УДК: 004.056.5:519.2:519.7 DOI 10.33111/mise.105.12

Позднякович О.Є.,
к.ф.-м.н., доцент кафедри системного аналізу та кібербезпеки,
КНЕУ імені Вадима Гетьмана
Каленюк А.Р.
здобувач першого (бакалаврського) рівня вищої освіти,
КНЕУ імені Вадима Гетьмана

Pozdniyakovych O.E.,
Candidate of Physical and Mathematical Sciences, Associate Professor
of System analysis and cybersecurity
KNEU named after V. Hetman
Kalenyuk A.R.
first (bachelor's) level higher education student,
KNEU named after V. Hetman

КІЛЬКІСНА ОЦІНКА СТІЙКОСТІ ПАРОЛІВ У СИСТЕМАХ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ЕНТРОПІЙНИХ ТА ЙМОВІРНІСНИХ МОДЕЛЕЙ

QUANTITATIVE EVALUATION OF PASSWORD STRENGTH IN AUTHENTICATION SYSTEMS BASED ON ENTROPY AND PROBABILISTIC MODELS

Анотація. *У статті розглядається проблема кількісної оцінки стійкості текстових паролів у сучасних системах автентифікації. Проаналізовано обмеження класичного ентропійного підходу Шеннона при оцінці реальних паролів, створених користувачами. Запропоновано комплексну методологію оцінки, що базується на поєднанні n-грамних моделей Маркова та метрики Guesswork (очікуваної кількості спроб вгадування). Встановлено математичні залежності між імовірністю пароля, «бітами стійкості» та реальним часом зламу з урахуванням сучасних стандартів хешування. Продемонстровано переваги запропонованого підходу в контексті вимог стандарту NIST SP 800-63B-4 щодо динамічного формування політик безпеки.*
Ключові слова: *стійкість паролів, ентропія Шеннона, Guesswork, n-грамні моделі Маркова, системи автентифікації, кібербезпека, NIST SP 800-63B-4, біти стійкості.*

Abstract. *The article discusses the problem of quantitative assessment of text password strength in modern authentication systems. It analyzes the limitations of Shannon's classic entropy approach when evaluating real passwords created by users. It proposes a comprehensive evaluation methodology based on a combination of Markov n-gram models and the Guesswork metric (the expected number of guess attempts). Mathematical dependencies between password probability, «bits of strength», and real-world cracking time are established, taking into account modern hashing standards. The advantages of the proposed approach are demonstrated in the context of the requirements of the NIST SP 800-63B-4 standard for dynamic security policy formation.*

Keywords: *password strength, Shannon entropy, guesswork, n-gram Markov models, authentication systems, cybersecurity, NIST SP 800-63B-4, bits of strength.*

Постановка проблеми. Зі зростанням кількості кіберзагроз та потужності обчислювальних ресурсів, питання надійної автентифікації стає критичним для будь-якої інформаційної системи. Незважаючи на впровадження біометричних технологій та багатофакторної автентифікації, текстові паролі залишаються найбільш розповсюдженим методом підтвердження особи в інформаційних системах. Проте ефективність парольного захисту критично залежить від здатності системи адекватно оцінювати складність пароля на етапі його створення.

Традиційно стійкість паролів оцінювалася за допомогою формальних правил (мінімальна довжина, наявність символів різних регістрів, цифр та спецсимволів), що базувалися на припущенні про рівномірний розподіл символів. Однак, як показує практика витоків даних, користувачі схильні використовувати передбачувані шаблони, власні імена та популярні послідовності. Як наслідок, виникає фундаментальний розрив між теоретичною ентропією простору ключів та реальною обчислювальною складністю підбору пароля зловмисником [1]. Існує нагальна потреба у переході від якісних («слабкий/сильний») до кількісних показників, що відображають очікуваний час зламу в умовах реальних стратегій атак.

