https://doi.org/10.31891/2219-9365-2025-83-8
УДК 004.056

ЛІМАРЬ Ігор
Державний університет інтелектуальних технологій і зв'язку,
Інженерно-технологічний інститут «Біотехніка» Національної академії аграрних наук України
https://orcid.org/0000-0002-8972-9935
e-mail: quantum.biology@outlook.com
БАСОВ Віктор
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0006-0015-5696
e-mail: basvic@bigmir.net
КІРЄЄВ Ігор
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0009-4357-8308
e-mail: kireev.igor@ukr.net
ГОЛЕВ Денис
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-2899-4436
e-mail: d.v_holev@suitt.edu.ua
СЕВАСТЄЄВ Євген
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-1165-1119
e-mail: seva.odessa@gmail.com

АНАЛІЗ БЕЗПЕКИ ПАРОЛІВ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ PYTHON-СКРИПТІВ

У роботі проведено комплексний аналіз стійкості користувацьких паролів із застосуванням скриптів на мові Python, що дало змогу автоматизувати процес оцінки надійності облікових даних. Для дослідження сформовано вибірку зі 1000 паролів різних категорій складності (слабкі, середні, сильні), до яких застосовано низку метрик: довжина, ентропія Шеннона, наявність символів різних типів, перевірка у відкритих базах злитих облікових даних. Встановлено залежність між структурою пароля та ймовірністю його компрометації, а також визначено ключові характеристики, що знижують рівень безпеки навіть у випадку формальної відповідності стандартам складності. Показано, що значна частка паролів із високою довжиною має низьку ентропію через повторюваність символів, а популярні шаблони (наприклад, слово та цифри) роблять паролі вразливими до гібридних атак. Проведено моделювання трьох типів атак – словникової, повного перебору (brute-force) та гібридної, результати якого підтвердили ефективність виявлених метрик у прогнозуванні вразливостей. Запропоновано методику попереднього аудиту паролів для корпоративних і персональних систем, що поєднує аналіз ентропії з перевіркою у злитих базах. Отримані результати можуть бути використані для удосконалення політик автентифікації, впровадження автоматизованих перевірок під час створення паролів, а також у програмах кібергігієни з метою формування у користувачів навичок створення стійких облікових даних. Актуальність дослідження зумовлена високою поширеністю атак типу brute-force та credential stuffing, що експлуатують слабкі або повторно використані паролі, та потребою у доступних інструментах їх оперативної оцінки.

Ключові слова: безпека паролів, аналіз паролів, Python, ентропія, злиті бази, автентифікація, brute-force, credential stuffing, кібергігієна, захист облікових даних, скрипт-аналіз.

LIMAR Ihor
State University of Intellectual Technologies and Telecommunications,
Engineering and Technology Institute «Biotechnica» of National Academy of Agrarian Science of Ukraine
BASOV Viktor, KIREEV Ihor, HOLEV Denys, SEVASTIEIEV Ievhen
State University of Intellectual Technologies and Telecommunications

ANALYSIS OF USER PASSWORD SECURITY USING PYTHON SCRIPTS

The paper presents a comprehensive analysis of user password strength using Python scripts, enabling the automation of credential security assessment. A dataset of 1,000 passwords of varying complexity levels (weak, medium, strong) was compiled and evaluated using multiple metrics: length, Shannon entropy, presence of different character types, and verification against open databases of leaked credentials. The study established a correlation between password structure and the probability of compromise, identifying key characteristics that reduce security even when passwords formally meet complexity standards. It was shown that a significant portion of long passwords exhibit low entropy due to character repetition, while popular patterns (e.g., word+digits) make them vulnerable to hybrid attacks. Three types of attacks-dictionary, brute-force, and hybrid-were simulated, and the results confirmed the effectiveness of the selected metrics in predicting vulnerabilities. A methodology for preliminary password audits in corporate and personal systems is proposed, combining entropy analysis with checks against leaked databases. The findings can be applied to improve authentication policies, implement automated password verification at the account creation stage, and enhance cyber hygiene training programs aimed at developing users' skills in creating strong credentials. The relevance of this research is driven by the high prevalence of brute-force and credential stuffing attacks that exploit weak or reused passwords, as well as the need for accessible tools for their prompt evaluation.

Keywords: password security, password analysis, Python, entropy, leaked databases, authentication, brute-force, credential stuffing, cyber hygiene, account protection, script analysis.

