства внутрішніх справ України та Національної поліції України.

Ключові слова: інформаційні системи; системи спеціального призначення, пароль; злом; стійкість парольного захисту до перебору, МВС України, Національна поліція України.

The relevance of the article lies in the fact that recently, in the system of the Ministry of Internal Affairs of Ukraine, for the purpose of digital transformation and information and analytical support of the Ministry of Internal Affairs of Ukraine and state bodies under its management, effective measures have been taken to create and implement various special-purpose information systems. The article provides a comprehensive approach to creating stable passwords for special purpose information systems of the Ministry of Internal Affairs and the National Police of Ukraine. Based on the analysis of 25 literary sources, the authors identified and analyzed 20 basic requirements for creating strong passwords. Unconditional compliance by users of information systems with the specified requirements will ensure a high level of resistance of password protection against hacking and almost avoid the illegal use by criminals of police officers' access rights to their departmental information resources. A comprehensive approach to creating strong passwords for users of special-purpose information systems of the Ministry of Internal Affairs of Ukraine and the National Police of Ukraine is proposed. We believe that unconditional compliance by users of these information systems with the specified requirements will ensure a high level of password protection resistance to brute force and almost avoid the misuse of police officers' access rights to their departmental information resources by attackers. Currently, there is no single approach to the format for creating passwords in authorization systems of various special-purpose information systems of the Ministry of Internal Affairs of Ukraine and the National Police of Ukraine, therefore, in our opinion, a single format for creating passwords in these systems should be developed taking into account the comprehensive approach we have proposed and the relevant recommendations for password testing. Further research will be aimed at studying the features of creating and using strong passwords for users of specific special-purpose information systems of the Ministry of Internal Affairs of Ukraine and the National Police of Ukraine.

Key words: information systems, special purpose systems, password, hacking, resistance of password protection to hacking, Ministry of Internal Affairs of Ukraine, National Police of Ukraine.

Вступ. Протягом останнього часу в системі Міністерства внутрішніх справ (далі – МВС) України з метою цифровій трансформації та інформаційно-аналітичного забезпечення МВС та державних органів, що находяться у сфері його управління, вживаються дієві заходи щодо створення та впровадження різноманітних інформаційних систем спеціального призначення (далі – ІССП).

При цьому відповідно до розпорядження Кабінету Міністрів України від 17 лютого 2021 р. № 365-р[1] при забезпеченні функціонування цих ІССП потребує свого

[1]Деякі питання цифрової трансформації : Розпорядження Кабінету Міністрів України від 17 лют. 2021 р. № 365-р. Верховна Рада України. Законодавство України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/365-2021-%D1%80/conv#Text.

вирішення важлива проблема щодо забезпечення захисту даних у національних електронних інформаційних ресурсах, що перебувають в підпорядкуванні органів системи МВС.

Серед окремих шляхів її вирішення є забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних ІССП, де одним із основних елементів організації цієї діяльності є забезпечення надійного авторизованого доступу користувачів до інформаційних ресурсів, зокрема за допомогою парольного доступу. Тобто, створення стійких (надійних) паролів до злому є важливою складовою інформаційної безпеки баз даних ІССП.

Отже, метою статті є розробка загального підходу (рекомендацій) щодо створення стійких паролів до ІССП, що, з урахуванням реалій сьогодення, є достатньо актуальною проблемою.

Огляд літератури. Паролі залишаються центральним механізмом аутентифікації для більшості онлайн-сервісів, проте одночасно часто є найслабшою ланкою через практики повторного використання, коротку довжину та слабку складність. Протягом останніх років збільшення швидкості обробки великих масивів даних за рахунок зростання обчислювальної потужності графічних процесорів (Graphics Processing Unit, GPU) та інтегральних схем спеціального призначення (Application-Specific Integrated Circuit, ASID) та застосування статистичних методів і ШІ-підходів для генерації гіпотез значно підвищило ефективність атак на паролі [5; 6; 8].

Методи здійснення атак на паролі можуть бути класифіковані наступним чином:

1) Онлайн-атаки: включають brute-force, password spraying та credential stuffing. Password spraying – один з методів брутфорса (brute-force), полягає в спробі використання невеликого набору широко розповсюджених паролів проти великої кількості облікових записів, що дозволяє уникнути обмежень за кількістю спроб [10]. Підбір скомпрометованих облікових даних – Credential Stuffing – тип кібератаки, коли зловмисники використовують викрадені комбінації імен користувачів та паролів, часто внаслідок витоку даних, щоб отримати несанкціонований доступ до кількох облікових записів. Автоматизуючи спроби входу на різні сайти, зловмисники користуються повторним використанням паролів користувачів.