Аналіз останніх досліджень і публікацій. Проблема кількісної оцінки стійкості паролів еволюціонувала від простих евристичних перевірок до складних імовірнісних моделей. Сучасні дослідження [2] доводять, що формальні метрики часто переоцінюють стійкість паролів, створюючи ілюзію безпеки, і обґрунтовують доцільність переходу до марковських моделей. У роботі [3] підтверджується, що імовірнісні моделі краще корелюють із часом зламу, ніж статичні правила.

Фундаментальний зв’язок між ентропією та кількістю спроб вгадування (Guesswork) встановив Джеймс Массі [4]. Його праці заклали основу для розуміння того, що ентропія визначає лише нижню межу зусиль зловмисника. Емпіричний аналіз великих масивів витоків даних, проведений у роботі [5], продемонстрував принцип «спадної віддачі» (diminishing returns) словникових атак, що вимагає використання методів, здатних до генералізації.

Сучасні індустріальні стандарти, зокрема NIST SP 800-63B-4 [6], офіційно відмовляються від жорстких вимог до композиції на користь перевірки паролів за базами скомпрометованих облікових

записів та імовірнісних оцінок. Для прикладних систем найбільш верифікованим методом залишається інтеграція метрики Guesswork та n-грамних моделей Маркова у контексті стандартів NIST для апроксимації розподілу ймовірностей [7].

Метою статті є проведення порівняльного аналізу ефективності класичних ентропійних метрик, евристичного алгоритму zxcvbn та n-грамних моделей Маркова, а також обґрунтування доцільності переходу до комплексної методології оцінки стійкості паролів на основі метрики Guesswork для імплементації в системах автентифікації відповідно до вимог стандарту NIST SP 800-63B-4.

Виклад основного матеріалу. *Обмеження ентропійного підходу та метрика Guesswork.* Ключовою проблемою оцінки стійкості пароля є розрив між теоретичною інформаційною невизначеністю та реальною обчислювальною складністю підбору [8]. Традиційною метрикою невизначеності є ентропія Шеннона (H) [9], яка для випадкової величини X (пароля) з розподілом ймовірностей $P = \{p_1, p_2, \dots, p_M\}$ визначається як:

$$H(X) = -\sum_{i=1}^{M} p_i \log_2 p_i ,$$

де M – кількість можливих значень у просторі паролів, а p_i – ймовірність вибору i-го пароля користувачем.

Однак, ентропія Шеннона є асимптотичною мірою і не завжди коректно відображає складність атаки методом перебору для скінченних, нерівномірних розподілів, характерних для людських паролів. Більш адекватною метрикою для криптографічного аналізу є метрика Guesswork ($G(X)$). Оптимальною стратегією зловмисника, яка мінімізує математичне сподівання кількості спроб $\mathbb{E}[G]$, є перевірка кандидатів у порядку спадання їхніх ймовірностей: $p_1 \geq p_2 \geq \dots \geq p_M$. У такому випадку очікувана кількість спроб вгадування $\mathbb{E}[G]$ визначається як перший момент величини G:

$$\mathbb{E}[G] = \sum_{i=1}^{M} i \cdot p_i ,$$

де i – ранг (позиція) пароля в списку за спаданням ймовірності.

У роботі [4] доведено, що ентропія визначає нижню межу зусиль зловмисника, для будь-якого розподілу з $H(X) \geq 2$ біт виконується нерівність

$$\mathbb{E}[G] \geq 2^{H(X)-2} + 1 .$$

Це підтверджує парадокс Массі: істинна ентропія розподілу може недооцінювати математичне сподівання $\mathbb{E}[G]$ для розподілів з «важкими хвостами». Однак на практиці ситуація зворотна: формальна (комбінаторна) ентропія зазвичай суттєво переоцінює реальну стійкість паролів, оскільки не враховує семантичних шаблонів користувачів. Саме тому математичне сподівання $\mathbb{E}[G]$ є кращою мірою складності перебору, ніж скалярна ентропія.

