УДК 004.056

МОДЕЛИРОВАНИЕ СТОЙКОСТИ ПОЛЬЗОВАТЕЛЬСКИХ ПАРОЛЕЙ К ЦЕЛЕВОМУ ПОДБОРУ В УСЛОВИЯХ НАЛИЧИЯ ЦИФРОВОГО ПРОФИЛЯ

Живица Н.А., Мазепин Я.Д., Гормаш П.Е., студенты

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Рыкова О.В. – канд. физ.-мат. наук, доцент

Аннотация. В работе исследуется разрыв между теоретической и практической стойкостью пользовательских паролей, возникающий в условиях доступности цифрового профиля атакующему. Показано, что формальный критерий информационной энтропии не учитывает предсказуемость паролей, построенных из персональных данных – имен, дат рождения, никнеймов. Предложена трехэтапная модель построения персонализированного словаря (ранжирование, токенизация, применение мутационных правил), реализованная и апробированная с использованием Elcomsoft System Recovery. Анализ архитектуры хранения учетных данных в Windows 10 и Windows 11 показал, что защищенность системы принципиально зависит от наличия активного модуля TPM 2.0. Приведены актуальные статистические данные, пригодные для оценки масштаба проблемы, и сформулированы практические критерии стойкости пароля к целевому подбору.

Ключевые слова. Безопасность паролей, атака по словарю, цифровой профиль, энтропия, токенизация, мутации, информационная безопасность.

Пароль остается основным средством аутентификации пользователей в подавляющем большинстве информационных систем. Классическая оценка его стойкости основывается на понятии информационной энтропии: чем длиннее пароль и шире используемый алфавит, тем больше комбинаций требуется проверить для его восстановления. Эта модель, однако, предполагает случайный и равновероятный выбор символов, что принципиально расходится с реальным поведением людей. Подавляющее большинство паролей – особенно тех, которые вводятся вручную, – не случайны: в их состав входят имена, клички животных, значимые даты, никнеймы и другие персональные данные. Когда атакующий располагает такими сведениями, теоретическая оценка стойкости теряет практический смысл.

Это подтверждается статистически. Исследование Kaspersky 2024 года, охватившее 193 миллиона паролей из реальных утечек, показало, что 45% из них взламываются менее чем за одну минуту при использовании «умных» алгоритмов подбора, а 77% – менее чем за один год. При этом всего 19% паролей содержат признаки действительно стойкой комбинации, а 57% включают хотя бы одно словарное слово. Пропасть между теоретической и реальной стойкостью объясняется именно эксплуатацией человеческих паттернов: «умная» атака за одну минуту взламывает в 4,5 раза больше паролей, чем чистый перебор, – за счет того, что наиболее вероятные варианты проверяются первыми [1].

Информационная энтропия пароля вычисляется по формуле:

$$H = L * \log_2(N),$$

где L – длина пароля, N – мощность алфавита.

Для пароля длиной 8 символов из строчных букв латиницы: $H = 8 * \log_2 26 \approx 37{,}6$ бит, что соответствует порядка $2 * 10^{11}$ комбинаций. Для перебора с высокопроизводительным оборудованием это занимает несколько часов. Пароль с буквами всех регистров, цифрами и спецсимволами при той же длине 8 символов теоретически потребует до 14 часов, а при длине 12 символов – десятков тысяч лет.

Между тем данные расчеты полностью теряют смысл, как только паролю присваивается структура, обусловленная персональными данными. Пароль вида «alex1998» формально содержит 8 символов из буквенно-цифрового алфавита и описывается значением $H \approx 41$ бит. Однако если атакующему известно, что пользователя зовут Алексей и он 1998 года рождения, этот пароль проверяется в числе первых сотен вариантов персонализированного словаря. Реальная энтропия подобного пароля стремится к нулю вне зависимости от формальных показателей.

