ORES

Научно-практический электронный журнал
**Оригинальные исследования (ОРИС)**, *ISSN 2222-0402*
www.ores.su
original-research.ru

**УДК 004.056**

# БЕЗОПАСНОСТЬ И НАДЁЖНОСТЬ АУТЕНТИФИКАЦИИ НА ОСНОВЕ РУКОПИСНОЙ ПОДПИСИ

**Дзямко-Гамулец Роман Николаевич**
Магистр
Московский технический университет связи и информатики
Факультет информационных технологий, кафедра информационной безопасности
roman.dzyamko-gamulets@outlook.com

**Аннотация**

В современной эпохе цифровизации процессов безопасность и надёжность методов аутентификации приобретают особую актуальность. Традиционный метод аутентификации личности на основе рукописной подписи, несмотря на свою длительную историю, подвергается новым угрозам, обусловленным технологическим прогрессом. Данная работа посвящена комплексному анализу потенциальных рисков, связанных с использованием рукописной подписи в качестве средства авторизации, начиная от традиционных методов подделывания подписей до современных методов цифрового вмешательства. Особое внимание уделено разработке рекомендаций, направленных на минимизацию этих рисков и повышение общей надёжности аутентификации на основе рукописного текста.

**Ключевые слова:** авторизация, рукописная подпись, безопасность, цифровое вмешательство, биометрия.

# SECURITY AND RELIABILITY OF HANDWRITTEN SIGNATURE AUTHENTICATION

**Roman N. Dzyamko-Gamulets**
Master
Moscow Technical University of Communications and Informatics
Faculty of Information Technology, Department of Information Security

ABSTRACT

In the modern era of digitalization of processes, the security and reliability of authentication methods are becoming particularly relevant. The traditional method of identification based on a handwritten signature, despite its long history, is exposed to new threats due to technological progress. This review is devoted to a comprehensive analysis of the potential risks associated with the use of a handwritten signature as a means of authorization, ranging from traditional methods of forgery to modern methods of digital intervention. Particular attention is paid to the

development of recommendations aimed at minimizing these risks and improving the overall reliability of handwritten authentication.

**Keywords:** authorization, handwritten signature, security, digital interference, biometrics.

**Введение**

Рукописная подпись, в качестве инструмента личной идентификации, исследовалась и применялась на протяжении многих столетий. Её уникальный характер, индивидуально формируемый с раннего возраста, стал одним из ключевых и наиболее доступных методов удостоверения личности. Это утверждение подтверждается не только историческим контекстом, но и широким применением в современных правовых и коммерческих системах. Однако, с приходом эры цифровизации и глобализации информационных процессов, традиционные методы аутентификации сталкиваются с рядом серьёзных вызовов. В контексте растущего числа киберугроз и развития технологий подмены цифрового отпечатка пользователей, рукописная подпись может быть подвергнута компрометации и фальсификации, что ставит под сомнение её надёжность как средства идентификации и аутентификации [1].

**Цель исследования**

Цель исследования заключается в анализе безопасности и надёжности аутентификации на основе рукописной подписи, идентификации возможных угроз и разработке методов для повышения её защищённости в цифровой среде.

Потенциальные угрозы аутентификации на основе рукописной подписи

Подделывание рукописной подписи всегда была актуальной проблемой, но с развитием современных технологий, особенно в области обработки изображений и искусственного интеллекта, угрозы данной проблемы значительно усилились. Понимание механизмов и методов, которыми злоумышленники могут создавать поддельные образцы подписи, становятся критически важными в обеспечении аутентичности документов.

