УДК 519.2

КОМБИНАТОРНЫЙ АНАЛИЗ НАДЕЖНОСТИ ПАРОЛЕЙ В СОЦИАЛЬНЫХ СЕТЯХ: ОЦЕНКА ЭНТРОПИИ И ВРЕМЕНИ ПЕРЕБОРА

Драгун Д.А., студент гр. ПСб-251, I курс
Научный руководитель: Липина Г.А., старший преподаватель
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

Стремительное развитие цифровых технологий и повсеместное распространение интернета привело к переводу основной массы информации в электронный формат. Это, в свою очередь, выдвигает на первый план проблему защиты персональных данных. На сегодняшний день наиболее распространенным средством аутентификации и разграничения доступа остается парольная защита.

Настоящее исследование посвящено анализу стойкости паролей с позиций дискретной математики. В работе применяются комбинаторные методы для оценки мощности пространства паролей, рассчитывается энтропия пароля согласно формуле Шеннона, а также производится оценка временных затрат, необходимых для его подбора методом полного перебора. Полученные результаты позволяют выработать математически обоснованные практические рекомендации по созданию надежных парольных комбинаций.

Актуальность темы обусловлена тем, что с ростом числа онлайн-сервисов пользователи вынуждены регистрироваться на множестве платформ, что порождает проблему выбора запоминающихся паролей. Стремясь к удобству, многие останавливаются на простых сочетаниях — личных датах, именах или общеупотребительных словах, что существенно снижает защищенность учетных записей. Основная цель данной работы заключается в применении аппарата комбинаторики и теории информации для количественной оценки надежности пароля в зависимости от двух ключевых параметров: его длины и мощности используемого алфавита символов.

Криптостойкость любого пароля в первую очередь определяется мощностью множества возможных комбинаций N, которые теоретически должен перебрать злоумышленник для гарантированного доступа (при условии, что не применяются словарные атаки). Данный показатель находится в прямой зависимости от двух величин: объема используемого алфавита A, то есть множества допустимых символов, и длины парольной последовательности L.

В соответствии с комбинаторным правилом умножения, общее число различных паролей (представляющих собой размещения с повторениями) рассчитывается по формуле:

$$N=A^L$$

Рассмотрим различные типы алфавитов:

1. Цифровой алфавит (*ПИН-код*): $A = 10$ (цифры от 0 до 9).
2. Алфавит нижнего регистра: $A = 26$ (латинские буквы a-z).
3. Алфавит нижнего и верхнего регистра: $A = 52$.
4. Расширенный алфавит (регистры + цифры): $A = 62$.
5. Полный алфавит (с учетом спецсимволов): $A \approx 95$ (стандартный набор символов *ASCII*).

Проведем расчеты для паролей разной длины (Таблица 1).

Таблица 1 – Количество возможных комбинаций в зависимости от алфавита и длины

Длина (L)	Цифры (10)	Нижний регистр (26)	Регистры + цифры (62)	Полный алфавит (95)
4	10^4	456 976	$14{,}8\cdot10^6$	$81{,}5\cdot10^6$
6	10^6	$308\cdot10^6$	$5{,}68\cdot10^{10}$	$7{,}35\cdot10^{11}$
8	10^8	$2{,}09\cdot10^{11}$	$2{,}18\cdot10^{14}$	$6{,}63\cdot10^{15}$
10	10^{10}	$1{,}41\cdot10^{14}$	$8{,}39\cdot10^{17}$	$5{,}99\cdot10^{19}$

Представленные в таблице результаты наглядно демонстрируют, что возрастание длины пароля и расширение используемого набора символов ведут к экспоненциальному росту числа возможных комбинаций. Это создает главный барьер для злоумышленника.

Оценка мощности пространства паролей является необходимой, но недостаточной мерой, поскольку она не отражает вероятностную природу выбора символов пользователем. Для более глубокого анализа применяется понятие информационной энтропии, введенное Клодом Шенноном. В предположении о равновероятном и независимом выборе символов энтропия H на один знак составляет log_2A бит. Тогда для пароля длины L полная энтропия вычисляется как:

$$H = L \cdot \log_2 A$$

Данная величина характеризует неопределенность пароля для злоумышленника: чем выше энтропия, тем больше информационная «емкость» пароля и тем сложнее его угадать. В практике информационной безопасности приняты следующие пороговые значения: при энтропии ниже 30 бит пароль считается крайне ненадежным; значение свыше 50 бит обеспечивает приемлемый уровень защиты для большинства прикладных задач.

Таблица 2 – Энтропия паролей (в битах)

Длина (L)	Только цифры $log_2(10) = 3.32$	Нижний регистр $log_2(26) = 4.70$	Полный алфавит $log_2(95) = 6.57$
6	19.9	28.2	39.4
8	26.6	37.6	52.6
10	33.2	47.0	65.7

Время для подбора пароля вычислим по формуле:

$$T = \frac{N}{V}$$

где N - число комбинаций, V - скорость перебора (число попыток в секунду).

Современные средства атаки очень быстро развиваются, поэтому требуется оперативно реагировать.

Есть два основных сценария:

- первый сценарий А - онлайн-атака;
- второй сценарий Б - офлайн-атака.

Проведем необходимые вычисления для пароля длиной восемь символов.

$$A = 95, N \approx 6,63 \cdot 10^{15}.$$

$$T_{сценарий\ А} = (6,63 \cdot 10^{15}) / 10^3 = 6,63 \cdot 10^{12} сек. \approx 210 тыс.лет)$$

$$T_{сценарий\ Б} = (6,63 \cdot 10^{15} / 10^9 = 6,63 \cdot 10^6 сек. \approx 77 дней)$$

По результатам расчетов можно сказать следующее: даже самый надежный пароль (с большим количеством комбинаций) в случае офлайн-атаки на высокопроизводительном оборудовании, может быть взломан за относительно небольшой промежуток времени. Поэтому необходимо выбирать не только сложный пароль, но необходимо обеспечить безопасное место его хранения.

В результате проделанной работы можно сделать следующие выводы по созданию надежного пароля:

- минимальная длина пароля не менее 10 –12 символов;
- использовать все доступные категории символов;
- активировать двухфакторную аутентификацию.

Список литературы:

1. Шеннон К. Работы по теории информации и кибернетике. Москва.: Изд-во иностр. лит., 1963. 832 с.

2. Виленкин, Н.Я. Комбинаторика / Н.Я. Виленкин. — Москва: Наука, 1969. — 328 с.