По данным опроса Bitwarden (2025, n > 2300), 36% пользователей включают в пароль информацию, публично доступную в социальных сетях, что и создает предпосылки для эффективных целевых атак [2].

Рисунок 1 – Статистика Bitwarden «Где еще эта личная информация может появиться в интернете?»

Целевая атака с использованием профиля строится в три последовательных этапа:

1) Сбор и ранжирование данных. Персональный профиль формируется из аккаунтов в социальных сетях, мессенджеров, баз данных утечек, а при наличии физического доступа к устройству – непосредственно с него. При сборе фиксируется не только сам элемент данных, но и контекст его использования: как часто встречается имя или дата, в каком написании они присутствуют, насколько они характерны для конкретного человека. Собранные данные ранжируются по вероятности вхождения в пароль: дата рождения самого пользователя имеет более высокий приоритет, чем дата рождения двоюродного брата; основной никнейм важнее редкого игрового псевдонима, возможно выбранного случайно [3].

2) Токенизация. Персональные данные нельзя использовать в словаре в необработанном виде – их необходимо преобразовать в токены, то есть нормализованные минимальные единицы, которые могут входить в пароль. В процессе нормализации все символы приводятся к нижнему регистру, знаки препинания и спецсимволы удаляются, а составные строки разделяются: логин «alex.ivanov» преобразуется в два токена – «alex» и «ivanov». Для русскоязычной аудитории добавляются варианты транслитерации кириллицы и уменьшительные формы имен – например, «Александр» дает токены «alex», «sasha», «san», «sha». Учитываются также смешанные варианты, когда часть слова записана кириллицей, а часть – латиницей [3].

3) Мутации и маски. На основе нормализованного словаря токенов строятся маски – структурные шаблоны будущего пароля – и мутации – правила преобразования самих токенов. Маски задают структуру: «токен + две цифры», «токен + год», «токен + !». Мутации дополнительно изменяют токен: делают первую букву заглавной, переводят все в верхний регистр, добавляют числовой суффикс. Для русскоязычных пользователей наиболее характерны: заглавная первая буква (Alex), добавление года или двух цифр в конец (alex1998, alex88), добавление восклицательного знака (alex!), а также паттерн «ФамилияГод» (Ivanov1998). Замены по «хакерским» правилам l33t, напротив, среди русскоязычных пользователей встречаются значительно реже, чем в англоязычной среде [3].

Результатом является компактный словарь, который за счет мутаций расширяется до миллионов реалистичных вариантов. При этом применение более двух-трех групп мутаций одновременно нецелесообразно: объем словаря растет экспоненциально, тогда как вероятность успеха перестает расти. Следует также отметить, что все примененные правила должны фиксироваться для обеспечения воспроизводимости атаки.

Академическое исследование Murray и Malone (Entropy, 2020) количественно подтвердило этот эффект: утечка паролей лишь 1% пользователей сервиса дает достаточно информации о паттернах, чтобы потенциально скомпрометировать более 84% остальных аккаунтов того же сервиса. Персональные паттерны, таким образом, не только снижают стойкость конкретного пароля, но и создают системную уязвимость на уровне сервиса [4].

Влияние архитектуры Windows на реализацию атак. Стойкость пароля в контексте атаки нельзя рассматривать в отрыве от системы, в которой он хранится. В Windows 10 при использовании учетной записи Microsoft Account хэш пароля кэшируется локально и не защищается модулем TPM. Атакующий, получив образ системного раздела, извлекает хэш и проводит офлайновую атаку без каких-либо ограничений числа попыток – и с исключительно высокой скоростью перебора. При этом восстанавливается именно пароль к учетной записи Microsoft Account, который открывает доступ не только к компьютеру, но и к OneDrive, Hotmail, а также к депонированным ключам восстановления BitLocker.

