UDK 004.4:005.92:005.5

Khoshaba O.M.

Tsuhel R.S.

DESIGN OF AN ELECTRONIC DOCUMENT MANAGEMENT SYSTEM WITH CONFIGURABLE APPROVAL ROUTING AND ASSIGNMENT DEADLINE CONTROL FOR IT COMPANIES

Vinnitsia National Technical University

Анотація.

Компанії інформаційних технологій часто обробляють критично важливі для операційної діяльності документи через засоби електронної пошти та обміну повідомленнями, що послаблює відстежуваність, цілісність версій та підзвітність у ланцюгах затвердження та виконання. У цій статті представлено концепцію розробки системи електронного документообігу (СЕД), яка підтримує реєстрацію та зберігання документів, налаштовувану маршрутизацію затверджень (робочі процеси віз), призначення відповідальних осіб та систематичний контроль термінів виконання за допомогою нагадувань та ескалацій. Рішення реалізовано як веб-система клієнт-сервер з інтерфейсом прикладного програмування (API) для передачі репрезентативного стану (REST) через протокол передачі гіпертексту (HTTP), використовуючи стандартизовані відповіді на помилки на основі деталей проблеми Request for Comments (RFC) 9457. Безпека та управління враховуються шляхом узгодження зі стандартами Міжнародної організації зі стандартизації / Міжнародної електротехнічної комісії (ISO/IEC) 27001:2022 та ISO/IEC 27002:2022, доповненими Open Worldwide Application Security Project (OWASP) Top 10:2021 та спеціальною публікацією (SP) 800-218 Secure Software Development Framework (SSDF) Національного інституту стандартів і технологій (NIST). Для забезпечення підзвітності та зменшення несанкціонованих дій пропонуються контроль доступу на основі ролей (RBAC), шифрування під час передачі за допомогою Transport Layer Security (TLS) та ведення журналу аудиту з захистом від несанкціонованого втручання. Там, де потрібні юридично значущі погодження, електронні підписи можуть бути підтримані за допомогою підходів інфраструктури відкритих ключів (PKI), узгоджених зі стандартом EN 319 102-1 Європейського інституту телекомунікаційних стандартів (ETSI). Якість даних забезпечується за допомогою схем метаданих та правил перевірки, що відповідають стандарту ISO 8000-1:2022, тоді як цільові показники доступності відповідають Керівним принципам доступності веб-контенту (WCAG) 2.2 Консорціуму Всесвітньої павутини (W3C). Оскільки емпіричні показники розгортання ще недоступні, у статті визначено план оцінювання, що охоплює показники функціональної повноти, надійності, продуктивності та управління, такі як час циклу, коефіцієнт прострочення та частота повторної роботи.

Ключові слова: *система електронного управління документами, електронне управління записами, маршрутизація затверджень, управління робочим процесом, контроль виконання завдань, моніторинг термінів, журнал аудиту, контроль доступу на основі ролей, безпечна розробка програмного забезпечення, веб-API, якість даних, доступність.*

Abstract.

Information technology companies frequently handle operationally critical documents through email and messaging tools, which weakens traceability, version integrity and accountability across approval and execution chains. This paper presents the design concept of an Electronic Document Management System (EDMS) that supports document registration and storage, configurable approval routing (visa workflows), assignment of responsible persons, and systematic control of execution deadlines with reminders and escalations. The solution is implemented as a web-based client–server system with a Representational State Transfer (REST) Application Programming Interface (API) over the Hypertext Transfer Protocol (HTTP), using standardised error responses based on Request for Comments (RFC) 9457 problem details. Security and governance are addressed through alignment with International Organisation for Standardisation / International Electrotechnical Commission (ISO/IEC) 27001:2022 and ISO/IEC 27002:2022, supplemented by the Open Worldwide Application Security Project (OWASP) Top 10:2021 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-218 Secure Software Development Framework (SSDF). Role-Based Access Control (RBAC), encryption in transit via Transport Layer Security (TLS), and tamper-evident audit logging are proposed to ensure accountability and reduce unauthorised actions. Where legally meaningful approvals are required, electronic signatures can be supported using Public Key Infrastructure (PKI) approaches aligned with European Telecommunications Standards Institute (ETSI) EN 319 102-1. Data quality is enforced through metadata schemas and validation rules that conform to ISO 8000-1:2022, while accessibility targets are mapped to the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.2. As empirical deployment metrics are not yet available, the paper defines an evaluation plan that covers functional completeness, reliability, performance, and governance indicators, such as cycle time, overdue rate, and rework frequency.

Keywords: *electronic document management system, electronic records management, approval routing, workflow management, task execution control, deadline monitoring, audit trail, role-based access control, secure software development, web API, data quality, accessibility.*

In information technology (IT) companies, a significant share of operational risk and coordination overhead is concentrated around “living” documents: architecture decision records, change requests, service contracts, security policies, incident post-mortems, procurement requests, and internal instructions. When such documents circulate through email threads and instant messaging, organisations typically lose a unified register, consistent metadata, a single source of truth for versions, and an auditable trail of who approved what and when. Empirical studies on document management in organisations emphasise that the transition from ad hoc file sharing to structured document management is a key enabler of digital transformation, as it reduces search time, mitigates duplication, and strengthens process discipline through traceability and accountability [1].

At the same time, contemporary approaches to enterprise electronic document management highlight the need to combine storage and metadata management with workflow automation, access control, and reporting to support managerial decision-making and compliance [2]. Therefore, the central problem addressed in this work is the design and implementation of a software tool that provides end-to-end electronic document circulation, configurable approval routing (visas), and systematic control of task execution (assignments), tailored to the operational realities of IT companies.

The aim of the work is to create a software system for registering and storing documents, setting up approval routes, assigning responsible persons, monitoring execution deadlines, and generating journals and reports that reflect the state and history of document passage.

The object of research is organisational document circulation in IT companies, and the subject of research is the methods and software design solutions that ensure reliable routing, version integrity, deadline control, and auditability in an electronic document management system (EDMS).

The main practical requirement is to reduce manual operations and user errors while preserving verifiable accountability: each document instance should have a clear lifecycle, each action should be attributable to an authenticated actor, and each transition should be reproducible for audit and analytics.

From a functional standpoint, the proposed EDMS is designed around a document register (for unique numbering, metadata, and classification), a repository (for file storage, versioning, and access), a workflow subsystem (for routing and approvals), a task subsystem (for assignments and deadline control), a notification subsystem (for reminders and escalations), and an analytical subsystem (for journals, dashboards, and downloadable reports).

A document is treated as a compound business entity that includes (i) immutable identifiers, (ii) structured metadata (author, unit, category, confidentiality level, retention class, related projects), (iii) content artifacts (files, attachments, linked resources), and (iv) a controlled set of states (draft, registered, under review, approved, rejected, completed, archived). The design principle is that the repository stores the "what" (content and versions), while the workflow and task subsystems store the "why/when/who" (decisions, assignments, and timing).

Approval routing is modelled as an explicit route specification. Instead of hard-coding sequences, the system supports route templates composed of steps of different semantic types: review, approval, acknowledgement, signature, information copy, and execution assignment. Each step includes role constraints (e.g., "team lead", "security officer"), actor resolution rules (direct user, organisational position, project role), and timing rules (due date, grace period, escalation interval). The route itself is represented as a directed graph that supports serial paths and parallel branches (e.g., legal and security review in parallel), merge rules (all-of, any-of, quorum), and controlled rework loops (return to the author with mandatory comments).

A formal view of document approval as a workflow, including explicit modelling of steps and transitions, is consistent with recent work proposing rigorous approval workflow definitions to reduce ambiguity and improve controllability of organisational processes [3]. In the proposed EDMS, each node in the route materialises as one or more work items; a work item is a task with an owner, a due date, a required action (approve/reject/comment/execute), and a status (new, in progress, completed, overdue, escalated).

Control of execution deadlines is achieved by combining time constraints with a transparent escalation policy. Each assignment defines a service-level objective (SLO) for completion time and a service-level agreement (SLA) when the organisation chooses to formalise internal expectations. The monitoring scheduler periodically evaluates remaining time, triggers reminders, and escalates overdue assignments to designated supervisors or alternative approvers. Escalation is not merely a notification; it can be configured to perform workflow actions (e.g., reassign, add an additional approver, or block further document movement until resolution). This provides a measurable governance mechanism: for any document, the system can compute cycle time, waiting time per step, number of reworks, and the proportion of overdue tasks, enabling management to detect systemic bottlenecks.

The system architecture is defined to ensure maintainability, security, and integration. A pragmatic approach is a modular monolith (with clearly separated modules and internal application programming interface (API) boundaries) for small-to-medium deployments, with a migration path to a service-oriented architecture for larger organisations.

Persistent storage is split into a relational database (for metadata, routes, tasks, and audit logs) and an object storage (for document binaries). Every state transition and user action is recorded in an append-only audit log; this event trail supports both compliance verification and subsequent analytical processing.

For interoperability with external systems (for example, project management tools, human resources systems, or identity providers), the EDMS exposes a Representational State Transfer (REST) API over Hypertext Transfer Protocol (HTTP). To standardise error responses and avoid ad hoc formats that complicate client integrations, the EDMS uses the "problem details" structure for API errors, as defined in RFC 9457 (Problem Details for HTTP APIs) [10]. This improves operational robustness because integration clients can reliably parse machine-readable error details and apply consistent retry or fallback strategies.

Security is treated as a first-class design constraint because IT companies routinely process documents containing personal data, commercial secrets, and security-sensitive information. At the organisational level, the system's security controls are aligned with the requirements of ISO/IEC 27001:2022 for an information security management system (ISMS), which establishes a risk-based management framework for protecting information [4].

At the control selection level, ISO/IEC 27002:2022 provides a catalogue of information security controls (including access management, logging, cryptography, and secure configuration) that can be mapped to EDMS features and operational procedures [5]. From a secure development perspective, the Secure Software Development Framework (SSDF) in NIST Special Publication 800-218 recommends integrating security practices across the software development life cycle, including secure coding, environment protection, and vulnerability response [6].

In addition, the OWASP Top 10:2021 highlights prevalent classes of web application risks (such as broken access control, injection, and security misconfiguration), which directly inform threat modelling and defensive requirements for the EDMS web layer [7]. Consequently, the EDMS design incorporates role-based access control (RBAC) with least-privilege defaults, multi-factor authentication (where supported by the identity provider), encryption in transit (Transport Layer Security) and at rest, tamper-evident audit logs, and defensive input validation.

For organisations that require legally meaningful approvals or strong non-repudiation, the EDMS supports electronic signatures based on public key infrastructure (PKI). The creation and validation of Advanced Electronic Signatures (AdES) can be implemented in accordance with ETSI EN 319 102-1 (procedures for creation and validation of AdES digital signatures) [8].

Although legal regimes differ by jurisdiction, the European Union's updated framework for electronic identification and trust services (as amended by Regulation (EU) 2024/1183) illustrates current regulatory expectations for trustworthy electronic transactions and identity mechanisms, and it is relevant for IT companies working with European partners or implementing cross-border compliant processes [9]. Even when legal qualification is out of scope, these standards provide concrete engineering guidance for signature workflows, validation evidence, and long-term verification artefacts.

Data quality is a recurring problem in real deployments: inconsistent metadata (e.g., missing project codes, ambiguous titles, or incorrect document classes) undermines searchability, reporting, and compliance. To address this, the EDMS enforces metadata schemas, controlled vocabularies, and validation rules, aligning the notion of "fitness for use" of data with the broader principles of the ISO 8000 series on data quality (overview defined in ISO 8000-1:2022) [12]. On the presentation side, the user interface (UI) is designed for accessibility and inclusiveness; conformance to the Web Content Accessibility Guidelines (WCAG) 2.2 serves as a baseline for web usability, including keyboard navigation, visible focus, and support for assistive technologies [11]. This is practically important for IT companies with distributed workforces and diverse user needs.

Testing and quality assurance are approached systematically, combining unit, integration, end-to-end, and security testing. To structure test design, the work uses test technique guidance consistent with ISO/IEC/IEEE 29119-4:2021, which defines a set of test design techniques applicable during test design and implementation [13].

Without relying on a physical experiment in this thesis format, a practical evaluation plan is proposed: (i) functional completeness (coverage of registration, routing, signing, and reporting scenarios), (ii) performance under load (throughput of task creation and document retrieval, latency of route transitions), (iii) reliability (recovery after partial failures, idempotent processing of repeated requests), (iv) governance metrics (cycle time, overdue rate, reassignment frequency), and (v) user error reduction (measured by reduction of rejected submissions due to incomplete metadata and by the number of "missing approval" incidents).