Современные алгоритмы глубокого обучения и нейронные сети предоставляют возможность моделировать и создавать изображения с поразительной детализацией. В этом контексте они могут быть применены для создания подписей, которые, хоть и являются искусственными, по своему внешнему виду практически неотличимы от настоящих. Однако, когда дело доходит до рукописной подписи, её уникальность и индивидуальность определяются не только внешним видом. Уникальная структура линий, места переплетений и мелкие прерывания в потоке подписи – всё это создаёт сложный портрет, который крайне сложно воссоздать в точности. Кроме того, динамика написания, включая такие параметры, как скорость, последовательность и давление, также служит дополнительным индикатором аутентичности. В данном контексте необходимо выработать методики исследования, которые могли бы учитывать все эти параметры в комплексе, обеспечивая тем самым глубокий анализ рукописной подписи. Например, использование специализированных датчиков для измерения давления при написании может дать детальное представление о характере письма конкретного пользователя, что в свою очередь может стать дополнительным средством проверки [2].Несмотря на постоянное развитие технологий и методов подделывания, существуют уникальные аспекты рукописной подписи, которые могут служить надёжными индикаторами её подлинности. Но для эффективного противостояния современным методам фальсификации необходимо внедрение глубоких и всеобъемлющих методов анализа. Развитие технологий сканирования и 3D-печати демонстрирует поразительные достижения, которые, однако,

несут в себе и риски. Современные сканеры, обладая возможностью фиксации деталей на микроскопическом уровне, предоставляют злоумышленникам инструментарий для копирования документов с высокой точностью. В этом контексте традиционные методы аутентификации и верификации документов могут стать уязвимыми, и потому требуют пересмотра и инноваций. Реализация уникальных идентификационных маркеров становится критически важной в свете этих технологических прорывов. Голограммы, способные реагировать на свет определенного спектра, предлагают средство идентификации, которое трудно подделать благодаря своим уникальным свойствам рефракции света. Также невидимые чернила, становящиеся видимыми только при освещении ультрафиолетовым светом, могут служить дополнительной мерой безопасности, скрытно маркируя документы. Однако, учитывая быстрый темп развития технологий, возможно, потребуется ещё более продвинутый уровень защиты. Микрочипы, которые могут быть встроены в документ, представляют собой высокотехнологичное решение, способное хранить информацию или даже интерактивно взаимодействовать с считывающими устройствами, предоставляя тем самым слой безопасности, который выходит за рамки простого физического документа. Эти инновационные методы аутентификации и верификации, когда рассматриваются в комплексе, создают надёжную систему обеспечения аутентичности документов в эпоху растущих технологических возможностей [3].

Электронные системы аутентификации, применяющие рукописную подпись в качестве одного из механизмов верификации, находятся под постоянным давлением со стороны различных киберугроз. Эти угрозы представляют собой комбинацию разнообразных тактик и методов, которые злоумышленники используют в попытках вторжений в информационные системы. Простые атаки по отказу в обслуживании могут прервать доступ к сервисам, в то время как более сложные межсетевые вторжения целенаправленно нацелены на получение и эксплуатацию конфиденциальных данных. С ростом популярности облачных технологий многие системы аутентификации выбирают интеграцию с облачными решениями, что, хоть и предоставляет множество преимуществ в плане масштабируемости и доступности, также увеличивает число потенциальных уязвимостей. Облачные платформы, объединяя в себе данные от множества источников, могут стать привлекательной целью для киберпреступников, стремящихся получить доступ к большому объёму информации. В рамках этих угроз и вызовов, криптографические протоколы становятся не просто дополнительным инструментом, но и основополагающим элементом стратегии защиты. Шифрование данных на всех этапах их обработки и передачи гарантирует, что даже в случае несанкционированного доступа к информации, она останется нечитаемой для посторонних [4]. Тем не менее, криптографическая защита должна дополняться рядом других мер безопасности. Регулярное тестирование систем на проникновение помогает идентифицировать и устранять уязвимости перед тем, как они будут эксплуатироваться. Многоуровневые системы аутентификации, такие как комбинация паролей, верификация биометрических данных и одноразовых кодов, усиливают защиту от несанкционированного доступа. Наконец, физическая безопасность серверов, на которых хранятся ценные данные, не должна упускаться из виду, поскольку взлом или физическое повреждение могут привести к катастрофическим последствиям. В таблице №1 представлен систематизированный обзор ключевых угроз, связанных с процессом аутентификации на основе рукописной подписи, в современном цифровом контексте. Для каждой из указанных угроз предложены потенциальные решения и методы минимизации риска, целями которых являются повышение безопасности и усиление доверия к процессу аутентификации.