Моделювання розподілу паролів за допомогою n-грам Маркова. Оскільки паролі не є випадковими наборами байтів, а підпорядковуються лінгвістичним та клавіатурним шаблонам, то для моделювання реальних розподілів використовуються n-грамні моделі, де пароль розглядається як послідовність символів $c_1, c_2, \dots, c_L$. У марковській моделі порядку $n-1$ ймовірність появи символу c_i залежить виключно від попередніх $n-1$ символів. Тоді ймовірність генерації цілого пароля $P(pw)$ визначається як добуток умовних ймовірностей переходів [7]:

$$P(pw) = \prod_{i=1}^{L} P(c_i | c_{i-n+1}, \dots, c_{i-1}).$$

Оцінка умовних ймовірностей здійснюється методом максимальної правдоподібності на основі частот у навчальному корпусі (базах витоків):

$$P(c_i | c_{i-n+1}, \dots, c_{i-1}) = \frac{Count(c_{i-n+1}, \dots, c_i)}{Count(c_{i-n+1}, \dots, c_{i-1})},$$

де $Count$ – кількість входжень відповідної n-грами в навчальні дані. Для уникнення проблеми нульових частот застосовуються алгоритми згладжування (smoothing), що дозволяє моделі оцінювати навіть ті паролі, які не зустрічалися раніше, але відповідають загальним паттернам мови.

Показник «бітів стійкості». Ключовим результатом застосування n-грамної моделі є перехід від скалярної ймовірності до логарифмічної міри ентропії конкретного пароля — «бітів стійкості»:

$$S_{pw} = -\log_2 P_{\text{n-gram}}(pw).$$

Ця величина є кількістю бінарних запитань, які в середньому потрібні, щоб відрізнити цей пароль від інших у моделі. Для

оптимальної стратегії показник Guesswork G_{pw} оцінюється через обернену ймовірність і пов'язаний з «бітами стійкості» співвідношенням [10]:

$$G_{pw} \approx \frac{1}{P(pw)} = 2^{S_{pw}} \ .$$

Це дозволяє класифікувати паролі не бінарно («сильний/слабкий»), а за неперервною шкалою. Наприклад, популярний пароль "Password123!" може формально відповідати вимогам (велика літера, цифри, спецсимвол), але його $P(pw)$ згідно з моделлю Маркова буде високою, а S_{pw} – низьким (близько 20–25 біт), що вказує на низьку реальну стійкість.

Оцінка часу зламу пароля. Щоб пов'язати кількість спроб вгадування пароля з реальним часом, використовують параметр R – швидкість перевірки кандидатів (хешів) обчислювальними засобами зловмисника. Очікуваний час зламу T:

$$T = \frac{\mathbb{E}[G]}{R}.$$

Сучасні системи використовують «повільні» хеш-функції (bcrypt, Argon2), які вводять коефіцієнт обчислювальної складності $f(k)$, що знижує ефективну швидкість R до $R_{effective} = \frac{R_{gpu}}{f(k)}$. Це дозволяє використовувати параметри хешування як інструмент для зміщення пароля з категорії «слабкий» у «сильний» у часовому вимірі. Таким чином, навіть пароль із середнім показником стійкості (наприклад, 60 біт) стає практично невразливим для офлайн-перебору протягом років. Пропонується вважати поріг $S_{pw} \approx 80$ біт як рівень «високої стійкості», що відповідає 2^{80} спробам – значенню, яке вважається криптографічно безпечним для більшості сучасних застосунків [8].

Оцінювач zxcvbn у контексті імовірнісного моделювання. Важливим етапом у розвитку методів кількісної оцінки стійкості паролів стала розробка алгоритму zxcvbn [11]. На відміну від традиційних систем, що оцінюють пароль на основі наявності символів різних регістрів або спецсимволів, zxcvbn базується на принципі зіставлення шаблонів та обчисленні комбінаторної ентропії.

Алгоритм розглядає пароль не як монолітний рядок, а як послідовність токенів (chunks), кожен з яких перевіряється за декількома словниками та детекторами патернів:

- словникові токени: пряме порівняння з базами поширених слів, імен, прізвищ та скомпрометованих паролів,
- трансформації (l33t-speak): розпізнавання замін (наприклад 0 на o), що дозволяє ідентифікувати приховані слова зі словника,
- просторові патерни: виявлення клавіатурних комбінацій (горизонтальні, вертикальні та зигзагоподібні ряди символів на розкладці QWERTY),
- хронологічні патерни: розпізнавання дат у різних форматах (день-місяць-рік).