2) Офлайн-атаки: коли атакувальник отримує дамп хешів – використовуються словникові та rule-based атаки, mask-атаки та комбіновані підходи з GPU-прискоренням [5; 8].

3) Фішинг і соціальна інженерія: залучення користувача до передачі облікових даних через підроблені інтерфейси. Сучасні методи соціальної інженерії стають дедалі персоналізованішими за рахунок отримання персональних даних з різних джерел [3].

Ключовими факторами підвищення ризику атак є [2; 4]:

GPU-прискорення інструментів для підбору паролів;

великі агреговані leaks-датасети, тоб то посилання на набори даних, що використовують для машинного навчання [11];

застосування методів машинного навчання (ML/AI) для генерації ймовірнісних словників;

активний рух до використання стандарту автентифікації, який дозволяє входити до облікових записів без пароля, використовуючи криптографічні ключі та біометрію або фізичні ключі безпеки – passwordless/passkeys (FIDO) – як захисного підходу.

В літературі розглянуті наступні методи та рекомендації щодо захисту паролів:

1) В процесі хешування та зберігання: використовувати memory-hard алгоритми (Argon2id як основний варіант), використовувати апаратні Hardware Security Module (апаратний модуль безпеки), для захисту криптографічних ключів. Налаштування параметрів функції формування ключа (key derivation function, KDF) слід переглядати регулярно з огляду на апаратні зміни [1; 7].

2) Дотримуватись політики паролів, а саме забороняти завідомо слабкі паролі (застосовувати механізм "чорного списку" – blacklist/HIBP API), ставити акцент на довжині (парольна фраза ≥12–16 символів, бажано до 32+) замість вимоги складних символів.

3) Використання методів підвищення безпеки облікових записів: MFA (додає додатковий рівень перевірки до традиційного пароля); passwordless (повністю його усуває використання традиційного пароля. MFA та passwordless: багатоаспектна аутентифікація та перехід на FIDO-паскі як найбільш ефективні засоби проти фішингу та credential stuffing [2; 3].

4) Створення технічних бар'єрів захисту: rate limiting – обмеження частоти, з якою клієнт може надсилати запити до сервісу за певний проміжок часу. Його основна мета – захист від перевантаження та зловживань, таких як атаки типу «відмова в обслуговуванні» (DDoS) або спроби перебору паролів (брутфорс), шляхом обмеження кількості запитів від одного джерела (наприклад, IP-адреси або облікового запису. Anti-bot/behavioral detection – захист веб-сайтів від негативних поведінкових бот-атак, моніторинг аномалій входу та швидка реакція на витоки інформації.

Матеріали та методи. Методологічну основу статті становлять загальнонаукові та спеціально-юридичні методи дослідження. Діалектичний метод використано для аналізу розвитку інституту спрощених процедур у контексті реформування судової системи. Системно-структурний підхід дозволив розглядати спрощене судочинство як цілісну систему взаємопов'язаних елементів. Порівняльно-правовий метод застосовано для зіставлення української моделі із закордонними процедурами (зокрема у Польщі, Франції та країнах ЄС). Формально-догматичний метод дав змогу проаналізувати норми ЦПК України (ст. ст. 19, 274–279), що регламентують спрощене провадження, і виявити їхні проблемні аспекти. Метод правового моделювання використано для розроблення пропозицій щодо вдосконалення термінології та правового регулювання.

Результати та їх обговорення. Як відомо, захист паролем – це метод керування доступом до інформаційної системи, який допомагає захистити важливу інформацію та ресурси системи від зловмисників, надаючи до них доступ лише тим користувачам, які мають відповідні облікові дані. Пароль призначений для підтвердження особистості або повноважень користувача.

Таким чином, ще на етапі створення користувачем ІСПП пароля необхідно передбачити виконання ним всіх належних вимог до паролю, що в комплексі забезпечать його стійкість до злому.

Як правило, пароль визначається користувачем особисто. Початковий пароль формується адміністратором безпеки ІССП під час реєстрації нового користувача. А користувач зобов'язаний змінити цей пароль під час першого сеансу роботи з ІССП (доступ до об'єктів обліку цієї системи йому буде наданий тільки після зміни початкового паролю, до цього моменту користувачеві заборонено будь-який доступ) [18].

Які можливості є у користувачів ІССП щодо створення паролів?