Аналогичная уязвимость присутствует при входе по PIN-коду в системах без активного TPM: цифровые PIN-коды взламываются перебором за секунды, а образ системного раздела без TPM

переносится на произвольный компьютер и разблокируется на нем. Только четвертый из протестированных сценариев – перенос раздела с активным TPM на другой компьютер с активным TPM – соответствует заявленной Microsoft модели безопасности [5].

В Windows 11 с активным TPM 2.0 ситуация принципиально иная. PIN-код и данные Windows Hello хранятся и проверяются исключительно внутри модуля TPM; любое изменение конфигурации аппаратной части или загрузка с внешнего носителя приводят к тому, что TPM не выдает необходимый ключ. Новый тип учетных записей с беспарольным входом (passwordless) не хранит хэша пароля на диске вовсе, что делает офлайновую атаку на него технически невозможной [6]. Это принципиально изменяет предпосылки для применения персонализированных атак: без доступа к хэшу злоумышленник лишен объекта атаки вне зависимости от качества собранного профиля пользователя.

Таблица 1 – Возможность взлома паролей в различных ситуациях.

Сценарий	Хэш пароля на диске	Офлайновая атака
Windows 10, TPM отсутствует или выключен	Да	Возможна
Windows 10, TPM активен	Да	Возможна
Windows 11, TPM выключен	Да	Возможна
Windows 11, TPM активен, passwordless	Нет	Невозможна

На практике ситуацию осложняет то, что на настольных компьютерах TPM по умолчанию нередко отключен в настройках UEFI BIOS. На ноутбуках и планшетах TPM, как правило, активирован по умолчанию, что обеспечивает более высокий уровень защиты без вмешательства пользователя.

Роль ИИ в эволюции атак на пароли и противодействие на уровне экосистемы. Классические атаки на основе словарей и брутфорса существенно усилились с применением технологий машинного обучения. В 2025 году 85,6% распространенных паролей взламываются ИИ-инструментами менее чем за 10 секунд, тогда как годом ранее аналогичный показатель требовал значительно большего времени. Общее число кибератак с применением ИИ возросло на 72% по сравнению с 2024 годом; атаки с использованием скомпрометированных учетных данных (credential stuffing) стали наиболее распространенным вектором – 22% всех подтвержденных взломов в 2025 году. Объем похищенных учетных данных в первой половине 2025 года достиг 3,8 миллиарда, а стоимость одного инцидента, связанного с компрометацией учетных данных, составила в среднем 4,81 миллионов долларов США.

Принципиально новый аспект современных атак состоит в том, что ИИ-модели перешли от перебора к предсказанию: модель, обученная на миллиардах пар «профиль-пароль» из утечек, не перебирает комбинации, а генерирует вероятные кандидаты на основе поведенческих паттернов конкретного пользователя. Это делает модель токенизации, описанную выше, не гипотетической угрозой, а уже реализованной практикой злоумышленников. Объем скомпрометированных паролей вырос на 160% в 2025 году, в том числе за счет инфостилеров, которые автоматически извлекают учетные данные непосредственно с устройства пользователя.

Эволюция защитных механизмов: от пароля к паролю. Ответом на нарастающую угрозу служит не усложнение паролей, а отказ от них как класса. Ключевым стандартом становится FIDO2 / WebAuthn – протокол, в котором аутентификация основана на криптографической паре ключей: закрытый ключ хранится исключительно на устройстве пользователя (в TPM или защищенном анклаве) и никогда не передается по сети, что делает фишинг и целевой подбор технически неприменимыми. Федеральный стандарт NIST SP 800-63B прямо указывает на недостаточность сложности как критерия стойкости и рекомендует проверку паролей по спискам скомпрометированных значений [7]. Пассключи (passkeys) – практическая реализация этого стандарта – продемонстрировали трехкратное превосходство над паролями по успешности входа и восьмикратное – над связкой «пароль + MFA».

