Дементьев Виталий Евгеньевич, д.т.н., профессор каф. измерительных и инфокоммуникационных технологий, vedementiev@yandex.ru

УДК 004.056

МОДЕЛИРОВАНИЕ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ ПРОВЕРКИ СТОЙКОСТИ ПАРОЛЕЙ

А.Г. Иванов, В.П. Лось
Российский государственный гуманитарный университет, г. Москва

Ключевые слова: пароль, стойкость пароля, рекомендательная система, словарная атака, атака по маске, атака с правилами.

Парольная аутентификация остаётся одним из наиболее распространённых механизмов защиты учётных записей. В большинстве информационных систем стойкость пароля по-прежнему оценивается по формальным признакам: минимальной длине, наличию букв разных регистров, цифр и специальных символов. Такой подход прост в реализации, однако ориентирован главным образом на противодействие полному перебору и недостаточно учитывает методы восстановления паролей, применяемые на практике. Целью настоящей работы является моделирование рекомендательной системы проверки стойкости паролей, оценивающей их устойчивость к современным сценариям подбора

Недостаток традиционных парольных политик состоит в том, что они нередко стимулируют создание предсказуемых конструкций. Пользователь, стремясь выполнить формальные требования, преобразует простое слово в шаблонный пароль вида «P@ssw0rd2026!@#». Несмотря на внешнюю сложность, такие пароли остаются уязвимыми для словарных атак, атак с правилами, атак по маске и комбинаторных атак. Аналогично слабы клавиатурные последовательности, повторяющиеся блоки, даты, имена и иные общеупотребительные основы. Следовательно, выполнение требований по составу символов ещё не означает наличие действительной стойкости пароля [1].

Современные средства восстановления паролей используют не только полный перебор, но и эвристики, основанные на типичном поведении пользователей. Наиболее распространены словари популярных слов и фраз, правила замены символов, шаблоны клавиатурного набора, комбинации коротких слов и маски вида «слово+число» или «имя+год». Поэтому система оценки должна учитывать не только формальную сложность, но и возможности подбора пароля с позиции атакующего.

Предлагаемая архитектура включает несколько модулей. На вход системы поступает пароль, а на выходе – формируется итоговая оценка стойкости и набор рекомендаций. Первый модуль выполняет предварительный разбор строки: определяет длину, состав символов,

наличие повторов и характер их чередования. Второй модуль осуществляет словарный анализ, выявляя полные и частичные совпадения с распространёнными словами, именами и типовыми основами. Например, пароли «password», «admin123» и «Qwerty2026» должны получать низкую оценку не из-за недостатка длины, а из-за высокой предсказуемости.

Третий модуль проверяет устойчивость к атакам с правилами. В нём анализируются типовые преобразования: замены «a→@», «o→0», «s→$», капитализация первого символа, добавление знаков в конец строки, присоединение года рождения или текущего года. Поэтому конструкция «P@ssw0rd!» не должна рассматриваться как качественно новый пароль по отношению к слову «password». Четвёртый модуль выявляет клавиатурные шаблоны, включая последовательности «qwerty», «123qwe», «!QAZ2wsx». Пятый модуль ориентирован на противодействие атакам по маске и комбинаторным атакам; он выявляет структуры вида «слово+число», «имя+год», «два коротких слова», а также повторяющиеся блоки [2].

Результаты работы модулей поступают в блок агрегации, где формируется риск-профиль пароля. В отличие от бинарной схемы «соответствует/не соответствует», система выдаёт многофакторную оценку и поясняет причины уязвимости. Если обнаружена словарная основа, пользователю предлагается отказаться от её модификации; при выявлении клавиатурного шаблона – разорвать последовательность; при наличии масочной структуры – исключить предсказуемые суффиксы. Такой подход позволяет не только отклонять слабые варианты, но и формировать для пользователя понятную обратную связь.

В соответствии с предложенной архитектурой был разработан программный код, реализующий словарный, основанный на правилах, клавиатурный и структурный анализ пароля с последующим формированием итоговой оценки и рекомендаций [3]. Фрагмент разработанного решения представлен на рисунке 1.

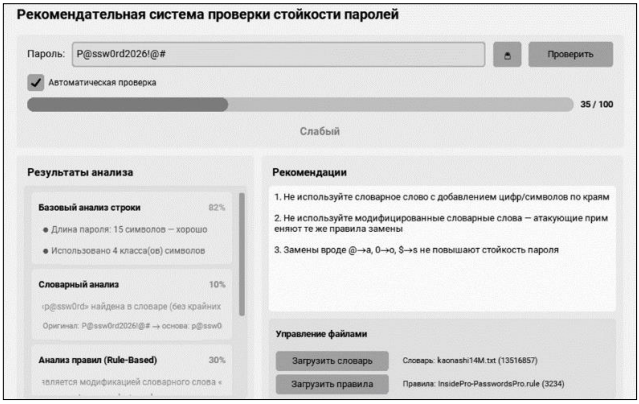

Рисунок 1 – Разработанное приложение

Таким образом, предложенная модель позволяет перейти от формальной проверки сложности к оценке практической стойкости пароля. Её применение повышает качество выявления слабых паролей и делает обратную связь более содержательной. Перспективы развития связаны с расширением словарной базы, адаптацией правил и настройкой весов критериев на основе экспериментальных данных.

Список использованных источников

1. Салита Д.С., Удовик А.А. Методы оценки надежности парольных систем // Проблемы правовой и технической защиты информации, 2020, № 8, С. 47-51.

2. Сидоркина И.Г., Михалищев С.В. Совершенствование метода оценки стойкости пароля аутентификации пользователя компьютерных систем на основе использования известных уязвимостей // Программные продукты и системы, 2024, № 4, С. 547-553.

3. Рекомендательная система проверки стойкости паролей [Электронный ресурс]. GitHub, 2026. URL: https://github.com/raOvOen/RPS-GUI/ (дата обращения: 10.03.2026).

Иванов Александр Григорьевич, аспирант РГГУ, alexandr.link.ivanov@gmail.com.
Лось Владимир Павлович, д.в.н., профессор, РГГУ, los-vladimir@yandex.ru

УДК 004.056:004.89

ВЛИЯНИЕ ТОПОЛОГИИ СЕТИ НА РАСПРОСТРАНЕНИЕ ДЕЗИНФОРМАЦИИ СРЕДИ LLM-АГЕНТОВ

В.П. Лось, А.К. Шувалов
Российский государственный гуманитарный университет, г. Москва

Дезинформация является одной из главной угроз современного общества. Проблемы и вызовы нового вектора атаки активно обсуждаются на международной арене. Вызвано это тем, что широкое распространение получили социальные сети, которые являются одним из главных средств распространения подобного контента. Также упростилось и создание материалов, так как теперь для этого используются LLM, качество генерации текста которых увеличиваются и становится почти не отличимо от написанного человеком [1]. Для анализа и защиты от подобных угроз активно используются LLM-агенты, которые способны воспринимать текст на естественном языке, рассуждать и принимать решения о передачи информации другим участникам сети [2, 3]. В работе рассматривается влияние выбора топологии сети на характер распространения дезинформации в системах с LLM-агентами.

К классическим моделям распространения информации можно отнести:

- SIR;
- Каскадная модель;
- Модели динамики мнений.