Всі паролі умовно можна розділити на три види [22]: 1) *легкі паролі* (наприклад: "123456"; "password"; "дата народження"; "пароль, що співпадає з ім'ям користувача"); 2) *паролі середньої складності*, в яких присутні літери і цифри, але вони складаються з добре впізнаваних їх комбінацій; 3) *стійкі паролі*, які важко зламати шляхом логічного вгадування або методом перебору за допомогою комп'ютерних програм.

За даними фахівців Української антивірусної компанії [23], близько 80 % користувачів недооцінюють роль пароля в кіберзахисті і легковажно ставляться до його створення і зберігання. Статистика невблаганна: 20 найпоширеніших паролів складають 10,3% взагалі використовуваних паролів [13], а 80% паролів – зазвичай прості, які легко підібрати [15].

Але надійний пароль – це пароль, який неможливо вгадати або зламати методом перебору [16]. Адже сучасним комп'ютерам не складає труднощів за лічені секунди зламати короткі паролі, що складаються тільки з літер і цифр [25; 28].

Таким чином, для створення стійкого пароля користувачі ІССП повинні дотримуватись, на наш погляд, наступного комплексного підходу до вимог щодо їх створення, сутність якого наведена далі.

1. Для створення паролю необхідно вибрати бажану мову.

Кириличні символи іноді некоректно обробляє авторизаційне програмне забезпечення, тому більш надійно створювати паролі латиницею [16].

2. Для створення пароля можна одночасно використовувати низку мов.

Як варіант, можна використовувати одночасно кирилицю і латиницю [23].

3. Кількість знаків у паролі повинна бути не менше 8…14 знаків.

Перш за все, користувач повинен переконатися, що його пароль довгий.

Відомчі інструкції МВС України щодо правил формування атрибуту «Пароль» окремих інформаційних систем протягом останніх десятиріч регламентували довжину пароля не менше 5 знаків [18]. Станом на сьогодні Департамент кіберполіції Національної поліції України та Державна служба спеціального зв'язку та захисту інформації України вважають, що пароль повинен містити не менше 8 знаків [14; 34]. Існують також інші думки фахівців – знаків повинно бути: не менше 8–10 [22], не менше 10–12 [15], не менше 14 [21]. Зрозуміло, що більш довгі паролі більш безпечні. Кожен додатковий знак в паролі експоненціально збільшує кількість можливих комбінацій. Це робить захист надійніше [16].

4. У паролі необхідно використовувати поєднання літер та цифр.

Зазначена вимога наявна в багатьох джерелах, зокрема в [14; 28; 34].

5. Пароль повинен містити літери верхнього та нижнього регістру.

Департамент кіберполіції вважає, що надійний пароль має складатися з літер верхнього та нижнього регістру [14]. Необхідно в паролі використовувати хоча б одну велику літеру і одну малу літеру [22]. А краще – їх більшу кількість. При цьому великі і малі літери не повинні групуватися. Їх змішування робить пароль складнішим [22; 28].

6. Бажано у складі паролю використовувати окремі спеціальні символи.

Надійний пароль, як вважає Департамент кіберполіції, має містити спеціальні символи [14]. До цих символів належать: ! # % & * / \ | ^ : ; } " ~ $ _ + – = ? ( ) @ тощо. Хоча використання спецсимволів в паролі – це дійсно хороший спосіб зробити їх більш надійними, але не всі облікові записи дозволяють використовувати будь-які символи [16]. Для додавання нових символів до паролів, не ускладнюючи їх запам'ятовування, можливо також використовувати смайлики, які складаються з розділових знаків, літер і (або) цифр [16].

7. Не використовувати пробіли в паролі.

Замість них бажано використовувати нижнє підкреслення "_" або дефіс "-" [22]. Також необхідно уникати використання пробілів на початку та кінці пароля. Хоча багато інформаційних систем не дозволяють використовувати фактичні пробіли в паролях.

8. Бажано у паролі використовувати заміну окремих символів на інші символи чи їх комбінацію, які схожі з ними за написанням [12].

Приклад 1: заміна Б ~ 6 ; В ~ 8 ; З ~ 3 ; И ~ Й (Н) ; Л ~ ^ ; Н ~ И; О ~ 0 ; С ~ S або (; Y (У) ~ V ; Ч ~ 4 ; S ~ $ (5) ; Z ~ 2.

Приклад 2: заміна Ж ~ >I< ; Л ~ /\ ; Ф ~ oIo ; Х ~ >< ; Ю ~ IO ; V ~ \/.

