Управление в социально-экономических системах
Control in social and economic systems

Научная статья
УДК 62; 004; 007
DOI: 10.14529/ctcr250207

ПРОБЛЕМАТИКА ВЕРИФИКАЦИИ ПОДЛИННОСТИ, АВТОРСКОГО ПРАВА И ЦЕЛОСТНОСТИ ЦИФРОВЫХ ДАННЫХ

***А.А. Шинкарев**, sania.kill@mail.ru*
***О.В. Логиновский**, loginovskiiov@susu.ru, https://orcid.org/0000-0003-3582-2795*
***Д.В. Стародубцев**, starodubtcev.d.v@gmail.com*
Южно-Уральский государственный университет, Челябинск, Россия

Аннотация. В настоящее время как никогда все большую актуальность обретает проблема обеспечения безопасности цифровых данных. Потребителями цифровых данных или же информации являются практически все люди в большинстве сфер жизнедеятельности. Безопасными данными в контексте исследования являются данные, происхождение которых достоверно, целостность не нарушена и авторские права соблюдаются. Методы защиты цифровых данных с каждым годом совершенствуются, стремясь предотвращать кражу информации и оберегать людей от недостоверных или заведомо ложных сведений. Однако при всем своем многообразии и технологической зрелости современные подходы к верификации подлинности, авторского права, целостности мультимедиа и инструменты на их основе не всегда могут защитить потребителей информации в полном объеме от современных киберугроз. При создании нового также не всегда устраняются концептуальные проблемы того, что было раньше. Новые подходы, инструменты и стандарты зачастую привносят новые уязвимости, которые используются злоумышленниками для атаки. **Цель исследования:** провести анализ современных методов и технологий верификации подлинности, авторского права и целостности мультимедийных данных, а также предложить комплексный подход, который может способствовать решению выявленных проблем. **Материалы и методы.** Используется ретроспективный метод для анализа исторического развития технологий защиты данных, криптографические подходы, а также современные решения на основе блокчейна и машинного обучения. **Результаты.** Анализ показал, что традиционные криптографические методы, несмотря на эффективность в обеспечении целостности данных, сталкиваются с ограничениями в распределенных системах из-за отсутствия единых стандартов и сложности масштабирования. **Заключение.** Несмотря на разнообразие существующих технологий подтверждения авторства, целостности, и аутентичности цифровых данных в общем и мультимедиа в частности, на сегодняшний день проблемы отсутствия стандартизации и фрагментированности решений остаются одними из ключевых вызовов в области обеспечения комплексной безопасности цифровых данных.

Ключевые слова: безопасность данных, верификация подлинности, цифровая подпись, блокчейн, NFT, машинное обучение, криптография, электронный документооборот

Для цитирования: Шинкарев А.А., Логиновский О.В., Стародубцев Д.В. Проблематика верификации подлинности, авторского права и целостности цифровых данных // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2025. Т. 25, № 2. С. 74–81. DOI: 10.14529/ctcr250207

Original article
DOI: 10.14529/ctcr250207

PROBLEMATICS OF AUTHENTICITY VERIFICATION, COPYRIGHT AND DIGITAL DATA INTEGRITY

***A.A. Shinkarev**, sania.kill@mail.ru*
***O.V. Loginovskiy**, loginovskiyo@mail.ru, https://orcid.org/0000-0003-3582-2795*
***D.V. Starodubtcev**, starodubtcev.d.v@gmail.com*
South Ural State University, Chelyabinsk, Russia

