Scientific Innovative Center Research

INTELLECTUAL PROPERTY: PROTECTION IN MODERN CONDITIONS

Monograph

Intellectual property: protection in modern conditions

Collective monograph edited by
Volodymyr Marchenko

Estonia, 2025

International databases and directories indexing publications:

- CrossRef (DOI: 10.36690);
- Google Scholar;
- National Library of Estonia;
- The ESTER e-catalog;

Recommended for publishing by the Academic Council of the Scientific Center of Innovative Research (№4 of 26.09.2025)

ISBN 978-9916-9389-5-9 (pdf)

Intellectual property: protection in modern conditions (2025). Monograph. In V. Marchenko (Ed.), Scientific Center of Innovative Research. Estonia. 208 p. https://doi.org/10.36690/IPP

The monograph examines a core challenge of the contemporary digital economy, namely how to protect and manage intellectual property under rapid technological change and the expansion of data driven environments. It analyzes the transformation of intellectual property rights under the influence of artificial intelligence, blockchain technologies, and global digital platforms, while also addressing the security challenges that the information society poses for public governance. The monograph integrates legal and technological perspectives by discussing not only contemporary legal mechanisms of protection, but also the practical use of innovative tools for registration, evidentiary substantiation, and enforcement of rights at national and international levels. Its structure consistently moves from issues of digital governance and information security, through legal and technological transformation of IP protection, to applied sectoral and procedural models, including trade secrets in corporate information flows, EU related operational IP management in digital product development, and online litigation as an enforcement pathway.

The monograph is intended for an academic and professional audience that needs a coherent, practice oriented understanding of intellectual property in the digitalized economy. It will be relevant for researchers and students working in law, public governance, and digital economy studies, as well as for legal practitioners, public officials, IT professionals, and corporate actors engaged in creating, managing, and protecting intellectual assets.

The monograph contributes an integrated framework that links doctrinal legal analysis with operational realities, emphasizing that effective IP protection today depends simultaneously on regulatory adaptability, technological instruments, evidence readiness, and enforceable procedures across jurisdictions and digital infrastructures.

Table of Contents

Introduction 4

Chapter 1. Digital Governance and Information Security in the Data-Driven Society: Public Administration and Corporate Information Protection 9
Section 1.1. Digital-Age Information Society: Security Threats and Modern Methods of Information Storage in Public Governance
Volodymyr Marchenko 10
Section 1.2. Intellectual Property Protection in Corporate Information Flows: Trade Secrets, Digital Risks, and Remedies
Hisham Jadallah Mansour Shakhatreh 27

Chapter 2. Legal and Technological Transformation of Intellectual Property Protection in the Digital Environment 44
Section 2.1. Contemporary Challenges in Intellectual Property Protection: Legal Transformations and Technological Disruptions
Inna Kilimnik 45
Section 2.2. Operational intellectual property management for EU game developers: from harmonization to scalable enforcement
Oleksandr Mihus **68**
Section 2.3. Legal Dimensions of Using Blockchain for Intellectual Property Protection
Alla Dombrovska 89

Chapter 3. Sectoral and Procedural Models of Applied Intellectual Property Management and Enforcement 106
Section 3.1. Features of Intellectual Property Protection in the Assessment of Corporate Business Reputation: International Aspects
Igor Korzhevskyi 107
Section 3.2. Intellectual Property Management in Polygraph Methodology Development Projects: Policies, Procedures, Compliance
Oleksandr Akimov **133**
Section 3.3. Intellectual Property Rights in the Digital Age: Challenges Posed by Artificial Intelligence and Digital Platforms
Inga Bochkova 151
Section 3.4. Intellectual Property Protection in Online Litigation
Vasyliev Sergii 170

Conclusion 187
References 192

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Introduction

The monograph Intellectual Property: Protection in Modern Conditions examines how legal systems, public governance mechanisms, and organizational practices can secure intellectual property under conditions of accelerated digitalization, platform mediated markets, and the diffusion of advanced technologies. It proceeds from the assumption that contemporary intellectual property protection is not limited to formal registration or dispute resolution, because digital environments change both the nature of creative products and the pathways through which infringements occur. In this context, the practical effectiveness of intellectual property regimes depends on the coherence of legal norms, the availability of reliable evidence, and the capacity of institutions to enforce rights across borders and online infrastructures. At the same time, the scaling of digital production and distribution increases systemic exposure to legal and security risks, including unauthorized reuse, misappropriation of trade secrets, manipulation of digital evidence, and the emergence of new infringement modalities driven by automated tools. These premises position intellectual property protection as an integrated governance domain where law, technology, and institutional capacity must evolve together to preserve innovation incentives, fair competition, and public trust.

A central analytical focus of the monograph is that technological progress simultaneously expands the opportunities for creative and innovative activity and raises the costs of inadequate protection, since violations can be replicated at scale and disseminated instantly through digital channels. This is particularly visible in domains shaped by artificial intelligence and data intensive production, where questions arise about authorship, originality, lawful use of datasets, and the legal status of outputs generated with algorithmic support. Therefore, the monograph treats intellectual property not only as a private law category, but also as a field of regulatory coordination that includes evidence standards, procedural safeguards, and cross border enforcement capacity. It also highlights that modern protection strategies require operational instruments, such as digital traceability mechanisms, technologically informed legal expertise, and organizational policies that translate abstract rights into

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

implementable compliance routines. In this sense, digital tools are interpreted not as neutral innovations, but as instruments that can strengthen or undermine protection depending on institutional design, accountability structures, and the ability to monitor, detect, and respond to infringement in real time.

Structurally, the monograph is organized into three chapters that develop a coherent trajectory from the governance and security foundations of the data driven society to technology shaped legal transformations and, finally, to applied sectoral and procedural models of intellectual property management and enforcement. This architecture reflects the logic that intellectual property protection in contemporary conditions cannot be treated as a purely doctrinal legal field, because it increasingly depends on information security, organizational controls, and technologically competent enforcement mechanisms.

Chapter 1, *"Digital Governance and Information Security in the Data Driven Society: Public Administration and Corporate Information Protection,"* formulates the security and governance foundations of contemporary intellectual property protection. It analyses the information society of the digital era as a security sensitive environment by outlining the prevailing threat landscape and modern approaches to information storage in public governance, which clarifies how institutional vulnerabilities and data handling routines shape the protection of intangible assets. The chapter then moves from the public sector to the corporate domain and examines intellectual property protection within internal information flows, with particular attention to trade secrets, recurrent digital risks, and available remedies. By doing so, it demonstrates that effective protection relies not only on formal legal entitlements, but also on organizational controls, internal governance procedures, and disciplined information management that operationalize rights in everyday practice.

Chapter 2, *"Legal and Technological Transformation of Intellectual Property Protection in the Digital Environment,"* systematizes the ways in which intellectual property law and its protection instruments are reconfigured under conditions of rapid technological change. It examines contemporary challenges by connecting legal transformations with shifts in the technical infrastructures of

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

creation, circulation, and infringement, thereby substantiating the need for adaptive regulation and operationally viable compliance strategies. The chapter further develops an applied lens through the case of EU game developers, demonstrating how harmonization can be translated into scalable enforcement and why cross border digital industries require protection models that are implementable, repeatable, and responsive to platform based markets. In addition, it analyses the legal dimensions of blockchain use for intellectual property protection, approaching blockchain not as a universal remedy but as a technological instrument whose legal effectiveness depends on evidentiary architecture, governance design, and compatibility with established enforcement procedures.

Chapter 3, *"Sectoral and Procedural Models of Applied Intellectual Property Management and Enforcement,"* moves from general legal and technological transformations to applied contexts in which intellectual property functions as a measurable component of organizational value, professional practice, and enforcement strategy. It examines the features of intellectual property protection within corporate business reputation assessment, emphasizing international dimensions and showing how the robustness of rights protection shapes reputational capital and market trust. The chapter also analyses intellectual property management in polygraph methodology development projects through the lenses of policies, procedures, and compliance, demonstrating that specialized innovation settings require clearly articulated internal regimes for ownership allocation, confidentiality safeguards, and lawful reuse. In addition, it addresses intellectual property rights in the digital age by focusing on challenges generated by artificial intelligence and digital platforms, where questions of authorship, originality, data dependence, and platform governance complicate both protection design and practical enforcement. The chapter concludes with intellectual property protection in online litigation, outlining procedural pathways and enforcement logic that become decisive when infringements emerge in environments defined by rapid dissemination, scalable harm, and multi jurisdictional complexity.

The monograph is designed for researchers in law, public administration, and digital economy studies, as well as for practitioners who operate at the intersection of regulation,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

technology, and innovation management. It is relevant for policymakers and public sector professionals involved in designing legal frameworks and institutional procedures for protecting intellectual property in digital markets, where enforcement often requires cross sector cooperation and technologically competent oversight. For corporate managers, compliance specialists, and innovators, the book offers a consolidated perspective on how to build protection strategies that combine legal instruments with internal governance, contract design, and information security measures. For legal professionals, it provides a logically connected view of how modern disputes and evidentiary challenges emerge online, and which procedural mechanisms are most relevant for effective enforcement. For graduate students and early career professionals, the monograph functions as an analytically consistent entry point into contemporary intellectual property protection as a domain shaped by technological transformation and evolving governance requirements.

The internal logic of the book emphasizes that modern intellectual property protection is successful when it ensures both innovation enablement and legal reliability, rather than when it only expands the formal scope of rights without enforceable mechanisms. In this sense, the contribution of the monograph consists in treating intellectual property protection as a governance system that requires alignment between substantive norms, technological realities, and institutional capacity. A further contribution lies in linking the protection of intellectual assets with information security, corporate practices, and digitally mediated enforcement procedures, thereby demonstrating that the maturity of intellectual property regimes is inseparable from the quality of digital evidence, organizational discipline, and cross border legal coordination. Through this integrative perspective, the monograph supports applied decision making by showing how conceptual legal principles can be translated into operational instruments for prevention, monitoring, and enforcement.

The directions for further research derived from the monograph's problem field concern, first, the development of methodological criteria for evaluating originality, authorship, and lawful use in contexts where creative products are produced with

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

algorithmic assistance and where training data governance becomes legally salient. Second, future studies should deepen the analysis of evidentiary standards and procedural fairness in online litigation, particularly in cases involving digital traceability, platform responsibility, and the admissibility of technologically generated proof. Third, longitudinal research is needed to evaluate how blockchain based and other digital registry instruments affect enforcement effectiveness, transaction costs, and trust in rights attribution under real market conditions. Comparative research across jurisdictions remains essential, because intellectual property protection depends on the interaction between national legal traditions, supranational harmonization, and institutional capacity for cross border cooperation. In addition, the monograph's attention to corporate information flows suggests a research agenda on trade secret governance, including the balance between transparency requirements, employee mobility, cybersecurity safeguards, and the proportionality of restrictions. Finally, the digital governance perspective motivates further work on platform mediated markets, where enforcement involves a complex mix of private ordering, administrative oversight, and judicial protection, and where resilience depends on institutional learning and adaptable regulatory design.