9. Не бажано використовувати одне ціле слово у якості паролю, краще використовувати парольну фразу.

Парольні фрази (набір слів, зашифрованих користувачем) набагато надійніше паролів з одного слова, оскільки вони зазвичай довше і їх складніше вгадати або перебрати. Тому замість слова, наприклад, бажано обрати будь-яку фразу (рядок із вірша, пісні, книжки тощо), видалити пробіли та замінити деякі літери цифрами, спецсимволами, перевести певні літери у верхній регістр, щоб створити на перший погляд випадкову комбінацію символів [25]. Також можна поміняти місцями слова і розділові знаки [16].

10. Пароль не повинен співпадати з логіном акаунту.

11. Не використовувати в паролі персональні дані.

Потрібно не використовувати у якості паролю персональну інформацію: ім'я, прізвище, дати народження своє та своїх близьких; номери телефонів; номери та серії документів, що посвідчують особу; номери власного автотранспорту; номери банківських карт; адреси реєстрації, своє ім'я або день народження або члена сім'ї тощо [14; 25; 27; 34]. Подібна інформація легко знаходиться хакерами [22]. Адже встановлено, що 59 % користувачів використовують своє ім'я або дату народження в паролі. А ще статистика Google показує, що 33 % користувачів послуговується кличкою свого улюбленця, 15 % – ім'ям свого партнера [19]. Опитування показало, що люди в 3 рази частіше використовують ім'я свого вихованця в якості пароля, ніж ім'я члена сім'ї [13].

12. Необхідно створювати паролі, не пов'язані зі сферою своєї діяльності.

Але можна використовувати особливу лексику. Наприклад, назви не дуже розповсюджених медичних препаратів, жаргон шахтарів і геологічні терміни відомі далеко не всім [22].

13. Не використовувати стандартні паролі, що засновані на повторенні символів, словникових словах, літерних або числових послідовностях, літерах або цифрах, які йдуть підряд в розкладці клавіатури.

Потрібно не використовувати послідовні комбінації клавіш (наприклад, "qwerty", "qazwsx", "123456") через те, що хакери точно зламають їх [14, 34]. Логіка така, якщо користувач не витратив жодних зусиль на придумування гарного пароля, хакерам не знадобиться багато зусиль, щоб його зламати [16].

14. При створенні складних паролів для їх легкого запам'ятовування бажано визначити власні правила їх формування.

Однозначно існує тонка грань між вибором пароля, який ніхто не зможе відгадати, і паролем, який легко запам'ятати [16]. Стійкій пароль має бути достатньо легким для користувача, щоб його запам'ятати, але складним для інших, щоб ніхто не міг його вгадати чи підібрати.

Головний недолік несподіваних паролів – це складність їх запам'ятовування. А користувачам з плином часу потрібно пам'ятати все більше і більше паролів. Тому є кілька способів придумати складний та надійний пароль, який легко запам'ятати. Для цього можна спробувати скорегувати за певними правилами відомі користувачу: текст із пісні чи вірша; цитату з фільму чи промови; відомі висловлювання; уривок із книги; набір слів, які асоціюються із чимось; графічні комбінації на клавіатурі клавіш, які становлять якийсь малюнок (трикутник, тупий кут, три

паралельні лінії); абревіатуру, наприклад, з перших літер кожного слова в реченні [22]. Незайвим буде кілька разів потренуватися написати пароль для задіяння м'язової пам'яті [16]. Якщо у користувача є низка паролів від облікових записів, то він може їх записати до надійного менеджера паролів (наприклад, KeePass, LastPass, 1Password чи інші), а потім захистити їх одним "головним паролем", тобто, користувачу доведеться запам'ятати тільки один надійний пароль [16].

15. Бажано використовувати випадкову (безглузду) комбінацію символів.

Такий результат можна отримати, наприклад, якщо набирати пароль кирилицею в латинській розкладці клавіатури або навпаки. Наприклад, пароль кирилицею "ДиНаМо_1927" в латинській розкладці виглядає як "LbYfVj_1927".

16. Для кожної ІССП обов'язково необхідно створювати свій унікальний надійний пароль.

За даними джерела [19] 13 % користувачів повторно використовують той самий пароль для всіх облікових записів, 52 % послуговуються одним і тим же паролем для декількох (але не для всіх) облікових записів, і тільки 35 % використовують різні паролі для кожного акаунта. Опитування показало, що 66 % людей використовують тільки 1 або 2 пароля для всіх своїх облікових записів [13].

