

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ГЕНЕРАЦИИ МНЕМОНИЧЕСКИХ ПАРОЛЕЙ В КРУПНЫХ ИНТЕРНЕТ-СЕРВИСАХ

Д.В. Кизимова¹, М.А. Миронов¹

¹*Поволжский государственный университет телекоммуникаций
и информатики, г. Самара
e-mail: audzava.koska2017@yandex.ru*

Аннотация

Проведен сравнительный анализ генераторов паролей Kaspersky, ESET, «Рандомус» и Яндекс ID на соответствие стандарту NIST SP 800-63B-4. Оценены длина, алфавит, энтропия, уникальность символов и время брутфорса. Выявлено, что пароли Яндекс ID имеют жесткую предсказуемую структуру и наименьшую стойкость. Предложены рекомендации по повышению безопасности генерируемых паролей.

Ключевые слова: генерация паролей, аутентификация, NIST SP 800-63B-4, энтропия, уникальность символов, брутфорс, менеджеры паролей, информационная безопасность.

Введение

Актуальность исследования. В эпоху цифровизации защита учётных данных остаётся ключевой проблемой информационной безопасности. По данным Verizon DBIR (2020) [1], 89 % взломов связаны с компрометацией учётных данных. Современные вычислительные мощности позволяют перебирать до 100 миллиардов паролей в секунду, делая короткие пароли уязвимыми [2]. При этом, по данным Nord Security (2023), пароль «123456» использовали более 4,5 миллиона пользователей, а за 2021–2023 гг. он встречался в утечках более 112 миллионов раз [1].

В ответ крупные сервисы внедряют генераторы паролей, но их подходы различаются: от коротких «запутанных» комбинаций до длинных mnemonic фраз.

Объект исследования – методы генерации паролей в крупных интернет-сервисах (Kaspersky Password Manager, ESET Password Manager, «Рандомус», генератор паролей Яндекс ID).

Предмет исследования – количественные и качественные характеристики генерируемых паролей и их соответствие современным стандартам аутентификации.

Цель работы – провести сравнительный анализ генераторов паролей по параметрам безопасности и удобства использования, оценить их соответствие рекомендациям NIST SP 800-63B-4.

1. Нормативная база исследования

Наиболее авторитетным источником в области аутентификации пользователей являются рекомендации Национального института стандартов и технологий США (NIST). Последняя редакция документа SP 800-63B-4 (август 2025 года) кардинально пересматривает подход к управлению паролями [3].

Кроме международных стандартов, в российской практике важную роль играют требования ФСТЭК России. Приказ №21 от 18.02.2013 устанавливает базовые требования к паролям для защиты персональных данных: длина не менее 8 символов, алфавит не менее 70 символов, ограничение на количество попыток ввода (не более 4) [4]. Эти требования также были учтены при проведении сравнительного анализа.

2. Методология исследования

Сравнительный анализ проведён для 4 генераторов паролей на российском рынке: Kaspersky Password Manager, ESET Password Manager, «Рандомус», Яндекс ID. Для каждого сгенерировано по 10 паролей (табл. 2).

3. Результаты исследования

Таблица 1 – Сгенерированные пароли (выборка по 10 паролей для каждого сервиса)

№	Kaspersky	Eset	Рандомус	Яндекс
1	_IZdEbP4UJLKez-	\$Q-f4u,xmVgZBoB	JAT%6P-T\$j9Hk_	3YZ-Kya-UaB-jag
2	&T6j6XVu#A*vcc+	*@wqH,(Cb)_c1cn	D+_iYpo(Fqp4b23	tmu-TG2-7SS-mU9
3	7*9(0R3nhRlo+x=	8lrGX@L65\;7)*2	WE)^_8_+X#2uGqK	M9A-5u6-XFm-AG6
4	t_!diG90ErF^&1v	tC\tjuBT<~6,3NY	ga1^HG_P5uNdzHr	UzR-xux-DLP-Ey9
5	GU6#Ql96\$9uQ10^	QmjmA%0rM!l6?Oj	L!^RML-0xNV5Q~&	fM4-vHC-JgE-GQs
6	\$X200bfl!zTAW-A	*@S!AcV6Q!b6mg>	uH_ie9I&8era^p~	VyU-a4R-CgD-Xvr
7	C@jBYfa0mGQ2X6f	z8W4lQb5R7\A<8m	rM5l#EHg4_o)nf6	dF6-EQG-CSP-LGr
8	lO*G2FcR6au)qvX	kaV+\$RV+H!7{(pJ	CVoDj8AZK)5ux\$_	suC-WQ7-fxU-wjz
9	Dle-e\$Rmt3oO+2-	sqT.G6#H:_%ue7w	PZw0~^~VHTsCZ5O	u4B-2rx-thn-irp
10	J+Jx9&C(h2@mBeb	eDc7Q{pp:V**?6o	uM_7AV4qR3RO\$a9	LjP-N56-6fV-XHH