For example, a representative workload for a medium IT company can be characterised by hundreds of concurrent users, tens of thousands of documents, and a daily peak in approval transitions driven by change management and procurement processes; the EDMS should remain responsive under such conditions while preserving audit integrity.

In summary, the work substantiates the design of an EDMS for IT companies that integrates document registration and storage with configurable approval routing and enforceable task-execution deadlines.

The proposed approach emphasises (i) explicit workflow modelling, (ii) auditability through append-only event trails, (iii) secure development and operation guided by modern security standards and recommendations, (iv) standardised API behaviour, and (v) disciplined metadata quality.

Future development directions include advanced analytics (for example, bottleneck detection and predictive overdue risk based on historical patterns), adaptive routing (rule-based branching by document class and risk level), integration with enterprise identity wallets where applicable, and automated compliance checks (for instance, verifying that certain document types always pass mandatory security review before release).

LIST OF REFERENCES

1. Jordan S., Sternad Zabukovšek S., Šišovska Klančnik I. Document Management System – A Way to Digital Transformation // Naše gospodarstvo/Our Economy. - 2022. - Vol. 68, No. 2. - P. 43–54. - DOI: 10.2478/ngoe-2022-0010.

2. Pasichnyk V., Kunanets N., Veretennikova N., Peleshchyshyn A., Babelyuk O. Technologies for Electronic Document Management in the Enterprise // Information Technologies and Systems. ITSM 2023. Lecture Notes in Networks and Systems. - Cham : Springer, 2024. - Vol. 873. - P. 1–9. - DOI: 10.1007/978-3-031-55908-3_1.

3. Velásquez-Angamarca C. E., Reis J., Pinto A., Gonçalves J. C. A Formal Document Approval Workflow for Business Process in Higher Education Institutions // Proceedings of the 19th Iberian Conference on Information Systems and Technologies (CISTI). Lecture Notes in Networks and Systems. - Cham : Springer Nature Switzerland, 2026. - Vol. 1747. - P. 74–83. - DOI: 10.1007/978-3-032-12879-9_8.

4. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. - Geneva : International Organization for Standardization, 2022.

5. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls. - Geneva : International Organization for Standardization, 2022.

6. Souppaya M., Scarfone K., Dodson D. NIST Special Publication 800-218. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. - Gaithersburg, MD : National Institute of Standards and Technology, 2022. - 36 p. - DOI: 10.6028/NIST.SP.800-218.

7. OWASP Top 10:2021. Web Application Security Risks : documentation. - OWASP Foundation, 2021. - Electronic resource. - Access date: 27.01.2026.

8. ETSI EN 319 102-1 V1.3.1 (2021-11). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. - ETSI, 2021. - Electronic resource. - Access date: 27.01.2026.

9. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework // Official Journal of the European Union. - 2024. - 30.04.2024. - Electronic resource. - Access date: 27.01.2026.

10. Nottingham M., Wilde E., Dalal S. Problem Details for HTTP APIs : RFC 9457. - IETF, 2023. - Published: July 2023. - Electronic resource. - DOI: 10.17487/RFC9457. - Access date: 27.01.2026.

11. Web Content Accessibility Guidelines (WCAG) 2.2 : W3C Recommendation. - World Wide Web Consortium (W3C), 2023. - Electronic resource. - Access date: 27.01.2026.

12. ISO 8000-1:2022. Data quality - Part 1: Overview. - Geneva : International Organization for Standardization, 2022.

13. ISO/IEC/IEEE 29119-4:2021. Software and systems engineering - Software testing - Part 4: Test techniques. - Geneva : International Organization for Standardization, 2021.

Хошаба Олександр Мирославович — канд. техн. наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет

Цугель Роман Сергійович — студент групи 3ПІ-22б, факультет інформаційних технологій та комп'ютерної інженерії, національний технічний університет, Вінниця, pzmag2022@gmail.com

Khoshaba Oleksandr M. — Cand. Sc. (Eng) Assistant Professor of the Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia

Tsuhel Roman S. — Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia, email: pzmag2022@gmail.com