Таблица 1. Классификация угроз аутентификации на основе

| Угроза | Описание проблемы | Решение |
|---|---|---|
| Фальсификация подписи | Имитация подписи с использованием современных технологических методов, создающих идентичную копию. | Изучение микроуровневых особенностей подписи и её уникальных признаков. |
| Сканирование и репликация | Возможность точного копирования документов с оригинальными подписями с использованием высококачественного сканирования. | Применение специальных методов защиты физической и технической защиты документации |
| Вмешательство в электронные системы | Уязвимость электронных систем аутентификации перед кибератаками. | Применение методов криптографической защиты, регулярное обновление систем безопасности. |

Рекомендации по минимизации рисков

Многофакторная аутентификация в современном контексте информационной безопасности занимает центральное место в стратегиях обеспечения защиты данных. Этот метод аутентификации выходит за рамки традиционных подходов, опираясь на несколько независимых каналов авторизации. При таком подходе не просто комбинируются различные методы аутентификации, но и создаётся система, в которой вероятность одновременного нарушения всех используемых каналов исчисляется крайне малыми величинами [5].

На практике это означает, что даже если один из компонентов системы, такой как рукописная подпись, окажется скомпрометированным, злоумышленник всё равно столкнётся с необходимостью преодоления дополнительных уровней защиты. К примеру, сценарий, при котором злоумышленник одновременно располагает и идеально поддельной рукописной подписью, и доступом к биометрическим данным жертвы, а также способностью генерировать или перехватывать одноразовые коды, является крайне маловероятным.

Следует также учитывать, что внедрение многофакторной аутентификации не просто умножает уровни безопасности, но и стимулирует использование методов, которые максимально дополняют и усиливают друг друга. Таким образом, многофакторная аутентификация представляет собой стратегию, которая позволяет создать глубокую и сложную для проникновения систему авторизации, обеспечивая при этом высокий уровень уверенности в истинном или ложном пользователе. В современной эпохе цифровизации и глобализации интенсивное развитие технологического сектора является неоспоримым фактом. С этим непрерывным прогрессом коррелирует и постоянное изменение спектра угроз, что делает задачу защиты информации особенно актуальной. Таким образом, регулярное обновление технологических решений превращается из рекомендованной процедуры в критически важный элемент обеспечения информационной безопасности [6].

Адаптация к новым реалиям включает в себя не только обновление аппаратных средств, но и программных компонентов. Аппаратные компоненты, такие как датчики и сканеры, подвергаются постоянным модификациям для повышения точности, надёжности и скорости работы. В то же время программные решения также не остаются на месте. Развитие алгоритмов искусственного интеллекта и машинного обучения позволяет более глубоко и точно анализировать и обрабатывать данные, обеспечивая высокий уровень

аутентификации и анализа. Тем не менее, прогресс в этой области не ограничивается лишь усовершенствованием детектирования и обработки информации.

Целостность и конфиденциальность передаваемых и хранимых данных играют решающую роль, и в этом контексте системы шифрования занимают центральное место. Внимательное отношение к выбору и реализации современных криптографических алгоритмов и протоколов обеспечивает защиту от несанкционированного доступа и предотвращает утечки конфиденциальной информации [7].Таким образом, в условиях быстро меняющегося технологического ландшафта и адаптирующихся к этому изменениям угроз, систематическое обновление технологических решений является не только стратегически важным, но и обязательным аспектом обеспечения информационной безопасности.