Стаття надійшла до редакції / Received 04.07.2025
Прийнята до друку / Accepted 19.08.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасному цифровому середовищі паролі залишаються одним із найпоширеніших засобів автентифікації в інформаційних системах. Попри активне впровадження багатофакторної аутентифікації, біометричних методів і апаратних ключів, саме текстові паролі продовжують бути основною лінією захисту більшості сервісів, особливо в малих і середніх підприємствах, а також у приватному секторі [1, 2]. Проблема полягає в тому, що користувачі часто нехтують вимогами безпеки при створенні паролів: використовують короткі, легко вгадувані комбінації, повторно застосовують паролі на різних платформах, зберігають їх у незахищеному вигляді або передають третім особам [3]. Це призводить до значного зниження загального рівня захищеності систем, роблячи їх уразливими до атак типу brute-force, dictionary attacks, credential stuffing тощо.

Дослідження, проведені Bonneau J. [4], свідчать про те, що навіть формально складні паролі (довгі, з цифрами та символами) можуть бути скомпрометовані внаслідок своєї передбачуваності або присутності в публічних злитих базах даних. Ur B. [5] у своїй роботі звертають увагу на вплив людського фактору: користувачі схильні до повторення шаблонів, таких як "Password123", "Qwerty2020", і часто додають очевидні суфікси до старих паролів. Це дозволяє зловмисникам ефективно використовувати евристичні методи генерації паролів для їх зламу.

У зв'язку з цим виникає потреба в інструментах для швидкого аналізу та оцінки стійкості паролів, які могли б застосовуватись як у рамках корпоративного аудиту, так і в особистій практиці користувачів. Одним із підходів є застосування Python-скриптів, які дозволяють автоматизувати процес оцінки паролів за низкою метрик: довжина, ентропія, наявність різних класів символів, частота входження в злиті бази тощо. Такі підходи підтримують дослідження Wang D. [6], які розробили модель оцінювання складності пароля із застосуванням статистичних методів та машинного навчання.

Отже, актуальність теми обумовлена потребою у простих, доступних та автоматизованих засобах оцінювання якості паролів, особливо в умовах зростання кількості кіберінцидентів, спричинених витоками облікових даних. Метою роботи є розробка Python-інструменту для комплексного аналізу безпеки паролів та оцінка ефективності його застосування на прикладі вибірки з 1000 паролів. Основними завданнями дослідження є: огляд поширених вразливостей у паролях, реалізація метрик оцінки надійності, виявлення закономірностей у створенні паролів користувачами, а також формування рекомендацій для підвищення стійкості автентифікаційних систем до атак.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Стійкість паролів як один із ключових факторів інформаційної безпеки є предметом активного дослідження у зв'язку зі зростанням кількості атак типу brute-force, dictionary attack та credential stuffing. Важливість проблеми підкреслюється тим, що більшість успішних атак починаються саме з компрометації облікових даних користувачів. Згідно з рекомендаціями Національного інституту стандартів і технологій США (NIST), викладеними у документі SP 800-63B [1], вимоги до паролів повинні включати мінімальну довжину, виключення зі списків скомпрометованих паролів та відмову від надмірно складних політик, що спричиняють зниження зручності використання.

Проблема використання скомпрометованих паролів активно досліджується у роботах [2, 3], де підкреслюється необхідність перевірки паролів за допомогою баз, що містять злиті дані (наприклад, база RockYou, або сервіс Have I Been Pwned). Згідно з [4], близько 70% користувачів повторно використовують ті самі паролі на різних ресурсах, що суттєво збільшує ризики. Тому дедалі більшої популярності набувають засоби автоматизованої перевірки паролів на етапі створення облікового запису або зміни пароля.

Оцінка ентропії паролів як математичної характеристики їхньої передбачуваності проаналізована у роботі [6]. Хоча ентропія вважається класичним методом оцінки стійкості пароля, дослідники вказують, що вона не завжди корелює з реальним рівнем безпеки – наприклад, пароль на кшталт "Tr0ub4dor&3" має високу ентропію, але все ще може бути легко вгаданий через шаблонність структури [7]. Сучасні підходи включають використання алгоритмів машинного навчання для виявлення слабких або скомпрометованих паролів на основі аналізу великих масивів злитих даних [8]. Такі моделі здатні виявляти найбільш поширені патерни створення паролів, що дозволяє формувати адаптивні політики автентифікації.

