Тонковид Ирина Дмитриевна
студент, кафедра защищенных систем связи
Санкт-Петербургский государственный университет
РФ, г. Санкт-Петербург
E-mail: irtonkovid@yandex.ru

БУДУЩЕЕ БЕЗ ПАРОЛЕЙ: РЕВОЛЮЦИЯ В БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Данная статья исследует актуальную проблему информационной безопасности в контексте перехода к биометрическим методам аутентификации. Рассматривая преимущества биометрической идентификации перед традиционными паролями, статья обсуждает технологические инновации и перспективы развития этого подхода. Подчеркивается важность соблюдения приватности при использовании биометрических данных и необходимость баланса между безопасностью и комфортом для обеспечения устойчивого цифрового будущего.

This article explores the current issue of information security in the context of the transition to biometric authentication methods. By examining the advantages of biometric identification over traditional passwords, the article discusses technological innovations and the future of this approach. It emphasizes the importance of maintaining privacy when using biometric data and the need for a balance between security and convenience to ensure a sustainable digital future.

Ключевые слова: будущее; пароли; биометрия; инновации; безопасность; технологии.

Keywords: future; passwords; biometrics; innovation; security; technology.

Введение

С увеличением числа цифровых угроз и постоянным стремлением к улучшению безопасности данных, технологии биометрической идентификации приходят на смену устаревшим методам, таким как использование паролей. В мире, где личная безопасность и конфиденциальность информации играют ключевую роль, биометрические технологии представляют собой революцию в способах аутентификации. Давайте исследуем, какие возможности открывает перед нами переход к будущему без паролей и как эта технология изменит нашу повседневную жизнь.

Преимущества биометрической идентификации

В мире, где цифровое пространство становится все более важным и уязвимым, вопросы безопасности идентификации занимают центральное место. Традиционные методы аутентификации, основанные на паролях, все чаще подвергаются критике из-за их

уязвимости и недостатков. В этой связи биометрическая идентификация представляет собой революционный подход, который обладает рядом явных преимуществ [1].

Таблица 1.

Сравнительная таблица обычной и биометрической идентификации

Критерий	Биометрическая идентификация	Обычная идентификация (пароль/код)
Принцип работы	Использует уникальные физические или поведенческие характеристики (отпечаток пальца, лицо, радужка глаза)	Использует знания пользователя (пароль, PIN-код)
Уровень безопасности	Высокий, сложно подделать или украсть	Средний, подвержен взлому, перехвату, подбору пароля
Риск утери	Отсутствует, характеристика всегда с пользователем	Высокий — можно забыть или потерять пароль
Возможность передачи	Практически невозможна	Пароль можно передать или украсть
Проблемы с конфиденциальностью	Вопросы хранения и защиты биометрических данных	Требует защиты паролей, но данные легко заменить

Биометрическая идентификация обеспечивает более высокий уровень безопасности благодаря использованию уникальных физических характеристик, что значительно усложняет её подделку и передачу третьим лицам. В то же время традиционные методы, такие как пароли и PIN-коды, проще с технической точки зрения и не требуют специализированного оборудования, однако они менее надежны из-за риска подбора, кражи или забвения. Для пользователя биометрия более удобна, поскольку исключает необходимость запоминать и вводить пароли, но требует наличия соответствующих сенсоров и надёжной защиты биометрических данных. Важным аспектом остаются вопросы конфиденциальности и безопасного хранения биометрической информации, которые требуют строгого контроля, тогда как пароли при необходимости можно легко изменить. Оптимальным решением часто становится комбинирование биометрических и традиционных методов, что позволяет повысить и безопасность, и удобство использования.

Технологический прогресс и будущие перспективы

Современный технологический прогресс стремительно меняет процесс биометрической идентификации, открывая новые горизонты в обеспечении безопасности и удобства пользователей. Развитие искусственного интеллекта и машинного обучения позволяет создавать модели, способные с высокой точностью распознавать даже мельчайшие биометрические особенности — от отпечатков пальцев и радужной оболочки глаза до анализа походки и микровыражения лица [4]. Улучшение сенсорных технологий делает устройства более компактными, быстрыми и надежными, что способствует широкому распространению биометрии в мобильных гаджетах, банковских системах и умных домах. В будущем ключевым трендом станет мультифакторная биометрия, сочетающая несколько идентификационных признаков для повышения безопасности и снижения вероятности ошибок. Кроме того, развивается технология защиты биометрических данных с помощью блокчейна и использования децентрализованных систем, что минимизирует риски утечек и несанкционированного доступа. В перспективе можно ожидать переход к полностью беспарольной аутентификации, где биометрия станет универсальным стандартом, обеспечивая мгновенную и надежную идентификацию в цифровом мире. Таким образом, технологический прогресс не только ускоряет внедрение биометрии, но и формирует основу для более безопасного, простого и персонализированного будущего без паролей.

Заключение

Будущее без паролей — это новый подход к цифровой безопасности и удобству. Биометрическая идентификация обеспечивает надежную защиту данных и снижает риски мошенничества. Благодаря достижениям в ИИ, сенсорах и криптографии беспарольные системы становятся массовыми и адаптируются под каждого пользователя. Несмотря на вопросы конфиденциальности, отрасль развивается в сторону безопасных и удобных решений. Биометрия открывает новую эру цифровой идентификации, где безопасность и простота идут рука об руку, а пароли уступают место инновациям.

Список литературы

1. Кушнир, Д. В. Исследование возможных методов аутентификации согласования данных в классическом канале в протоколах квантовой криптографии / Д. В. Кушнир, С. Н. Шемякин // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – № 4. – С. 63-67. – URL: https://www.elibrary.ru/item.asp?edn=qhhwyg&ysclid=mcnu63chbu360581602 (дата обращения 01.07.25)

2. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270. – URL: https://www.elibrary.ru/item.asp?edn=gtihbt&ysclid=mcnu6r73co950921319 (дата обращения 01.07.25)
3. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220. – URL: https://www.elibrary.ru/item.asp?edn=tfjjha&ysclid=mcnu7qrh8p818982259 (дата обращения 03.07.25)
4. Будько М. Ю., Миняев А. А. Метод оценки эффективности системы защиты персональных данных //Информатизация и связь. – 2016. – №. 2. – С. 85-87. – URL: https://www.elibrary.ru/item.asp?id=25922237&ysclid=mcnu8assxn814085874 (дата обращения 02.07.25)
5. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 111-114. – URL: https://www.elibrary.ru/item.asp?id=35231535&ysclid=mcnu94mmxs451492451 (дата обращения 03.07.25)
6. Биометрия-Wikipedia, 2025. – URL: https://ru.wikipedia.org/wiki/Биометрия (дата обращения 01.07.25)