Chief editor of the monograph
Prof., Dr., Volodymyr Marchenko

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Section 3.2. Intellectual Property Management in Polygraph Methodology Development Projects: Policies, Procedures, Compliance

Oleksandr Akimov[1]

[1]*Doctor of Sciences in Public Administration, Professor, Honored Economist of Ukraine, Professor, Scientific and Methodological Centre of Personnel Policy of the Ministry of Defence of Ukraine, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-9557-2276*

Citation:
Akimov, O. (2025). Intellectual Property Management in Polygraph Methodology Development Projects: Policies, Procedures, Compliance. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions*. 208 p. (pp. 133-150). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-133-150

Abstract. *Polygraph assessment methodologies should be conceptualized as composite intellectual assets rather than as a single protectable method, since they integrate expressive materials, functional workflow logic, confidential know how, and digital implementation components. This structure determines the protection strategy because copyright is limited by the idea versus expression boundary, and software copyright protects the expression of a program rather than the underlying principles that the software operationalizes. As a result, legally robust protection requires a portfolio approach in which each layer of the methodology is aligned with the most appropriate legal instrument and with a corresponding governance mechanism that can be demonstrated in practice. The study aims to systematize legal routes for protecting polygraph methodology components through copyright, trade secrets, and operational controls, while maintaining legitimacy through controlled transparency. The analysis uses a doctrinal and policy synthesis of relevant international and EU frameworks and translates these norms into an operational segmentation model and an evidence readiness logic for enforcement. The results show that protectability increases when methodology content is segmented into public, partner, and restricted components, since this enables principled disclosure without sacrificing confidentiality of calibration and decision rules. The findings also demonstrate that trade secret protection is governance dependent, because enforceability requires proof of secrecy, commercial value derived from secrecy, and reasonable steps to preserve confidentiality, which elevates access discipline and documentation to core protection instruments. In addition, the study identifies evidence readiness as decisive, because copyright and trade secret claims rely on different proof packages, including version histories, secret registers, access logs, and contract documentation. Finally, the study operationalizes reasonable steps as layered controls that map key risks to specific evidence outputs, strengthening cross border defensibility and improving response capacity. The effective legal protection of polygraph methodologies is portfolio based and operational, combining protection of authored expression with secrecy governance, licensing discipline, and evidence preservation embedded into project workflows. Future research should test how particular evidence artifacts, access controls, and licensing constraints influence dispute outcomes, and the long term durability of secrecy in training intensive ecosystems.*

Keywords: *polygraph methodology; intellectual property portfolio; copyright scope; idea expression dichotomy; software copyright; trade secrets; undisclosed know how; reasonable steps; evidence readiness; licensing governance; access control; cross border enforcement.*

ISBN 978-9916-9389-5-9 (pdf)

1. Polygraph methodologies as layered IP assets: what can be protected and how. Polygraph assessment methodologies should be treated as composite intellectual assets rather than as a single protectable "method." In operational terms, a methodology usually includes at least four layers: (1) expressive materials (manuals, protocols, scripts, training content), (2) functional logic (workflow rules, question sequencing logic, decision rules), (3) confidential know-how (interpretation heuristics, calibration thresholds, internal quality assurance routines), and (4) digital implementation (software-assisted capture, processing, reporting, and evidence storage). This decomposition matters because intellectual property law protects different layers through different legal tools, and the failure to separate them creates unrealistic protection claims and weak enforcement positions.

The first boundary is the idea–expression dichotomy: copyright protects expression, not ideas, procedures, methods of operation, or mathematical concepts as such (World Intellectual Property Organization [WIPO], 2025). In practice, this means a competitor may be able to replicate a functional approach while avoiding infringement if they do not copy protectable expression. Consequently, the methodology's defensible core often shifts toward the materials' originality and the governance of non-public know-how.

The second boundary concerns software-supported methodologies. EU law clarifies that only the expression of a computer program is protected, while ideas and principles underlying elements of a program, including interfaces, are not protected by copyright under the specific regime for computer programs (European Parliament and Council, 2009). This is particularly relevant when a polygraph methodology is embedded in tooling that automates scoring assistance, report generation, or pattern comparison. The protectable object is the code and its expressive architecture, whereas the abstract logic of the scoring approach may require confidentiality, contractual controls, or other legal strategies.

The third boundary concerns trade secrets and confidential know-how. Under TRIPS, protection of undisclosed information depends on three criteria: secrecy, commercial value because of secrecy, and reasonable steps under the circumstances to keep it secret (World Trade Organization, 1994). EU law aligns with this approach through the Trade Secrets Directive, which frames trade secrets as protectable business information and sets remedies for unlawful acquisition, use, and disclosure, including breaches of confidentiality duties and duties limiting use (European Parliament and Council, 2016). This alignment supports a coherent cross-border rationale: the more the methodology relies on internal heuristics and calibration, the

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

more the project should invest in proving "reasonable steps," since protectability depends on demonstrable governance rather than on registration.

To make this logic operational, the methodology should be segmented into "public," "partner," and "restricted" components. Public components can be disclosed for transparency, marketing, or training previews without destroying the value of secrecy. Restricted components include the elements that create competitive advantage or reduce error, such as examiner decision heuristics, internal case libraries, calibration rules, and quality control thresholds. Partner components sit between the two and are shared under strict license scope, auditability, and dissemination limitations. This segmentation allows the project to remain credible in compliance contexts while preserving the legal prerequisites for trade secret protection.

The table 3.13 clarifies how typical polygraph methodology components map to the most realistic protection instruments.

Table 3.13. Legal characterization of polygraph methodology components

Component	Primary legal nature	Most realistic protection route	Typical governance requirement
Manuals, protocols, diagrams, training texts	Expression	Copyright	Authorship and version control (WIPO, 2025)
Training videos, slides, tests	Expression	Copyright	Licensing and controlled reuse (WIPO, 2025)
Question sets and structured scripts	Expression plus compilation features	Copyright for wording and selection; secrecy for restricted sets	Tiered access and controlled distribution
Workflow logic and scoring methodology (abstract)	Method of operation	Not protected by copyright as such	Protect refined variants through secrecy and contracts (WIPO, 2025)
Interpretation heuristics and calibration thresholds	Confidential know-how	Trade secret	Reasonable steps and access governance (World Trade Organization, 1994; European Parliament and Council, 2016)
Software implementing capture, analysis, reporting	Expression of program	Copyright for code and structure	Repository governance and clean ownership (European Parliament and Council, 2009)
Method name, certification label, program identity	Distinctive sign	Trademark strategy	Anti-confusion governance and monitoring

Sources: (World Intellectual Property Organization, 2025; World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2009).

Table 3.13 indicates that the strongest protection strategy is portfolio-based, with copyright shielding the expressive layer and trade secrets protecting the competitive core that must remain confidential.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

A second operational question is how to decide, at design time, whether an element should be published, licensed, or kept secret. The decision should be driven by the legal preconditions of trade secret protection and by the reputational need for defensible transparency, particularly when a methodology is used in sensitive evaluations.

Table 3.14. Decision matrix for disclosure, licensing, and secrecy

Decision factor	If high, preferred route	Reason	Practical consequence
Competitive advantage comes from the element	Keep restricted as trade secret	Value depends on secrecy (World Trade Organization, 1994)	Tight access, logs, restricted training cohorts
Element must be publicly explained for legitimacy	Publish expressive explanation, restrict operational details	Copyright covers explanation, secrecy covers heuristics (WIPO, 2025)	Two-layer documentation, public guide plus restricted annex
Element must be shared with partners to operate	License with strict scope plus secrecy controls	Trade secret protection requires reasonable steps (European Parliament and Council, 2016)	NDA, audit rights, no redistribution, breach remedies
Element is embedded in software tooling	Protect code; keep key parameters confidential	Code is protected as expression (European Parliament and Council, 2009)	Repository controls and parameter secrecy

Sources: (World Intellectual Property Organization, 2025; World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2009).

Table 3.14 shows that the same methodology can remain transparent at the level of principles while preserving protectability and enforceability through controlled secrecy of high-value operational details.

Table 3.15. Evidence artifacts needed to support each protection route

Protection route	What must be proven	Core evidence artifacts	Why it matters
Copyright	Ownership, originality, copying of expression	Dated versions, authorship records, publication history, similarity analysis	Supports fast takedown and civil claims (WIPO, 2025)
Trade secret	Secrecy, value due to secrecy, reasonable steps, unlawful use or disclosure	Secret register, access logs, NDAs, tier policies, incident records	Protectability depends on governance performance (World Trade Organization, 1994; European Parliament and Council, 2016)
Software copyright	Expression of program, ownership, infringing reproduction	Repository logs, contributor agreements, dependency licensing ledger	Clean chain of title reduces dispute risk (European Parliament and Council, 2009)
Trademark (if used)	Distinctiveness, likelihood of confusion, unauthorized use	Clearance files, monitoring screenshots, use evidence	Prevents reputational dilution through confusing branding

Sources: (World Intellectual Property Organization, 2025; World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2009).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Finally, a layered IP approach must be "evidence-ready." Copyright and trade secret protection both depend on traceability, but the proof points differ. Copyright disputes emphasize originality, copying, and ownership, while trade secret disputes emphasize secrecy status, reasonable steps, and unlawful acquisition, use, or disclosure (World Trade Organization, 1994; European Parliament and Council, 2016).

Table 3.15 confirms that legal protection is inseparable from documentation discipline, because enforceability requires different proof packages depending on the right invoked.

A polygraph methodology is best protected through structured asset segmentation: copyright protects the expressive documentation and software expression, while trade secrets protect calibration know-how and internal heuristics, provided that secrecy and reasonable steps are consistently demonstrated under TRIPS and EU standards (World Trade Organization, 1994; European Parliament and Council, 2016; WIPO, 2025).

