УДК 004.056.53

ОЦЕНКА ПАРОЛЕЙ НА УРОВЕНЬ СЛОЖНОСТИ С ПОМОЩЬЮ БИБЛИОТЕК PASSWORDMETER И ZXCVBN

Рудер Давыд Давыдович, Кашлева Анастасия Евгеньевна

Алтайский государственный университет, г. Барнаул
e-mail: ddruder@gmail.com

EVALUATION OF PASSWORDS FOR THE LEVEL OF COMPLEXITY USING THE PASSWORDMETER AND ZXCVBN LIBRARIES

Ruder Davyd D., Kashleva Anastasia E.

Altai State University, Barnaul

Аннотация. В работе проводится сравнительный анализ оценки уровней сложности и надежности паролей с использованием библиотек passwordmeter и zxcvbn в среде программирования PyCharm Community Edition 2022.2.3. Для анализа были подготовлены 15 паролей разной длины, разделенных на 3 группы по уровню сложности. Библиотеки passwordmeter и zxcvbn позволяют оценить по шкале сложность паролей и выводят значение информационной энтропии по формуле Шеннона. В работе показано, что увеличение длины паролей несущественно влияет на повышение уровня сложности паролей. Результатом работы является подтверждение тезиса о том, что наиболее безопасными являются сгенерированные пароли. Показано, что запоминающиеся пароли, составленные из зашифрованных слов и комбинации цифр, являются достаточно надежными.

Ключевые слова: аутентификация по паролю, информационная энтропия, надежный пароль, оценка сложности пароля.

Abstract. The work provides a comparative analysis of assessing the levels of complexity and strength of passwords using the passwordmeter and zxcvbn libraries in the PyCharm Community Edition 2022.2.3 programming environment. For analysis, 15 passwords of different lengths were prepared, divided into 3 groups according to difficulty level. The passwordmeter and zxcvbn libraries allow you to evaluate the complexity of passwords on a scale and display the value of information entropy using the Shannon formula. The work shows that increasing the length of passwords does not significantly affect the increase in the level of password complexity. The result of the work is confirmation of the thesis that generated passwords are the most secure. Memorable passwords made from encrypted words and a combination of numbers have been shown to be quite strong.

Keywords: password authentication, information entropy, strong password, assessment of password complexity.

Для цитирования: Рудер Д.Д., Кашлева А.Е. Оценка паролей на уровень сложности с помощью библиотек passwordmeter и zxcvbn // Проблемы правовой и технической защиты информации. 2023. №11. С. 46-51.

For citation: Ruder D.D., Kashleva A.E. Evaluation of passwords for the level of complexity using the passwordmeter and zxcvbn libraries // Legal and Technical Problems Information Protection. 2023. No. 11. P. 46-51.

С развитием технологий и переходом общества в информационную эпоху возникли новые проблемы, такие как несанкционированный доступ к аккаунтам в

сети Интернет и утечка конфиденциальных данных. В исследовании предпринята попытка сравнения автоматизированных оценок уровня сложности паролей разной длины, полученные путем вычислений информационной энтропии с помощью языка программирования Python и библиотек passwordmeter и zxcvbn. Актуальность исследования заключается в том, что пользователи сети Интернет часто подвергаются кибер-атакам из-за халатного отношения к аутентификации на различных интернет-ресурсах и в социальных сетях. Необходимо практически показать, как требования к надежному паролю влияют на его уровень защиты.

Достижение цели осуществлялось путем изучения требований к созданию надежного пароля, способов создания пароля и атак, разработки программы на языке программирования Python, реализации генератора паролей и алгоритма оценки уровня сложности паролей и информационной энтропии путем сравнения результатов библиотек passwordmeter и zxcvbn.

Способов реализации алгоритма для получения правильной парольной комбинации существует несколько: от метода «грубой силы», в котором последовательно перебираются всевозможные пароли, до метода с использованием графических ускорителей, что производит вычисления с использованием технологии NVIDIA для параллельного вычисления [1]. Разнообразие способов атаки приводит к выводу о том, что необходимо тщательно подходить к вопросу создания пароля. Каждый пароль должен обладать хорошим уровнем защищенности, а потому регулярная оценка надёжности паролей крайне необходима и является важным направлением в сфере исследований, посвященных вопросам информационной безопасности. Известно, что надёжность создаваемого пароля зависит от таких факторов как: длина, сложность, непредсказуемость и наличия различных комбинаций сочетаний прописных и заглавных букв, цифр и букв, специальных символов и др. [2]

По вышеперечисленным признакам можно дать количественную оценку стойкости любого пароля и понять, как много времени злоумышленник потратит на его взлом. Критерии оценки могут различаться в зависимости от области применения, однако существуют минимальные требования к мощности, которые должны соблюдаться всегда: наличие цифр, символов в верхнем и нижнем регистрах, специальные символы и длина пароля не менее 6 символов [3]. Но про такую последовательность нельзя сказать, что она обладает высоким уровнем защиты. Для хранения паролей можно использовать специализированные инструменты, которые генерируют пароли в соответствии с заданными параметрами. Для облегчения задачи можно обратиться к сервисам, которые помогают управлять паролями, либо вводить замаскированные пароли во избежание их перехвата [4].

Для автоматизации оценки сложностей паролей разной длины необходимо подключить библиотеки zxcvbn-python и passwordmeter. Zxcvbn-python – это библиотека, которая реализует алгоритм оценки сложности паролей, разработанный компанией Dropbox. Производится оценка качество пароля по шкале от 0 до 4, где 0 –очень слабый пароль, а 4 –очень сильный пароль. Библиотека также предоставляет дополнительную информацию о пароле, такую как его энтропия, количество возможных комбинаций символов и т.д. Passwordmeter – библиотека, которая предоставляет функцию для оценки сложности пароля. Данная библиотека анализирует пароль на наличие различных типов символов, повторение символов, использует ли пароль распространенные слова и т.д. Результат оценки представляется в виде числа от 0 до 100, где 0 –очень слабый пароль, а 100 –очень сильный пароль. Библиотека дает рекомендации по улучшению парольной комбинации.

В конце анализа библиотеками выводится значение энтропии. Концепция статистической энтропии была предложена Шенноном в качестве основного понятия в теории информации, которое характеризует среднее количество отсутствующей информации в случайном событии. В контексте энтропии эта концепция устанавливает ограничения в теоремах о кодировании и сжатии данных [5 Тюрин]. Значение энтропии находится по следующей формуле Шеннона:

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

где H – количество информации; N – количество возможных событий (общее количество символов, которые могут быть использованы); p_i – вероятность отдельных событий. По данной формуле рассчитана энтропия с учетом количества вхождений одного и того же символа. На рисунках 1-2 представлен результат загрузки библиотек в PyCharm Community Edition 2022.2.3.

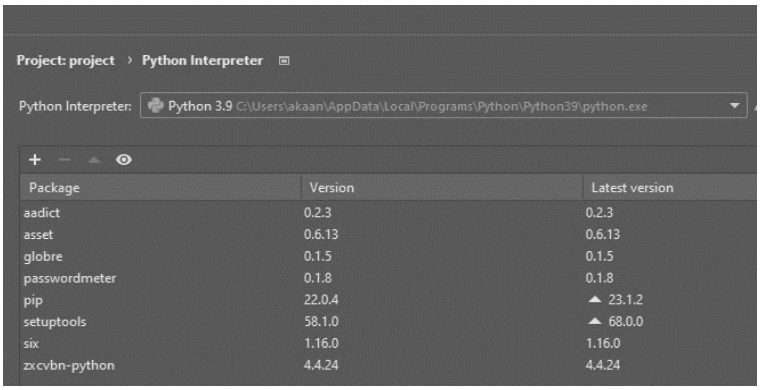

Рисунок 1. Наличие библиотек zxcvbn-python и passwordmeter

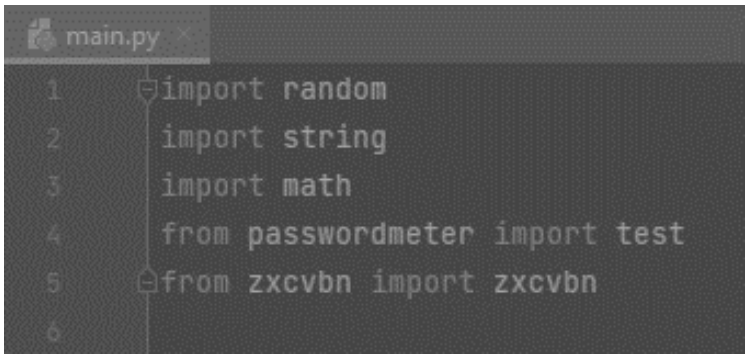

Рисунок 2. Подключение библиотек zxcvbn-python и passwordmeter

В ходе исследования при оценке были использованы три группы паролей. В каждой группе по 5 паролей различной длины (L = 8, 12, 16, 20, 24) для учета влияния длины паролей на уровень сложности и показатель энтропии.

1 группа easyPass – простые пароли, под которыми понимаются простые комбинации, которые достаточно легко подобрать;

2 группа randPass – рандомизированная (пароль составляется при помощи генератора пароля с учетом использования цифр, прописных и строчных букв, специальных символов.);

3 группа goodPass – сложные пароли, созданные с упором на основные требования с учетом человеческого фактора (запоминающиеся пароли).

Для исследование был разработан генератор паролей. Ниже реализован код для группы randPass. Данный генератор учитывает символы ASCII, особые знаки и цифры. При использовании необходимо лишь указать длину генерируемой последовательности, к которой он будет применен. На рисунке 3 представлен код

для высчитывания информационной энтропии паролей с учетом количества символов в парольной комбинации, с расчетом вероятности повторения каждого символа.

Пароли для группы easyPass легко расшифровать, а комбинации из цифр не самые сложные (таблица 1). Некоторые комбинации состоят из часто используемых слов. Обе библиотеки все пароли оценивают как «слабые». В данном случае увеличение количества символов в пароле мало помогает. Энтропия, начиная с 16 символьного пароля, имеет большой показатель, однако для такой длины пароля это слишком маленькое значение. Исходя из нее, можно сделать вывод, что времени на взлом понадобится чуть больше, однако несанкционированный доступ все равно будет получен достаточно быстро.

```
def passEntropy(pas):
        """Возвращает информационнцю энтропию пароля"""
        # Количество символов в пароле
        L = len(pas)
        # Словарь для подсчета количества вхождений каждого символа в пароле
        char_count = {}
        # Заполнение словаря
        for char in pas:
            if char in char_count:
                char_count[char] += 1
            else:
                char_count[char] = 1
        # Рассчет вероятности каждого символа
        probabilities = [count / L for count in char_count.values()]
        # Рассчет информационной энтропии
        entropy = -sum([p * math.log2(p) for p in probabilities])
        return entropy * L
```

Рисунок 3. Расчет значения энтропии с учетом частоты вхождения символов

Таблица 1. Оценка сложности паролей группы easyPass

Пароль	L	Passwordmeter, баллов	Zxcvbn, баллов	Энтропия, бит
qwertyui	8	11	0	24
abcdefj00000	12	25	1	31
helloworld222212	16	25	1	45
11111barnaulcity2022	20	26	2	60
anastasiakashlevaevg2002	24	26	2	81

Результаты для группы randPass приведены в таблице 2. Пароли длиной 16 символов и 20 символов оцениваются обеими программами одинаково, однако значения энтропии разные. Это, очевидно, связано с большим количеством повтором символов в пароле длиной 20 символов, потому passwordmeter считает эти пароли равноценными. Однако энтропия все же выше, потому как злоумышленнику может потребоваться более чем 10^{20} попыток. Данное значение энтропии означает еще и то, что время взлома пароля длиной в 20 символов превышает время для взлома пароля длиной 16 символов (более чем 10^{16} попыток).

Результаты для группы goodPass приведены в таблице 3. Данная группа паролей отличается от группы сгенерированных тем, что эти парольные комбинации легче запоминаются человеком. Энтропия группы goodPass ниже, чем у группы randPass. Здесь VKz@m0G1 – VK (название социальной сети) + зашифрованное слово «password» с удалением символов S и D из слова; 84sk37b4LL_! – это зашифрованное слово «баскетбол; Vjt_WzUtfYUTk8y@ – пароль

«меня зовут не ангелина», написанный на английской раскладке с некоторыми замененными символами; iN3ht_@S4dwichiW7tEr – пароль «NightsSandwichWinter», в котором были переставлены первые и вторые символы слов, а также заменены некоторые буквы на специальные символы и цифры. Ah@W3@SERR3!nMUcQmPut3R – здесь зашифрованный следующий пароль «IHaveASecretInMyComputer».

Таблица 2. Оценка сложности паролей группы randPass

Пароль	L	Passwordmeter, баллов	Zxcvbn, баллов	Энтропия, бит
;`o_jK5_	8	89	2	22
TAI"#2Amt%L	12	93	4	41
Ns1NVFQ?JM;hGwR;	16	92	4	60
uGL*K15vvJV_J-F/'qx5	20	92	4	80
p.hfxEb`8e9agIVk;jNliwf<	24	94	4	108

Таблица 3. Оценка сложности паролей группы goodPass

Пароль	L	Passwordmeter, баллов	Zxcvbn, баллов	Энтропия, бит
VKp@sV0r	8	90	2	22
84sk37b4LL_!	12	92	4	39
Vjt_WzUtfYUTk8y@	16	92	4	60
iN3ht_@S4dwichiW7tEr	20	93	4	77
Ah@W3@SERR3!nMUcQmPut3R	24	94	4	96

Очевидно, что пароль, состоящий из случайной расстановки никак не связанных друг с другом символов, будет надежнее. Однако действительно важно учитывать тот факт, что человеку сложно запоминать последовательности, которые он не может ни с чем ассоциировать. Тем более, последовательности, состоящие из 20 и более символов. Библиотека zxcvbn вновь оценивает парольную комбинацию из 8 символов как ненадежную. Итогом можно считать то, что из всех групп наиболее надежной является группа randPass – сгенерированные пароли. На первое место эту группу выдвигает уровень среднего значения энтропии, который является наиболее высоким в сравнении с другими значениями. Высокий показатель энтропии свидетельствует о большом количестве необходимых попыток перебора пароля прежде, чем получится его отгадать. Однако, если учитывать человеческий фактор, а именно то, что нашему мозгу сложно ассоциировать с чем-либо комбинацию из случайных символов, более надежной считается группа goodPass с меньшим значением энтропии. Связано это с тем, что группа goodPass представляет пароли различной длины, которые состоят из последовательности зашифрованных слов, которые более привычны, а энтропия меньше из-за частых повторов символов в пароле, что, несомненно, уменьшает ее значение, т.к. энтропия высчитывалась с учетом частоты вхождения символов. Также библиотека passwordmeter дала данной группе оценку больше, нежели группе randPass, из-за использования зашифрованных предложений и фраз, т.е. сохраняющих свой вид, но затрудняющих анализ. Группа easyPass – это группа с легко взламываемыми паролями. Присутствуют часто используемые пароли, пароли с чередованием одной-двух цифр, а также слова, которые никак не зашифрованы и легко читаются. Данные пароли библиотеки

passwordmeter и zxcvbn оценивают как крайне опасные за счет того, что для взлома таких паролей необходимо не так много попыток. Энтропия данной группы низка по той же причине.

Таким образом, выяснено, что пароли трех разных групп оцениваются библиотеками passwordmeter и zxcvbn по-разному. Показано, что увеличение длины паролей не существенно влияет на повышение уровня сложности паролей. Подтверждено, что наиболее безопасными являются сгенерированные пароли. Показано, что запоминающиеся пароли, составленные из зашифрованных слов и комбинации цифр, являются достаточно надежными.

Библиографический список

1. *Снегуров А.В., Чакрян В.Х. Анализ устойчивости к взлому современных механизмов парольной защиты операционных систем // Прикладные информационные технологии, Харьков, 2011 г. – Харьков, 2011. – С. 27–29.*
2. *Назаров Д.М., Калашников В.Г. Методика проверки надежности пароля с использованием облачных сервисов // Умная цифровая экономика, Екатеринбург, 2022 г. – Екатеринбург, 2022 г. – С. 6–11.*
3. *Салита Д.С., Удовик А.А. Методы оценки надежности парольных систем // Проблемы правовой и технической защиты информации, Барнаул, 2020 г. – Барнаул, 2020 г. – С. 47–51.*
4. *Абидарова А.А. Анализ надежности паролей для обеспечения информационной безопасности // Известия ТулГУ, Технические науки, Тула, 2021 г. – Тула, 2021 г. – С. 66–68.*
5. *Тюрин К.А., Семин Р.В. Анализ стойкости парольных фраз на основе информационной энтропии // Известия ЮФУ. Технические науки, Ростов-на-Дону, 2015 г. – Ростов-на-Дону, 2015 г. – С. 18–27.*