17. При зміні паролю необхідно забезпечити те, щоб новий пароль значно відрізнявся від попереднього.

Адже користувачі схильні повторно використовувати паролі з невеликими варіаціями, як-от одне-два додаткове число чи символ.

18. Використовувати можливості генераторів паролів.

Це програмне забезпечення (наприклад, згадані раніше KeePass, LastPass, 1Password), як правило, дозволяє автоматично створювати складні комбінації, які користувач потім може змінити на свій розсуд для більш простого запам'ятовування [22, 28].

Як правило, користувач у налаштуваннях генератора паролів може вибрати: 1) тип генератора (*словниковий* – для генерації пароля використовуються слова зі словника, які простіше для запам'ятовування і теоретично складніше підібрати; *комп'ютерний* – генерує складні паролі (чим вони довші, тим важче їх підібрати); *сегментний* – генерує складні паролі, це аналог комп'ютерного, але з додаванням роздільника у вигляді тире, щоб було легше запам'ятати); 2) довжину пароля: min="5", max="30"; 3) набори символів: великі літери; малі літери; цифри; спеціальні символи; виключити повторення. Після цього генерується результат. Тобто, ці менеджери можуть допомогти користувачу створити унікальні одноразові паролі та автоматично заповнити їх в облікових записах, до яких вони прив'язані [16].

Для створення складних паролів рекомендовано використовувати наступні сервіси генерації паролів [25]:

– https://www.eset.com/ua/home/generator-paroley/

– https://www.avast.ua/random-password-generator#pc

– https://identitysafe.norton.com/password-generator

– програма Password Tech Portable (колишня назва PWGen).

19. Бажано проводити перевірку пароля на його відсутність у реєстрах зламаних та найпопулярніших паролів.

Це також є важливими, на наш погляд, заходами щодо створення стійких паролів. Зокрема, свій пароль можна перевірити за веб-адресами: https://haveibeenpwned.com/ [16]; https://nordpass.com/most-common-passwords-list/ [25].

20. При створенні паролю необхідно використовувати можливість його оцінки програмними засобами за ступенем надійності.

Перевірка пароля на надійність – це елементарний тест на те, чи зможуть зламати обліковий запис користувача чи ні [22]. Щоб самостійно пройти перевірку надійності пароля онлайн, потрібно зайти на спеціальний сайт з програмою-тестувальником, ввести свій пароль і дочекатися результату. Пара секунд – і алгоритм зробить висновок про надійність пароля користувача [22].

Перевірити наскільки надійний пароль можна за допомогою:

– програми Password Meter (цей сервіс складність паролю оцінює за шкалою: "занадто короткий", "дуже слабкий", "слабкий", "добре", "сильний", "дуже сильний" [20]);

– https://www.security.org/how-secure-is-my-password/ (цей сервіс складність паролю оцінює за часом злому [25]);

– https://zillya.ua/check-password (цей сервіс для ознайомчих цілей [25]).

Таким чином, нами розглянуті всі основні, на наш погляд, вимоги до створення стійких паролів для роботи в ІССП, які треба комплексно використовувати користувачами цих систем.

Висновки. Запропоновано комплексний підхід щодо створення стійких паролів користувачів інформаційних систем спеціального призначення МВС та Національної поліції України. Вважаємо, що безумовне дотримання користувачами цих інформаційних систем зазначених вимог дозволить забезпечити високий рівень стійкості парольного захисту до перебору та майже уникнути неправомірне використання зловмисниками правами доступу поліцейських до їх відомчих інформаційних ресурсів.

На даний час немає єдиного підходу щодо формату створення паролів в системах авторизації різних інформаційних системах спеціального призначення МВС та НПУ, тому, на нашу думку, єдиний формат створення паролів в цих системах необхідно розробляти з урахуванням запропонованого нами комплексного підходу та відповідних рекомендацій з тестування паролів.

Подальші дослідження будуть спрямовані на вивчення особливостей створення та використання стійких паролів користувачів конкретних інформаційних систем спеціального призначення МВС та Національної поліції України.

ЛІТЕРАТУРА

1. OWASP Foundation. Password Storage Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html.

2. FIDO Alliance. Passkeys: Passwordless Authentication. URL: https://fidoalliance.org/passkeys/.

3. Dashlane / The Verge. Dashlane report: Passkey adoption increase (coverage). URL: https://www.theverge.com/2024/7/30/24209395/dashlane-passkey-report-adoption-passwordless-sign-on.

4. Verizon. Data Breach Investigations Report (DBIR) 2025. URL: https://www.verizon.com/business/resources/reports/dbir/.

5. Hashcat team. Hashcat forum – benchmarks & optimisation notes. URL: https://hashcat.net/forum/thread-11751.html.

6. Z. Huang, D. Wang, Y. Zou. Prob-Hashcat: Accelerating Probabilistic Password Guessing with Hashcat by Hundreds of Times. URL: https://www.researchgate.net/publication/382462171_Prob-Hashcat_Accelerating_Probabilistic_Password_Guessing_with_Hashcat_by_Hundreds_of_Times.

7. V. Fedorchenko et al.. Password hashing methods and algorithms on the .NET platform. URL: https://ais.khpi.edu.ua/article/view/314569.

8. Cyberdigi / Medium. Unblocking Hashcat GPU optimisations – practical report. URL: https://cyberdigi.medium.com/unlocking-hashcats-full-potential-how-gpu-optimization-reduced-cracking-time-by-85-a-wordlist-17565a7832c5.

9. Have I Been Pwned (T. Hunt). Pwned accounts / breached datasets statistics (2023–2025). URL: https://haveibeenpwned.com/.

10. Palo Alto Networks. What is credential stuffing? – explainer and mitigation. URL: https://www.paloaltonetworks.com/cyberpedia/credential-stuffing.

11. ResearchGate / RockYou analysis. RockYou 2024 analysis and breached accounts. URL: https://www.researchgate.net/figure/Number-of-breached-accounts-listed-in-have-I-been-Pwned_fig1_353910058.

12. Кудінов В. А. Підвищення стійкості парольного захисту інформаційної системи до перебору шляхом використання даних рейтингових списків найбільш популярних в світі паролів. *Сучасна спеціальна техніка.* 2022. № 2. С. 67–76.

13. Всесвітній день паролів. *Ділова мова* : [сайт]. URL: https://www.dilovamova.com/index.php?page=10&event=203384

14. Правила створення та використання надійних паролів – рекомендації кіберполіції. *Кіберполіція України* : [сайт]. URL: https://cyberpolice.gov.ua/article/pravyla-stvorennya-ta-vykorystannya-nadijnyx-paroliv--rekomendacziyi-kiberpolicziyi-3711/

15. Як створити надійний пароль? Поради експерта. *СУСПІЛЬНЕ* : [сайт]. URL: https://suspilne.media/128333-ak-stvoriti-nadijnij-parol-poradi-eksperta/

16. Як створити по-справжньому надійний пароль: докладний посібник. *SPILNO* : [сайт]. URL: https://spilno.org/article/yak-stvoryty-po-spravzhnomu-nadiinyi-parol-dokladnyi-posibnyk

17. Основні правила кібергігієни. *CERT-UA* : [сайт]. URL: https://cert.gov.ua/recommendation/2502

18. Кудінов В. А. До проблеми щодо створення надійних паролів користувачів Інтегрованої інформаційно-пошукової системи МВС України. *Актуальні проблеми управління інформаційною безпекою держави* : матеріали VIII наук.-практ. конф. (Київ, 24 трав. 2017 р.). Київ: Нац. акад. СБ України, 2017. С. 54–56.

19. 10 дивних фактів про паролі. *Kharkiv IT Cluster* : [сайт]. URL: https://it-kharkiv.com/10-dyvnyh-faktiv-pro-paroli/ (дата звернення: 03.07.2023).

20. Test Your Password. *The Password Meter* : [сайт]. URL: http://www.passwordmeter.com/

21. Надійний пароль починається з 14 символів – швидкість зламу паролів різної довжини https://techtoday.in.ua/news/nadijnyj-parol-pochynayetsya-z-14-symvoliv-shvydkist-zlamu-paroliv-riznoyi-dovzhyny-151114.html

22. Безкоштовні онлайн генератори. *Generator Online* : [сайт]. URL: https://generator-online.com

23. Яким має бути безпечний пароль? *Zillya Антивірус* : [сайт]. URL: https://zillya.ua/yakim-ma-buti-bezpechnii-parol

24. Akamai. Web Application & API Attacks Report 2024–2025. URL: https://www.akamai.com/.

25. Рекомендації щодо протидії кіберзагрозам на робочих місцях, розроблені Департаментом інформатизації МВС України : Лист директора Департаменту освіти, науки та спорту МВС України від 25.10.2022 № 32060/48-2022.