Abstract. Nowadays, the problem of ensuring the security of digital data is becoming more urgent than ever. Consumers of digital data or information are almost all people in most spheres of life. Secure data in the context of research is data whose origin is reliable, its integrity is intact, and copyrights are respected. Digital data protection methods are being improved every year in an effort to prevent information theft and protect people from false or deliberately false information. However, with all its diversity and technological maturity, modern approaches to verifying the authenticity, copyright and integrity of multimedia and tools based on them cannot always fully protect consumers of information from modern cyber threats. Introduction of something new does not always eliminate the conceptual problems of what was before. New approaches, tools, and standards often introduce new vulnerabilities that are used by attackers. **Research goal.** To analyze modern methods and technologies for verifying authenticity, copyright and integrity of multimedia data, as well as to propose an integrated approach that can help to solve the identified problems. **Materials and methods.** Retrospective method is used to analyze the historical development of data protection technologies, cryptographic approaches, as well as modern solutions based on blockchain and machine learning. **Results.** The analysis showed that traditional cryptographic methods, despite their effectiveness in ensuring data integrity, face limitations in distributed systems due to the lack of uniform standards and the complexity of scaling. **Conclusion.** Despite the variety of existing technologies for verifying the authorship, integrity, and authenticity of digital data in general and multimedia in particular, today the problems of lack of standardization and fragmentation of solutions remain among key challenges in the area of making digital data secure in its entirety.

Keywords: data security, authentication, digital signature, blockchain, NFT, machine learning, cryptography, electronic document management

For citation: Shinkarev A.A., Loginovskiy O.V., Starodubtcev D.V. Problematics of authenticity verification, copyright and digital data integrity. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2025;25(2):74–81. (In Russ.) DOI: 10.14529/ctcr250207

Введение

В настоящее время проблема безопасности цифровых данных становится более явной из-за увеличения числа кибератак, утечек информации и роста объемов цифровых данных, которые ежедневно обрабатываются и передаются через Интернет. Ситуация также обостряется по причине экономической и внешнеполитической нестабильности в мире. В соответствии с отчетом Лаборатории Касперского [1] в первом полугодии 2024 года количество атак выросло на 39 % по сравнению с аналогичным периодом 2023 года. Повышенная активность киберпреступников также сопровождается ростом количества утечек персональных данных пользователей вебсервисов. По данным экспертно-аналитического центра ГК InfoWatch [2], в первом полугодии 2024 года в России количество случаев кражи личной информации выросло на 10,1 %, скомпрометировано 986 миллионов записей. Приведенная статистика свидетельствует об обострении ситуации в области обеспечения безопасности в киберпространстве. Эта сфера со всеми ее вызовами все больше привлекает внимание как общества, так и государства.

Актуальность обеспечения безопасности при работе с цифровыми данными подтверждает стратегия технологического развития Российской Федерации до 2030 года [3], важным аспектом которой является необходимость обеспечения безопасности информационной инфраструктуры предприятий. С ускорением цифровизации и цифровой трансформации ключевых сфер общественной и экономической деятельности все важнее становится разработка новых и освоение суще-

ствующих алгоритмов и методов для защиты данных в системах связи и электронного документооборота, что имеет особую важность для государственных и муниципальных организаций, коммерческих структур и разработчиков программного обеспечения, ответственных за безопасность информационных систем. Разрабатываемые методы защиты, согласно триаде безопасности [4], должны обеспечить конфиденциальность, целостность и защиту чувствительной информации. Рассмотрим развитие подходов и механизмов обеспечения подлинности цифровых данных в исторической ретроспективе, чтобы выявить проблемы, которые они были призваны решить, и ответить на вопрос о том, насколько это удалось сделать.

1. Развитие методов проверки подлинности данных в исторической ретроспективе

Защита и верификация подлинности данных берет начало в глубокой древности, когда письменность только начинала зарождаться. Одними из первых методов защиты информации были физические метки и уникальные знаки. Например, в Месопотамии информацию фиксировали на глиняных табличках, на которых наносились отметки с помощью специальных печатей цилиндрической формы с индивидуальными надписями. В свою очередь, в Древнем Риме также использовались особые знаки для установления авторства документа, это могли быть инициалы или личные знаки. К тому же применялся метод запечатывания с использованием колецпечатей [5].

С развитием государств и торговли потребность в верификации подлинности документов выросла, дополнительно к печатям (уже гербовым) стали использовать водяные знаки на бумаге. Они могли служить клеймом, символизирующим конкретное производство, или же устанавливать его географическое положение.