2. Copyright protection of methodological materials: scope, limits, and evidence discipline. Copyright is most effective for polygraph methodology projects when the methodology is expressed in fixed, original materials, such as manuals, structured examiner protocols, training modules, video lectures, and software code. This is because copyright protects the author's expression, while it does not protect ideas, procedures, methods of operation, or abstract principles as such (World Intellectual Property Organization, 2025). In the polygraph context, this boundary is decisive: the functional logic of testing can often be reproduced in another form, whereas the concrete expression of how the method is described, structured, and taught can remain legally protectable. A second core element is originality. In EU copyright doctrine, protection is tied to originality understood as the author's own intellectual creation, a standard articulated in EU case law and applied broadly across subject matter (Court of Justice of the European Union, 2009; European Parliament and Council, 2001). As a result, the practical strengthening of the copyright layer depends on deliberate authorial choices in sequence, explanatory architecture, terminology systems, examples, and didactic design rather than on the method's functional novelty.

A further complication arises when a polygraph methodology is embedded in software, for example scoring assistance tools, report generators, or data capture pipelines. Under the EU Software Directive, only the expression of a computer program is protected, while ideas and principles underlying any element of a program are not protected by copyright (European Parliament and Council, 2009). This implies that code, interface

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

layouts as expressive choices, and documentation can be protected, whereas the underlying scoring logic is more safely managed through confidentiality and contract-based controls. When methodological materials are distributed digitally, additional relevance arises from harmonized EU rules on reproduction and communication to the public, because copying, sharing in closed groups, and hosting on platforms can trigger distinct exclusive rights and exceptions (European Parliament and Council, 2001).

Table 3.16. Copyright scope in polygraph methodology materials: protectable expression versus functional content

Material type	What is typically protected	What is typically not protected	Practical design implication
Manuals and protocols	Structure, narrative, diagrams, examples as expression	The procedure itself as a method of operation	Increase original explanatory architecture and systematization
Training slides and videos	Script, visuals, editing and pedagogical sequencing	General teaching ideas	Separate "public overview" from "restricted operational detail"
Question sets and scripted scenarios	Wording, selection and arrangement	Generic questions and functional constraints	Maintain differentiated restricted sets and controlled distribution
Scoring explanations and rubrics	Explanatory text, illustrative cases	Abstract scoring logic and thresholds	Keep thresholds and heuristics confidential while publishing rationale
Software code and documentation	Code and documentation as expression	Underlying algorithms and principles	Isolate confidential parameters from publishable documentation

Sources: (World Intellectual Property Organization, 2025; European Parliament and Council, 2001; European Parliament and Council, 2009).

Table 3.16 indicates that copyright strength can be increased through intentional authorial design, while the functional core should be positioned for complementary protection, especially through secrecy and contracting.

Because methodology projects frequently involve joint authorship, outsourced content production, and iterative revisions, evidence discipline becomes the bridge between legal theory and enforceability. In EU practice, the originality threshold and the assessment of "copying" often depend on whether the claimant can show a coherent creation history and a stable chain of title. This is why internal documentation must be treated as a core IP governance artifact rather than as administrative overhead. The logic is strengthened by the EU originality approach emphasized in Infopaq, which links protection to the author's intellectual creation and requires a concrete assessment of protected expression (Court of Justice of the European Union, 2009).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.17. Evidence package for copyright enforceability in methodology projects

Evidence artifact	What it demonstrates	Typical use case	Minimum operational standard
Version-controlled master files	Timeline of creation and evolution	Authorship disputes, priority claims	Immutable timestamps, locked releases
Authorship and contribution records	Identity of creators and scope of contribution	Joint work and contractor conflicts	Signed contribution statements
Assignment and licensing agreements	Ownership and permitted use	Enforcement standing and licensing clarity	Mandatory for all contractors and trainers
Distribution register	Controlled dissemination and scope	Defense against implied license arguments	Recipient, purpose, and date tracking
Similarity comparison dossier	Copying of protected expression	Litigation and takedown escalation	Side-by-side mapping of copied fragments

Sources: (World Intellectual Property Organization, 2025; Court of Justice of the European Union, 2009; European Parliament and Council, 2001).

Table 3.17 shows that enforceability relies on the ability to reconstruct the work's provenance and to show controlled dissemination consistent with legitimate licensing expectations.

Methodology projects also face recurring operational risks specific to training and certification ecosystems. Content is often reproduced informally, recorded during trainings, shared inside institutional networks, or modified into derivative materials that circulate without supervision. These patterns require a licensing structure that distinguishes internal use, instructor rights, derivative work permissions, and reuse conditions. In digital distribution settings, clarity on reproduction and making-available behaviors becomes important because unauthorized copying and sharing can be scaled quickly through platforms, even when the initial violation is small (European Parliament and Council, 2001).

Table 3.18. Licensing architecture for polygraph methodology materials

Licensing scenario	Core permission granted	Key restriction	Recommended control
Institutional internal training	Internal use of materials	No redistribution, no recording	Access-limited portals and audit clause
Certified examiner program	Use of restricted materials by credentialed users	No sharing outside cohort	Credential revocation and watermarking
Trainer or franchise model	Delivery rights for training	No derivative works without approval	Pre-approval workflow for updates
Software-enabled methodology	Use of tool plus documentation	No reverse engineering and no extraction of parameters	License keys, logs, and restricted parameter access

Sources: (European Parliament and Council, 2001; European Parliament and Council, 2009).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.18 supports the conclusion that copyright must be operationalized through licensing segmentation, because the main threat is not only copying by competitors but uncontrolled diffusion through legitimate user networks.

Finally, a polygraph methodology often relies on structured collections, including question libraries, case templates, and standardized reporting fragments. Even when a collection is not treated as a "database" in a strict legal sense, the EU framework highlights that selection and arrangement can be protected when it reflects the author's own intellectual creation, and that separate database-related protections may become relevant where systematic compilation is central (European Parliament and Council, 1996; Court of Justice of the European Union, 2009). This reinforces a practical drafting strategy: emphasize original selection logic, categorization, and the explanatory rationale that ties the materials into a coherent authored system.

Table 3.19. Design strategies to maximize protectable expression without disclosing core know-how

Strategy	What it strengthens	What it avoids	Implementation example
Two-layer documentation	Copyright in the "open" explanation	Exposure of thresholds and heuristics	Public guide plus restricted annex
Modular authored structure	Original selection and arrangement	Easy paraphrase by competitors	Unique taxonomy and decision-tree narration
Controlled examples	Demonstrates originality and pedagogy	Disclosure of real case library	Synthetic cases with safeguarded parameters
Separation of parameters from narrative	Protects text while keeping logic secret	Reverse engineering of scoring rules	Narrative rationale with withheld thresholds

Sources: (World Intellectual Property Organization, 2025; European Parliament and Council, 1996; Court of Justice of the European Union, 2009).

Table 3.19 indicates that the most resilient approach is to publish enough expression to ensure legitimacy and teachability, while preserving the competitive core through confidentiality and restricted access.

Copyright protection for polygraph methodology projects is strongest when the expressive layer is intentionally authored, originality is reinforced through structured presentation, and enforceability is supported by provenance evidence, clean chain of title, and segmented licensing for training and digital dissemination (World Intellectual Property Organization, 2025; European Parliament and Council, 2001; European Parliament and Council, 2009; Court of Justice of the European Union, 2009).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

3. Commercial secrecy, trade secrets, and know-how: legal criteria and "reasonable steps". Trade secret protection is the most structurally compatible mechanism for safeguarding the operational core of polygraph methodologies, especially where competitive advantage lies in calibration, interpretation heuristics, internal validation routines, and examiner decision rules that are not intended for public disclosure. Unlike registered IP rights, trade secrets remain enforceable only while confidentiality and control are preserved, which makes governance performance a constitutive element of protection rather than a secondary compliance layer. The minimum international baseline is articulated in TRIPS Article 39, which links the protectability of undisclosed information to secrecy, commercial value because of secrecy, and reasonable steps to keep the information secret. In the EU, Directive (EU) 2016/943 aligns with this logic by defining a "trade secret" through the same three-part test and by providing civil law remedies against unlawful acquisition, use, and disclosure.

A critical methodological implication for polygraph projects is that trade secret claims typically fail when the holder cannot specify what the secret is and cannot demonstrate proportional protective measures. WIPO emphasizes that reasonable steps should not be treated as a formal hurdle but as a practical risk management discipline calibrated to the value of the information and the threat landscape. For methodologies deployed through training ecosystems and institutional clients, this calibration must account for the predictable leakage channels: repeated exposure in trainings, informal reproduction inside corporate or public sector networks, contractor access, and digital storage vulnerabilities. Where disputes emerge, confidentiality preservation in proceedings becomes strategically important, because litigation can otherwise force disclosure of the very information the claimant seeks to protect. The Trade Secrets Directive therefore requires Member States to ensure confidentiality of trade secrets in the course of legal proceedings through obligations on parties and other participants, alongside the possibility of specific confidentiality-preserving measures.

Table 3.20 systematizes the legal test and translates it into proof requirements that can be operationalized in methodology governance.

Table 3.20 suggests that "reasonable steps" should be treated as a designed control system that produces auditable evidence, because the legal definition itself requires a demonstrable governance posture.

Beyond the definition, polygraph methodology projects must anticipate lawful acquisition pathways that weaken enforceability if not managed.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.20. Trade secret legal test and evidentiary proof points for polygraph methodologies

Legal element	Core meaning in practice	Typical proof expected	Polygraph-specific implication
Secrecy	Not generally known or readily accessible in relevant professional circles	Restricted access records; controlled dissemination; "restricted annex" structure	Distinguish public principles from restricted operational rules
Value because of secrecy	Competitive or operational advantage is tied to confidentiality	Business rationale; reliance evidence; differentiation narrative	Show how calibration and heuristics reduce error or improve consistency
Reasonable steps	Proportionate measures under the circumstances	NDAs; access controls; labeling; logs; training restrictions	Demonstrate tiering across manuals, trainings, and client deliverables

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; World Intellectual Property Organization, 2019; World Intellectual Property Organization, 2025).

Under the EU Directive, acquisition is lawful, for example, through independent discovery or by observation, study, disassembly, or testing of a product that is publicly available or lawfully possessed without a duty to limit acquisition. This provision is especially relevant when methodology outputs are packaged as tools, templates, or software features that can be inspected by users. The governance response is to design deliverables so that exposure of functional outputs does not reveal the confidential internal configuration, thresholds, and decision rules that constitute the secret. This is one reason why separating parameters from explanatory narratives, and keeping high-value calibration logic server-side or access-restricted, tends to be more defensible than distributing complete operational rulebooks to broad audiences.

Table 3.21 links common polygraph know-how assets to a risk taxonomy, clarifying where misappropriation pressure is highest.

Table 3.21 indicates that the highest-risk assets are precisely those most likely to be exposed repeatedly, namely through trainings, partner deployments, and routine operational access, which makes human-factor controls and contractual architecture decisive.

