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

УДК 004.056

СОВМЕСТНОЕ ПРИМЕНЕНИЕ РУКОПИСНОЙ И ЭЛЕКТРОННОЙ ПОДПИСИ ПРИ АВТОРИЗАЦИИ

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

Аннотация

В условиях быстрого темпа глобализации информационных технологий и усиления киберугроз, методы аутентификации и идентификации требуют усовершенствования. Многофакторная аутентификация, объединяющая традиционные и цифровые методы авторизации, предлагает решение для повышения уровня безопасности данных и систем. В частности, совмещение рукописной подписи, давно признанной уникальным и личностным атрибутом индивида, с электронной подписью (ЭП), обеспечивающей гарантии аутентичности и целостности передаваемой информации, представляет собой подход к современной защите данных. Данная статья детально рассматривает принципы и механизмы работы такой комбинированной системы, выделяет её ключевые преимущества в контексте современных киберугроз и обозначает потенциальные ограничения и сложности её реализации.

Ключевые слова: многофакторная аутентификация, рукописная подпись, ЭП, цифровая безопасность, авторизация.

JOINT USE OF HANDWRITTEN AND ELECTRONIC SIGNATURES DURING AUTHORIZATION

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

ABSTRACT

In the context of the rapid pace of globalization of information technologies and increasing cyber threats, authentication and identification methods require improvements. Multi-factor authentication, combining traditional and digital authorization methods, offers a solution to increase level of security of data and systems. In particular, combining a handwritten signature, which has long been recognized as a unique and personal attribute of an individual, with an

electronic digital signature (EDS), which guarantees the authenticity and integrity of the transmitted information, is an intriguing approach to modern data protection. This article examines in detail the principles and mechanisms of operation of such combined system, highlights its key advantages in the context of modern cyber threats and identifies the potential limitations and difficulties of its implementation.

Keywords: multifactor authentication, handwritten signature, digital signature, digital security, authorization.

Введение

С появлением цифровой эры и интенсивной интеграцией информационных технологий во все сферы человеческой деятельности, критическая зависимость от цифровых платформ становится неоспоримой реальностью. Эта тенденция, несмотря на все свои преимущества, приносит с собой новые вызовы в области информационной безопасности, особенно в контексте аутентификации и авторизации пользователей. Традиционные методы аутентификации, такие как стандартные пароли и пин-коды, долгое время служили основой для обеспечения безопасности существующих систем. Однако с ростом уровня киберпреступности и появлением более сложных методов атаки, одиночные методы стали всё более уязвимыми. Происшествия, связанные с утечками данных, подтверждают, что стандартные пароли могут быть легко скомпрометированы, а их использование как единственного метода защиты не обеспечивает адекватный уровень безопасности [1].

В данном контексте, комбинированные методы аутентификации, объединяющие несколько уровней защиты, представляют особый интерес. Один из таких методов – это совмещение рукописной подписи с электронной подписью (ЭП). Рукописная подпись представляет собой уникальный биометрический признак, который сложно подделать и воспроизвести, тогда как ЭП обеспечивает целостность и аутентичность цифровой информации. По мере развития технологий и возрастания киберугроз, комбинация рукописной подписи и ЭП может предложить новый, более надёжный уровень защиты, чем традиционные методы. Данное исследование призвано рассмотреть принципы, преимущества и ограничения такого подхода при авторизации [2].

Таким образом, с учётом текущих вызовов в области информационной безопасности, настоятельно требуется глубокий анализ и оценка потенциала комбинированных методов аутентификации, таких как рукописная подпись в сочетании с ЭП.

Цель исследования

Цель исследования заключается в оценке эффективности и надёжности комбинированного метода аутентификации, объединяющего рукописную подпись и ЭП, для повышения уровня безопасности данных и систем в условиях усиления киберугроз. Исследование направлено на анализ принципов работы и механизмов такой системы, выявление её ключевых преимуществ перед традиционными методами аутентификации, а также определение потенциальных ограничений и сложностей реализации данного подхода в современных условиях информационной безопасности.

Рукописная подпись как инструмент аутентификации

Рукописная подпись, используемая на протяжении веков как средство идентификации личности и подтверждения намерений, представляет собой комплексный биометрический признак. Уникальная динамика и структура делают её не просто символом согласия или идентичности, но и мощным инструментом аутентификации в современных условиях. Для начала рассмотрим структурные аспекты рукописной подписи.