Для кожного знайденого токена алгоритм обчислює кількість можливих спроб G_{token}, необхідних для його вгадування. Оскільки пароль може бути розбитий на токени різними способами, алгоритм аналізує всі можливі варіанти сегментації та обирає той, що дає найменшу загальну кількість спроб (найбільш імовірний шлях підбору для зловмисника). Відповідно, загальна оцінка Guesswork для пароля визначається як мінімум серед усіх можливих варіантів розбиття:

$$G_{total} = \min_{S \in Partitions} \left(\prod_{i=1}^{k} G_{token_i} \cdot C_{order} \right),$$

де $S -$ конкретний варіант розбиття пароля на k токенів із множини всіх можливих розбиттів $Partitions$, $G_{token_i} -$ оцінка кількості спроб для вгадування i-го токена, $C_{order} -$ комбінаторний множник, що враховує кількість способів розміщення (композиції) знайдених токенів у рядку. Ентропія в такому випадку обчислюється як $H = log_2 G_{total}$.

Алгоритм zxcvbn виступає як високорівнева евристична модель, тоді як n-грамні моделі Маркова забезпечують низькорівневий статистичний аналіз.

Порівняльний аналіз методів оцінки стійкості. Порівняння трьох підходів до оцінки стійкості: класичної ентропії Шеннона, алгоритма zxcvbn та n-грамної моделі Маркова наведено у табл. 1.

Аналіз даних таблиці дозволяє зробити такі висновки. По-перше, класична ентропія Шеннона залишається лише теоретичним орієнтиром і не може слугувати єдиним критерієм оцінки безпеки через ігнорування семантичних структур паролів. По-друге, хоча алгоритм zxcvbn ефективно виявляє структуровані одиниці (словникові слова, дати, клавіатурні патерни), він має обмеження щодо неструктурованих, але статистично передбачуваних послідовностей символів. Саме такі закономірності успішно

ідентифікуються n-грамною моделлю Маркова. На відміну від евристичних підходів, що спираються на статичні словники, марковська модель адаптується безпосередньо до корпусу навчальних даних, виявляючи приховані лінгвістичні патерни, характерні для специфічних груп користувачів (наприклад, професійний жаргон або національні особливості транслітерації).

Таблиця 1

ПОРІВНЯННЯ ПІДХОДІВ ДО ОЦІНКИ СТІЙКОСТІ ПАРОЛІВ

Характеристика	*Ентропія Шеннона*	*Алгоритм zxcvbn*	*n-грамна модель Маркова*
Базис оцінки	Розмір алфавіту та довжина пароля	Словники частот, паттерни.	Умовні ймовірності переходів між символами.
Чутливість до контексту	Низька. Ігнорує лінгвістичні структури.	Середня. Залежить від наповнення вбудованих словників.	Висока. Навчається на специфічних корпусах витоків.
Оцінка часу злому	$T \approx 2^{H-1}$ (переоцінка)	Ранжування патернів.	$G_{pw} \approx 2^{S_{pw}}$ (Guesswork)
Застосування	Формальні політики.	Front-end зворотний зв'язок.	Серверна аналітика.

Джерело: розроблено авторами

Імплементація згідно з вимогами NIST SP 800-63B-4. Алгоритм zxcvbn став одним із перших інструментів, що повністю реалізував вимоги NIST SP 800-63B-4 [6], які закликають верифікаторів оцінювати саме «складність вгадування» (guessability), а не формальний склад пароля.

Використання n-грамної моделі Маркова дозволяє розширити цей підхід, переходячи від статичних «чорних списків» до імовірнісного блокування. Якщо оцінена ймовірність пароля $P_{\mathrm{n-gram}}(pw)$ перевищує порогове значення (тобто S_{pw} є нижчим за допустимий рівень, наприклад 40 біт), такий пароль підлягає відхиленню як передбачуваний, навіть якщо він відсутній у базі відомих витоків.