The "reasonable steps" requirement becomes actionable when measures are selected as a coherent, layered set that maps to specific risks and produces evidence artifacts. WIPO's guidance frames trade secret management as a plan with steps that include identifying and valuing secrets, assessing risks, applying reasonable measures, and monitoring and reacting to misappropriation or leakage.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.21. Risk taxonomy for polygraph methodology know-how and typical misappropriation channels

Know-how asset	Why it is sensitive	Primary risk channel	Secondary risk channel
Scoring thresholds and calibration rules	Enables replication of accuracy profile	Insider leakage during role transition	Contractor reuse across clients
Interpretation heuristics and decision trees	Encodes expert judgment and consistency	Recording or copying during trainings	Informal sharing inside institutions
Internal case libraries and validation datasets	Demonstrates performance and edge cases	Unauthorized duplication from shared drives	Accidental disclosure via cloud links
Quality assurance protocols and audit rubrics	Enables "certification mimicry"	Partner overreach beyond license scope	Competing programs adopting identical rubrics
Software configuration parameters	Makes tooling replicable	Reverse engineering of client-side components	Credential compromise and scraping

Sources: (World Intellectual Property Organization, 2019; World Intellectual Property Organization, 2025; European Parliament and Council, 2016).

This planning approach is especially suitable for polygraph methodologies, because the asset portfolio changes over time as scripts, thresholds, and training materials evolve. It also supports a proportionality logic: controls for a restricted calibration annex should be more stringent than controls for a general overview brochure, even if both are part of the same methodology package.

Table 3.22 operationalizes reasonable steps into a control catalogue that can be embedded in methodology development and deployment.

Table 3.22. Control catalogue for "reasonable steps" in polygraph methodology projects

Control layer	Measures	Evidence artifact produced	Primary legal function
Asset identification	Trade secret register; component tiering	Dated register; scope definitions	Specifies what is claimed as secret
Access governance	Role-based access; least privilege; cohort rules	Access logs; credential lists	Demonstrates secrecy and control
Contractual controls	NDAs; confidentiality clauses; use limitations	Signed agreements; audit clauses	Establishes duties and breach basis
Document discipline	"Confidential" marking; controlled exports	Watermarked copies; distribution register	Proves notice and controlled dissemination
Technical security	Encryption; secure repositories; monitored sharing	System logs; incident reports	Supports traceability and containment
Training governance	No-recording policy; restricted modules	Attendance logs; policy acknowledgements	Reduces predictable training leakage
Monitoring and response	Leak detection; escalation workflow	Evidence preservation pack	Enables timely remedies

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; World Intellectual Property Organization, 2019; World Intellectual Property Organization, 2025).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.22 supports the conclusion that trade secret protection is governance-intensive but scalable, because each measure both reduces risk and produces proof that the reasonable steps condition is met.

Finally, polygraph methodology disputes require a confidentiality-preserving enforcement stance to avoid "self-defeating litigation," where the attempt to enforce secrecy triggers broader exposure. The EU Directive explicitly addresses this risk by requiring confidentiality obligations in legal proceedings and by allowing measures necessary to preserve confidentiality of trade secrets or alleged trade secrets used or referred to during proceedings. This design makes trade secret enforcement more practicable for methodology holders, provided that the claimant can define the secret precisely, demonstrate reasonable steps, and preserve evidence early. The same Directive also provides for damages appropriate to actual prejudice and specifies factors relevant to assessing damages, which is relevant when disclosure causes both economic harm and longer-term degradation of competitive position.

For polygraph methodologies, trade secret and know-how protection is the legally coherent route for safeguarding calibration, heuristics, and internal validation routines, but it is viable only when the holder can demonstrate the TRIPS and EU three-part test and can show a proportional, evidence-producing system of reasonable steps, including confidentiality-preserving litigation readiness.

4. Contracting, licensing, and enforcement: making protection scalable and dispute-ready. Polygraph methodology projects are implemented through multi-actor ecosystems that typically include developers, certified examiners, trainers, institutional clients, software vendors, and sometimes public authorities. In such settings, intellectual property protection cannot rely only on the abstract existence of rights. It must be converted into operational control over access, permitted uses, and evidence creation, especially because trade secret protection depends on demonstrable secrecy measures and enforceable confidentiality duties (World Trade Organization, 1994; European Parliament and Council, 2016). Contracting and licensing therefore function as the "connective tissue" between copyright in materials, trade secrets in know-how, and the practical reality of repeated dissemination during trainings and deployments.

A robust contractual architecture begins with clear allocation of ownership and authorship for manuals, training modules, templates, and software components, with special attention to contractor-created deliverables and joint development. This is complemented by licensing clauses that define scope (internal use only, named users, geographic limits,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

term), prohibit unauthorized copying and redistribution, and regulate derivative works such as updated protocols or localized training programs. For the confidentiality layer, agreements should define the protected confidential information precisely, impose duties to limit use to authorized purposes, and introduce auditability and incident notification obligations. These elements are directly aligned with the EU trade secrets framework, where unlawful use or disclosure often hinges on breaches of confidentiality duties or contractual duties limiting use (European Parliament and Council, 2016). In parallel, dispute readiness requires drafting that anticipates evidence preservation and proportionate remedies, consistent with EU civil enforcement standards for IP-related disputes (European Parliament and Council, 2004).

The table 3.23 distinguishes the most common agreement types used in polygraph methodology ecosystems and the protection function each one serves.

Table 3.23. Contract stack for polygraph methodology projects and its IP function

Agreement type	Typical parties	Primary IP function	Core operational risk addressed
Authorship and assignment agreement	Developers, contractors, trainers	Secures chain of title for materials and software	Ownership disputes and unenforceable rights
NDA and confidentiality agreement	All collaborators and clients	Establishes secrecy duties and limits use	Trade secret leakage through informal sharing
Methodology license agreement	Provider and institutional client	Defines scope of use and controls redistribution	Uncontrolled diffusion within institutions
Certification and examiner agreement	Provider and certified examiner	Restricts access to “restricted tier” know-how	Credential misuse, copying during practice
Trainer agreement	Provider and trainers	Controls derivative works and recording	Unlicensed updates and content drift
Software terms and access policy	Provider and users	Controls tool access and parameter exposure	Reverse engineering and scraping risks
Incident notification and cooperation addendum	Provider and key partners	Creates rapid containment coordination	Delayed response and evidentiary gaps

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

Table 3.23 indicates that scalability is achieved not by adding more documents, but by ensuring that each agreement produces a specific form of control or evidence that supports later enforcement.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

A common failure pattern in methodology projects is that contracts are drafted as generic templates that do not map to realistic risks. A more reliable approach is clause-to-risk engineering, where each critical clause is justified by a specific threat model and evidence need.

Table 3.24. Clause-to-risk mapping for polygraph methodology licensing and secrecy governance

Clause group	Minimum clause content	Risk it mitigates	Evidence it generates
Definitions of confidential information	Tiered definition with examples and exclusions	Ambiguity that undermines trade secret claims	Clear secret scope and notice to recipients
Purpose limitation	Use only for defined assessments or training	Repurposing methods outside license	Proof of unauthorized use beyond scope
Dissemination limits	Named users, internal network limits, no forwarding	"Institutional leakage" through internal sharing	Distribution trail and breach traceability
No recording and no extraction	Ban recording trainings and extracting parameters	Copying through recordings and screenshots	Policy acknowledgements and compliance basis
Derivative works and updates	Approval workflow for modifications and translations	Uncontrolled adaptations that erode exclusivity	Change logs and authorized update trail
Audit rights and compliance reporting	Audit triggers, remediation timelines	Hidden non-compliance and silent diffusion	Audit reports and corrective action records
Offboarding and credential revocation	Return or destruction, access termination	Leakage at role transition	Offboarding checklist and termination evidence
Incident notification and cooperation	Time limits, containment duties, evidence hold	Delayed response magnifying harm	Incident logs and preservation chain

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016).

Table 3.24 supports the conclusion that enforceability is strengthened when contracts are drafted as operational controls that create predictable evidence outputs, rather than as purely formal legal instruments.

Because polygraph methodologies are often used in sensitive contexts, enforcement must be designed to preserve confidentiality while still enabling effective remedies. The EU trade secrets regime explicitly supports confidentiality-preserving litigation measures, which reduces the risk that enforcement actions inadvertently expose protected know-how (European Parliament and Council, 2016). At the same time, general IP enforcement principles in the EU emphasize effective, proportionate, and dissuasive measures, along with tools for preserving evidence and stopping ongoing infringement, which can be adapted to methodology disputes that involve

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

copyrighted manuals or unauthorized distribution of training content (European Parliament and Council, 2004).

The table 3.25 proposes a dispute-ready enforcement workflow that aligns with confidentiality needs and cross-border practicalities.

Table 3.25. Enforcement workflow for polygraph methodology disputes with confidentiality safeguards

Phase	Key action	Primary objective	Confidentiality safeguard
1. Triage	Classify event: copyright copy, trade secret leak, license breach	Choose correct legal basis early	Limit internal circulation of facts
2. Containment	Revoke access, suspend credentials, stop distribution	Prevent ongoing exposure	Evidence hold and restricted access to records
3. Evidence preservation	Secure logs, versions, agreements, and copies	Support later remedies	Sealed evidence pack with chain-of-custody
4. Notice and negotiation	Send structured notice, demand cessation, propose remediation	Resolve quickly and quietly when possible	Use controlled disclosure of secret details
5. Platform and intermediary steps	Takedown or marketplace reporting where relevant	Rapid removal of distributed copies	Provide only necessary proof materials
6. Litigation readiness	Select forum, request confidentiality measures	Secure enforceable remedies	Protective orders and limited access filing
7. Recovery and hardening	Update controls and training	Reduce recurrence	Post-incident control review and audit

Sources: (European Parliament and Council, 2016; European Parliament and Council, 2004).

Table 3.25 shows that the core enforcement problem is sequencing: confidentiality protection improves when evidence is preserved first, disclosure is minimized, and escalation is proportional to harm.