Методы верификации подлинности документов постоянно совершенствовались. Вводились новые стандарты в делопроизводстве, что позволяло поддерживать высокий уровень безопасности документов. Одним из таких методов стала подпись документов с помощью пера и чернил. Уникальность почерка подписанта стала играть важную роль при проверке подлинности документов. Это позволило значительно сократить количество фальсификаций ввиду сложности подделки индивидуальных особенностей почерка [6].

В эпоху развития информационных технологий методы защиты данных кардинально изменились. В Первую и Вторую мировые войны использовались механические шифраторы, такие как машина «Энигма». Шифрование сообщений применялось и в древнее время, но с появлением подобных машин получилось автоматизировать данный процесс, что способствовало значительному росту уровня качества и скорости шифрования и помогло обеспечить лучшую защиту военных сообщений [7].

Позже, с момента распространения компьютеров, начали разрабатываться алгоритмы верификации подлинности данных, такие как хеширование и цифровые подписи. Принцип цифровой подписи построен на асимметричном шифровании с открытым ключом. Однако шифрование данных больших размеров, например, видео или фото, является ресурсозатратным процессом, именно поэтому внедрили использование алгоритмов хеширования. Подобные алгоритмы позволили сократить исходное количество данных в несколько раз и при этом оставили возможность удостовериться в их целостности. Этот подход задал высочайший уровень защиты данных [8].

Похожий принцип используется для установки защищенного соединения при применении протокола передачи данных HTTP, который называется HTTPS. В основе данной системы применяются алгоритмы симметричного и асимметричного шифрования, что позволяет обеспечить конфиденциальность и целостность передаваемой информации [9].

Еще одной важной вехой в развитии безопасности данных является применение биометрического распознавания для установки личности человека. Распознавание лиц, отпечатков пальцев и других биометрических данных активно используется для аутентификации пользователей, чтобы предотвратить нелегитимный доступ к информации [10].

В современном мире для защиты данных задействуются децентрализованные технологии, такие как блокчейн, которые обеспечивают неизменность данных, позволяя проверять их подлинность без центрального органа. Данная технология активно развивается и применяется во многих сферах общества, где так или иначе необходимо устанавливать подлинность информации, например, в области финансовых операций и кибербезопасности [11].

От первых печатей и подписей до сложных алгоритмов и биометрических данных человечество прошло долгий путь в развитии методов проверки подлинности и защиты данных. Современные технологии не только обеспечивают высокую степень безопасности, но и открывают новые горизонты для автоматизации и улучшения систем защиты данных. Однако методы фальсификации цифровых данных развиваются с такой же скоростью и требуют все более пристального внимания со стороны разработчиков подходов и инструментов для защиты данных.

2. Проблематика обеспечения безопасности цифровых данных в современных условиях

Особую значимость проблема безопасности цифровых данных приобретает в контексте цифровой экономики, которая опирается на доверие к цифровым платформам и данным, которыми они оперируют. Способность эффективно проверять подлинность и целостность информации становится критически важной для устойчивого функционирования цифровой среды. Одним из ключевых аспектов информационной безопасности является обеспечение подлинности цифровых данных, включая данные, циркулирующие в системах электронного документооборота. Это не только способствует предотвращению несанкционированного доступа и подмены данных, но и укрепляет доверие к цифровым инструментам, формирующим основу современной экономики и социальных взаимодействий.

Помимо всего прочего, существует тенденция роста объемов цифровых данных [12], что является следствием появления широкого спектра инструментов для создания и редактирования различного рода цифровых данных, таких как фото, видео и аудио. Современные технологии позволяют пользователям с минимальными техническими знаниями создавать текстовые, визуальные и аудиоданные, что, с одной стороны, делает это доступным для людей без соответствующих навыков, но, с другой стороны, развитие технологий порождает новые вызовы в области защиты интеллектуальной собственности.

Одной из ключевых проблем в этом контексте становится верификация авторства, установка подлинности и целостности цифровых данных. Технологическая доступность инструментов для обработки и манипуляции с данными упрощает несанкционированное копирование, переработку и даже коммерческое использование данных без ведома и разрешения правообладателя. Такие действия нарушают авторские права и подрывают доверие к цифровым платформам как к среде безопасного распространения творческих и профессиональных работ.