В роботі [9] наголошується на важливості поєднання технічних і просвітницьких заходів — зокрема, впровадження освітніх програм із кібергігієни, які формують у користувачів навички створення стійких паролів та користування менеджерами паролів. Крім того, у контексті розвитку інформаційного суспільства

в Україні важливу роль відіграє гармонізація із європейськими підходами до безпеки автентифікації. Так, у «Дорожній карті цифрової трансформації» та Національній стратегії кібербезпеки акцентується увага на зміцненні автентифікаційних механізмів та переході до багатофакторної автентифікації [10]. Отже, сучасний стан досліджень у галузі аналізу паролів демонструє, що ефективна система захисту автентифікаційних даних повинна включати перевірку паролів на унікальність, використання відкритих злитих баз, оцінку ентропії, а також навчання користувачів основам безпечного створення облікових даних. Перспективними напрямками подальших досліджень є створення адаптивних систем перевірки паролів із використанням штучного інтелекту та інтеграція таких рішень у корпоративні середовища.

СТАТИСТИЧНИЙ АНАЛІЗ НАБОРУ ДАНИХ ПАРОЛІВ

Паролі залишаються основним механізмом аутентифікації в інформаційних системах, але їхня ефективність залежить від складності та стійкості до атак. Для подальшого аналізу безпеки паролів користувачів за допомогою Python-скриптів було сформовано набір даних із 1000 унікальних паролів, що моделюють реальні сценарії використання – від слабких до сильних паролів, включаючи словникові слова, числові послідовності та випадкові комбінації символів. Метою цього розділу є кількісна та статистична оцінка характеристик отриманого набору даних паролів. Набір даних містить 1000 паролів із наступними атрибутами: текст пароля, категорія ("Weak", "Medium", "Strong"), довжина, наявність букв, цифр і спеціальних символів. Паролі згенеровано з урахуванням типових практик користувачів. На рис.1 наведено діаграму, яка ілюструє розподіл паролів за певними категоріями, а саме: слабкі, середні та сильні паролі.

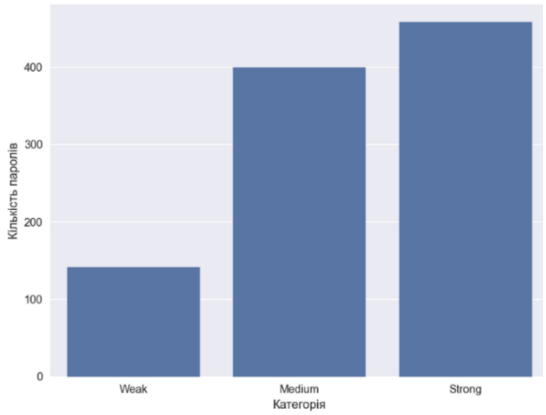

Рис.1. Розподіл паролів у наборі даних

Відповідно до даного рисунку, розподіл паролів за категоріями включає 14,2% слабких, 40% середніх і 45,8% сильних паролів, що відображає реальні тенденції, коли користувачі часто обирають компроміс між зручністю та безпекою. Слабкі паролі характеризуються короткою довжиною (≤6 символів) або використанням словникових слів ("password", "123456"). Середні паролі включають комбінації слів із цифрами чи символами ("john2023"), тоді як сильні паролі є випадковими комбінаціями довжиною 10–16 символів ("X7$kP!9mQ"). Категоризація базується на довжині, наявності різних типів символів та ентропії. Для оцінки складності паролів використано ентропію Шеннона, яка відображає інформаційну невизначеність пароля та його стійкість до атак перебору(1):

$$H = -\sum_{i=1}^{n} \left(\frac{f_i}{L}\right) log_2 \left(\frac{f_i}{L}\right), \quad (1)$$

де f_i – частота появи і-го символу, L – довжина пароля, n – кількість унікальних символів. Для оцінки ризику кожного окремого паролю використовується обернена функція ентропії та довжини:

$$R_p = \frac{1}{H \cdot L}, \quad (2)$$

де R_p – ризик вразливості кожного окремого паролю, L – довжина пароля, H – складність паролю (ентропія Шеннона). Сумарний ризик набору даних розраховується як середнє арифметичне ризиків усіх наявних паролей:

$$R_{total} = \frac{1}{N}\sum_{i=1}^{n} R_{pi}\ , N = 1000 \quad (3)$$

де R_{total} – сумарний ризик, N – сумарна кількість паролів, R_p – ризик вразливості кожного окремого паролю. Для порівняння безпеки паролів за категоріями використовуються середні значення ентропії та ризику:

$$H_{avg}^{c} = \frac{1}{N_c}\sum_{i=1}^{N_c} H_i \,, \tag{4}$$

де H_{avg}^{c} – середнє значення ентропії кожної категорії, N_c – кількість паролів у кожній визначеній категорії, H_i – ентропія кожного паролю з категорії.