Эти аспекты относятся к постоянным характеристикам, таким как форма букв, соединения линий и углы между ними, а также к различным элементам дизайна подписи. Они могут варьироваться от одного индивида к другому, создавая уникальный «отпечаток» для каждой личности. Динамические характеристики, с другой стороны, охватывают элементы, связанные с процессом создания подписи. Это может включать в себя скорость написания, давление, а также последовательность и направление движений. Сочетание всех этих факторов обеспечивает глубокую уникальность каждой рукописной подписи, даже если визуально они могут казаться схожими [3]. Различия в рукописных подписях, в первую очередь, происходят из-за индивидуальных физиологических особенностей человека. Анатомия кисти, длина и гибкость пальцев, мышечная сила – всё это влияет на форму полученной подписи. Помимо физиологических факторов, психологические составляющие, такие как эмоциональное состояние, уровень стресса или даже уровень усталости, могут также влиять на динамику и характеристики подписи. Эмоциональные колебания могут привести к изменениям в давлении на перо или скорости написаниях [4]. Использование рукописной подписи в качестве метода аутентификации представляет собой перспективный подход, учитывая её уникальность и сложность подделки. Тем не менее, она также сталкивается с рядом ограничений. Изменения в состоянии здоровья, старение или даже временные травмы могут повлиять на динамику и соответственно форму изображения подписи. Поэтому, несмотря на все преимущества, важно рассматривать рукописную подпись в комплексе с другими методами аутентификации [5].Рукописная подпись, будучи глубоко индивидуальным и сложным для воспроизведения биометрическим методом, предлагает значительные возможности для аутентификации. Однако её использование требует тщательного анализа и применения в сочетании с другими методами для обеспечения максимальной эффективности и надёжности.

ЭП как гарант целостности данных

ЭП стала важным компонентом современных систем информационной безопасности. Она служит не только как средство подтверждения аутентичности отправителя или содержания, но и как инструмент, гарантирующий целостность данных в электронном виде. Для понимания роли ЭП в обеспечении целостности данных необходимо понимать её базовые принципы работы. ЭП базируется на криптографических алгоритмах, в основе которых лежит использование пары ключей: открытого и закрытого. Когда информация подписывается закрытым ключом, она может быть проверена любым, кто имеет доступ к соответствующему открытому ключу [6].Одним из ключевых аспектов ЭП, который гарантирует целостность данных, является процесс хэширования. Перед тем как данные будут подписаны, они преобразуются в хэш-код – фиксированную строку символов. Любое изменение исходных данных, даже наиболее незначительное, приведёт к радикальному изменению хэш-кода. Таким образом, при проверке ЭП можно убедиться не только в аутентичности данных, но и в их неизменности с момента подписания. В мире, где электронные данные стали критически важными, обеспечение целостности становится первостепенной задачей. Искажение или намеренное изменение данных может привести к катастрофическим последствиям, особенно в сферах финансов, здравоохранения или государственного управления. ЭП предоставляет надёжный механизм для гарантии того, что информация остаётся нетронутой после её создания. Несмотря на все преимущества, использование ЭП также представляет ряд вызовов. Ключевым является необходимость обеспечения безопасности закрытого ключа. Его компрометация может поставить под угрозу все данные, подписанные данным ключом. Также важным является выбор криптостойкого алгоритма хэширования и его регулярное обновление. ЭП играет решающую роль в обеспечении целостности данных в цифровой среде. Её способность гарантировать неизменность и аутентичность информации делает её ценным

инструментом в арсенале методов аутентификации и безопасности данных. Однако правильное и ответственное использование ЭП требует понимания её принципов и возможных рисков [7].

Совмещение рукописной подписи и ЭП

В эпоху цифровизации, где многие операции перешли из реального мира в виртуальное пространство, необходимость в совершенствовании механизмов аутентификации никогда не была такой актуальной. Совмещение традиционной рукописной подписи с современными технологиями, такими как ЭП, представляет собой комбинированный подход к обеспечению безопасности. Ключевым преимуществом совместного использования рукописной подписи и ЭП является введение двойной системы проверки. При таком подходе, даже если один из методов подвергнется компрометации, другой служит дополнительным барьером, препятствующим неправомерному доступу или фальсификации данных.