В условиях необходимости обеспечения защиты авторских прав требуется внедрение и совершенствование алгоритмов и методов верификации подлинности цифровых данных. Это может включать в себя разработку и внедрение технологий цифровых водяных знаков, систем цифровой подписи, блокчейн-технологий для отслеживания происхождения и изменения данных, а также применение методов машинного обучения для автоматического выявления случаев нарушения авторских прав. Совершенствование таких методов становится ключевым для создания доверительной цифровой среды, в которой интеллектуальная собственность защищена на всех этапах ее существования и распространения.

Развитие нейронных сетей, особенно таких как генеративно-состязательные сети (GAN) [13] и трансформеры (transformers) [14], привело к значительному прогрессу в области синтеза мультимедийных данных. Эти алгоритмы способны с высокой степенью реалистичности создавать изображения, видео и аудио.

Одной из существенных проблем, вытекающих из этого технологического достижения, является возможность создания поддельных документов и материалов, включая так называемые дипфейки (deepfakes) [15]. Эти фальсифицированные материалы характеризуются высокой степенью правдоподобности, относительно невысокой стоимостью создания и доступностью широким кругам непрофессионалов. Дипфейки высокого качества, поданные аудитории в правильный момент и получившие поддержку с помощью методов социальной инженерии, могут быть практически неотличимы от достоверных оригинальных данных без применения профессионалами специальных методов анализа.

В результате возникает ряд угроз, связанных как с индивидуальной, так и с общественной безопасностью, таких как нарушение конфиденциальности, дискредитация лиц через поддельные высказывания, фальсификация официальных документов и утрата доверия к визуальным и аудиодоказательствам.

Особенно критична данная проблема в контексте систем электронного документооборота, где подлинность и целостность документов являются основой для принятия юридически значимых решений. Утечки персональных данных пользователей только усугубляют существующую ситуацию, давая злоумышленникам больше исходных данных для фальсификации критически важных документов. Объем и детализация украденной информации существенно увеличивают вероятность создания поддельных материалов, обладающих высокой степенью достоверности. Это, в свою очередь, ставит под угрозу безопасность как индивидуальных пользователей, так и организаций, поскольку нарушается целостность и доверие к документам, используемым в деловой и юридической практике. Использование электронных цифровых подписей (ЭЦП) позволяет значительно повысить уровень защиты документов. ЭЦП работает на основе криптографических алгоритмов, которые обеспечивают уникальность и неизменность подписи. Когда документ подписывается электронной подписью, создается своего рода цифровой отпечаток, который привязан к содержимому документа. Если злоумышленник попытается изменить документ, подпись станет недействительной, что сразу выявит факт фальсификации. Таким образом, ЭЦП не только подтверждает авторство, но и гарантирует, что документ не был изменен после подписания. Это делает кражу и подделку документа крайне сложной, так как для успешной фальсификации потребуется не только доступ к самой подписи, но и взлом криптографической защиты. Однако, несмотря на высокий уровень безопасности, ЭЦП не является абсолютно неуязвимой. Во-первых, безопасность электронной подписи напрямую зависит от надежности закрытого ключа, который используется для ее создания. Если злоумышленник получит доступ к закрытому ключу (например, через фишинг, вредоносное ПО или кражу устройства, на котором он хранится), он сможет подписывать документы от имени владельца подписи. Во-вторых, устаревшие или слабые криптографические алгоритмы могут быть взломаны с использованием современных вычислительных мощностей, что делает подпись уязвимой. В-третьих, человеческий фактор также играет важную роль: небрежное хранение ключей или использование простых паролей для их защиты может свести на нет все преимущества ЭЦП.