Но в эпоху цифровой революции технологические системы становятся всё более сложными и многофункциональными. Однако многие из них, вне зависимости от уровня их продвинутости, остаются уязвимыми перед лицом человеческого фактора. Так, даже наиболее современные и надёжные системы безопасности могут быть скомпрометированы из-за ошибок или недостатка знаний со стороны конечного пользователя. Это делает задачу систематического образования и обучения пользователей одной из наиболее приоритетных при эксплуатации средств защиты информации. Базовое понимание принципов безопасности, методов аутентификации и потенциальных угроз является ключевым фактором в обеспечении надёжной работы любой информационной системы. Если пользователь не осведомлён о потенциальных рисках или не знает, как правильно использовать инструменты безопасности, это может привести к серьёзным последствиям, вплоть до утечки конфиденциальных данных или нарушения функционирования системы. Обучение, следовательно, должно быть глубоким и всеобъемлющим. Оно должно охватывать как базовые принципы безопасного поведения в сети, так и более сложные аспекты, связанные с конкретными системами и технологиями. Кроме того, учитывая динамичный характер современного цифрового мира, где постоянно возникают новые угрозы и методы их нейтрализации, обучение не должно ограничиваться единичными сессиями. Оно должно быть непрерывным процессом, в котором пользователи регулярно обновляют свои знания и навыки.

Таким образом, можно утверждать, что в современной цифровой эпохе обучение пользователей становится не просто дополнительным элементом системы безопасности, а её критически важным компонентом. Только всесторонне подготовленный и осведомлённый пользователь может стать надёжным звеном в цепи защиты от цифровых угроз [8].

Усиление надёжности рукописной подписи

Динамический анализ рукописной подписи представляет собой новаторское направление в сфере исследования методов верификации подписи, которое акцентирует внимание не столько на конечном результате написания, сколько на самом процессе его создания. В отличие от статического анализа, который преимущественно фокусируется на геометрических и морфологических характеристиках рукописи, динамический метод детально исследует такие параметры, как временные интервалы, давление на инструмент написания и траекторию движения. Основываясь на предположении о том, что каждый пользователь имеет уникальные особенности написания, динамический анализ стремится выявить те особенности написания, которые проявляются в процессе создания подписи. Например, интервалы времени между отдельными элементами подписи могут отражать индивидуальную скорость и последовательность написания подписи, что становится весьма ценной информацией при анализе и сравнении.

Давление, которое человек оказывает на инструмент при написании, также служит важным маркером. Этот параметр может раскрывать тончайшие детали особенностей написания, изменение давления в определенных моментах написания практически невозможно подделать без глубокого знания динамики написания конкретного пользователя. Траектория движения, в свою очередь, охватывает путь, который проходит инструмент в процессе создания подписи.

Этот аспект анализа включает в себя изучение поворотов, изменений направления и скорости, каждый из которых может служить дополнительным доказательством подлинности или фальсификации подписи. Современные цифровые технологии, такие как специализированные планшеты и сенсорные экраны, предоставляют исследователям мощные инструменты для регистрации и анализа всех этих параметров с высокой степенью точности. Эффективное применение динамического анализа в сочетании с передовыми технологическими решениями может значительно повысить надёжность систем верификации личности на основе рукописной подписи [9].Технология блокчейна и криптографические методы, проникая в различные сферы человеческой деятельности, существенно модифицируют подходы к обеспечению безопасности рукописной подписи, предоставляя передовые инструменты для её надёжной верификации и сохранности данных. Блокчейн, представляя собой децентрализованную систему записей, основанную на принципах неподдельности и транспарентности, предлагает революционный метод хранения информации о рукописной подписи. Эти данные, размещённые в блоках, подтверждаются консенсусом многих узлов в сети, что делает блокчейн устойчивым к попыткам несанкционированного доступа, модификации или подделки. В данном контексте криптографические методы действуют как вспомогательный, но не менее важный инструмент для обеспечения дополнительного уровня защиты. Применение цифровой подписи, в частности, гарантирует целостность информации и удостоверяет её происхождение, гарантируя, что данные остались нетронутыми с момента их исходного создания. В случае любых изменений или попыток искажения информации, криптографические алгоритмы немедленно фиксируют такие девиации, что обеспечивает высокий стандарт безопасности. Совместное использование блокчейна и криптографических методов обеспечивает комплексное решение, которое укрепляет доверие к аутентификации на основе рукописной подписи. Важно подчеркнуть, что эта интеграция не просто адаптирует существующие механизмы к новым реалиям, но и позволяет адаптировать системы верификации таким образом, чтобы они соответствовали современным, постоянно развивающимся стандартам безопасности в цифровую эпоху.