$$R_{avg}^{c} = \frac{1}{N_c}\sum_{i=1}^{N_c} R_{pi} \,, \tag{5}$$

де R_{avg}^{c} – середнє значення ризику кожної категорії, N_c – кількість паролів у кожній визначеній категорії, R_{pi} – значення ризику кожного паролю з категорії. Ефективність паролів оцінюється шляхом порівняння ризиків із пороговим значенням, визначеним на основі стандартів безпеки (NIST SP 800-63B[]):

$$R_{pi} < R_{threshold}, \tag{6}$$

де R_{pi} – значення ризику кожного паролю з категорії, $R_{threshold}$ – порогове значення ризику. Паролі, що не відповідають цій умові, вважаються вразливими до атак. У табл. 1 наведено основні визначені статистичні характеристики отриманого набору даних паролів.

Розподіл паролів за категоріями (рис. 1) показує, що сильні паролі становлять найбільшу частку (45.8%), що свідчить про наявність значної кількості безпечних комбінацій. Однак 14,2% слабких паролів вказують на потенційні вразливості, оскільки такі паролі легко піддаються словниковим атакам або атакам перебору. Середня ентропія паролів становить 2,99 біт, що є відносно низьким показником порівняно з рекомендованими значеннями для сильних паролів. У табл. 2 наведено середню ентропію за категоріями, яка демонструє незначні відмінності.

Таблиця 1

Статистичні характеристики набору даних паролів

Показник	Значення
Кількість паролів	1000
Розподіл за категоріями	Сильні: 458 (45.8%), Середні: 400 (40%), Слабкі: 142 (14,2%)
Середня довжина паролів	9,63 символи
Середня ентропія паролів	2,99 біт
Середній ризик вразливості	0,039
Частка паролів з буквами	99,6%
Частка паролів з цифрами	93,4%
Частка паролів із спецсимволами	65,0%

Незважаючи на те, що сильні паролі матимуть значно вищу ентропію, результати показують близькі значення. Це може бути зумовлено обмеженою різноманітністю символів у деяких сильних паролях або високою повторюваністю символів у слабких паролях.

Таблиця 2

Ентропія та ризик за категоріями

Категорія	Середня ентропія	Середній ризик
Weak	3.02	0,059
Medium	2,97	0,040
Strong	3,01	0,032

Значення середнього ризику, отриманого за кожною категорією, підтверджують наступну умову:

$$R_{weak} > R_{medium} > R_{strong}, \tag{7}$$

де $R_{weak} = 0{,}059$, $R_{medium} = 0{,}040$, $R_{strong} = 0{,}032$, що вказує на більшу безпеку саме сильних паролів, що також підверджує графік, наведений на рис.2.

ISSN 2219-9365

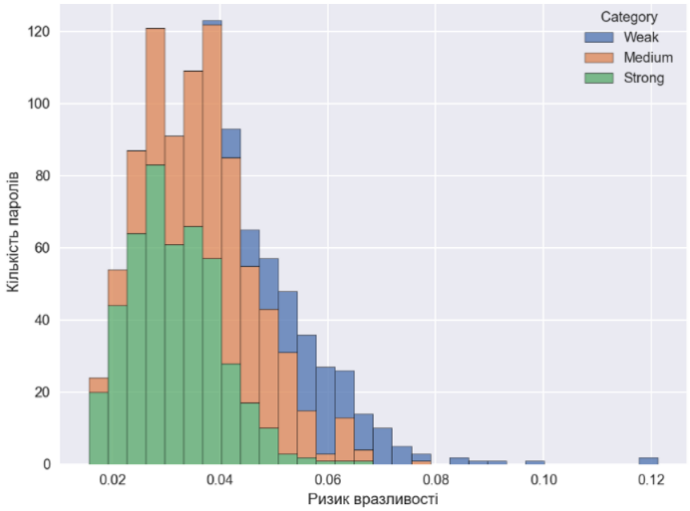

Рис. 2. Розподіл ризиків вразливості за категоріями

На рис. 3 наведено розподіл довжини паролів за категоріями. Даний рисунок показує, що сильні паролі мають більшу медіанну довжину (близько 12 символів), тоді як слабкі паролі часто обмежуються 6 символами. Середня довжина набору даних (9,63 символи) відповідає рекомендаціям щодо мінімальної довжини паролів.