A dispute-ready strategy also requires a standardized evidence pack. This is particularly important because methodology disputes often include mixed claims, for example a copyright claim for copying manuals and a trade secret claim for leaking scoring heuristics. The table 3.26 offers a structured checklist that can be used as a governance artifact. Table 3.26 indicates that evidence readiness is not a litigation-only practice. It is a continuous governance capability that reduces response time and prevents avoidable disclosure of confidential materials.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.26. Evidence pack checklist for mixed copyright and trade secret disputes

Evidence category	What it contains	Supports which claim	Typical mistake avoided
Chain of title	Assignments, contributor agreements, ownership policy	Copyright and software rights	Lack of standing to enforce
Work provenance	Version history, timestamps, authorship records	Copyright	Inability to show originality and priority
Dissemination control	Distribution register, watermarks, access lists	Both	Defense that content was "freely shared"
Secrecy governance	Secret register, tier policy, training restrictions	Trade secrets	Failure to prove reasonable steps
Access traces	Logs, credential histories, offboarding records	Trade secrets	No attribution or timing evidence
Breach proof	Copies, screenshots, repository snapshots, witness notes	Both	Late collection and spoliation risk
Remedy mapping	Harm narrative, business impact, proposed injunction scope	Both	Overbroad claims that expose secrets

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

Finally, polygraph methodology projects frequently operate across borders through training partners or multinational clients. Cross-border deployment increases the relevance of harmonized legal baselines (TRIPS and EU directives), but it also introduces practical decisions about which remedies are realistic and how to coordinate actions.

Table 3.27. Cross-border deployment scenarios and preferred protection posture

Cross-border scenario	Main risk	Preferred protection lever	Practical priority
Multi-country institutional client	Internal redistribution across affiliates	License scope and auditability	Named-user limits and reporting
Training partner in another jurisdiction	Derivative works and uncontrolled updates	Trainer agreement and update governance	Approval workflow and watermarking
Remote examiner network	Credential misuse and copying	Certification agreement plus access controls	Revocation mechanism and cohort segmentation
Software-enabled methodology abroad	Parameter exposure and reverse engineering	Tool access policy and confidentiality layer	Server-side storage of sensitive parameters
Online diffusion of materials	Rapid mass distribution	Copyright enforcement plus platform steps	Fast takedown and evidence pack

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.27 reinforces that cross-border protection is strongest when legal instruments are paired with operational controls that limit dissemination and maintain traceability.

Contracting and licensing translate IP doctrine into enforceable control over dissemination, use, and evidence production. In polygraph methodology projects, this translation is essential because trade secret protection depends on demonstrable secrecy and use-limitation duties, while copyright protection depends on provable authorship, controlled dissemination, and clear licensing scope (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

Conclusion. Legal protection of polygraph assessment methodologies is strongest when implemented as a portfolio that reflects the layered structure of the asset. Copyright is effective for manuals, training content, and software expression, but it does not confer exclusivity over procedures or methods of operation, which makes the confidentiality layer essential. Trade secret protection and know-how governance are therefore central, because TRIPS and the EU Trade Secrets Directive provide a coherent test grounded in secrecy, value, and reasonable steps, and they attach legal consequences to unlawful acquisition, use, or disclosure, including breaches of confidentiality and use-limitation duties. Finally, contracting and enforcement readiness transform rights into operational capability, because licensing scope, access governance, and rapid evidence preservation determine whether remedies are achievable without unnecessarily expanding disclosure of the very information that must remain confidential.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

References:

1. Akimov, O., & Andrusiak, M. (2025). Professional standardization of polygraph examiner's psychophysiological competencies in the context of ukraine's national security. *Society and Security*, (2(8), 72–79. https://doi.org/10.26642/sas-2025-2(8)-72-79
2. Akimov, O. O., Andrusiak, M. V. & Rusetskyi, R. Y. (2025). Tools for enhancing personnel security under martial law: an interdisciplinary approach to polygraph application. *Efficiency of Public Administration*, *1*(82/83), 86–93. https://doi.org/10.36930/508211
3. Court of Justice of the European Union. (2009, July 16). *Infopaq International A/S v Danske Dagblades Forening* (Case C-5/08) [Judgment]. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62008CJ0005
4. European Parliament and Council of the European Union. (1996, March 11). *Directive 96/9/EC on the legal protection of databases*. *Official Journal of the European Communities*, L 77, 20–28. EUR-Lex. https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng
5. European Parliament and Council of the European Union. (2001, May 22). *Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*. *Official Journal of the European Communities*, L 167, 10–19. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
6. European Parliament and Council of the European Union. (2004, April 29). *Directive 2004/48/EC on the enforcement of intellectual property rights*. *Official Journal of the European Union*, L 157, 45–86. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0048
7. European Parliament and Council of the European Union. (2009, April 23). *Directive 2009/24/EC on the legal protection of computer programs (codified version)*. *Official Journal of the European Union*, L 111, 16–22. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2009/24/oj/eng
8. European Parliament and Council of the European Union. (2016, June 8). *Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. *Official Journal of the European Union*, L 157, 1–18. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
9. World Intellectual Property Organization. (1996, December 20). *WIPO Copyright Treaty (WCT)*. WIPO Lex. https://www.wipo.int/wipolex/en/treaties/textdetails/12740
10. World Intellectual Property Organization. (2019). *Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps"*. *WIPO Magazine* (Issue 5/2019). https://shorturl.at/9IM2Q
11. World Intellectual Property Organization. (2025). *Copyright*. Retrieved December 15, 2025, from https://www.wipo.int/en/web/copyright
12. World Trade Organization. (1994). *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)* (Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization). https://www.wto.org/english/docs_e/legal_e/27-trips.pdf

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Conclusion

Based on the research results presented by the authors in this monograph, the following conclusions can be drawn:

1. The research was conducted and demonstrated that the rapid digital transformation of public administration elevates information security to a strategic priority for modern states. In the Ukrainian context, where digital modernization is closely linked to European integration, the establishment of a resilient and coherent e document management system was substantiated as essential for transparency, democratic governance, and the protection of citizens' rights. At the same time, it was identified that the existing system continues to face structural challenges, including legal inconsistencies, fragmented institutional responsibilities, limited technical and financial capacity, weak interoperability and coordination, and safeguards that are not fully proportional to current risks. These vulnerabilities were shown to increase exposure to cybercrime, espionage, unauthorized access, and data manipulation, which undermines trust and constrains the development of digital public services.

2. The intellectual property protection in corporate information flows should be treated as a governance and control problem rather than as a set of isolated legal declarations. It was found that protection effectiveness depends primarily on daily information handling, especially the ability to preserve confidentiality across functions, platforms, and external partners through disciplined classification, access governance, and boundary management. It was also established that digital transformation expands exposure by increasing the number of flow points, accelerating dissemination, and complicating traceability after incidents, which makes lifecycle continuity and "safe pathways" for legitimate sharing essential. A portfolio approach was substantiated as more resilient than reliance on any single legal mechanism, because coherent combinations of confidentiality controls, contractual duties, and complementary IP tools improve enforceability. Finally, it was shown that evidence readiness functions as a continuous organizational capability, and that scalable protection is achieved when confidentiality is operationalized as measurable behavior embedded in accountability and repeatable controls.

3. The contemporary intellectual property landscape, globally and in Ukraine, is undergoing structural transformation driven by digitalization, data centric business models, and the rapid diffusion of artificial intelligence and distributed technologies. It was established that classical doctrinal

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

foundations increasingly interact with technological realities that challenge conventional assumptions about authorship, originality, territoriality, infringement detection, and long term preservation, while platformized cross border markets amplify legal conflicts and cybersecurity risks. For Ukraine, the analysis indicated that effective modernization requires a hybrid legal technological model of IP governance in which legal reform, institutional oversight, cybersecurity standards, and interoperable registries function together, because neither legal instruments nor technical tools are sufficient in isolation. It was also demonstrated that emerging technologies create new risks yet offer modernization opportunities, provided that auditability, safeguards, and dispute resolution frameworks are embedded into implementation, especially given wartime vulnerabilities of digital infrastructures. Future research was defined around empirical assessment of stakeholder behavior under new rules, comparative evaluation of leading innovation economies, technological study of distributed systems for archival preservation, and interdisciplinary work integrating IP law, information science, cybersecurity, and computational methods. Overall, it was concluded that Ukraine's transition to a resilient and innovation oriented IP regime depends on integrated harmonization, institutional strengthening, and technological modernization that balances rights protection with digital openness.

4. The strengthening IP protection in the EU games sector requires operational governance that links harmonised legal rules with practical controls and evidence ready enforcement. It was established that the Information Society framework supports the protection of technological measures, while the DSM architecture and Article 17 related guidance reshapes platform responsibilities around licensing and user uploaded content management. It was also shown that trademark protection and trade secret governance remain decisive because brand integrity and confidential know how underpin competitive advantage in game development and distribution. In addition, civil enforcement instruments and rapid online mechanisms, including UDRP procedures, were identified as important for limiting reputational harm in cases of piracy, impersonation, and deceptive domain practices. Overall, it was concluded that a resilient model treats IP as a measurable capability set integrating rights clarity, technical and contractual controls, market integrity measures, and enforcement readiness, while preserving legitimate user creativity and trust.

5. The blockchain technology has significant potential to strengthen the protection and management of intellectual property rights, while its legal integration remains incomplete and uneven across jurisdictions. It was

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

demonstrated that distributed ledger systems can support evidentiary certainty by enabling immutable time stamping and verifiable record keeping that assists in establishing authorship, priority, and chains of title, which is particularly valuable in copyright and patent disputes where proof is decisive. The analysis also found that smart contracts can automate licensing, lower transaction costs, and improve the transparency of royalty distribution, especially in digital content markets. Comparative review indicated that although blockchain records may be accepted as evidence in some jurisdictions, there is still no harmonized framework defining their legal effect, and regulatory initiatives that reference blockchain often remain fragmented and under specified, particularly regarding tokenized assets and decentralized ownership patterns. It was further established that the legal status of NFTs remains ambiguous, since courts and policymakers continue to struggle with fitting token based transactions into traditional categories of copyright and property. Practical evaluation confirmed that blockchain can enhance traceability and support anti counterfeiting efforts, yet it cannot independently verify originality or prevent piracy, and therefore functions primarily as a complementary evidentiary and transactional tool within a broader protection ecosystem. The study also demonstrated that core doctrinal principles, including territoriality, registration requirements, and the originality standard, are not replaced by blockchain records, but instead require interpretive alignment and explicit statutory anchoring for legal certainty. Finally, it was concluded that the most effective pathway is a hybrid legal technological model in which blockchain is integrated with statutory regimes, contractual safeguards, and judicial oversight, supported by coherent legislative guidance, harmonized technical standards, and stronger international coordination to address cross border enforcement complexity.

6. The international aspects of IP protection are inseparable from contemporary assessments of business reputation because IP simultaneously provides legal defensibility and signals governance maturity. It was established that global instruments, including TRIPS and WIPO administered treaties, set baseline expectations and enable cross border protection pathways that influence how stakeholders interpret a firm's diligence, integrity, and compliance culture. The analysis also showed that cross border branding amplifies reputational exposure through counterfeiting, cybersquatting, and inadvertent infringement, which makes continuous monitoring and rapid response capacity decisive for trust preservation. Methodologically, it was substantiated that IP can be embedded in reputation assessment through indicators reflecting portfolio

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

robustness, enforcement performance, governance quality, and value linkage, with standards such as ISO 10668 and ISO 56005 supporting transparency and comparability across contexts. It was further found that in disputes, evidence quality and procedural readiness shape whether reputational harm escalates or is reframed as a resilience narrative grounded in effective governance. Overall, it was concluded that firms that operationalize IP due diligence, build robust contract architectures, and maintain digital enforcement capabilities are better positioned to protect intangible assets and sustain stakeholder trust across jurisdictions.

7. Legal protection of polygraph assessment methodologies is most robust when it is implemented as a portfolio that mirrors the layered structure of the underlying asset and its use context. Copyright protection is well suited to the expression of the methodology in tangible form, including manuals, training materials, structured reports, and software code, yet it does not grant exclusivity over the functional procedure itself or over methods of operation. This doctrinal limitation makes confidentiality a decisive layer in practice, because the competitive value of the methodology often resides in calibrated decision rules, scoring logic, procedural sequencing, and expert know how that can be replicated if disclosure occurs (World Intellectual Property Organization, 1996; World Intellectual Property Organization, 2025). Accordingly, trade secret protection and systematic know how governance become central, since the TRIPS framework and the EU Trade Secrets Directive converge on a coherent legal test based on secrecy, commercial value, and reasonable protective steps, while also attaching liability to unlawful acquisition, use, or disclosure, including breaches of confidentiality and use limitation obligations (World Trade Organization, 1994; European Parliament and Council, 2016). Within this portfolio logic, contracting and enforcement readiness operationalize rights and determine their practical effectiveness, because the design of licensing scope, role based access controls, audit trails, and rapid evidence preservation strongly influences whether remedies can be pursued without expanding disclosure of the very information that must remain confidential (European Parliament and Council, 2004; European Parliament and Council, 2016).

8. The EU's legal regulation of artificial intelligence is being shaped as an integrated framework in which the AI Act is closely connected with Directive (EU) 2019/790 on copyright in the Digital Single Market. In this configuration, copyright compliance becomes a formal governance obligation for providers of general purpose AI models, who must adopt a clearly defined policy that takes into account the Directive's "reservation of rights" mechanism. This shifts responsibility beyond purely technical

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

transparency or labelling requirements and toward internal organizational and legal procedures for handling rights holder claims, including licensing options and, where justified, restricting or removing the use of protected works. The synergy between the AI Act and the DSM Directive does not rewrite copyright law directly, but it creates a compliance infrastructure that sets a minimum standard of good faith conduct in the AI market through transparency and documentation expectations. For Ukraine, this model serves as a practical benchmark for future AI regulation and for IP harmonization within the European integration trajectory. It implies that rights holders should prepare to use training data summaries for risk identification and evidence building, while AI providers should implement machine readable labelling and structured compliance processes that balance disclosure duties with protection of trade secrets. Finally, effective implementation depends on workable harmonized standards, so that these mechanisms operate as functional, unified tools rather than remaining declaratory.

9. Online IP litigation should be treated as a coordinated enforcement strategy because digital infringement spreads quickly across platforms and jurisdictions, while evidence can be erased or recreated with minimal effort. Effective outcomes depend not only on the legal merits of the claim, but also on early sequencing: rapid containment, immediate preservation of proof, reliable attribution, and precisely targeted remedies that match the actor and the operational leverage point. A robust approach combines forum selection with evidence packages suitable for adversarial scrutiny and uses both liability focused actions and disruption measures against intermediaries where appropriate. Overall, procedural discipline and operational readiness, including coordinated work across legal, security, and business functions, enable litigation to shift from episodic takedowns to sustained deterrence and protection of intangible value.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

References

1. 100 mist – krok vpered. Monitorynh vprovadzhennia instrumentiv elektronnoho uriaduvannia, yak osnovy nadannia administratyvnykh posluh v elektronnomu vyhliadi [100 Cities – A Step Forward. Monitoring the Implementation of E-Governance Tools as the Basis for Providing Administrative Services in Electronic.
2. Akimov, O. O., Andrusiak, M. V. & Rusetskyi, R. Y. (2025). Tools for enhancing personnel security under martial law: an interdisciplinary approach to polygraph application. *Efficiency of Public Administration*, *1*(82/83), 86–93. https://doi.org/10.36930/508211
3. Akimov, O., & Andrusiak, M. (2025). Professional standardization of polygraph examiner's psychophysiological competencies in the context of ukraine's national security. *Society and Security*, (2(8), 72–79. https://doi.org/10.26642/sas-2025-2(8)-72-79
4. Bajwa, R., & Meem, F. T. (2024). Intellectual Property Blockchain Odyssey: Navigating Challenges and Seizing Opportunities. URL: https://arxiv.org/html/2410.08359v1
5. Berne Notification No. 169. [Berne Convention for the Protection of Literary and Artistic Works]. Accession by Ukraine. URL: https://surl.li/cwovek
6. Bilyk, P. (2024). *AI Act: A new era of artificial intelligence regulation in Europe*. Liga Zakon: Analytics. https://surl.lt/xrykty
7. Blockchain and Intellectual Property. (2019). URL: https://www.wipo.int/en/web/cws/blockchain-and-ip
8. Blockchain technologies and IP ecosystems: A WIPO white paper. (2022). URL: https://surl.li/kgsezu
9. Brittain, B. (2024, May 20). *OpenAI loses fight to keep ChatGPT logs secret in copyright case*. Reuters. https://surl.li/kwewyy
10. Bryntsev, O. V. (2016). "Electronic Court" in Ukraine: Experience and prospects [Monograph]. Kharkiv: Pravo.
11. Claeys, A. S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the situational crisis communication theory and the moderating effects of locus of control. *Public Relations Review, 36*(3), 256–262. https://doi.org/10.1016/j.pubrev.2010.05.004
12. Clark, B. (2018). Blockchain and IP Law: A Match made in Crypto Heaven? URL: https://surl.lt/ukevhm

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

13. Concept for the Development of E-Government in Ukraine. (2010). URL: http://zakon2.rada.gov.ua/laws/show/2250-2010-%D1%80/ed20110926
14. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.108. [E-resource]. – Access mode: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
15. Coombs, W. T. (2007). Protecting organizational reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*, 163–176. https://doi.org/10.1057/palgrave.crr.1550049
16. Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. https://rm.coe.int/1680afae3c
17. Court of Justice of the European Union. (2009, July 16). *Infopaq International A/S v Danske Dagblades Forening* (Case C-5/08) [Judgment]. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62008CJ0005
18. Court of Justice of the European Union. (2013). *Peter Pinckney v KDG Mediatech AG* (Case C-170/12). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0170
19. Court of Justice of the European Union. (2014). *Nintendo Co. Ltd and Others v PC Box Srl and 9Net Srl (Case C-355/12).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0355
20. Court of Justice of the European Union. (2020). *Constantin Film Verleih GmbH v YouTube LLC and Google Inc.* (Case C-264/19). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0264
21. Danilchenko, O. (2017). Blokchejn: yurist iz mashiny [Blockchain: Lawyer in the Car]. [YURIST&ZAKON. 2017. № 21]. URL: http://uz.ligazakon.ua/magazine_article/EA010438
22. Data as an IP Asset. (2023). URL: https://surl.li/ogsheh
23. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. URL: https://surl.lu/bpozhj
24. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). URL: https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

25. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). URL: https://surl.li/vpnsdn
26. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal L 281. 23/11/1995. - P. 0031-0050.
27. Directive 98/34/EC Of the European Parliament and of the Council of 22 June 1998 on the laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services // Official Journal L 204. 21.7.1998. – P.37
28. Djamane, D. (2025). Smart Contracts: Global Perspectives and Legal Realities – Part 2 - Daily Jus URL: https://surl.lt/nmgknb
29. Dorigo, L. (2022). Smart Contracts work – but do they hold up in court? | Pestalozzi Attorneys at Law. URL: https://surl.li/mndszc
30. Dubov, D. Dubova S. (2006). Osnovy elektronnoho uriaduvannia. Navchalnyi posibnyk [Fundamentals of electronic governance. Textbook]. [Kyiv: Tsentr navchalnoi literatury]. –176p.
31. Dynis, G. G. (2011). International legal concepts of global law, Internet law or cyberlaw and transformation of international law. Journal of the Kyiv University of Law, 2, 283.
32. ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection. (2023) URL: https://surl.li/nivgkp
33. Epic Games. (2025). *Fan Content Policy*. Retrieved December 14, 2025, from: https://www.epicgames.com/site/en-US/fan-art-policy
34. EUIPO connects to TMview and DesignView through blockchain. URL: https://surl.li/hvhixr
35. EUR-Lex. (2018, June 11). *Enforcement of intellectual property rights* (summary). https://eur-lex.europa.eu/EN/legal-content/summary/enforcement-of-intellectual-property-rights.html
36. European Commission. (2021). *Guidance on Article 17 of Directive (EU) 2019/790 on copyright in the Digital Single Market* (COM/2021/288 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0288
37. European Parliament & Council of the European Union. (2016, April 27). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free*

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://surl.lu/offgny

38. European Parliament & Council of the European Union. (2019, April 17). *Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*. Official Journal of the European Union, L 130, 92–125. https://surl.li/mdoooy
39. European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 on artificial intelligence (AI Act)*. Official Journal of the European Union, L 1689. https://surl.li/ylettv
40. European Parliament & Council. (1996). *Directive 96/9/EC of 11 March 1996 on the legal protection of databases*. https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng
41. European Parliament & Council. (1998). *Directive 98/71/EC of 13 October 1998 on the legal protection of designs*. https://eur-lex.europa.eu/eli/dir/1998/71/oj/eng
42. European Parliament & Council. (2001). *Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
43. European Parliament & Council. (2004). *Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights*. https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng
44. European Parliament & Council. (2009). *Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs*. https://eur-lex.europa.eu/eli/dir/2009/24/oj/eng
45. European Parliament & Council. (2012). *Regulation (EU) No 386/2012 of 19 April 2012 on entrusting the Office for Harmonization in the Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0386
46. European Parliament & Council. (2015). *Directive (EU) 2015/2436 of 16 December 2015 to approximate the laws of the Member States relating to trade marks (recast)*. https://eur-lex.europa.eu/eli/dir/2015/2436/oj/eng
47. European Parliament & Council. (2016). *Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

48. European Parliament & Council. (2017). *Regulation (EU) 2017/1001 of 14 June 2017 on the European Union trade mark (codification).* https://eur-lex.europa.eu/eli/reg/2017/1001/oj/eng
49. European Parliament & Council. (2019). *Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770
50. European Parliament & Council. (2019). *Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market*. https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng
51. European Parliament & Council. (2022). *Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
52. European Parliament & Council. (2024). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
53. European Parliament and Council of the European Union. (1996, March 11). *Directive 96/9/EC on the legal protection of databases*. *Official Journal of the European Communities*, L 77, 20–28. EUR-Lex. https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng
54. European Parliament and Council of the European Union. (2000). *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive).* https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng
55. European Parliament and Council of the European Union. (2001, May 22). *Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*. *Official Journal of the European Communities*, L 167, 10–19. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
56. European Parliament and Council of the European Union. (2004, April 29). *Directive 2004/48/EC on the enforcement of intellectual property rights*. *Official Journal of the European Union*, L 157, 45–86. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0048
57. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC on the enforcement of intellectual property rights.* https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

58. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights*. https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng
59. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048
60. European Parliament and Council of the European Union. (2007). *Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II)*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007R0864
61. European Parliament and Council of the European Union. (2009, April 23). *Directive 2009/24/EC on the legal protection of computer programs (codified version)*. *Official Journal of the European Union*, L 111, 16–22. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2009/24/oj/eng
62. European Parliament and Council of the European Union. (2012). *Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Recast)*. https://eur-lex.europa.eu/eli/reg/2012/1215/oj/eng
63. European Parliament and Council of the European Union. (2014). *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910
64. European Parliament and Council of the European Union. (2016, June 8). *Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. *Official Journal of the European Union*, L 157, 1–18. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
65. European Parliament and Council of the European Union. (2016). *Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

66. European Parliament and Council of the European Union. (2017). *Regulation (EU) 2017/1001 on the European Union trade mark.* https://eur-lex.europa.eu/eli/reg/2017/1001/oj/eng
67. European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Services Act).* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
68. European Union Intellectual Property Office. (2019). *The risks posed by counterfeits to consumers: A qualitative study*. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers/2019_Risks_Posed_by_Counterfeits_to_Consumers_FullR_en.pdf
69. European Union Intellectual Property Office. (2019). *The risks posed by counterfeits to consumers: A qualitative study.*https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers/2019_Risks_Posed_by_Counterfeits_to_Consumers_FullR_en.pdf
70. European Union. (2002). *Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs.* https://eur-lex.europa.eu/eli/reg/2002/6/oj/eng
71. European Union. (2016). *Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
72. For the first time in ukraine, copyright is registered for works that include AI-generated images. (2024). URL: https://surl.li/cvslic
73. Fortune Media. (2025, January 29). *World's most admired companies*. https://fortune.com/ranking/worlds-most-admired-companies/ Fortune
74. Harasym, O. R., Komova, M. V., & Lytvyn, V. V. (2010). Orhanizatsiia zakhyshchenoho elektronnoho dokumentoobihu v merezhakh elektronnoho uriaduvannia [Organization of Secure Electronic Document Workflow in E-Governance Networks]. URL: https://lnk.ua/q462yyO4J
75. Hasselbalch, G. (2029). *A human-centric approach to AI: The EU Ethics Guidelines for AI*. DataEthics. https://surl.li/frmohg
76. Hayashi Y., Johoka Shakai (1969). Hado no Shakai Kara Sofuto no Shakai e [The Information Society: From Hard to Soft Society]. Tokyo: Kodansha Gendai Shinso, 1969. 209 p.
77. Hohn-Hein, N. (2022). EU IP Office launches first blockchain-based

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

IP register, Anti-Counterfeiting Blockathon Forum. URL: https://surli.cc/leegiq
78. ICANN. (2020). *Uniform Domain Name Dispute Resolution Policy (UDRP)*. https://www.icann.org/resources/pages/policy-2012-02-25-en
79. Intellectual Property (Stanford Encyclopedia of Philosophy). URL: https://plato.stanford.edu/entries/intellectual-property/
80. Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art. (2022). URL: https://surl.li/yttfdp
81. International Organization for Standardization, & International Electrotechnical Commission. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements.* ISO. https://www.iso.org/standard/27001
82. International Organization for Standardization, & International Electrotechnical Commission. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: Information security controls.* ISO. https://www.iso.org/standard/75652.html
83. International Organization for Standardization. (2010). *Brand valuation: Requirements for monetary brand valuation (ISO 10668:2010)*. https://www.iso.org/standard/46032.html
84. International Organization for Standardization. (2012). *ISO/IEC 27037:2012 Information technology: Security techniques: Guidelines for identification, collection, acquisition, and preservation of digital evidence.*https://www.iso.org/standard/44381.html
85. International Organization for Standardization. (2020). *Innovation management: Tools and methods for intellectual property management: Guidance (ISO 56005:2020)*. https://www.iso.org/standard/72761.html
86. Internet Corporation for Assigned Names and Numbers. (2020). *Uniform Domain-Name Dispute-Resolution Policy (UDRP).* https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-01-01-2020-en
87. Internet Corporation for Assigned Names and Numbers. (2020). *Uniform Domain-Name Dispute-Resolution Policy*. https://www.icann.org/resources/pages/uniform-domain-name-dispute-resolution-policy-01-01-2020-en

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

88. Kim, P. H., Dirks, K. T., & Cooper, C. D. (2009). The repair of trust: A dynamic bilateral perspective and multilevel conceptualization. *Academy of Management Review, 34*(3), 401–422. https://doi.org/10.5465/amr.2009.40631887
89. Korzhevskyi, I. (2025). A Conceptual Approach to Enhancing Enterprise Economic Security Under the Influence of Business. *Economy and Society*, (73). https://doi.org/10.32782/2524-0072/2025-73-121
90. Korzhevskyi, I. (2025). Methodological Approaches to Assessing Corporate Reputation and Economic Security of Enterprises. *Economics, Finance and Management Review*, (3(23), 106–118. https://doi.org/10.36690/2674-5208-2025-3-106-118
91. Krat, V. (2024). *Will artificial intelligence rule the "authorial" world: A judge's thoughts on the nature of AI regulation*. Supreme Court: Expert discussion "Sui generis right to protect AI 'creations'". https://surl.li/dcbbek
92. Kyrylenko, A. (2024). Ukrainian IP Office registers works incorporating AI-generated content protected under new sui generis right - The IPKat. URL: https://surl.li/gzujju
93. Law of Ukraine "Pro elektronni dokumenty ta elektronnyi dokumentoobih" [On Electronic Documents and Electronic Document Management] (2003). (No. 851-IV). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
94. Lee, E. (2023) NFTs as Decentralized Intellectual Property. URL: https://illinoislawreview.org/wp-content/uploads/2023/08/Lee.pdf
95. Len, G. D., & Mann, E. C. Benefits and Considerations of Protecting Your IP With Blockchain Technology. (2025). URL: https://surl.lu/zzqvsv
96. Levi, S. D., & Ghaemmaghami, M. (2025). Copyright Office Weighs In on AI Training and Fair Use | Skadden, Arps, Slate, Meagher & Flom LLP. URL: https://surl.li/hztxut
97. Li, C. (2025). Japan unveils 2025 IP strategy to climb global innovation rankings | Asia IP. URL: https://surl.lt/eienqg
98. Lince, T., Little, T., &Diakun B. (2021). EUIPO approves blockchain platform; NFT trademark mystery; SHOP SAFE Act hearing set – news digest. URL: https://surl.li/gqzhxf
99. Maidannyk, L. (2024). *Towards the EU: Legislative changes in Ukraine regarding copyright*. *Yuridichna Gazeta*, 3(781). https://surl.li/avlhyw

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

100. Marchenko V. V. Elektronne uriaduvannia v orhanakh vykonavchoi vlady: administratyvno-pravovi zasady [Electronic Governance in Executive Bodies: Administrative and Legal Basis] : Monograph / V. V. Marchenko. – Kharkiv: Panov, 2016. – 444p.
101. Marchenko, V., & Dombrovska, A. (2025). GLOBAL SOLUTIONS FOR SAFEGUARDING INTELLECTUAL PROPERTY: HOW BLOCKCHAIN REVOLUTIONIZES DIGITAL RIGHTS MANAGEMENT. *Public Administration and Law Review*, (2(22), 81–89. https://doi.org/10.36690/2674-5216-2025-2-81-89
102. Marchenko, V.. The Evolution of Information Security Framework in Ukraine: European Integration and Legal Perspectives. In *International conference on Economics, Accounting and Finance*. Retrieved from https://conf.scnchub.com/index.php/ICEAF/ICEAF-2024/paper/view/806
103. Markets in Crypto-Assets Regulation (MiCA). (2025). URL: https://surli.cc/iknsyg
104. Masuda, Y. (1980). The information society as a post-industrial society. World Future Society.
105. McGowan, B. (2025). Deepfake threats to companies. URL: https://surl.li/aygtyg
106. Meta. (2025, October 25). *Privacy Policy*. https://www.facebook.com/privacy/genai
107. Mihus, O. (2024). STRENGTHENING INTELLECTUAL PROPERTY PROTECTION IN THE EU: IT LAW AND ITS IMPACT ON THE COMPUTER GAMES INDUSTRY. *Public Administration and Law Review*, (4(20), 20–34. https://doi.org/10.36690/2674-5216-2024-4-20-34
108. Ministry of Digital Transformation of Ukraine & Office of the Ombudsman of Ukraine. (2024). *Human rights in the age of artificial intelligence: Challenges and legal regulation*. https://surli.cc/dhwont
109. Ministry of Digital Transformation of Ukraine. (2024, January). *Guidelines for responsible use of artificial intelligence for media*. https://surl.li/ejekki
110. Ministry of Digital Transformation of Ukraine. (2024). *Glossary of terms in the field of artificial intelligence*. https://surl.li/pucezu
111. Ministry of Digital Transformation of Ukraine. (2024). *White paper on the regulation of artificial intelligence in Ukraine: Vision of the Ministry of Digital Transformation (Consultation version)*. https://surl.li/vgnrns

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

112. Ministry of Digital Transformation of Ukraine. (2025, July). *Guidelines for responsible use of artificial intelligence for legal professionals*. https://surli.cc/qrmood
113. Ministry of Economy and WIPO sign Memorandum of Cooperation. URL:https://surl.li/plmgvj
114. Ministry of Economy of Ukraine, Intellectual Property and Innovation Office. (2024, November). *Guidelines on responsible use of artificial intelligence: Intellectual property issues*. https://surli.cc/tbvymf
115. Moille, C. (2025). France Takes Pioneering Step in Recognizing Blockchain Time-Stamping as Proof of Authorship in Intellectual Property. URL: https://surl.lt/vtmrui
116. Mojang Studios. (2025). *Minecraft usage guidelines.* Retrieved December 14, 2025, from: https://www.minecraft.net/en-us/usage-guidelines
117. Naisbitt, J. (1982). Megatrends: Ten new directions transforming our lives. Warner Books.
118. Non-Fungible Tokens and Intellectual Property: A Report to Congress. (2024). URL: https://surl.li/jcrygm
119. OECD. (2021). *Illicit trade: Misuse of e-commerce and online platforms for trade in counterfeits.* OECD Publishing. https://www.oecd.org/en/publications/illicit-trade-misuse-of-e-commerce-and-online-platforms-for-trade-in-counterfeits_07d1032d-en.html
120. OECD. (2025). *Mapping the global trade in fakes: Global trends and enforcement challenges.* OECD Publishing. https://www.oecd.org/en/publications/mapping-the-global-trade-in-fakes_8b2be95f-en.html
121. OpenAI. (2025, October 25). *Terms of Use*. https://openai.com/uk-UA/policies/usage-policies/
122. Organisation for Economic Co-operation and Development, & European Union Intellectual Property Office. (2025). *Mapping the global trade in fakes: Global trends and enforcement challenges*. OECD Publishing. https://www.oecd.org/en/publications/mapping-the-global-trade-in-fakes_8b2be95f-en.html
123. Organisation for Economic Co-operation and Development. (2021). *Illicit trade: Misuse of e-commerce and online platforms for trade in counterfeits*. OECD Publishing. https://www.oecd.org/en/publications/illicit-trade-misuse-of-e-commerce-and-online-platforms-for-trade-in-counterfeits_07d1032d-en.html

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

124. Oxford Insights. (2022–2024). *Identifying risks in public contracts: Generative AI and the Company Analysis Tool*. https://surl.li/nfgyye
125. Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Papers, NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
126. Preparing for the Ukraine-European Commission negotiating: copyright. URL: https://nipo.gov.ua/en/ua-mock-session-7-d2-en/
127. Ramalho, A. (2021). *Intellectual property protection for AI-generated creations*. Routledge. https://surl.li/lfskzy
128. Ramos, A. (2022). The metaverse, NFTs and IP rights: to regulate or not to regulate? URL: https://surl.li/ycypcv
129. Rechardt, L. (2015). Streaming and Copyright: a Recording Industry Perspective. URL: https://surl.lu/vdwavt
130. Reggianini, E. (2025). Standardizing On-chain IP Rights Management. URL:https://surl.li/dxyajr
131. Reputation Institute. (2016, March 22). *2016 Global RepTrak® 100: The world's most reputable companies*. https://www.rankingthebrands.com/PDF/Global%20RepTrak%20100%20Report%202016%2C%20Reputation%20Institute.pdf
132. Reuters. (2025, July 15). *Roblox launches IP licensing platform, partners with Netflix, Lionsgate.* https://www.reuters.com/business/media-telecom/roblox-launches-ip-licensing-platform-partners-with-netflix-lionsgate-2025-07-15/
133. Rindova, V. P., Williamson, I. O., Petkova, A. P., & Sever, J. M. (2005). Being good or being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal, 48*(6), 1033–1049. https://doi.org/10.5465/amj.2005.19573108
134. Roblox. (2025-a). *Roblox Terms of Use.* Retrieved December 14, 2025, from: https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use
135. Roblox. (2025-b). *License Manager Terms.* Retrieved December 14, 2025, from: https://en.help.roblox.com/hc/en-us/articles/42542704086548-License-Manager-Terms
136. Rosati, E. (2022). The missing link: How blockchain technology can help protect IP owners and consumers. URL: https://surl.li/pngeso
137. Rose, A. (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. URL: https://surl.li/sdrxzm

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

138. Rose, A. (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. URL: https://surl.li/inkqba
139. Rota, D., & Douglass S. M. (2024). Don't Forget About NFTs! USPTO and USCO Issue Joint Study on the Interplay Between NFTs and Intellectual Property. URL: https://surl.li/vlyuzq
140. Roth, E. (2025, November 12). *Roblox is opening up its IP licensing platform. The Verge.* https://www.theverge.com/news/819407/roblox-is-opening-up-its-ip-licensing-platform
141. Rubryka. (2024, September 24). *Solutions from Ukraine: Ukrainian IP Office grants copyright to AI-generated images for first time*. https://surl.li/czcath
142. Sabreen, A. (2023). Online courts and private and public aspects of open justice: Enhancing access to court or violating the right to privacy? The Age of Human Rights Journal, 20. https://doi.org/10.17561/tahrj.v20.7516
143. Savchuk, V., & Tsurkan, O. (2025). Legal Landscapes: Ukraine – Intellectual Property. URL: https://surl.li/crdlvh
144. Schmalenberger, A. (2022). Smart contracts in the Data Act. URL: https://surl.li/xybtvw
145. Shakhatreh, H. (2024). Comparison of Commercial Dispute Resolution Mechanisms in Jordan and the Middle East. *Public Administration and Law Review*, (2(18), 51–66. https://doi.org/10.36690/2674-5216-2024-2-51-66
146. Shakhatreh, H. J. M. (2023). Development of E-Commerce within the Framework of Compliance with Financial Law. *Financial and Credit Activity Problems of Theory and Practice*, *4*(51), 429–439. https://doi.org/10.55643/fcaptp.4.51.2023.4123
147. Shakhatreh, H., & Ababneh, E. M. (2023). The main ways of leaking commercial secrets and measures to protect them. *Economics, Finance and Management Review*, (2), 76–82. https://doi.org/10.36690/2674-5208-2023-2-76-82
148. Sharp, A. J. & Lobel, O. (2023). Smart Royalties: Tackling the Music Industry's Copyright Data Discrepancies through Blockchain Technology, Smart Contracts, and Non-Fungible Tokens. URL: https://surl.li/cfjdvc
149. Somal, S. (2025). The Increasing Threat of Cyber Espionage and Its Impact on Trade Secret Protection. URL: https://surl.li/zgdecf

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

150. Susskind, R. (2020). Online court and the future of justice. Oxford University
Press. https://doi.org/10.1093/oso/9780198838364.001.0001
151. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.
152. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.
153. The Green Paper on the Electronic Governance in Ukraine. URL: http://etransformation.org.ua/2014/11/24/355/
154. The RepTrak Company. (2020). *2020 Global RepTrak: A decade of reputation leaders*. https://www.reptrak.com/wp-content/uploads/2022/04/2020-Global-RepTrak-Report.pdf
155. Toffler, A. (1980). The third wave. Morrow. URL: https://surl.li/qfsbhv
156. UANIPIO is in the process of integration with WIPO digital platforms. URL: https://nipo.gov.ua/en/integration-wipo-digital-platforms-ga-2025/
157. Vasyliev, S. (2025). The Genesis of Online Dispute Resolution in Ukraine. *Public Administration and Law Review*, (3(23), 65–79. https://doi.org/10.36690/2674-5216-2025-3-65-79
158. Verkhovna Rada of Ukraine. (2022, December 1). *Law of Ukraine "On copyright and related rights" (No. 2811-IX). https://surl.li/bnqgnt*
159. Walport, M. (2016). Distributed ledger technology: Beyond blockchain. UK Government Office for Science.
160. WCT Notification No. 30. [WIPO Copyright Treaty]. Accession by Ukraine. URL: https://surl.lt/hbopek
161. What is Intellectual Property? URL: https://surl.li/vgmkpj
162. Whiddington, R. (2024, August 15). *Artists have won a small victory in a potentially landmark artificial intelligence copyright case*. Artnet. https://surli.cc/heagsn
163. World Intellectual Property Organization. (1996, December 20). *WIPO Copyright Treaty (WCT)*. WIPO Lex. https://www.wipo.int/wipolex/en/treaties/textdetails/12740
164. World Intellectual Property Organization. (2017). *WIPO Overview 3.0: WIPO Panel Views on Selected UDRP Questions*.https://www.wipo.int/amc/en/domains/search/overview3.0/
165. World Intellectual Property Organization. (2019). *Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps". WIPO Magazine* (Issue 5/2019). https://shorturl.at/9IM2Q

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

166. World Intellectual Property Organization. (2019). *Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps". WIPO Magazine.* https://www.wipo.int/en/web/wipo-magazine/articles/protecting-trade-secrets-how-organizations-can-meet-the-challenge-of-taking-reasonable-steps-41043
167. World Intellectual Property Organization. (2025). *Copyright*. Retrieved December 15, 2025, from https://www.wipo.int/en/web/copyright
168. World Intellectual Property Organization. (2025). *Summary of the Berne Convention for the Protection of Literary and Artistic Works (1886)*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/ip/berne/summary_berne
169. World Intellectual Property Organization. (2025). *Summary of the Paris Convention for the Protection of Industrial Property*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/ip/paris/summary_paris
170. World Intellectual Property Organization. (2025). *Summary of the Madrid Agreement concerning the international registration of marks*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/registration/madrid/summary_madrid_marks
171. World Intellectual Property Organization. (2025). *Summary of the Patent Cooperation Treaty (PCT) (1970)*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/registration/pct/summary_pct
172. World Intellectual Property Organization. (2025). *Trade secrets*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/trade-secrets
173. World Intellectual Property Organization. (2025). *WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).* https://www.wipo.int/amc/en/domains/guide/
174. World Intellectual Property Organization. (2025). *WIPO guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*. Retrieved December 14, 2025, from https://www.wipo.int/amc/en/domains/guide/
175. World Intellectual Property Organization. (2025). *WIPO guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).* Retrieved December 14, 2025, from: https://www.wipo.int/amc/en/domains/guide/

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

176. World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization). https://www.wto.org/english/docs_e/legal_e/27-trips.pdf Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177–186. https://doi.org/10.1016/S0363-8111(97)90023-0
177. World Trade Organization. (1994). *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization)*.https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm
178. World Trade Organization. (2025). *Agreement on Trade-Related Aspects of Intellectual Property Rights: Part III, enforcement of intellectual property rights*. Retrieved December 14, 2025, from https://www.wto.org/english/docs_e/legal_e/27-trips_05_e.htm
179. Xalabarder, R. (2002). Copyright: Choice of Law and Jurisdiction in the Digital Age. URL: https://surl.li/krkbzb

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Intellectual property: protection in modern conditions

Monograph

Number of copies: 300
First printing: December 17, 2025
DOI: https://doi.org/10.36690/IPP
Distributed worldwide by ***Scientific Center of Innovative Research OÜ***
office@scnchub.com
Full text available online at https://scnchub.com

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)