**Заключение**

Рукописная подпись, служившая традиционным средством идентификации и аутентификации пользователя на протяжении многих веков, по-прежнему играет ключевую роль в процессах авторизации в различных сферах деятельности. Однако в контексте бурного развития информационных технологий и роста угроз в области информационной безопасности актуализируется проблема обеспечения надёжности и безопасности этого метода верификации.

Современные условия диктуют необходимость пересмотра и адаптации традиционных методов аутентификации к новым реалиям. Это, в свою очередь, требует глубокого понимания и интеграции новейших технологических решений, направленных на усиление защиты и повышение надёжности рукописной подписи. Применение таких методов, как динамический анализ, криптографическая защита и использование блокчейн-технологий, представляется перспективным в контексте создания комплексных систем аутентификации. Такие системы способны адаптироваться к меняющемуся технологическому ландшафту, обеспечивая, тем самым, долгосрочную эффективность и

защищённость процессов авторизации на основе рукописной подписи [10].Таким образом, для обеспечения надёжности рукописной подписи в качестве средства аутентификации необходимо стремление к гармоничному сочетанию проверенных временем методов и новаторских технологических решений, что позволит адекватно реагировать на современные вызовы и угрозы в области информационной безопасности.

**Список литературы:**


1. Алимсеитова Ж., Боскебеев К.Д. Технологии распознавания образов с использованием биометрии личности // Известия Кыргызского государственного технического университета им. И. Раззакова. 2017. № 1-2 (41). С. 11-17[Электронный ресурс] // Elibrary. 2017. Режим доступа: https://elibrary.ru/download/elibrary_30480854_59590585.pdf
2. Андреевских Д.А., Коломников Р.Е. Локальные и глобальные признаки при аутентификации пользователя по рукописной подписи // Сборник избранных статей научной сессии ТУСУР. 2021. № 1-2. С. 193-196. [Электронный ресурс] // Elibrary. 2021. Режим доступа: https://elibrary.ru/download/elibrary_46714461_40174996.pdf
3. Самотуга А.Е. Распознавание субъектов и их психофизиологических состояний на основе параметров подписи для защиты документооборота // Системная инженерия и информационные технологии. 2023. Т. 5. № 2 (11). С. 56-65.[Электронный ресурс] // Elibrary. 2023. Режим доступа: https://elibrary.ru/download/elibrary_54303806_60816934.pdf
4. Баранов Р.П. Идентификация личной подписи человека // Решетневские чтения. 2011. Т. 2. С. 603-604. [Электронный ресурс] // Elibrary. 2011. Режим доступа: https://elibrary.ru/download/elibrary_24375656_26269051.pdf
5. Волков Д.А. Оценка информативности биометрических признаков, получаемых из рукописной подписи субъекта // Россия молодая: передовые технологии – в промышленность. 2017. № 2. С. 8-13 [Электронный ресурс] // Elibrary. 2017. Режим доступа: https://elibrary.ru/download/elibrary_29073771_26024606.pdf
6. Баянов Б.И. Аутентификация по маскированному изображению на основе биометрических данных рукописного почерка // Математические методы в технологиях и технике. 2023. № 1. С. 93-96. [Электронный ресурс] // Elibrary. 2023. Режим доступа: https://elibrary.ru/download/elibrary_50386143_47674538.pdf
7. Подволоцкий И.Н., Бодров Н.Ф. К вопросу о традиционных и современных способах технической подделки подписей и рукописных записей // Законы России: опыт, анализ, практика. 2011. № 12. С. 84-89. [Электронный ресурс] // Elibrary. 2011. Режим доступа: https://elibrary.ru/download/elibrary_17232242_48149697.pdf
8. Костюченко Е.Ю., Кривоносов Е.О. Комплексный подход к аутентификации пользователей на основе рукописной подписи // В сборнике: Безопасные информационные технологии. Сборник трудов Восьмой всероссийской научно технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 255-258. [Электронный ресурс] // Elibrary. 2017. Режим доступа: https://elibrary.ru/download/elibrary_35532230_88045174.pdf

9. Жиляков Е.Г., Заливин А.Н., Белов С.П., Черноморец Д.А., Васильева Н.В. О прецедентной идентификации фрагментов изображений сканированного рукописного текста // Инфокоммуникационные технологии. 2021. Т. 19. № 3.С.309-316. [Электронный ресурс] // Elibrary. 2021. Режим доступа: https://www.elibrary.ru/download/elibrary_47829361_66178262.pdf
10. Литвиненко Д.И. Разработка способа практической реализации технологии применения электронной подписи в рамках предприятия // В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С. 251-253. [Электронный ресурс] // Elibrary. 2019. Режим доступа: https://www.elibrary.ru/download/elibrary_42483698_44366280.pdf

**References:**

1. Alimseitova Zh., Boskebeev K.D. Image recognition technologies using personality biometrics // Proceedings of the Kyrgyz State Technical University named after I. Razzakov. 2017. №. 1-2 (41). P. 11-17. [Electronic resource] // Elibrary. 2017. Access mode: https://elibrary.ru/download/elibrary_30480854_59590585.pdf
2. Andreevskikh D.A., Kolomnikov R.E. Local and global signs when authenticating a user by handwritten signature // Collection of selected articles of the scientific session of TUSUR. 2021. №. 1-2. P. 193-196. [Electronic resource] // Elibrary. 2021. Access mode: https://elibrary.ru/download/elibrary_46714461_40174996.pdf
3. Samotuga A.E. Recognition of subjects and their psychophysiological states based on signature parameters to protect document flow // System engineering and information technology. 2023. Vol. 5. №. 2 (11). P. 56-65. [Electronic resource] // Elibrary. 2023. Access mode: https://elibrary.ru/download/elibrary_54303806_60816934.pdf
4. Baranov R.P. Identification of a person's personal signature // Reshetnev readings. 2011. Vol. 2. P. 603-604. [Electronic resource] // Elibrary. 2011. Access mode: https://elibrary.ru/download/elibrary_24375656_26269051.pdf
5. Volkov D.A. Assessment of the informativeness of biometric features obtained from the handwritten signature of the subject // Russia is young: advanced technologies are being introduced into industry. 2017. №. 2. P. 8-13 [Electronic resource] // Elibrary. 2017. Access mode: https://elibrary.ru/download/elibrary_29073771_26024606.pdf
6. Bayanov B.I. Masked image authentication based on biometric handwriting data // Mathematical methods in technology and engineering. 2023. №. 1. P. 93-96. [Electronic resource] // Elibrary. 2023. Access mode: https://elibrary.ru/download/elibrary_50386143_47674538.pdf
7. Podvolotsky I.N., Bodrov N.F. On the question of traditional and modern methods of technical forgery of signatures and handwritten records // Laws of Russia: experience, analysis, practice. 2011. №. 12. P. 84-89. [Electronic resource] // Elibrary. 2011. Access mode: https://elibrary.ru/download/elibrary_17232242_48149697.pdf
8. Kostyuchenko E.Yu., Krivonosov E.O. An integrated approach to user authentication based on a handwritten signature // In the collection: Secure information technologies. Proceedings of the Eighth All-Russian Scientific and Technical Conference. NUC "Informatics and control systems". Edited by M.A.Basarab. 2017. P. 255-258. [Electronic

resource] // Elibrary. 2017. Access mode: https://elibrary.ru/download/elibrary_35532230_88045174.pdf

9. Zhilyakov E.G., Zalivin A.N., Belov S.P., Chernomorets D.A., Vasilyeva N.V. On precedent identification of fragments of scanned handwritten text images // Infocommunication technologies. 2021. Vol. 19. №. 3. P. 309-316. [Electronic resource] //Elibrary. 2021. Access mode: https://www.elibrary.ru/download/elibrary_47829361_66178262.pdf
10. Litvinenko D.I. Development of a method for the practical implementation of electronic signature technology within the enterprise // In the collection: Secure information technologies. Proceedings of the Tenth International Scientific and Technical Conference. 2019. P. 251-253. [Electronic resource] // Elibrary. 2019. Access mode: https://www.elibrary.ru/download/elibrary_42483698_44366280.pdf