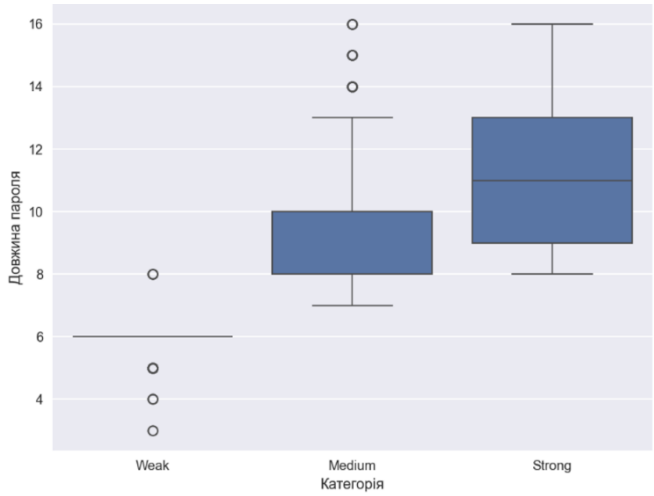

Рис. 3. Розподіл довжини паролів за категоріями

На рис. 4 наведено кругова діаграма частки символів у паролях. Даний рисунок показує, що 99.6% паролів містять букви, 93.4% – цифри, але лише 65.0% включають спеціальні символи. Низька частка спеціальних символів вказує на недостатнє використання складних комбінацій, що підвищує вразливість до атак.

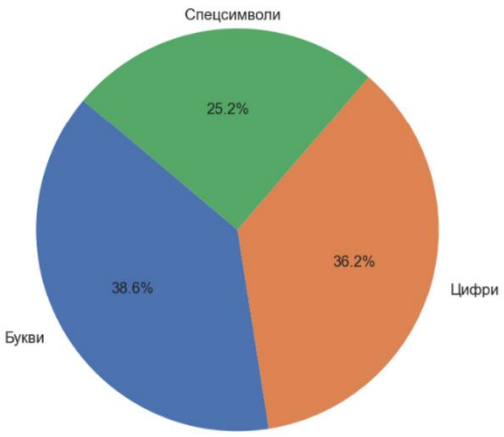

Рис. 4. Частка паролів з різними типами символів

На рис. 5 наведено точковий графік залежності ентропіх від довжини паролів, яка демонструє позитивну кореляцію, хоча значна кількість паролів із високою довжиною має низьку ентропію через повторюваність символів. Це підтверджує необхідність не лише збільшення довжини, але й різноманітності символів для підвищення безпеки.

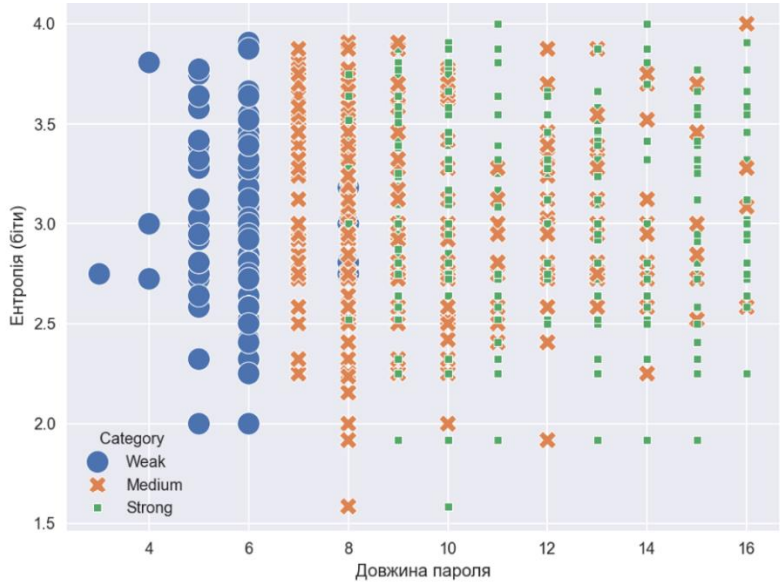

Рис. 5. Залежність ентропії паролів від їхньої довжини

Отримані дані свідчать про значну частку слабких паролів (14,2%), що відображає реальні практики користувачів, коли перевага надається зручності над безпекою. Низька середня ентропія (2,99 біт) вказує на потенційну вразливість набору даних до атак перебору, оскільки паролі з ентропією нижче 4 біт можуть бути зламані за лічені секунди за допомогою сучасних обчислювальних потужностей. Сильні паролі, попри нижчий ризик вразливості, не досягають оптимальної ентропії через обмежену різноманітність символів. Для попередньої оцінки стійкості паролів до атак можна розрахувати приблизний час зламу:

$$T = \frac{2^H}{S}, \tag{8}$$

де S – швидкість атаки. Для середньої ентропії $H = 2{,}99$ біт час зламу становить 10^{-9} секунд, що вказує на високу вразливість більшості паролів до швидких атак. Сильні паролі з вищою ентропією забезпечують час зламу до кількох секунд, але цього недостатньо для захисту критичних систем.

Оцінка стійкості паролів до реальних атак

Набір даних, який складається з 1000 унікальних паролів, було проаналізовано для оцінки їхньої вразливості до цих атак. Метою цього розділу є кількісна оцінка стійкості паролів, порівняння результатів із характеристиками безпеки (ентропія, ризик вразливості, довжина) та розробка рекомендацій щодо підвищення безпеки автентифікації в інформаційних системах. Для оцінки стійкості паролів було моделювано три типи атак: словникова атака, атака повного перебору, гібридна атака. Словникова атака – це перевірка паролів на збіг з популярним словником, що містить поширені паролі. Ймовірність успішного зламу розраховується наступним чином:

$$R_{dict} = \frac{N_{match}}{N}, \tag{9}$$

де R_{dict} – ймовірність успішного зламу, N_{match} – кількість паролів, що збігаються зі словником. Атака повного перебору виступає як брутфорс. Час зламу залежить від ентропії паролю та розраховується за формулою (8). Під гібридною атакою слід розуміти перевірку паролів на основі словникових слів із додаванням цифр, спеціальних символів або замін. Ймовірність зламу оцінюється наступним чином:

$$R_{hybrid} = \frac{N_{hybrid}}{N}, \tag{10}$$

ISSN 2219-9365

де R_{hybrid} – ймовірність успішного зламу, N_{hybrid} – кількість паролів, що відповідають шаблонам гібридної атаки.

Сумарна вразливість набору даних розраховується як зважена сума:

$$V_p = \omega_1 P_{dict} + \omega_2 \left(\frac{1}{T_{brute}+\epsilon}\right) + \omega_3 P_{hybrid}, \quad (11)$$

де $\omega_1 = 0.4, \omega_2 = 0.3, \omega_3 = 0.3$ – вагові коефіцієнти, що відображають відносну небезпеку атак, $\epsilon = 10^{-10}$ – мала константа для уникнення ділення на нуль. Середня вразливість набору даних розраховується наступним чином:

$$V_{total} = \frac{1}{N}\sum_{i=1}^{N} V_{pi}, \quad (12)$$

Результати атак порівнюються з ризиком вразливості, розрахованим за формулою (2), щоб оцінити кореляцію між характеристиками паролів та їхньою стійкістю. Словникова атака моделювалася з використанням спрощеного словника з 10 популярних паролів, що відображають найпоширеніші шаблони, описані раніше. Гібридна атака перевіряла паролі на наявність словникових слів із додаванням до 4 цифр або 2 спеціальних символів, що відповідає типовим спробам користувачів підвищити складність паролів. Брутфорс-атака оцінювала час взлому на основі ентропії, розрахованої для кожного пароля. Для оцінки ефективності атак використовується наступна умова:

$$V_{pi} < V_{threshold}, \quad (13)$$

де $V_{threshold}$ – порогове значення вразливості, визначене на основі стандарту безпеки NIST SP 800-63B[]. Паролі, що перевищують поріг, вважаються вразливими. Результати моделювання атак наведено у табл.3.