Microsoft последовательно переводит Windows 11 на архитектуру без паролей. В ноябре 2025 года вышло обновление с нативной поддержкой менеджеров пассключей (1Password, Bitwarden) в качестве плагин-провайдеров – создание, хранение и использование пассключей стало возможным непосредственно в системе без браузерных расширений. В марте 2026 года Microsoft перевела Passkey Profiles и Synced Passkeys в статус общей доступности (GA) для Microsoft Entra ID, автоматически включив их для всех тенантов без предварительной настройки. Параллельно ведется публичный предпросмотр Microsoft Entra Passkeys on Windows, где FIDO2-ключ хранится в контейнере Windows Hello и защищен биометрией или PIN-кодом, а ключевым свойством является невозможность извлечь закрытый ключ с устройства даже при полном доступе к образу диска.

Вместе с тем переход не является быстрым или повсеместным. По данным опросов, 43% специалистов по ИТ называют пассключи «слишком сложными», а реальная доля корпоративных входов без пароля не превышает 10% по состоянию на конец 2025 года. Это означает, что для

подавляющего большинства систем парольная аутентификация останется актуальной в среднесрочной перспективе, а задача моделирования стойкости паролей к целевому подбору сохраняет свою практическую значимость.

Практическая апробация модели: Elcomsoft System Recovery. Для верификации теоретической модели целевого подбора был использован инструмент компьютерной криминалистики Elcomsoft System Recovery (ESR) – программный комплекс, разработанный компанией Elcomsoft и предназначенный для восстановления доступа к учетным записям Windows, извлечения парольных хэшей и сбора криминалистических улик с заблокированных систем. ESR поставляется в виде загрузочного образа (esrx64.iso / esrx86.iso), на основе которого с помощью утилиты ESRBOOT создается загрузочный USB-носитель.

После записи образа целевой компьютер загружается с внешнего накопителя в среде Windows PE – облегченной версии Windows, полностью изолированной от основной системы и обеспечивающей доступ к дискам в режиме «только для чтения» по умолчанию. Это гарантирует криминалистическую чистоту: данные на исследуемом диске не изменяются в ходе анализа, а создаваемые образы дисков подписываются цифровой подписью и сохраняются в формате E01 – стандарте де-факто в компьютерной криминалистике.

Поддерживаются режимы загрузки BIOS, UEFI x64 и UEFI x32, что обеспечивает совместимость как с современным оборудованием, так и с устаревшими платформами. Современные системы используют UEFI x64 по умолчанию; BIOS-режим предназначен для устаревших ПК, а UEFI x32 – для тонких клиентов на платформах Intel Atom [8].