3. Современные методы верификации подлинности, авторского права и целостности цифровых данных

Современные технологии, такие как блокчейн и NFT (невзаимозаменяемые токены), предлагают инновационные подходы к решению задач верификации подлинности, авторского права и целостности мультимедиа. Блокчейн благодаря своей децентрализованной природе и свойствам неизменяемости данных может служить надежным инструментом для фиксации и проверки авторства цифрового контента. Например, платформа Ethereum активно используется для создания NFT, которые позволяют художникам и создателям контента закреплять права на свои работы. Однако, несмотря на преимущества блокчейна, существуют ограничения, связанные с тем, что NFT, используемые для подтверждения прав на цифровые активы, не хранят сами мультимедийные данные, а лишь содержат ссылки на них. В случае утраты или модификации исходных данных NFT теряют свою функциональность в контексте подтверждения подлинности. Это подчеркивает необходимость разработки дополнительных механизмов, обеспечивающих сохранность и неизменность исходных данных, а не временной ссылки на их текущее местоположение. Например, проект Arweave предлагает решение для долговременного хранения данных в децентрализованной сети, что может быть использовано в сочетании с NFT для обеспечения сохранности мультимедиа [16].

В системах электронного документооборота (ЭДО), таких как Контур.Диадок или КриптоПро, криптографические методы играют ключевую роль в обеспечении безопасности данных. Электронная подпись (ЭП) используется для подтверждения авторства и целостности документов, что делает криптографию основой для защиты информации от несанкционированного доступа и подделки. Криптографические алгоритмы, такие как хэш-функции и асимметричное шифрование, обеспечивают не только конфиденциальность данных, но и их неизменность, что является критически важным для верификации подлинности мультимедиа. Например, стандарт SHA-256 широко используется для создания уникальных хэш-сумм, которые позволяют проверять целостность данных. Даже минимальное изменение в документе (например, добавление одного символа или пробела) приведет к тому, что хэш-сумма станет совершенно другой. Например, если в тексте

«Договор № 123» изменить «123» на «124», хэш-сумма изменится кардинально, что сразу выявит факт подделки. Вероятность того, что возникнет коллизия (два разных документа будут иметь одинаковую хэш-сумму), крайне мала [17].

С развитием технологий создания дипфейков проблема идентификации поддельного контента становится все более актуальной. Современные методы машинного обучения, в частности нейронные сети, активно применяются для выявления поддельных видео- и аудиозаписей. Эти методы основаны на анализе специфических признаков, таких как аномалии в движении глаз, текстуре кожи или артефактах в аудиосигналах. Например, исследователи из Калифорнийского университета в Беркли разработали алгоритм, который анализирует микроэкспрессии лица для обнаружения дипфейков [18]. Данный подход выделяется корректностью определения поддельных данных, однако все же не всегда корректно может определить использование генеративных нейронных сетей.

Одной из ключевых проблем в области верификации цифрового контента остается отсутствие стандартизации. Без единого подхода к верификации подлинности цифровых данных решения остаются фрагментированными и несовместимыми между собой. В этом контексте важную роль играют совместные инициативы, такие как C2PA (Coalition for Content Provenance and Authenticity), которые направлены на создание универсальных стандартов для верификации цифровых данных. C2PA позволяет встраивать метаданные, фиксирующие происхождение и историю изменений исходных данных, что открывает путь к созданию унифицированной системы верификации, минимизирующей необходимость человеческого вмешательства. Например, компания Adobe уже интегрировала поддержку C2PA в свои продукты, что позволяет пользователям проверять подлинность изображений [19]. Однако C2PA основывается на честности создателя цифровых данных, так как именно он предоставляет метаданные о происхождении и истории изменений. Если создатель изначально предоставляет ложную информацию или использует генеративные нейронные сети для создания контента, система C2PA не сможет самостоятельно выявить это, так как она не проводит глубокий анализ на предмет использования таких технологий. В отличие от блокчейна и NFT, где проблема заключается в хранении данных (ссылки на данные, которые могут быть утеряны или изменены), C2PA интегрирует подпись и метаданные непосредственно в сам контент. Это делает подпись неотъемлемой частью данных, что повышает их защищенность и упрощает проверку подлинности. Тем не менее такой подход все еще требует доверия к создателю контента, что остается слабым звеном в системе.

Заключение

Несмотря на разнообразие существующих технологий, единого универсального решения для обеспечения подлинности, авторского права и целостности мультимедиа на данный момент не существует. Каждая из технологий предлагает свои уникальные методы, в основе большинства из них лежат криптографические принципы. Криптография обеспечивает защиту данных за счет таких механизмов, как шифрование, цифровые подписи и хэш-функции, которые гарантируют конфиденциальность и целостность данных. Эти принципы являются фундаментальными для создания надежных систем верификации, но не дают полной гарантии корректной верификации подлинности данных.

Таким образом, для решения проблем верификации подлинности, авторского права и целостности мультимедиа необходим комплексный подход, объединяющий лучшие аспекты существующих технологий. Такой подход должен обеспечивать не только целостность и конфиденциальность данных, но и учитывать возможность их модификации с использованием современных технологий, таких как нейронные сети. Кроме того, важно создание единой структуры, которая позволит интегрировать данные из различных источников и обеспечивать их верификацию на основе универсальных стандартов. Это требует дальнейших исследований и разработок, а также активного взаимодействия между научным сообществом, индустрией и регуляторными органами.

Список литературы

1. Kaspersky Security Bulletin 2024: Statistics [Электронный ресурс]. URL: https://securelist.ru/ksb-2024-statistics/111289/ (дата обращения: 15.12.2024).
2. ГК InfoWatch: Утечки информации в мире и России за первое полугодие 2024 года [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/utechki-informatsii-v-mire-i-rossii-za-pervoye-polugodiye-dve-tysyachi-dvadtsat-chetvertogo-goda.pdf (дата обращения: 15.12.2024).
3. Концепция технологического развития на период до 2030 года. Утверждена распоряжением Правительства Российской Федерации от 20 мая 2023 г. № 1315-р.
4. Stallings W. Network Security Essentials: Applications and Standards. Prentice Hall, Pearson Education, 2011. 432 p.
5. Collon D. First Impressions: Cylinder Seals in the Ancient Near East. London, British Museum Publications, 1988. 208 p.
6. Щепкин В.Н. Русская палеография. М.: Наука, 1967. 225 с.
7. Smith J. Emerging Technologies in Cybersecurity // Journal of Cybersecurity Trends. 2017. 6 p.
8. Черемушкин А.В. О содержании понятия «электронная подпись» // Прикладная дискретная математика. 2012. № 3 (17). С. 53–69.
9. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force (IETF), 2018. 160 p.
10. Jain A.K., Ross A., Nandakumar K. Introduction to Biometrics. Springer, 2016. 328 p.
11. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. 9 p.
12. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2016. 996 с.
13. Generative adversarial networks / I. Goodfellow, J. Pouget-Abadie, M. Mirza et al. // Advances in neural information processing systems. 2014. 9 p.
14. Attention Is All You Need / A. Vaswani et al. // 31st Conference on Neural Information Processing Systems. 2017. 15 p.
15. Chesney R., Citron D. Deepfakes and the New Disinformation War // Foreign Affairs. 2019. P. 147–155.
16. Arweave [Электронный ресурс]. URL: https://arweave.org/ (дата обращения: 20.12.2024).
17. Secure Hash Standard (SHS). National Institute of Standards and Technology (NIST). FIPS PUB 180–4, 2015. 36 p.
18. Negi S., Jayachandran M., Upadhyay S. Deep fake: An Understanding of Fake Images and Videos // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021. Vol. 7 (3). P. 183–189. DOI: 10.32628/CSEIT217334
19. Content Authenticity Initiative [Электронный ресурс]. URL: https://contentauthenticity.org/ (дата обращения: 25.12.2024).

References

1. Kaspersky Security Bulletin 2024: Statistics. Available at: https://securelist.ru/ksb-2024-statistics/111289/ (accessed 15 December 2024).
2. *GK InfoWatch: Utechki informatsii v mire i Rossii za pervoe polugodie 2024 goda* [InfoWatch: Information leaks in the world and Russia in the first half of 2024]. (In Russ.) Available at: https://www.infowatch.ru/analytics/utechki-informatsii-v-mire-i-rossii-za-pervoye-polugodiye-dve-tysyachi-dvadtsat-chetvertogo-goda.pdf (accessed 15 December 2024).
3. *Kontseptsiya tekhnologicheskogo razvitiya na period do 2030 goda. Utverzhdena rasporyazheniem Pravitel'stva Rossiyskoy Federatsii ot 20 maya 2023 g. No. 1315-r.* [The concept of technological development for the period up to 2030. Approved by the order of the Government of the Russian Federation of May 20, 2023 No. 1315-r.]. (In Russ.)
4. Stallings W. *Network Security Essentials: Applications and Standards*. Prentice Hall, Pearson Education; 2011. 432 p.
5. Collon D. *First Impressions: Cylinder Seals in the Ancient Near East*. London, British Museum Publications; 1988. 208 p.
6. Shchepkin V.N. *Russkaya paleografiya* [Russian paleography]. Moscow: Nauka; 1967. 225 p. (In Russ.)
7. Smith J. Emerging Technologies in Cybersecurity. *Journal of Cybersecurity Trends*. 2017. 6 p.

8. Cheremushkin A.V. On the notion of electronic signature. *Applied discrete mathematics*. 2012;3(17):53–69. (In Russ.)

9. Rescorla E. *The Transport Layer Security (TLS) Protocol Version 1.3*. Internet Engineering Task Force (IETF), 2018. 160 p.

10. Jain A.K., Ross A., Nandakumar K. *Introduction to Biometrics*. Springer; 2016. 328 p.

11. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. 9 p.

12. Olifer V.G., Olifer N.A. *Komp'yuternye seti. Printsipy, tekhnologii, protokoly* [Computer networks. Principles, technologies, protocols]. St. Petersburg: Piter; 2016. 996 p. (In Russ.)

13. Goodfellow I., Pouget-Abadie J., Mirza M. et al. Generative adversarial networks. In: *Advances in neural information processing systems*. 2014. 9 p.

14. Vaswani A. et al. Attention Is All You Need. In: *31st Conference on Neural Information Processing Systems*. 2017. 15 p.

15. Chesney R., Citron D. Deepfakes and the New Disinformation War. In: *Foreign Affairs*. 2019. P. 147–155.

16. Arweave. Available at: https://arweave.org/ (accessed 20 December 2024).

17. *Secure Hash Standard (SHS)*. National Institute of Standards and Technology (NIST). FIPS PUB 180–4; 2015. 36 p.

18. Negi S., Jayachandran M., Upadhyay S. Deep fake: An Understanding of Fake Images and Videos. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2021;7(3):183–189. DOI: 10.32628/CSEIT217334

19. Content Authenticity Initiative. Available at: https://contentauthenticity.org/ (accessed 25 December 2024).

Информация об авторах

Шинкарев Александр Андреевич, канд. техн. наук, доц. кафедры информационно-аналитического обеспечения управления в социальных и экономических системах, Южно-Уральский государственный университет, Челябинск, Россия; sania.kill@mail.ru.

Логиновский Олег Витальевич, д-р техн. наук, проф., заведующий кафедрой информационно-аналитического обеспечения управления в социальных и экономических системах, Южно-Уральский государственный университет, Челябинск, Россия; loginovskiiov@susu.ru.

Стародубцев Дмитрий Владимирович, аспирант кафедры информационно-аналитического обеспечения управления в социальных и экономических системах, Южно-Уральский государственный университет, Челябинск, Россия; starodubtcev.d.v@gmail.com.

Information about the authors

Aleksandr A. Shinkarev, Cand. Sci. (Eng.), Ass. Prof. of the Department of Informational and Analytical Support of Control in Social and Economic Systems, South Ural State University, Chelyabinsk, Russia; sania.kill@mail.ru.

Oleg V. Loginovskiy, Dr. Sci. (Eng.), Prof., Head of the Department of Informational and Analytical Support of Control in Social and Economic Systems, South Ural State University, Chelyabinsk, Russia; loginovskiiov@susu.ru.

Dmitriy V. Starodubtcev, Postgraduate student of the Department of Informational and Analytical Support of Control in Social and Economic Systems, South Ural State University, Chelyabinsk, Russia; starodubtcev.d.v@gmail.com.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

Статья поступила в редакцию 27.12.2024
The article was submitted 27.12.2024