Рукописная подпись несёт в себе уникальные черты каждого пользователя. Её динамика, структура и даже давление при написании зависят от множества физиологических и психологических факторов. Таким образом, подделка рукописной подписи требует не только высокого мастерства, но и глубокого понимания индивидуальных особенностей человека. В то время как рукописная подпись фокусируется на индивидуальности, ЭП предоставляет технологическую гарантию целостности данных. Она основана на сложных криптографических алгоритмах и служит своего рода печатью, подтверждающей, что данные не были изменены после их создания. Совместное использование обоих методов может быть особенно полезным в ситуациях, где требуется дополнительная защита, например, при подписании юридически значимых документов, финансовых операциях или при доступе к конфиденциальной информации. Такой комбинированный подход обеспечивает как личную, так и технологическую защиту данных. Совмещение рукописной подписи с ЭП представляет собой продвинутую стратегию аутентификации, сочетающую в себе лучшие стороны традиционных и современных методов. Они обеспечивают уровень безопасности, который сложно достичь, опираясь лишь на один из методов, и предоставляют сильную защиту в среде, где угрозы безопасности постоянно эволюционируют [8].

Преимущества и риски совмещения рукописной подписи и ЭП

В контексте глобализации и ускоренного развития информационных технологий, стремление к оптимизации и усилению мер безопасности является неизбежным. Совмещение рукописной подписи и ЭП представляет собой одно из инновационных решений в этой области. Однако, как и любое техническое или организационное нововведение, данный метод имеет свои преимущества и недостатки.

Преимущества:

- Комбинированный подход обеспечивает двойной барьер для потенциальных нарушителей. Даже если один из методов будет скомпрометирован, другой служит дополнительным слоем защиты.
- По статистике, многократная аутентификация существенно снижает вероятность успешных кибератак.
- В случае, если атакующий добывает данные, отсутствие одного из ключей (ЭП или рукописной подписи) делает эти данные бесполезными.

Недостатки:

- Интеграция двух систем требует высококвалифицированных специалистов и сложных программных решений.
- Технологии распознавания рукописной подписи не идеальны. Факторы, такие как изменение стиля подписи из-за усталости или стресса, могут привести к ошибкам.

• Переход на комбинированный метод требует значительных капиталовложений, обучения персонала и времени на адаптацию системы.

Хотя совмещение рукописной подписи и ЭП предлагает обширные преимущества в контексте безопасности, необходимо тщательно взвешивать потенциальные риски. Эффективное внедрение и успешное использование такой системы требует комплексного подхода, включая тщательное планирование, обучение и постоянный мониторинг [9].

Заключение

В условиях быстрого развития цифровых технологий и возрастающей угрозы кибератак, стремление к эффективным и надёжным методам аутентификации стоит в центре внимания научного и технологического сообщества. Принимая во внимание текущую динамику, комбинированный подход, объединяющий рукописную подпись и ЭП, представляет собой значимый шаг вперёд в этом направлении. Совмещение уникальных характеристик рукописной подписи

с надёжностью и проверенной эффективностью ЭП, создаёт систему, которая может служить гарантом аутентичности данных и пользователя. Этот подход может не только усилить текущие меры безопасности, но и послужить отправной точкой для создания новых, более продвинутых систем аутентификации [10].Тем не менее, несмотря на очевидные преимущества, совмещение двух методов представляет ряд вызовов. Техническая интеграция, оптимизация процессов распознавания и учёт возможных ошибок требуют глубокого научного анализа. Будущие исследования должны быть направлены на разработку алгоритмов, улучшение процесса распознавания и снижение вероятности ошибок.

В дополнение к научным исследованиям, проблема внедрения новых технологических решений остаётся актуальной. Необходимость адаптации к существующим системам, разработка нового программного обеспечения и оборудования, а также обучение персонала представляют собой значимые препятствия на пути к широкому применению комбинированного подхода [11]. В заключение следует отметить, что комбинированный подход в виде совмещения рукописной подписи и ЭП, несомненно, представляет собой перспективное направление в области аутентификации. Однако для его успешного внедрения необходимо провести ряд дополнительных исследований, а также разработать комплексные технологические решения. Надежда на создание надёжной и эффективной системы аутентификации в будущем зависит от усилий научного сообщества и технологических инноваторов в данной области.

Список литературы:

1. Абдалла Али Ахмед Абдельрахман. Разработка математического и алгоритмического обеспечения автоматической верификации подписи // Автореферат диссертации на соискание учёной степени кандидата технических наук / Владимирский государственный университет. Владимир, 2009. [Электронный ресурс] // РГБ. 2009. Режим доступа: https://viewer.rsl.ru/ru/rsl01003489732?page=1&rotate=0&theme=black
2. Анисимова Э.С. О проблеме верификации с использованием рукописных подписей // Современная техника и технологии. 2016. № 3 (55). С. 13-15. [Электронный ресурс] // Современная техника и технологии. 2016. Режим доступа: https://technology.snauka.ru/2016/03/9715
3. Калыбекова А.К., Сембиев О.З., Баумуратова Д.Б. Методики распознавания, верификации и визуализации подписи // Научные труды ЮКГУ им. М. Ауэзова.

2015. № 2 (33). С. 32-34. [Электронный ресурс] // Elibrary. 2015. Режим доступа: https://www.elibrary.ru/download/elibrary_42202085_67569405.pdf

4. Волков Д.А., Пасенчук В.А. Использование биометрических признаков для осуществления двухфакторной аутентификации // В сборнике: Инфографика и информационный дизайн: Визуализация данных в науке. Материалы Международной научно-практической конференции. Омск, 2017. С. 231-241. [Электронный ресурс] // Elibrary. 2017. Режим доступа: https://www.elibrary.ru/download/elibrary_30761193_53587930.pdf
5. Иванов А.И., Ложников П.С., Сулавко А.Е. Оценка надёжности верификации автографа на основе искусственных нейронных сетей, сетей многомерных функционалов Байеса и сетей квадратичных форм // Компьютерная оптика. 2017. Т. 41. № 5. С. 765-774. [Электронный ресурс] // Компьютерная оптика. 2017. Режим доступа: https://computeroptics.ru/KO/PDF/KO41-5/410520.pdf
6. Молдовян Д.Н., Молдовян А.А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2 (48). С. 7-17. [Электронный ресурс] // Elibrary. 2022. Режим доступа: https://www.elibrary.ru/download/elibrary_48417750_95828988.pdf
7. Кудж С.А., Майоров А.А., Шкуров Ф.В., Трофимов С.В. Исследование, анализ и прогноз возможных результатов применения ЭЦП на рынке цифровой картографической продукции // Приложение к журналу Известия вузов. Геодезия и аэрофотосъёмка. Сборник статей по итогам научно-технической конференции. 2008. № 1. С. 59-62. [Электронный ресурс] // Elibrary. 2008. Режим доступа: https://www.elibrary.ru/download/elibrary_27651142_30144479.pdf
8. Гафаров Ф.М., Ризвонова У.М., Иброхимов С.Ю. Технологии на основе инфраструктуры открытых ключей: Сущность ЭЦП // Вестник Технологического университета Таджикистана. 2021. № 1 (44). С. 77-85. [Электронный ресурс] // Elibrary. 2021. Режим доступа: https://www.elibrary.ru/download/elibrary_47244405_61754891.pdf
9. Козина Е.В., Кузьмин А.А., Лукичев А.А. Использование ЭЦП для верификации документов на бумажном носителе // В сборнике: Череповецкие научные чтения - 2012. Материалы Всероссийской научно-практической конференции. Ответственный редактор Н.П. Павлова. 2013. С. 114-115. [Электронный ресурс] // Elibrary. 2013. Режим доступа: https://www.elibrary.ru/download/elibrary_23428256_94480416.pdf
10. Бушинский А.С., Самойлова Т.А. Распознавание рукописной подписи методом опорных векторов // Системы компьютерной математики и их приложения. 2017. № 18. С. 63-65. [Электронный ресурс] // Elibrary. 2017. Режим доступа: https://www.elibrary.ru/download/elibrary_30469402_21160409.pdf
11. Сулавко А.Е. Высоконадёжная аутентификация по рукописным паролям на основе гибридных нейронных сетей с обеспечением защиты биометрических эталонов от компрометации // Информационно-управляющие системы. 2020. № 4 (107). С. 61-77. [Электронный ресурс] // Elibrary. 2020. Режим доступа: https://www.elibrary.ru/download/elibrary_43838379_18968636.pdf

References:

1. Abdullah Ali Ahmed Abdelrahman. Development of mathematical and algorithmic support for automatic signature verification // Abstract of the dissertation for the degree of Candidate of Technical Sciences / Vladimir State University. Vladimir, 2009. [Electronic resource] // RGB. 2009. Access mode: https://viewer.rsl.ru/ru/rsl01003489732?page=1&rotate=0&theme=black
2. Anisimova E.S. On the problem of verification using handwritten signatures // Modern equipment and technologies. 2016. №. 3 (55). P. 13-15. [Electronic resource] // Modern technology and technologies. 2016. Access mode: https://technology.snauka.ru/2016/03/9715
3. Kalybekova A.K., Sembiev O.Z., Baumuratova D.B. Methods of recognition, verification and visualization of signatures // Scientific works of M. Auezov SKSU. 2015. №. 2 (33). P. 32-34. [Electronic resource] // Elibrary. 2015. Access mode: https://www.elibrary.ru/download/elibrary_42202085_67569405.pdf
4. Volkov D.A., Pasenchuk V.A. The use of biometric features for two-factor authentication // In the collection: Infographics and information design: Data Visualization in Science. Materials of the International Scientific and Practical Conference. Omsk, 2017. P. 231-241. [Electronic resource] // Elibrary. 2017. Access mode: https://www.elibrary.ru/download/elibrary_30761193_53587930.pdf
5. Ivanov A.I., Lozhnikov P.S., Sulavko A.E. Assessment of the reliability of autograph verification based on artificial neural networks, networks of multidimensional Bayesian functionals and networks of quadratic forms // Computer optics. 2017. Vol. 41. №. 5. P. 765-774. [Electronic resource] // Computer optics. 2017. Access mode: https://computeroptics.ru/KO/PDF/KO41-5/410520.pdf
6. Moldovyan D.N., Moldovyan A.A. Algebraic algorithms of EDS based on the difficulty of solving systems of equations // Cybersecurity issues. 2022. №. 2 (48). P. 7-17. [Electronic resource] // Elibrary. 2022. Access mode: https://www.elibrary.ru/download/elibrary_48417750_95828988.pdf
7. Kudzh S.A., Mayorov A.A., Shkurov F.V., Trofimov S.V. Research, analysis and forecast of possible results of using EDS in the market of digital cartographic products // Appendix to the journal Izvestiya vuzov. Geodesy and aerial photography. Collection of articles based on the results of the scientific and technical conference. 2008. №. 1. P. 59-62. [Electronic resource] // Elibrary. 2008. Access mode: https://www.elibrary.ru/download/elibrary_27651142_30144479.pdf
8. Gafarov F.M., Rizvonova U.M., Ibrokhimov S.Y. Technologies based on public key infrastructure: The essence of EDS // Bulletin of the Technological University of Tajikistan. 2021. №. 1 (44). P. 77-85. [Electronic resource] // Elibrary. 2021. Access mode: https://www.elibrary.ru/download/elibrary_47244405_61754891.pdf
9. Kozina E.V., Kuzmin A.A., Lukichev A.A. Using EDS for verification of documents on paper // In the collection: Cherepovets scientific readings - 2012. Materials of the All-Russian scientific and practical conference. The responsible editor is N.P. Pavlova. 2013. P. 114-115. [Electronic resource] // Elibrary. 2013. Access mode: https://www.elibrary.ru/download/elibrary_23428256_94480416.pdf

10. Bushinsky A.S., Samoilova T.A. Handwritten signature recognition by the method of support vectors // Systems of computer mathematics and their applications. 2017. №. 18. P. 63-65. [Electronic resource] // Elibrary. 2017. Access mode: https://www.elibrary.ru/download/elibrary_30469402_21160409.pdf
11. Sulavko A.E. Highly reliable authentication by handwritten passwords based on hybrid neural networks with protection of biometric standards from compromise // Information management systems. 2020. №. 4 (107). P. 61-77. [Electronic resource] // Elibrary. 2020. Access mode: https://www.elibrary.ru/download/elibrary_43838379_18968636.pdf