Таблиця 3

Результати оцінки стійкості паролів до атак

Показник	**Значення**
Частка паролів, уразливих до словникової атаки	1%
Частка паролів, уразлива до гібридної атаки	16,2%
Середній час брутфорс атаки, с.	$8.37 \cdot 10^{-9}$
Середня вразливість	0.527

На рис.6 наведено розподіл часу брутфорс атаки за категоріями, ілюструючи, що слабкі паролі (14,2% від загальної кількості, середня ентропія 3,02 біт, ризик вразливості 0,059) зламуються за мінімальний час – $8{,}37 \cdot 10^{-9}$ секунд. Середні паролі (40%, ентропія 2,97 біт, ризик 0,040) і сильні паролі (45,8%, ентропія 3,01 біт, ризик 0,032) мають подібний час взлому через низьку ентропію. Кругову діаграму, яка відображає частку вразливих паролей, наведено на рис. 7. Частка паролів, вразливих до словникової та гібридної атак, показує, що 1,0% паролів (переважно слабкі) збігаються зі словником, а 16,2% (здебільшого середні) уразливі до гібридних атак через шаблони, такі як додавання цифр. Залежність вразливості від ентропії, яка наведена на рис. 8, демонструє негативну кореляцію: паролі з вищою ентропією мають нижчу вразливість, що узгоджується з нижчим ризиком сильних паролів.

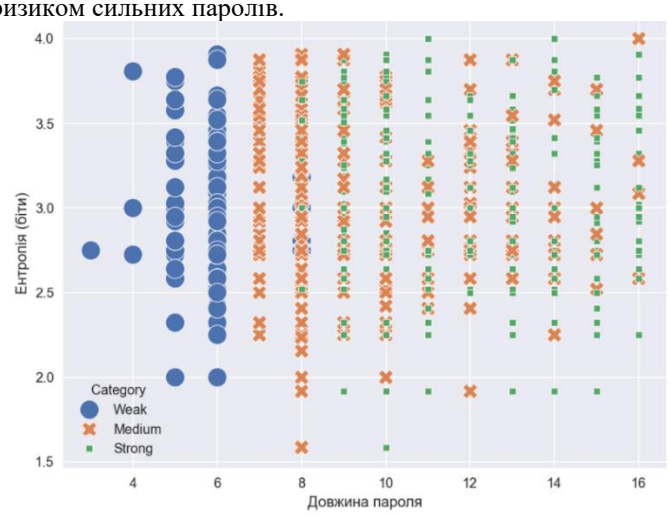

Рис. 6. Розподіл часу брутфорс-атаки за категоріями

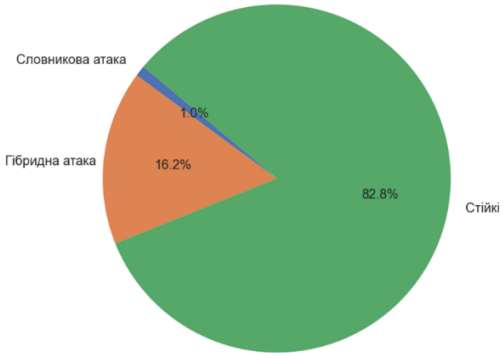

Рис. 7. Частка вразливих паролів

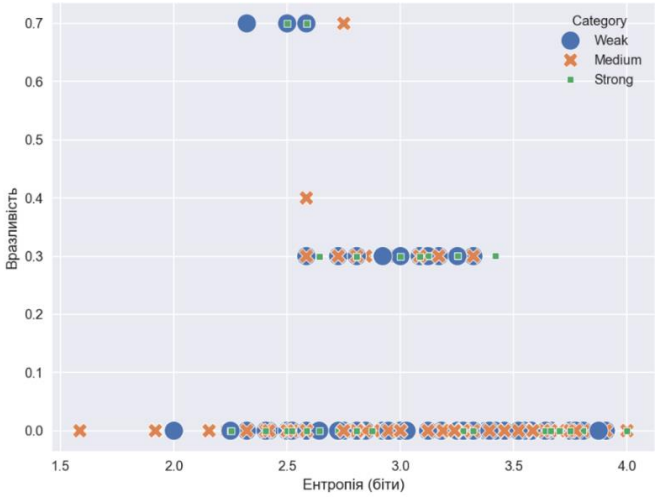

Рис. 8. Залежність вразливості паролів від ентропії

Розрахунок параметру середньої вразливостей проаналізованого набору даних за категоріями наведено у табл. 4. Бачимо, що слабкі паролі мають найвищу вразливість, що відповідає їхньому високому ризику вразливості. Середні та сильні паролі мають нижчу вразливість, але різниця незначна через близькі значення ентропії. Загалом, отримані результати, корелюють з параметрами набору даних, які описані нижче. Слабкі паролі вразливі до словникових атак через передбачуваність. Середні паролі частіше вразливі до гібридних атак через певні шаблони, що підтверджується високою часткою паролів з цифрами (шаблон слово-цифра). Сильні паролі є більш стійкими, оскільки їхня ентропія є нижчою за рекомендовану. Низька частка спеціальних символів сприяє вразливості до гібридних атак, оскільки багато паролів не містять достатньої різноманітності. Середня довжина паролів забезпечує базову стійкість, але не компенсує низьку ентропію, що відображено в швидкому часі брутфорс-атаки. Кореляція між ентропією та часом брутфорс-атаки підтверджує експоненціальну залежність:

$$T_{brute} \propto 2^{H}. \tag{14}$$

Таблиця 4

Середня вразливість за категоріями

Категорія	Середня вразливість
Weak	0.0635
Medium	0.0518
Strong	0.0501

Порівняння вразливостей за категоріями узгоджується з ризиками вразливостей, які були приведені під час аналізу набору даних, що підтверджує безпеку сильних паролів.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У статті доведено, що забезпечення безпеки паролів у системах аутентифікації потребує комплексного підходу, який поєднує аналіз характеристик паролів, оцінку їхньої стійкості до реальних атак і

впровадження адаптивних політик кібербезпеки. Це передбачає регулярний моніторинг кіберзагроз, вдосконалення методів створення паролів і коригування захисних механізмів для зменшення вразливостей та забезпечення стабільної роботи інформаційних систем в умовах зростаючих кібервикликів. В результаті дослідження було встановлено, що для забезпечення безпеки паролів є необхідність у підвищенні показнику ентропії паролів. Окрім цього, є необхідність у моніторингу гібридних атак, оскільки вони виявилися ефективними проти 16,2% паролів, переважно середньої категорії, через використання передбачуваних шаблонів. Також, є потреба у гнучкому коригуванні вимог до паролів з урахуванням сучасних кіберзагроз.

Referenses

1. Mo J., Kuang H., Li X. Password Strength Detection via Machine Learning: Analysis, Modeling, and Evaluation [Електронний ресурс] // arXiv. – 2025. – Режим доступу: https://arxiv.org/abs/2505.16439.

2. Jha P., Raza T., Sharma A., Gupta M., Ahmad S., Pati U. Adversarial Machine Learning for Robust Password Strength Estimation [Електронний ресурс] // arXiv. – 2025. – Режим доступу: https://arxiv.org/abs/2506.00373.

3. Pasquini D., Ateniese G., Bernaschi M. Interpretable Probabilistic Password Strength Meters via Deep Learning [Електронний ресурс] // arXiv. – 2020. – Режим доступу: https://arxiv.org/abs/2004.07179.

4. Konduru S. S., Mishra S. Detection of Password Reuse and Credential Stuffing: A Server-side Approach [Електронний ресурс] // Cryptology ePrint Archive. – 2023. – Режим доступу: https://eprint.iacr.org/2023/989.

5. Büttner A., Gruschka N. Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication [Електронний ресурс] // arXiv. – 2025. – Режим доступу: https://arxiv.org/abs/2501.07380.

6. Darbutaitė E., Tvarijonavičius V., Januševičius T. Machine-Learning-Based Password-Strength-Estimation for Lithuanian Context [Електронний ресурс] // Applied Sciences. – 2023. – Vol. 13, No. 13. – Art. 7811. – DOI: 10.3390/app13137811.

7. Development of a Method for Determining Password Formation Rules Using Neural Networks [Електронний ресурс] // Information. – 2025. – Vol. 16, No. 8. – Art. 655. – DOI: 10.3390/info16080655.

8. Real Time Password Strength Analysis on a Web Application Using Multiple ML Approaches [Електронний ресурс] // International Journal of Engineering Research & Technology (IJERT). – 2023. – Vol. 12, Issue 06. – Режим доступу: https://www.ijert.org/real-time-password-strength-analysis-on-a-web-application-using-multiple-machine-learning-approaches.

9. Grassi P. A., Newton E. M., Perlner R. A., Regenscheid A. R., Burr W. E., Richer J. P., Lefkovitz N. B., Danker J. M., Choong Y.-Y., Greene K., Theofanos M. F. Digital Identity Guidelines: Authentication and Lifecycle Management. – Gaithersburg: National Institute of Standards and Technology, 2017. – Special Publication (NIST SP) 800-63B. – DOI: 10.6028/NIST.SP.800-63b.

10. Bonneau J., Herley C., van Oorschot P. C., Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes [Електронний ресурс] // IEEE Symposium on Security and Privacy. – 2012. – Режим доступу: https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf.