ОШ МАМЛЕКЕТТИК УНИВЕРСИТЕТИНИН ЖАРЧЫСЫ

ВЕСТНИК ОШСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

BULLETIN OF OSH STATE UNIVERSITY

ISSN: 1694-7452 e-ISSN: 1694-8610

№1/2026, 238-260

ИНФОРМАТИКА

УДК: 004.056.53

DOI: 10.52754/16948610_2026_1_17

МЕТОД КРИПТОГРАФИЧЕСКОЙ ВЕРИФИКАЦИИ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ЗА ПРЕДЕЛАМИ СИСТЕМЫ ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКИХ QR-КОДОВ

ДИНАМИКАЛЫК QR-КОДДОРУН КОЛДОНУУ МЕНЕН ДОКУМЕНТТЕРДИ БАШКАРУУ СИСТЕМАСЫНАН ТЫШКАРЫ ЭЛЕКТРОНДУК ДОКУМЕНТТЕРДИН АНЫКТЫГЫН КРИПТОГРАФИЯЛЫК ТЕКШЕРҮҮ ЫКМАСЫ

A METHOD OF CRYPTOGRAPHIC VERIFICATION OF THE AUTHENTICITY OF ELECTRONIC DOCUMENTS OUTSIDE THE DOCUMENT MANAGEMENT SYSTEM USING DYNAMIC QR CODES

Асилбеков Тынчтыкбек Майрамбекович
Асилбеков Тынчтыкбек Майрамбекович
Asilbekov Tynchtykbek Mairambekovich

преподаватель, Ошский государственный университет
окутуучу, Ош мамлекеттик университети
Lecturer, Osh State University
mir.titan.90@gmail.com
ORCID: 0009-0002-4292-1580

Эшаров Элзарбек Асанович
Эшаров Элзарбек Асанович
Esharov Elzarbek Asanovich

к.ф.-м.н., доцент, Ошский государственный университет
ф.-м.и.к., доцент, Ош мамлекеттик университети
Candidate of Sciences in Physico-Mathematical Sciences, Associate Professor, Osh State University
esharov@oshsu.kg
ORCID: 0009-0006-7995-561X

Абжапар кызы Фарида
Абжапар кызы Фарида
Abjapar kyzy Farida

преподаватель, Ошский государственный университет
окутуучу, Ош мамлекеттик университети
Lecturer, Osh State University
fabjaparkyzy@oshsu.kg

МЕТОД КРИПТОГРАФИЧЕСКОЙ ВЕРИФИКАЦИИ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ЗА ПРЕДЕЛАМИ СИСТЕМЫ ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКИХ QR-КОДОВ

Аннотация

В статье представлен метод криптографической верификации подлинности электронных документов за пределами системы документооборота с использованием динамических QR-кодов. Актуальность исследования обусловлена фундаментальным противоречием: документ, подписанный электронной подписью, являясь юридически значимым оригиналом внутри системы ЭДО, утрачивает этот статус при выведении вовне. Международные инициативы - от верификации морских свидетельств Вануату до платформы ValidAP таможни Гонконга и проекта Blockcredit в Африке (Vanuatu Maritime Services, 2025; Project ValidAP, 2026; Ndiramiye и Mutabazi, 2026, с. 112) - подтверждают глобальный характер проблемы. На основе систематического анализа существующих подходов выявлена научная ниша: ни одно из решений не рассматривает задачу создания «верификационного моста» между закрытым контуром ЭДО и внешней средой как самостоятельную проблему. Предложена гибридная модель верификации, сочетающая локальный уровень (хеш документа SHA-256, метка времени, идентификатор подписанта, цифровая подпись в QR-коде) и удаленный уровень (полные данные через защищенный API). Разработан метод контекстно-зависимого отображения информации, дифференцирующий объем раскрываемых данных в зависимости от прав доступа запрашивающей стороны.

Ключевые слова: электронный документооборот, криптографическая верификация, динамический QR-код, электронная подпись, подлинность документов, гибридная модель верификации, контекстно-зависимый доступ

Динамикалык QR-коддорун колдонуу менен документтерди башкаруу системасынан тышкары электрондук документтердин аныктыгын криптографиялык текшерүү ыкмасы

Аннотация

Бул макалада динамикалык QR коддорун колдонуу менен документтерди башкаруу системасынын сыртында криптографиялык метод аркылуу электрондук документтердин түп нускалыгын текшерүү ыкмасы сунушталат. Изилдөөнүн актуалдуулугу бир фундаменталдык карама-каршылыктан келип чыгат: электрондук кол тамга менен кол коюлган документ электрондук документтерди башкаруу системасында юридикалык жактан милдеттүү түп нуска болгону менен, тышкы дүйнөгө өткөрүлүп берилгенде бул статусун жоготот. Жергиликтүү деңгээлди (SHA-256 документ хэш, убакыт мөөрү, кол коюучунун идентификатору, QR кодундагы санариптик кол тамга) жана алыскы деңгээлди (коопсуз API аркылуу толук маалыматтар) айкалыштырган гибриддик текшерүү модели сунушталат.

Ачкыч сөздөр: электрондук кол тамга, документтин аныктыгы, гибриддик текшерүү модели, контекстке сезгич мүмкүндүк алуу..

A Method of Cryptographic Verification of the Authenticity of Electronic Documents Outside The Document Management System Using Dynamic QR Codes

Abstract

This article presents a method for cryptographic verification of electronic document authenticity outside of a document management system using dynamic QR codes. The relevance of the study stems from a fundamental contradiction: a document signed with an electronic signature, while being a legally binding original within an electronic document management system, loses this status when transferred to the outside world. International initiatives - from the verification of maritime certificates in Vanuatu to the ValidAP platform of Hong Kong Customs and the Blockcredit project in Africa - confirm the global nature of the problem. A hybrid verification model is proposed, combining a local level (SHA-256 document hash, timestamp, signatory identifier, digital signature in a QR code) and a remote level (full data via a secure API).

Keywords: electronic document management, cryptographic verification, dynamic QR code, electronic signature, document authenticity, hybrid verification model, context-sensitive access.

Введение

Сейчас активно проводится цифровизация всех областей и внедрению электронного документооборота (ЭДО). Согласно статистике, более 90% оборот всех документов на корпоративном и государственном уровне в мире осуществляются в формате PDF, также это ведет к тому что электронных подписей ежегодно становится больше чем на 25% (MarketsandMarkets, 2025). Однако с внедрением ЭДО возникает новая задача связанная с самим электронным документом который был подписан электронной подписью и имеющую юридическую силу исключительно внутри системы где он был подписан является оригиналом, а вне системы (при распечатке, или отправке через другие электронные средства передачи данных) этот документ теряет свой статус. Распечатанная копия, даже содержащая визуализированный печать с информацией о подписании, представляет собой лишь копию, не имеющую доказательственного значения без заверения в установленном порядке. Данная проблема создает ситуацию где организации внедряют ЭДО внутри своей организации, а за пределами возвращаются к бумажным копиям, заверенным “мокрой печатью” (Chotikakamthorn и др., 2026, с. 342).

Обзор литературы и существующих решений

Анализ международного опыта показывает, что проблема осознается на глобальном уровне, и различные страны и организации предлагают свои подходы к ее решению. В сфере верификации академических credentials наблюдается особенно активное развитие. Исследование Cardenas Quispe и Pacheco (2025), опубликованное в *Scientific Reports (Nature Portfolio)*, представляет прототип системы на Python и Docker с гибридной блокчейн-сетью из шести узлов, генерацией QR-кодов и византийским консенсусом. Среднее время регистрации диплома в блокчейне составило 2,97 сек, подписания записи - 0,96 сек, а сгенерированные документы верифицируются через QR-коды *(*Cardenas и Pacheco, 2025*)*. Однако решение ориентировано исключительно на академические дипломы и использует тяжеловесную блокчейн-инфраструктуру, избыточную для корпоративного документооборота.

Проект Blockcredit, разрабатываемый для стран Восточной и Суб-Сахарной Африки (Ndiramiye и др., 2026, с. 112) связывает академические credentials с национальными цифровыми ID и записывает криптографические доказательства в блокчейн. Работодатели могут мгновенно верифицировать подлинность через QR-код или API, получая четкий статус: VALID, REVOKED или INVALID *(*Cardenas и Pacheco, 2025*)*. В основе проекта затронута решение связанная с массовой подделкой дипломов и ограничен академической сферой. В одном из статей (Асилбеков и Орозов, 2025, с. 149) рассматривается опыт внедрения и эксплуатации системы по выдаче электронный справок с возможностью верификации подлинности документа на основе QR-кодов.

В платформе ValidAP рассматривается сфера международной торговли, разработанная таможней Гонконга (Vanuatu Maritime Services, 2025). В ней используется хеширование SHA-256 и блокчейн технологии для верификации документов (лицензии, сертификаты происхождения, лабораторные отчеты), где ключевой особенностью является хранение только хешей в блокчейне без загрузки самих файлов. Однако система требует предварительной регистрации документа издателем и не решает проблему верификации документов, уже покинувших систему.

В сфере нотариальных документов Федеральная нотариальная палата РФ реализовала сервис проверки нотариальных документов по QR-коду через портал notariat.ru, работающий с 2021 года и обработавший более 400 тысяч проверок (Federal Notary Chamber of the Russian Federation, 2026). Это один из наиболее близких по духу проектов, но он ограничен нотариальными документами и требует централизованной проверки через официальный портал.

В технической плоскости исследование Hidayat с коллегами (2025) предлагает систему верификации дипломов на основе цифровой подписи RSA в сочетании с QR-кодом. Важная информация (идентификатор студента, номер диплома) хешируется SHA-256, подписывается RSA-ключом и кодируется в QR-код. Тестирование на PDF размером 45 КБ показало среднее время подписания 164,0 мс и вставки QR-кода 7,1 мс (Hidayat и др., 2025, с. 1). Работа Nasereddin и Salem (2024) исследует интеграцию цифровых подписей в печатные документы (Nasereddin и Salem, 2024, с. 45) с созданием уникального хеша содержимого, шифруемого паролем пользователя. Исследование Suhardi (2024) реализует на PHP/MySQL метод DSA для аутентификации студенческих документов (Suhardi, 2024, с. 23).

В сфере безопасности QR-кодов исследование El-Taj с коллегами (2026) «QRify Secure» отмечает, что инциденты с QR-фишингом выросли на 433% между 2021 и 2023 годами, а существующие стратегии защиты остаются фрагментированными: решения, ориентированные на шифрование, обеспечивают конфиденциальность без верификации подлинности; сканеры предлагают проверку репутации URL, которая не работает против zero-day угроз (Vanuatu Maritime Services, 2025). Исследование предлагает систему с backend-генерацией, RSA-криптографией и серверной валидацией с контролем одноразового использования.

Выявление научной ниши

Проведенный анализ позволяет сделать важный вывод: существующие работы можно классифицировать следующим образом:

1. **Доменно-специфичные решения**: академические дипломы (Cardenas Quispe, Hidayat, Blockcredit), нотариальные документы (ФНП), таможенные документы (ValidAP), справочные документы (Vanuatu Maritime Services, 2025; Project ValidAP, 2025; Ndiramiye и др., 2026, с. 342; Federal Notary Chamber of the Russian Federation, 2026, с. 12; Hidayat и др., 2025, с. 2). В каждом вышеперечисленном решении имеется привязаность к конкретному типу документов и не обладает универсальностью.
2. **Технические реализации**: основана на криптографических алгоритмах (RSA, SHA, DSA), времени генерации и верификации, но без исследования юридической значимости результатов.
3. **Блокчейн-ориентированные подходы:** использование распределенных реестров для **хранения** хешей, что обеспечивает неизменность, но создает избыточную сложность для корпоративного ЭДО.
4. **Решения для верификации при выпуске**: все существующие системы **предполагают**, что документ регистрируется в момент создания (в блокчейне, централизованной БД и т.д.).

Что не сделано (научная ниша):

• Ни одно исследование не рассматривает проблему **верификации документов, уже покинувших защищенный контур ЭДО**, как самостоятельную научную задачу (Vanuatu Maritime Services, 2025; Project ValidAP, 2025; Ndiramiye и др., 2026, с. 342; Federal Notary Chamber of the Russian Federation, 2026, с. 12; Hidayat и др., 2025, с. 2, Асилбеков и Орозов, 2025, с. 153).

• Нет работ, предлагающих **гибридную модель** (локальная проверка по QR + удаленная через API) для баланса между скоростью/офлайн-доступом и полнотой данных.

• Нет концепции **«верификационного моста»** между закрытым контуром ЭДО и внешней средой, не требующей изменения архитектуры существующих систем.

• Нет исследований по **контекстно-зависимому доступу** при верификации (разный объем данных для разных категорий проверяющих).

• **Юридическая значимость** результатов верификации не исследована ни в одной работе — все ограничиваются технической реализацией.

• Нет **универсального решения** для любый документов ЭДО - все существующие работы привязаны к конкретному домену.

Данное исследование закрывает выявленный пробелы и предлогается метод который позволяет верифицировать документы вне внутри самой системы ЭДО тоесть за пределами, без изменения архитектуры самой системы и без требования предварительной регистрации.

Научная проблема и гипотеза исследования

Научная проблема заключается в отсутствии формализованных методов и архитектурных решений, обеспечивающих криптографически связи как доказательство между электронным оригиналом документа и его представлением за пределами системы ЭДО. Существующие подходы либо требуют полного раскрытия содержимого закрытого контура (предоставление доступа к API системы ЭДО), либо полагаются на человеческий фактор при заверении копий.

Цель и задачи исследования

Целью данного исследования – это разработка и обоснование метода криптографической верификации, то есть подлинности электронных документов за пределами самой системы ЭДО где основную роль будут выполнять динамические QR-коды. Также с она должна быть адаптируема под различные правовые режимы и не требовать изменения архитектуры существующих систем ЭДО.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Провести сравнительный анализ международных правовых режимов электронной подписи (eIDAS в ЕС, ESIGN в США, UNCITRAL Model Law, законодательство КНР) и существующих технических подходов к верификации документов вне ЭДО.

2. Выявить требования к криптографической защите и форматам данных для обеспечения юридической значимости верификации в различных юрисдикциях.

3. Разработать архитектуру гибридной модели верификации, сочетающей «легкую» проверку через QR-код и «полную» проверку через защищенный API.

4. Предложить метод динамического формирования содержимого QR-кода с учетом контекста запроса и прав доступа.

5. Экспериментально апробировать разработанный метод на базе действующей системы ЭДО и оценить его эффективность в сравнении с существующими подходами.

Научная новизна и практическая значимость.

Научная новизна исследования заключается в следующем:

1. ***Концептуальная новизна:*** впервые предложена и формализована задача создания «верификационного моста» между закрытым контуром ЭДО и внешней средой как самостоятельная научная проблема, отличная от задачи верификации документов при выпуске.

2. ***Архитектурная новизна:*** разработана гибридная модель верификации, сочетающая локальный уровень (криптографически защищенный QR-код с хешем документа, меткой времени и подписью) и удаленный уровень (API верификации с полными данными), что не представлено в существующих работах, ориентированных либо на чисто локальное, либо на чисто серверное хранение.

3. ***Методологическая новизна:*** предложен метод контекстно-зависимого отображения информации при верификации, дифференцирующий объем раскрываемых данных в зависимости от прав доступа запрашивающей стороны (анонимный пользователь, авторизованный контрагент, контролирующий орган).

4. ***Прикладная новизна:*** впервые исследована возможность придания юридической значимости результатам верификации документов вне ЭДО без изменения архитектуры существующих систем, с учетом различных международных правовых режимов.

Практическая значимость работы определяется возможностью непосредственного внедрения ***разработанного*** метода в существующие системы электронного документооборота, что позволит:

- Обеспечить юридически значимое взаимодействие с контрагентами, не подключенными к ЭДО;
- Сократить издержки на заверение копий и архивное хранение;
- Создать единое пространство доверия к документам независимо от формы их представления;
- Противодействовать росту числа поддельных документов, создаваемых с использованием генеративных моделей;
- Обеспечить кросс-бордер верификацию документов в различных юрисдикциях.

Теоретические основы и анализ существующих подходов

Международные правовые режимы электронной подписи

Для разработки метода необходимо рассмотреть все различии в правовых режимах электронной подписи. Регламент Европейского Парламента и Совета № 910/2014 (eIDAS) (European Parliament and Council, 2014, с. 80) устанавливает три уровня электронных подписей: простая, усиленная и квалифицированная. В США федеральный закон ESIGN

(Electronic Signatures in Global and National Commerce Act) и Единый закон об электронных транзакциях (UETA), говорится что электронная подпись не может быть лишена юридической силы если она в электронной форме. В отличие от европейского подхода, американское законодательство не создает иерархию видов электронных подписей, а основывается на технологической нейтральности (United States Congress, 2000).

Китай: Закон об электронной подписи. Закон КНР об электронной подписи 2004 года (с изменениями) устанавливает три категории: надежная электронная подпись, обычная электронная подпись и электронная подпись, требующая подтверждения. Надежная электронная подпись требует, чтобы ключ подписи принадлежал исключительно подписывающему лицу и мог однозначно идентифицировать подписанта (National People's Congress of China, 2004). **UNCITRAL Model Law on Electronic Signatures**. Типовой закон ЮНСИТРАЛ об электронных подписях (2001) устанавливает международные стандарты для признания электронных подписей и служит основой для национальных законодательств многих стран, особенно развивающихся (United Nations Commission on International Trade Law, 2001, с. 22).

Ключевой проблемой для кросс-бордер верификации остается взаимное признание электронных подписей. Как отмечается в исследовании Chotikakamthorn (2024), существующие методы верификации часто несовместимы со стандартами W3C Verifiable Credentials, что создает дополнительные барьеры (World Wide Web Consortium, 2023).

Криптографические основы верификации документов. Хеширование документов. Криптографические хеш-функции (SHA-256, SHA-3) создают уникальный «цифровой отпечаток» документа фиксированной длины. Любое изменение документа, даже изменение одного бита, приводит к полному изменению хеша. Это свойство делает хеширование фундаментом для проверки целостности документа. **Электронная подпись**. Цифровая подпись, создаваемая с использованием закрытого ключа подписанта и проверяемая с использованием открытого ключа, обеспечивает аутентификацию (подтверждение авторства) и неотказуемость (невозможность отказа от подписи). В международной практике распространены алгоритмы RSA, ECDSA, EdDSA. В российском контексте применяется ГОСТ Р 34.10-2012.

QR-коды как носители криптографических данных. Технология QR-кодов, разработанная в 1994 году Масахиро Хара из Denso Wave, предоставляет удобный механизм кодирования двоичных данных для печати и последующего считывания камерами мобильных устройств (Denso Wave Incorporated, 1994). QR-коды используют коррекцию ошибок Рида-Соломона на четырех уровнях, что позволяет восстанавливать данные при частичном повреждении изображения. Максимальная емкость QR-кода версии 40 позволяет хранить до 2953 байт двоичных данных (International Organization for Standardization, 2015).

Однако важно понимать, что QR-коды как стандарт кодирования не включают механизмов шифрования или цифровой подписи — они лишь предоставляют контейнер для данных. В безопасных приложениях payload шифруется или подписывается до генерации QR-кода, а после сканирования и декодирования происходит расшифровка или проверка подписи (El-Taj и др., 2026, с. 3; Jacob, 2026).

Классификация существующих подходов к верификации. На основе проведенного анализа можно выделить следующие подходы к верификации документов:

По месту хранения верификационных данных.

Локальное хранение: все данные для верификации хранятся непосредственно в QR-коде. В исследование Hidayat (2025), где хеш документа и подпись кодируются в QR-коде на дипломе (Hidayat и др., 2025, с. 2), рассматривается возможность офлайн-проверки тоесть отсутствиуют зависимости от сервера и в то же время это является недостатком тоесть ограниченный объем данных, невозможность обновления статуса документа (отзыв, аннулирование).

Централизованное хранение: в QR-коде хранится только идентификатор документа, а полные данные и статус проверяются через централизованный API или веб-портал. Пример: сервис Федеральной нотариальной палаты РФ (Federal Notary Chamber of the Russian Federation, 2026, с. 12). Преимущества: актуальная информация о статусе, неограниченный объем данных. Недостатки: зависимость от доступности сервера, необходимость онлайн-соединения.

Распределенное хранение (блокчейн): хеши документов хранятся в распределенном реестре. Примеры: ValidAP, Blockcredit, исследование Cardenas Quispe (2025). Преимущества: децентрализация, неизменность, независимость от одного провайдера. Недостатки: сложность инфраструктуры, затраты на транзакции, вопросы масштабирования.

По области применения.

- **Академические документы**: дипломы, сертификаты, транскрипты (большинство исследований).
- **Нотариальные документы**: сервис ФНП РФ.
- **Торговые/таможенные документы**: ValidAP (Гонконг).
- **Товарная верификация**: системы проверки подлинности продукции с использованием блокчейна (Kumar и др., 2025, с. 115).
- **Универсальные решения**: отсутствуют.

По криптографическому подходу.

- **Простое хеширование**: проверка целостности без аутентификации.
- **Цифровая подпись**: асимметричная криптография для аутентификации и неотказуемости.
- **Блокчейн и цифровая подпись**: комбинированный подход.

Проблема подделки документов в цифровую эпоху. В исследовании El-Taj (2026) указано что инциденты с QR-фишингом выросли на 433% между 2021 и 2023 годами (El-Taj et al., 2026, с. 3). С развитием генеративных моделей (deepfake) появляется новый класс угроз – создание поддельных документов эти документы визуально не отличимы от оригинала. В исследованиях указана что традиционный метод защиты, который основывается на метаданных уже не работает потому что водяные знаки можно скопировать с оригинала на копию (Gao и др., 2025, с. 5).

В сфере академических документов основная проблема — это поддельные дипломы, которые имеют глобальный характер. Carmichael и Eaton (2023) в своем исследовании

подчеркивают, что международные синдикаты и «фабрики дипломов» производят поддельные сертификаты в промышленных масштабах (Carmichael и Eaton, 2023, с. 250).

Выводы и обоснование необходимости нового подхода

Проведенный анализ позволяет сделать следующие выводы:

1. **Проблема носит глобальный характер**, но существующие решения фрагментированы по доменам и юрисдикциям.

2. **Все существующие решения ориентированы на верификацию при выпуске** документа (регистрация в блокчейне, централизованной БД и т.д.). Задача верификации документов, **уже покинувших закрытый контур ЭДО**, не рассматривается как самостоятельная.

3. **Отсутствует гибридный подход**, сочетающий преимущества локального хранения (скорость, офлайн-доступ) и удаленного доступа (актуальный статус, полнота данных).

4. **Не исследован контекстно-зависимый доступ** при верификации — возможность предоставления разного объема информации разным категориям проверяющих.

5. **Юридическая значимость** результатов верификации документов вне ЭДО не исследована в технических работах.

Таким образом, существует четкая научная ниша для разработки метода, который:

- Создает «верификационный мост» между закрытым контуром ЭДО и внешней средой;
- Не требует изменения архитектуры существующих систем ЭДО;
- Обеспечивает криптографическую доказуемость подлинности;
- Адаптируется под различные правовые режимы;
- Предоставляет дифференцированный доступ к информации.

Разработка метода криптографической верификации с использованием динамических QR-кодов

Требования к разрабатываемому методу. На основе проведенного анализа сформулируем требования к системе верификации документов за пределами ЭДО:

1. **Криптографическая доказуемость**. Система должна обеспечивать возможность криптографической проверки подлинности документа без необходимости доступа к исходному файлу электронной подписи.

2. **Динамичность**. Информация о статусе документа (действителен, отозван, изменен) должна обновляться в реальном времени.

3. **Дифференцированный доступ**. Объем раскрываемой информации должен зависеть от прав доступа запрашивающей стороны.

4. **Устойчивость к подделке**. Механизм должен исключать возможность создания поддельных QR-кодов, имитирующих подлинные документы.

5. **Юридическая значимость**. Результат верификации должен быть приемлем в качестве доказательства в различных юрисдикциях.

6. **Неинтрузивность**. Метод не должен требовать изменения архитектуры существующих систем ЭДО.

7. **Масштабируемость**. Решение должно работать с произвольным объемом документов без деградации производительности.

8. **Интероперабельность**. Система должна быть совместима с международными стандартами (ISO/IEC 18013-5, W3C Verifiable Credentials, PAdES) (United States Congress, 2000; International Organization for Standardization, 2023; European Telecommunications Standards Institute, 2023).

Архитектура гибридной модели верификации. Предлагаемая архитектура гибридной модели верификации базируется на разделении верификационных данных на два уровня: локальный (кодируемый непосредственно в QR-коде) и удаленный (доступный через защищенный API).

Структура данных локального уровня (QR-код). Базовый набор данных, включаемый в QR-код при генерации:


```
{
 "schema_version": "1.0",
 "document_id": "550e8400-e29b-41d4-a716-446655440000",
 "hash_algorithm": "SHA-256",
 "document_hash": "3a7bd3e2360a3d29eea436fcfb7e44c735d117c42d1c1835420b6b9942dd4f1b",
 "timestamp": "2026-03-15T14:30:00Z",
 "issuer": {
  "id": "mir.titan.90@organization.com",
  "name": "Organization Name",
  "jurisdiction": "RU"
 },
 "signer_info": {
  "id": "signer@organization.com",
  "cert_thumbprint": "a1b2c3d4e5f6..."
 },
 "access_policy": {
  "anonymous": ["status", "issuer", "timestamp"],
  "authenticated": ["metadata", "document_type"],
  "trusted": ["full_document"]
 },
 "signature": "MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC..."
}
```


Критически важным является включение цифровой подписи самого QR-кода, формируемой с использованием ключа системы ЭДО. Это исключает возможность создания поддельных QR-кодов, имитирующих подлинные документы. Размер данных в типичной конфигурации составляет 350-400 символов (после base64-кодирования подписи), что

позволяет использовать QR-коды версии 3 (29×29 модулей), читаемые большинством мобильных устройств.

Структура удаленного уровня (API верификации)

API верификации предоставляет расширенную информацию о документе в зависимости от прав доступа:

Эндпоинт: `POST /api/verify/{document_id}`

Запрос (анонимный):


```
{
  "access_level": "anonymous",
  "document_hash": "3a7bd3e2360a3d29eea436fcfb7e44c735d117c42d1c1835420b6b9942dd4f1b"
}
```


Ответ (анонимный):


```
{
  "status": "valid",
  "verification": {
    "timestamp": "2026-03-15T14:35:00Z",
    "integrity_check": "passed"
  },
  "document": {
    "issuer": "Organization Name",
    "issuance_date": "2026-03-15",
    "document_type": "contract",
    "signer": "signer@organization.com"
  }
}
```


Запрос (авторизованный контрагент):


```
{
  "access_level": "authenticated",
  "document_hash": "3a7bd3e2360a3d29eea436fcfb7e44c735d117c42d1c1835420b6b9942dd4f1b",
  "auth_token": "eyJhbGciOiJIUzI1NiIs..."
}
```


Ответ (авторизованный) — дополняет анонимный ответ:


```
{
  "document": {
    "metadata": {
      "parties": ["Name", "User name"],
      "contract_number": "DOC-2026-001",
      "…": …,
      "..": "…"
```

```
   }
  }
}
```


Запрос (доверенный проверяющий):


```
{
  "access_level": "trusted",
  "document_hash": "3a7bd3e2360a3d29eea436fcfb7e44c735d117c42d1c1835420b6b9942dd4f1b",
  "auth_token": "trusted_authority_token",
  "request_reason": "judicial_request",
  "case_number": "A40-12345/2026"
}
```


Ответ (доверенный):


```
{
  "document": {
    "full_document_url": "https://api.edo.kg/documents/550e8400.../download",
    "original_signature": "https://api.edo.kg/signatures/550e8400...",
    "certificate_chain": [...],
    "audit_log": [...]
  }
}
```


Протокол взаимодействия с API верификации

Протокол взаимодействия включает следующие этапы:

Этап 1: Сканирование QR-кода. Пользователь считывает QR-код с распечатанного документа с помощью мобильного приложения или веб-камеры.

Этап 2: Локальная проверка. Приложение проверяет:

- Цифровую подпись QR-кода с использованием публичного ключа системы ЭДО (кэшированного или полученного из доверенного источника);
- Целостность данных (отсутствие повреждений);
- Срок действия (если применимо).

Если локальная проверка успешна, отображается базовая информация: дата подписания, наименование подписанта, статус документа («действителен» согласно данным QR-кода на момент генерации).

Этап 3: Запрос к API (опционально). Для получения актуального статуса или расширенной информации приложение отправляет запрос к API верификации, включая:

- document_id из QR-кода;
- Уровень запрашиваемых прав (анонимный, авторизованный, доверенный);
- При необходимости — учетные данные пользователя.

Этап 4: Проверка прав доступа. Система определяет объем информации, доступной для раскрытия, на основе:

- Политик доступа, указанных в QR-коде (поле access_policy);
- Роли и аутентификации запрашивающей стороны;
- Контекста запроса.

Этап 5: Формирование ответа. API возвращает запрошенную информацию, подписанную ключом системы для обеспечения доказуемости. Ответ включает метку времени для фиксации момента проверки.

Метод контекстно-зависимого отображения информации

Разработан метод контекстно-зависимого отображения информации, основанный на следующих принципах:

Принцип минимальной достаточности. Для анонимных пользователей предоставляется информацию, которая подтверждает, что документ существует и то что он подписан, то есть остальная информации где имеются данные конфиденциального характера он не показывает. Этот принцип согласуется с требованиями GDPR (European Parliament and Council, 2016).

Принцип гранулярного доступа. Предоставление доступа определенным полям в зависимости от прав доступа, например, можно прочитать строки, связанные с суммой договора, а не весь документ. Как отмечается в исследовании по verifiable credentials, такой подход соответствует стандартам W3C и позволяет реализовать selective disclosure (United States Congress, 2000).

Принцип аудируемости. Каждый запрос к API фиксируется в защищенном логе с указанием времени, запрошенных данных и результата предоставления доступа. Это создает возможность для последующего аудита и расследования инцидентов.

Принцип временной привязки. **Со временем с**татус документа может изменяться, то есть в том случаи если договор был расторгнут. Другими словами, из системы можно проверить статус самого документа на промежутке определенного времени.

3.5. Криптографическая защита и обеспечение целостности

Для обеспечения криптографической защиты предлагается использовать следующий стек технологий:

Хеширование (SHA-256) - устойчив к коллизиям, широкая поддержка в программном обеспечении и соответствует международным стандартам.

Электронная подпись. Поддержка нескольких алгоритмов для обеспечения интероперабельности:

- RSA (для совместимости с существующими PKI-инфраструктурами);
- ECDSA (для более высокой производительности);
- ГОСТ Р 34.10-2012 (для российского контекста).

Защита от повторного использования. Каждый QR-код содержит уникальный идентификатор документа и временную метку, что исключает возможность копирования кода с одного документа на другой. Дополнительно может применяться контроль одноразового использования (one-time-use) для особо чувствительных документов, как предложено в исследовании QRify Secure (El-Taj и др., 2026, с. 3).

Долговременное хранение **(Long-term validation).** Для документов длительного - архивного хранения где истекает срока действия сертификатов предусмотрен механизм периодического переподписания хешей документов новыми ключами. Это соответствует требованиям стандартов PAdES (PDF Advanced Electronic Signatures) для долговременного сохранения юридической значимости (European Telecommunications Standards Institute, 2023).

Экспериментальная апробация и оценка эффективности

Разработка прототипа на базе действующей системы ЭДО

Для апробации разработанного метода был создан прототип на базе действующей системы электронного документооборота (Асилбеков и Имаралиев, 2025, с. 112; Бектемир кызы, Исраилова, 2024, с. 167). Система включала следующие компоненты:

Модуль генерации QR-кодов. При генерации PDF документа для каждой страницы генерируется QR-код, содержащий структурированные данные в формате JSON с цифровой подписью.

API верификации. RESTful API предоставляющий методы для проверки статуса документов и получения расширенной информации в зависимости от прав доступа.

Веб-интерфейс проверки. Простая веб-страница, позволяющая загрузить изображение с QR-кодом или ввести идентификатор документа для проверки, с отображением результатов согласно правам доступа.

Мобильное приложение **(тестовая версия)**. Приложение для Android (Dart Flutter), демонстрирующее сценарии использования: сканирование QR-кода, локальную проверку подписи, запрос к API.

Экспериментальные данные и методика тестирования

Экспериментальное тестирование проводилось на выборке из 10 000 документов различных типов, характерных для корпоративного документооборота:

- Приказы (45%)
- Кадровые документы (30%)
- Остальные документы (25%)
- Для каждого документа фиксировались:
- Время генерации QR-кода;
- Размер QR-кода (в символах и версия);
- Время локальной проверки (без обращения к API);
- Время полной проверки через API (с различными уровнями доступа);
- Количество успешных верификаций;
- Результаты тестирования устойчивости к атакам.

Результаты экспериментальной апробации

Производительность генерации

Таблица 1. Производительность генерации

Параметр	Значение	Сравнение с аналогами
Среднее время генерации QR-кода	0,31 сек	Hidayat (2025): 0,164 сек (подпись) + 0,007 сек (QR) (Hidayat и др., 2025, с. 2)
Медианное время генерации	0,28 сек	—
95-й перцентиль	0,42 сек	—
Средний размер данных в QR-коде	372 символа	Версия 3 (29×29), читается всеми устройствами

Время генерации включает: формирование JSON, вычисление хеша документа (SHA-256), создание цифровой подписи, кодирование в QR-код. Полученные результаты сопоставимы с показателями Hidayat (164 мс на подпись + 7,1 мс на QR) и Suhardi (реализация на PHP/MySQL) (Suhardi, 2024, с. 25), что подтверждает приемлемость для production-использования.

Производительность верификации

Таблица 2. Производительность верификации

Тип проверки	Среднее время	Условия
Локальная проверка (без API)	0,12 сек	Только проверка подписи QR, без обращения к серверу
API-проверка (анонимный уровень)	0,53 сек	Включает сетевой запрос, проверку статуса
API-проверка (авторизованный)	0,87 сек	Дополнительно: аутентификация, загрузка метаданных
API-проверка (доверенный)	1,31 сек	Дополнительно: генерация ссылок на полные документы

Для сравнения: в исследовании Cardenas Quispe (2025) регистрация диплома в блокчейне занимала 2,97 сек, а проверка — 0,96 сек (без учета времени на подтверждение в сети) (Cardenas Quispe и Pacheco, 2025, с. 3). Предлагаемый метод обеспечивает более высокую скорость верификации за счет гибридного подхода, не требующего обращения к распределенному реестру для базовых проверок.

Точность верификации. Из 10 000 протестированных документов:

- 9 987 (99,87%) успешно верифицированы с первой попытки;
- 13 (0,13%) потребовали повторной проверки из-за временных сбоев сети;
- Ложных срабатываний (подтверждение подлинности поддельного документа) не зафиксировано.

Показатель точности 99,87% соответствует требованиям к промышленным системам и превышает показатели некоторых блокчейн-решений, где возможны задержки из-за консенсусных механизмов (Cardenas Quispe и Pacheco, 2025, с. 3).

Устойчивость к атакам. В ходе тестирования предпринимались попытки различных видов атак:

Таблица 3. Результаты тестирования атаки

Тип атаки	Метод проверки	Результат
Копирование QR-кода на другой документ	Сравнение хеша документа из QR с реальным хешем	Выявлено (несовпадение хеша)
Модификация данных в QR-коде	Проверка цифровой подписи QR	Выявлено (недействительная подпись)
Повторное использование старого QR-кода после изменения документа	Сравнение хеша с актуальной версией в API	Выявлено (несовпадение хеша)
Подделка ответа API (MITM)	TLS + подпись ответа	Выявлено (недействительная подпись ответа)
Атака на один раз (replay)	Проверка временной метки + опционально one-time-use	Предотвращено (для sensitive-документов)

Система продемонстрировала высокую устойчивость к основным видам атак, что согласуется с требованиями, сформулированными в исследовании QRify Secure для защищенных QR-систем (El-Taj и др., 2026, с. 3).

Сравнительный анализ с существующими подходами.

Таблица 4. Сравнение методов верификации документов вне ЭДО

Критерий	Традиционное заверение копий	Статический QR-код	Блокчейн-решения (ValidAP, Blockcredit)	Предлагаемый метод
Юридическая значимость	Требует заверения	Отсутствует	Для конкретного домена	Частичная + API
Защита от подделки	Подпись + печать	Отсутствует	Криптографическая	Криптографи-ческая
Динамическое обновление статуса	Нет	Нет	Да (через блокчейн)	Да (через API ЭДО)
Дифференцированный доступ	Нет	Нет	Нет	Да
Офлайн-проверка	Да	Да	Нет (требуется доступ к блокчейну)	Частично (локальная)

Критерий	Традиционное заверение копий	Статический QR-код	Блокчейн-решения (ValidAP, Blockcredit)	Предлагаемый метод
Интероперабельность	Нет	Нет	Ограниченная	Высокая (гибкие алгоритмы)
Интеграция с существующим ЭДО	Ручная	Автоматическая	Требует регистрации	Без изменения архитектуры

Как видно из сравнения, предлагаемый метод сочетает преимущества криптографической защиты с возможностью дифференцированного доступа и частичной офлайн-проверки, что выгодно отличает его от существующих решений и закрывает выявленную научную нишу.

Обсуждение результатов и перспективы развития

Интерпретация полученных результатов. Полученные результаты подтверждают выдвинутую гипотезу о возможности создания криптографического «моста» между защищенным контуром ЭДО и внешней средой с использованием динамических QR-кодов. Разработанный метод обеспечивает:

1. **Доказуемую подлинность**. Цифровая подпись QR-кода и возможность проверки через API исключают подделку документов, что соответствует требованиям, предъявляемым к защищенным QR-системам в исследовании El-Taj (2026) (El-Taj и др., 2026, с. 3).

2. **Гибридную архитектуру**. Сочетание локального и удаленного уровней позволяет обеспечить баланс между скоростью/доступностью офлайн и полнотой/актуальностью данных онлайн.

3. **Дифференцированный доступ**. Возможность раскрывать разный объем информации разным категориям проверяющих соответствует принципам selective disclosure, реализованным в стандартах W3C Verifiable Credentials (World Wide Web Consortium, 2023).

4. **Неинтрузивность**. Метод не требует изменения архитектуры существующих систем ЭДО, что критически важно для практического внедрения.

Сравнение с теоретическими ожиданиями. Экспериментальные результаты в целом соответствуют теоретическим ожиданиям. Некоторые расхождения требуют обсуждения:

- **Время генерации QR-кода** (0,31 сек) оказалось несколько выше, чем сумма времени подписания и вставки QR в исследовании Hidayat (0,171 сек) (Hidayat и др., 2025, с. 2). Это объясняется дополнительными операциями: формированием структурированного JSON, включением метаданных и политик доступа.

- **Время API-проверки** (0,53–1,31 сек) существенно ниже времени регистрации в блокчейн-решениях (2,97 сек в Cardenas Quispe (Cardenas Quispe и Pacheco, 2025, с. 3)), что подтверждает преимущества гибридного подхода для задач оперативной верификации.

- **Точность верификации** (99,87%) соответствует ожидаемой для криптографических систем и превышает показатели систем, полагающихся только на централизованные реестры, подверженные сбоям.

Ограничения исследования. Проведенное исследование имеет ряд ограничений, которые следует учитывать при интерпретации результатов и планировании дальнейших работ:

Технические ограничения:

- Зависимость от доступности API для полной верификации (офлайн-проверка дает только базовую информацию);
- Отсутствие встроенных механизмов для документов с ограниченным сроком действия;
- Необходимость управления ключами для подписи QR-кодов.

Юридические ограничения:

- Отсутствие устоявшейся судебной практики по признанию результатов такой верификации в различных юрисдикциях;
- Различия в законодательстве разных стран относительно признания электронных доказательств;
- Вопросы признания результатов проверки при ликвидации организации-эмитента.

Масштабируемость:

- Тестирование проводилось на выборке 10 000 документов; для систем с миллионами документов требуется дополнительная валидация.

Направления дальнейших исследований. Выявленные ограничения открывают перспективы для дальнейших исследований:

1. Интеграция с технологией распределенного реестра (блокчейн).

Децентрализованное хранение хешей документов позволит обеспечить верификацию даже в случае недоступности API системы ЭДО или ликвидации организации. Как показано в исследованиях ValidAP (Hong Kong Customs and Excise Department, 2026), Blockcredit (Ndiramiye и др., 2026) и Cardenas Quispe (Cardenas Quispe и Pacheco, 2025, с. 3), блокчейн обеспечивает неизменность и децентрализацию. Возможна гибридная архитектура, где «легкая» верификация выполняется через QR/API, а для арбитража и долговременного хранения используются распределенные реестры (Government Technology Agency of Singapore, 2023).

2. Использование технологий с нулевым разглашением (Zero-Knowledge Proofs).

Развитие идей, заложенных в проекте zkPDF (Privacy и Scaling Explorations, 2025), для создания доказательств с полным сохранением конфиденциальности. Это позволит, например, подтвердить наличие определенной суммы в договоре или факт подписания документа конкретным лицом без раскрытия остальных данных.

3. Интеграция с постквантовой криптографией.

С учетом развития квантовых вычислений и угрозы «собери сейчас, расшифруй потом», актуальным направлением является адаптация метода для использования постквантовых алгоритмов, устойчивых к атакам с использованием квантовых компьютеров. Исследования в области цифрового копирайта уже рассматривают возможность интеграции постквантовой криптографии (Gao и др., 2025, p. 5).

4. Автоматическая классификация документов по уровню чувствительности.

Разработка ML-моделей для определения необходимого уровня защиты в зависимости от содержимого документа и автоматической настройки политик доступа в поле access_policy.

5. Исследование юридической значимости в различных юрисдикциях.

Проведение комплексного юридического анализа признания результатов верификации в качестве доказательств в судах различных стран, а также разработка рекомендаций по нормативному закреплению статуса таких верифицированных копий.

6. Масштабирование и оптимизация производительности.

Исследование поведения системы при нагрузке в миллионы документов, оптимизация времени ответа API, внедрение кэширования и CDN для публичных запросов.

6.1. Рекомендации по практическому внедрению. Для организаций, планирующих внедрение подобных систем, можно сформулировать следующие рекомендации:

Начинать с пилотного проекта. Ограничить внедрение одним типом документов (например, счетами или договорами) для отработки технологии и процедур.

Обеспечить юридическое сопровождение. Разработать локальные нормативные акты, регламентирующие статус распечатанных копий с QR-кодами, и согласовать порядок их признания с ключевыми контрагентами.

Обеспечить интероперабельность. Использовать гибкие алгоритмы подписи и форматы данных, допускающие адаптацию под различные юрисдикции.

Внедрить многоуровневую систему доступа. Четко определить категории проверяющих и соответствующие объемы раскрываемой информации.

Обеспечить резервирование. Предусмотреть альтернативные каналы верификации на случай технических сбоев.

Вести мониторинг юридической практики. Отслеживать решения судов относительно признания результатов подобной верификации для своевременной корректировки подходов.

Заключение

В настоящем исследовании разработан и обоснован метод криптографической верификации подлинности электронных документов за пределами системы документооборота с использованием динамических QR-кодов. Основные научные и практические результаты работы заключаются в следующем:

1. Проведен комплексный анализ международных правовых режимов электронной подписи (eIDAS в ЕС, ESIGN в США, UNCITRAL Model Law) и существующих технических подходов к верификации документов. Выявлено фундаментальное противоречие между юридическим статусом электронного оригинала и его физических копий, сохраняющееся во всех юрисдикциях.

2. На основе систематического анализа существующих исследований (Cardenas Quispe, 2025; Hidayat, 2025; El-Taj, 2026; ValidAP, 2026; Blockcredit, 2026) установлено, что ни одно

из существующих решений не рассматривает задачу создания «верификационного моста» между закрытым контуром ЭДО и внешней средой как самостоятельную проблему. Все существующие работы ориентированы на верификацию при выпуске документа и привязаны к конкретным доменам (академические дипломы, нотариат, таможня).

3. Впервые предложена концепция «верификационного моста», рассматривающая QR-код как динамический интерфейс для криптографической доказуемости подлинности документов, покинувших защищенный контур ЭДО. Разработана гибридная модель хранения верификационных данных, сочетающая локальный уровень (хеш документа SHA-256, метка времени, идентификатор подписанта, цифровая подпись QR-кода) и удаленный уровень (полные данные через защищенный API).

4. Разработан метод контекстно-зависимого отображения информации, дифференцирующий объем раскрываемых данных в зависимости от прав доступа запрашивающей стороны. Это позволяет соблюсти баланс между открытостью информации и защитой конфиденциальных данных, а также соответствует принципам selective disclosure, реализованным в стандартах W3C Verifiable Credentials (World Wide Web Consortium, 2023).

5. Экспериментальная апробация на базе действующей системы ЭДО (Laravel) на выборке из 10 000 документов подтвердила эффективность предложенного метода: время генерации QR-кода составляет 0,31 сек, время локальной проверки — 0,12 сек, время API-проверки — от 0,53 до 1,31 сек в зависимости от уровня доступа, точность верификации — 99,87% при отсутствии ложных срабатываний. Метод продемонстрировал устойчивость к основным видам атак (копирование, модификация, повторное использование).

6. Проведен сравнительный анализ разработанного метода с существующими подходами, показавший преимущества предлагаемого решения: сочетание офлайн- и онлайн-проверок, дифференцированный доступ, неинтрузивность по отношению к существующим системам ЭДО, интероперабельность с различными юрисдикциями.

7. Определены направления дальнейших исследований, включая интеграцию с технологией блокчейн, использование постквантовой криптографии, применение методов с нулевым разглашением, разработку автоматизированных систем классификации документов по уровню чувствительности и исследование юридической значимости результатов верификации в различных правовых системах.

Практическая значимость работы подтверждается возможностью непосредственного внедрения разработанного метода в существующие системы электронного документооборота, что позволит:

- Обеспечить юридически значимое взаимодействие с контрагентами, не подключенными к ЭДО;
- Сократить издержки на заверение копий и архивное хранение;
- Создать единое пространство доверия к документам независимо от формы их представления;
- Противодействовать росту числа поддельных документов, создаваемых с использованием генеративных моделей.

Таким образом, цель исследования достигнута, поставленные задачи решены в полном объеме. Разработанный метод закрывает выявленную научную нишу и может быть рекомендован к внедрению в корпоративных информационных системах и системах электронного документооборота различных юрисдикций.

Список литературы

1. Асилбеков, Т.М., Имаралиев, О.Р. (2025). Электронный документооборот в высших учебных заведениях кыргызской республики: современное состояние и перспективы развития. *Вестник Ошского государственного университета,* (2), 109–121. https://doi.org/10.52754/16948610_2025_2_10
2. Асилбеков, Т.М., Орозов, М.О., (2025). Веб-сервис автоматизированной выдачи цифровых документов в образовательном учреждении ОшГУ. *Евразийский Журнал Научных и Мультидисциплинарных Исследований,* 2, 149-160.
3. Бектемир кызы, Б., Исмаилова, Р. (2024). Систематический обзор литературы технологий блокчейн в системах документооборота. *Вестник Ошского государственного университета*, (4), 164–177. https://doi.org/10.52754/16948610_2024_4_17
4. Cardenas Quispe, M.A. & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. *Scientific Reports,* 15, 9281
5. Carmichael, J.J. & Eaton, S.E. (2023). Fake Degrees and Fraudulent Credentials in Higher Education: Conclusions and Future Directions. In: Eaton, S.E., Carmichael, J.J. & Pethrick, H. (eds.) Fake Degrees and Fraudulent Credentials in Higher Education. *Ethics and Integrity in Educational Contexts*, vol. 5. Cham: Springer, pp. 245-267.
6. Chotikakamthorn, N., Mi San, A. & Sathitwiriyawong, C. (2024). On-Chain Verifiable Credential with Applications in Education. *ECTI-CIT Transactions,* 18(3), pp. 342-355.
7. *Denso Wave Incorporated.* (1994). QR Code Standardization and Development History. Kariya: Denso Wave Technical Report. Available at: https://www.qrcode.com/en/history/ (Дата обращения: 13.05.2026).
8. El-Taj, H., Al-Gafri, M., Al-Sousi, D. & Bin Homran, R. (2026). QRify Secure: A Comprehensive Secure QR System Integrating Backend-Driven Code Generation, RSA Public-Key Cryptography, and Server-Side Validation with One-Time-Use Controls. *Journal of International Research for Engineering and Management (JOIREM),* 4(1), pp. 1-7.
9. European Parliament and Council. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). *Official Journal of the European Union,* L 257, pp. 73-114.
10. European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union,* L 119, pp. 1-88.

11. *European Telecommunications Standards Institute* (ETSI). (2023). ETSI TS 102 778 V1.2.1: PDF Advanced Electronic Signatures (PAdES). Sophia Antipolis: ETSI.
12. *Federal Notary Chamber of the Russian Federation.* (2026). Annual Report on Digital Notary Services 2021-2026. Moscow: FNC Publishing.
13. Gao, Y., Chen, L., Wang, X. & Zhang, J. (2025). AI-Enhanced Perceptual Hashing with Blockchain for Secure and Transparent Digital Copyright Management. *Cryptography*, 10(1), 2.
14. *Government Technology Agency of Singapore* (GovTech). (2023). OpenAttestation: Document Endorsement and Verification Framework. Singapore: GovTech.
15. Hidayat, A.N., Zainudin, A. & Yuliana, M. (2025). Implementation of Digital Signatures and QR Codes for the Verification of Certificates of Authenticity for Diplomas. 2025 *International Electronics Symposium (IES)*, Surabaya, Indonesia, 5-7 August, pp. 1-6.
16. *Hong Kong Customs and Excise Department* (2026). Project ValidAP: A Blockchain-Based Document Validation Platform. WCO News, Issue 1-2026, pp. 24-27.
17. *International Organization for Standardization.* (2015). ISO/IEC 18004:2015 Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification. Geneva: ISO.
18. *International Organization for Standardization.* (2023). ISO/IEC 18013-5:2023 Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application. Geneva: ISO.
19. Jacob, C. (2026). *QPI – QR-Pixel Imaging: Turning QR Codes into Offline, Verifiable Image Files.* DEV Community.
20. Kumar, A., Singh, R., Sharma, V. & Gupta, P. (2025). A Novel Strategy for Product Verification via Decentralized Blockchain Networks. *2025 IEEE International Conference on Blockchain*, Copenhagen, Denmark, 22-25 July, pp. 112-119.
21. *MarketsandMarkets* (2025). Digital Signature Market by Component, Solution, Deployment Mode, Organization Size, Vertical and Region — Global Forecast to 2030. MarketsandMarkets Research Private Limited.
22. Nasereddin, J. & Salem, A.A. (2024). Enhancing Printed Document Security with QR Code-Based Digital Signatures. *International Journal of Information Security Research,* 14(2), pp. 45-58.
23. *National People's Congress of China.* (2004). Electronic Signature Law of the People's Republic of China (amended 2019). Beijing: National People's Congress Publishing.
24. Ndiramiye, N.P., Mutabazi, E., Uwimana, C. Habimana, J. (2026). Blockcredit: Blockchain-Based Platform for Tamper-Proof Digital Academic Certificates. *Proceedings of the 2026 Africa Digital Week Conference,* Kigali, Rwanda, 15-17 March, pp. 112-121.
25. *Privacy & Scaling Explorations (PSE).* (2025). zkPDF: Unlocking Verifiable Data in the World's Most Popular Document Format. Ethereum Foundation. Available at: https://pse.dev/blog/zkpdf-unlocking-verifiable-data (Дата обращения: 13.05.2026).

26. Suhardi, S. (2024). Use of QRCode and Digital Signature Using The DSA Method to Authenticate Student Academic Documents. *Journal of Applied Computer Science and Technology*, 5(1), pp. 23-31.

27. *United Nations Commission on International Trade Law (UNCITRAL).* (2001). UNCITRAL Model Law on Electronic Signatures with Guide to Enactment. Vienna: United Nations Publications.

28. *United States Congress.* (2000). Electronic Signatures in Global and National Commerce Act (ESIGN). Public Law 106-229, 114 Stat. 464. 106th Congress.

29. *Vanuatu Maritime Services* (2025). Maritime Certificates Verification System: Annual Report 2025.

30. *W3C (World Wide Web Consortium).* (2023). Verifiable Credentials Data Model v2.0. W3C Working Draft. Edited by Sporny, M., Longley, D. & Chadwick, D. Available at: https://www.w3.org/TR/vc-data-model-2.0/ (Дата обращения: 13.05.2026).