Висновки та перспективи подальшого дослідження. На основі проведеного порівняльного аналізу доведено, що класична ентропія Шеннона є недостатньою мірою для оцінки реальної захищеності паролів, оскільки вона ігнорує нерівномірний розподіл

вибору користувачами та лінгвістичні шаблони, що призводить до суттєвої переоцінки стійкості. Обґрунтовано доцільність використання комплексної методології на базі n -грам Маркова та метрики Guesswork, яка дозволяє математично формалізувати поняття «сили» пароля через очікувану кількість спроб вгадування, а не абстрактну невизначеність. Встановлено, що хоча алгоритм zxcvbn є важливим базисом для порівняння та ефективно виявляє структуровані одиниці, такі як слова, дати та клавіатурні патерни, він може бути менш ефективним проти неструктурованих, але статистично передбачуваних послідовностей, які успішно виявляють низькорівневі марковські моделі, що навчаються безпосередньо на корпусах даних витоків.

Використання метрики Guesswork у поєднанні з ймовірнісними моделями надає інструментарій для переведення оцінки у шкалу «бітів стійкості», що має пряму фізичну інтерпретацію через очікуваний час зламу з урахуванням сучасних стандартів хешування. Це дозволяє перейти від бінарної класифікації до неперервної кількісної оцінки ризику та встановити обґрунтовані пороги відсіювання (на рівні 40–60 біт для базового захисту та 80 біт для високої стійкості), що повністю відповідає вимогам стандарту NIST SP 800-63B-4 щодо відмови від жорстких правил композиції символів на користь перевірки на ймовірність вгадування. Запропонована методологія забезпечує баланс між безпекою та зручністю користувача і може бути інтегрована як у серверні системи верифікації для превентивного блокування слабких паролів, так і у клієнтські інтерфейси для надання зрозумілого зворотного зв'язку. Перспективним є поєднання запропонованої моделі з алгоритмами глибокого навчання та контекстно-вільними граматиками [12] для виявлення складних прихованих патернів у довгих парольних фразах.

Бібліографічні посилання

1. Bonneau J., Herley C., van Oorschot P. C., Stajano F. Passwords and the Evolution of Imperfect Authentication. Communications of the ACM. 2015. Vol. 58, No. 7. P. 78–87.
2. Kelley P. G., Komanduri S., et al. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. 2012 IEEE Symposium on Security and Privacy. 2012. P. 523–537.
3. Ma J., Yang W., Luo M., Li N. A Study of Probabilistic Password Models. 2014 IEEE Symposium on Security and Privacy. 2014. P. 689–704.
4. Massey J. L. Guessing and entropy. Proceedings of 1994 IEEE International Symposium on Information Theory. 1994. P. 204.

5. Dell'Amico M., Michiardi P., Roudier Y. Password Strength: An Empirical Analysis. INFOCOM, 2010 Proceedings IEEE. 2010. P. 1–9.
6. NIST. Digital Identity Guidelines. SP 800-63B-4 (Draft). 2024/2025. URL: https://pages.nist.gov/800-63-4/
7. Castelluccia C., Dürmuth M., Perito D. Adaptive Password-Strength Meters from Markov Models. Proceedings of the 19th NDSS. 2012.
8. Pliam J. O. The Disparity between Work and Entropy in Cryptology. IACR Cryptology ePrint Archive. 1998. Report 1998/024.
9. Shannon C. E. A Mathematical Theory of Communication. Bell System Technical Journal. 1948. Vol. 27.
10. Reaz K., Wunder G. Expectation Entropy as a Password Strength Metric. arXiv preprint arXiv:2404.16853. 2024.
11. Wheeler D. L. zxcvbn: Low-Budget Password Strength Estimation. 25th USENIX Security Symposium. 2016. P. 157–173.
12. Weir M. et al. Password Cracking Using Probabilistic Context-Free Grammars. 2009 IEEE Symposium on Security and Privacy. 2009. P. 391–405.