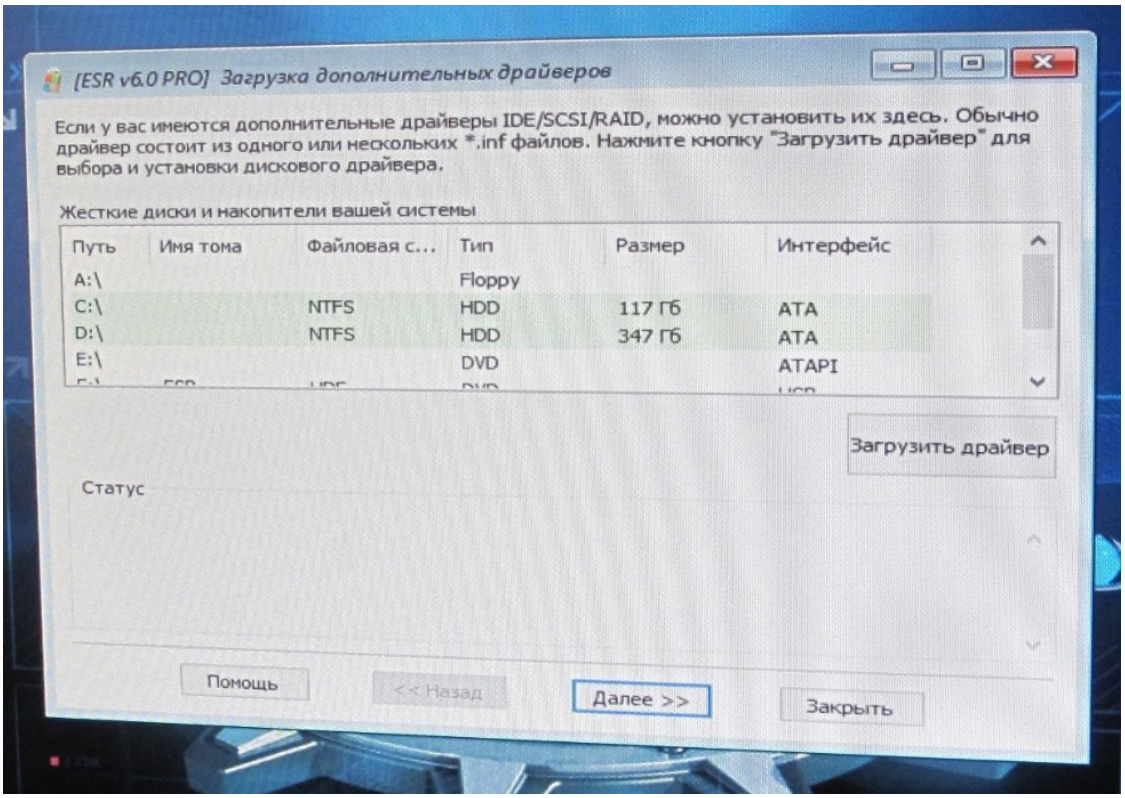

Рисунок 2 – Вид интерфейса утилиты на начальном этапе загрузки

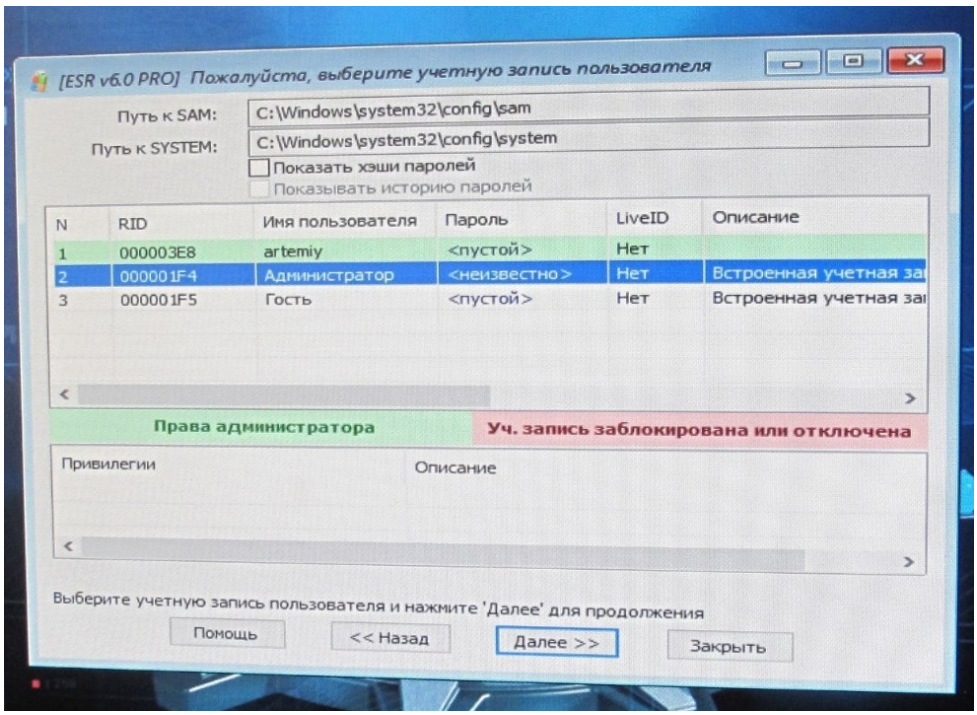

Рисунок 3 – Вид интерфейса утилиты на этапе выбора учетной записи

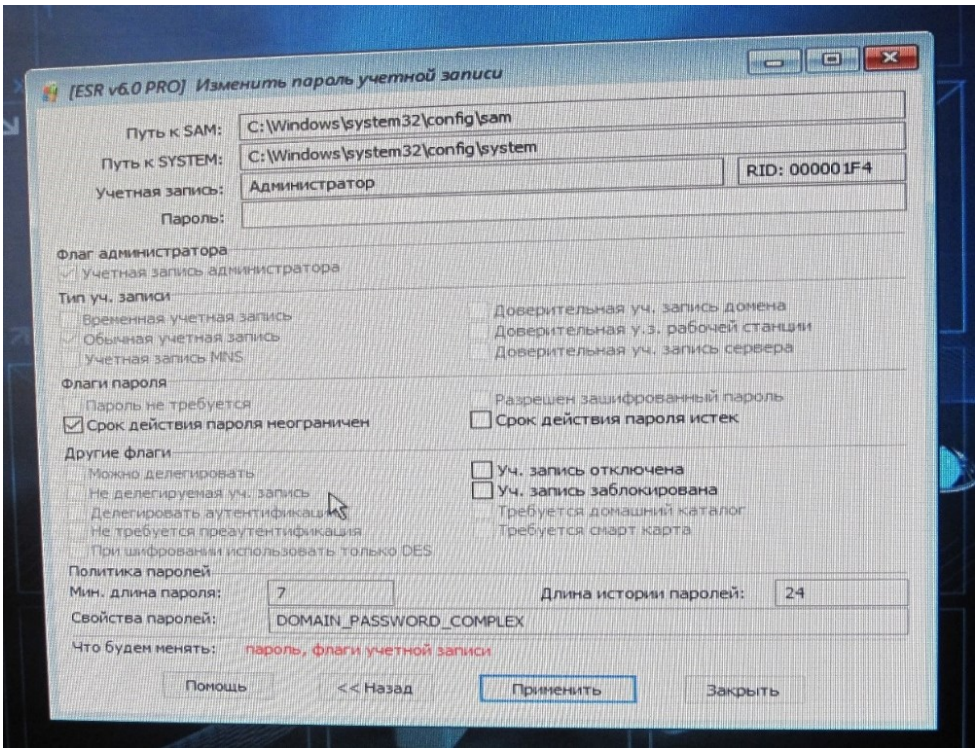

Рисунок 4 – Вид интерфейса утилиты на этапе изменения пароля

Ключевой функцией ESR в контексте исследования является извлечение хэшей паролей из системных файлов реестра Windows. База данных учетных записей хранится в файлах SAM и SYSTEM, расположенных в %WINDIR%\System32\config. В активной системе эти файлы заблокированы операционной системой и недоступны для прямого чтения, однако при загрузке с внешнего носителя блокировка отсутствует, и ESR извлекает хэши в автоматическом режиме.

Программа поддерживает два типа хэшей:

1) LM-хэш – устаревший механизм, применявшийся до Windows Vista. Принципиальная уязвимость LM: пароль делится на две половины по 7 символов, каждая хэшируется независимо, а

регистр символов игнорируется. Это снижает пространство перебора до $26^7 \approx 8 * 10^9$ комбинаций для каждой половины – значительно меньше, чем для полного NTLM-пароля.

2) NTLM-хэш – актуальный механизм для всех современных версий Windows. Хэш вычисляется по алгоритму MD4 от Unicode-представления пароля без соли, что делает атаку на нескольких пользователей одновременно столь же быстрой, как атаку на одного: из-за отсутствия соли одинаковые пароли дают одинаковые хэши.