4. Анализ характеристик паролей

Таблица 2 – Сравнительный анализ параметров генерации паролей

Параметр	Kaspersky	ESET	Рандомус	Яндекс
Длина (символы)	4–1000+	4–64	5–30	15
Разрешены пробелы	Нет	Нет	Да	Нет
Доп. символы (число типов)	15	25	12	1
Средняя энтропия (бит)	3,74	3,74	3,8	3,44
Время brutфорса (при 1 млрд/сек), млрд лет	628	3926	346	30
Мнемоническая структура	Нет	Нет	Нет	Формат xxx-xxx-xxx-xxx

5. Уникальность символов

Таблица 3 – Анализ уникальности символов

Критерий	Kaspersky	Eset	Рандомус	Яндекс
Средняя уникальность	0,92	0,92	0,94	0,79
Минимальная уникальность	0,8	0,87	0,93	0,73
Доля паролей с уникальностью = 1,0	0,3	0,2	0,2	0

Заключение

В результате проведенного сравнительного анализа методов генерации паролей в крупных интернет-сервисах были сделаны следующие выводы:

1) ни один из исследованных сервисов не реализует в полной мере рекомендации NIST SP 800-63B-4. Наиболее критичными недостатками являются отсутствие поддержки мнемонических фраз и Unicode-символов;

2) ESET и Kaspersky демонстрируют наиболее высокие показатели энтропии и времени брутфорса, а также предоставляют пользователю широкий диапазон длин паролей;

3) проблемная зона – генератор Яндекс ID. Фиксированная длина (15 символов), жесткая предсказуемая структура (xxx-xxx-xxx-xxx) и ограниченный алфавит снижают общую стойкость генерируемых паролей по сравнению с конкурентами. При этом уникальность символов в паролях Яндекса также оказалась наименьшей среди всех исследованных сервисов.

Список использованных источников

1. Сидоркина, И.Г. Совершенствование метода оценки стойкости пароля аутентификации пользователя компьютерных систем с использованием программного комплекса / И.Г. Сидоркина, С.В. Михалищев // Программные продукты и системы. – 2024. – № 4. – С. 2–4.

2. Fast Company. The end of complex passwords: NIST's new guidelines explained. – 2025. – URL: <https://www.fastcompany.com> (дата обращения: 28.03.2026).

3. National Institute of Standards and Technology. NIST Special Publication 800-63B-4: Digital Identity Guidelines – Authentication and Lifecycle Management. – Gaithersburg, MD : NIST, 2025. – 9 с.

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями).

5. Verizon. 2020 Data Breach Investigations Report. – Verizon Enterprise Solutions, 2020. – URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата обращения: 28.03.2026).

COMPARATIVE ANALYSIS OF MNEMONIC PASSWORD GENERATION METHODS IN MAJOR INTERNET SERVICES

D.V. Kizimova¹, M.A. Mironov¹

*¹Povolzhsky State University of Telecommunications and Informatics, Samara
e-mail: audzava.koska2017@yandex.ru*

Abstract

A comparative analysis of password generators from Kaspersky, ESET, Randomus, and Yandex ID was conducted for compliance with the NIST SP 800-63B-4 standard. The study evaluated password length, character set, entropy, character uniqueness, and brute-force time. It was revealed that Yandex ID passwords have a rigid predictable structure and the lowest resistance to attacks. Recommendations are proposed to improve the security of generated passwords.

Keywords: password generation, authentication, NIST SP 800-63B-4, entropy, character uniqueness, brute-force, password managers, information security.