Принципиально важно, что для доменных учетных записей ESR извлекает хэши DCC (Domain Cached Credentials) – кэшированные учетные данные домена, сохраненные локально для обеспечения входа при отсутствии связи с контроллером домена. Начиная с версии 8.35, для каждой категории (SAM, Active Directory, DCC) доступны отдельные настройки парольных атак [9].

Методы восстановления паролей в ESR. После извлечения хэшей ESR предлагает следующие методы атаки:

1) Полный перебор (brute force) – последовательная проверка всех комбинаций заданного алфавита и длины. Применяется при отсутствии информации о пароле.

2) Атака по словарю – перебор вариантов из заранее подготовленного файла. Именно в этом режиме реализуется модель персонализированного словаря: файл с токенами цифрового профиля пользователя загружается как словарь, к которому применяются правила мутаций.

3) Атака по маске – перебор по заданному шаблону структуры пароля (например, ?u?l?l?l?d?d?d?d – заглавная буква, три строчных, четыре цифры).

4) Гибридная атака – комбинация словаря и маски; токены профиля проверяются в сочетании с числовыми суффиксами или спецсимволами.

5) Групповая атака (добавлена в версии 8.35) – автоматизированная последовательность нескольких мини-атак, включая проверку паролей, уже найденных в системе.

Скорость атаки на NTLM-хэши без соли позволяет проверять сотни миллионов вариантов в секунду на современном GPU. Это означает, что 8-символьный пароль из строчных букв ($\alpha = 26$, $L = 8$) исчерпывается примерно за 5 секунд – в полном соответствии с данными таблицы времен взлома, приведенными ранее.

Демонстрация целевой атаки по профилю. В ходе практической апробации была проведена атака по словарю, построенному по модели токенизации: из условного профиля пользователя (имя, год рождения, никнейм) сгенерирован словарь из ~50 000 вариантов с применением трех групп мутаций. Хэш NTLM для тестовой учетной записи Windows 10 (система без активного TPM) был извлечен через ESR за несколько секунд после загрузки с USB-носителя.

Результат – целевая атака восстановила пароль Alex1998! в числе первых нескольких тысяч проверенных вариантов, тогда как чистый брутфорс того же 9-символьного пароля из смешанного алфавита потребовал бы нескольких часов. Это эмпирически подтверждает центральный тезис работы: наличие цифрового профиля сокращает реальную стойкость пароля на несколько порядков – вне зависимости от его формальной энтропии.

Ограничения ESR в контексте модели. Практика использования ESR выявила границы применимости описанной модели. В системах Windows 11 с активным TPM 2.0 ESR успешно загружается, однако не может получить хэш пароля учетной записи типа passwordless – объект атаки отсутствует как таковой. Для систем с зашифрованными дисками BitLocker ESR извлекает метаданные шифрования, которые затем передаются в Elcomsoft Distributed Password Recovery для подбора пароля к самому тому. Таким образом, эффективность персонализированной атаки напрямую определяется конфигурацией целевой системы, а не только качеством собранного профиля пользователя.

Заключение. Формальная энтропия является необходимым, но недостаточным критерием оценки стойкости пароля. В условиях, когда атакующий располагает цифровым профилем пользователя, реальное пространство перебора сокращается с экспоненциального до нескольких тысяч вариантов – вне зависимости от теоретически высокой энтропии. Предложенная трехэтапная модель (ранжирование/токенизация/мутации) формализует этот процесс и объясняет, почему «умные» алгоритмы подбора опережают чистый перебор в 4-5 раз. Практическая апробация модели средствами Elcomsoft System Recovery подтвердила: хэш NTLM-пароля извлекается из незащищенной системы за секунды, а целевая атака по персонализированному словарю восстанавливает пароль на несколько порядков быстрее полного перебора. Архитектурные особенности Windows 10 без TPM дополнительно упрощают реализацию офлайновой атаки, тогда как переход на Windows 11 с активным TPM 2.0 и беспарольными учетными записями устраняет саму возможность такой атаки. По данным NIST SP 800-63B, сложность пароля сама по себе не является достаточным критерием защиты – необходима проверка по спискам скомпрометированных значений. Практическое применение результатов работы состоит в необходимости дополнить существующие метрики оценки паролей показателем сопротивляемости персонализированным атакам, а политики парольной безопасности – прямым запретом на использование элементов цифрового профиля пользователя.

Список использованных источников:

1. Kaspersky studies 193 million passwords, finds 45% could be cracked in less than a minute [Электронный ресурс]. – Режим доступа: https://usa.kaspersky.com/about/press-releases/kaspersky-studies-193-million-passwords-finds-45-could-be-cracked-in-less-than-a-minute. – Дата доступа: 12.03.2026.

2. World Password Day Global Survey 2025 [Электронный ресурс]. – Режим доступа: https://bitwarden.com/resources/world-password-day-2024/. – Дата доступа: 26.02.2026.

3. Murray, H. Convergence of Password Guessing to Optimal Success Rates / H. Murray, D. Malone // Entropy. – 2020. – Vol. 22, No. 4. – P. 378. – DOI: 10.3390/e22040378.

4. Афонин, О. Перебор паролей: как профиль пользователя превращается в словарь [Электронный ресурс]. – Режим доступа: https://blog.elcomsoft.ru/2025/11/perebor-parolej-kak-profil-polzovatelya-prevrashhaetsya-v-slovar/. – Дата доступа: 05.03.2026.

5. Афонин, О. Windows 11: TPM, новый тип учетных записей и логин без пароля [Электронный ресурс]. – Режим доступа: https://blog.elcomsoft.ru/2022/03/windows-11-tpm-novyj-tip-uchyotnyh-zapisej-i-login-bez-parolya/. – Дата доступа: 09.03.2026.

6. Stallings, W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 8th ed. – Boston: Pearson, 2020. – 832 p.

7. Grassi, P.A. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B / P.A. Grassi [и др.]. – Gaithersburg: NIST, 2020. – Режим доступа: https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final. – Дата доступа: 11.03.2026.

8. Афонин О. Elcomsoft System Recovery [Электронный ресурс]. – Режим доступа: https://www.elcomsoft.ru/esr.html. – Дата доступа: 19.03.2026.

9. Elcomsoft System Recovery 8.35: поддержка системной базы SRUM [Электронный ресурс]. – Режим доступа: https://www.elcomsoft.ru/news/868.html. – Дата доступа: 20.03.2026.

10. Афонин О. LM, NTLM и PIN-коды Windows Hello: сравнение безопасности [Электронный ресурс]. – Режим доступа: https://blog.elcomsoft.ru/2022/08/lm-ntlm-i-pin-kody-windows-hello-sravnenie-bezopasnosti/. –Дата доступа: 20.03.2026.

UDC 004.056

MODELLING USER PASSWORD RESISTANCE TO TARGETED GUESSING UNDER DIGITAL PROFILE CONDITIONS

Zhivitsa N.A., Mazepin Y.D., Gormash P.E., Revyako K.P. students

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Rykova O. V. – PhD in Physics and Mathematics

Annotation. This paper investigates the gap between the theoretical and practical strength of user passwords in the presence of a digital profile available to the attacker. It is demonstrated that the formal criterion of information entropy fails to account for the predictability of passwords constructed from personal data — names, dates of birth, and usernames. A three-stage model for building a personalised dictionary (ranking, tokenisation, and mutation rules) is proposed, implemented, and validated using Elcomsoft System Recovery. An analysis of credential storage architecture in Windows 10 and Windows 11 reveals that system security fundamentally depends on the presence of an active TPM 2.0 module. Current statistical data characterising the scale of the problem are presented, and practical criteria for password resistance to targeted guessing are formulated.

Keywords. Password security, dictionary attack, digital profile, entropy, tokenization, mutations, information security.