Saidov Bakhodirkhuja Nosirkhujaevich
Independent Researcher of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Scientific Supervisor: Khayrulla Mamatovich Kilichev,
Head of the Department of Civil Law Disciplines,
Doctor of Philosophy (PhD) in Law, Associate Professor.

“PROSPECTS FOR THE IMPROVEMENT OF CIVIL LAW RELATIONS ARISING FROM CONTRACTS ON ENSURING THE CYBERSECURITY OF PROTECTED OBJECTS”

Abstract: This article analyzes the prospects for improving the civil law regulation of contracts related to ensuring the cybersecurity of protected facilities. The study substantiates that, in the context of the digital economy and information society, the legal nature of protected facilities is undergoing significant transformation, thereby necessitating the legal regulation of contractual relations aimed at ensuring cybersecurity alongside traditional security service relations. The article examines the legal nature of cybersecurity service contracts, their place within the system of civil law, the rights and obligations of the parties, as well as existing legal issues related to liability for cyber incidents, compensation for damages, and the application of penalty clauses. Based on a comparative analysis of national legislation and the legal practices of foreign countries, the author develops scientific proposals and recommendations aimed at improving the legal regulation of contracts concerning the cybersecurity of protected facilities, determining the legal status of cyber objects, introducing special contractual frameworks, and establishing effective liability mechanisms.

Keywords: Security contract, cybersecurity, protected facility, cyber object, information system, digital infrastructure, cyber incident, cyberattack, contractual relations, civil liability, penalty clause, compensation for damages, legal gap, digital economy, information security, legislative improvement, contract law, cybersecurity service.

Although the Law of the Republic of Uzbekistan No. ZRU-778 “On Security Activities” dated 15 June 2022 (hereinafter referred to as “Law No. ZRU-778”) does not provide a direct legal definition of the term “security,” it does define the concept of “security activities.” According to the Law, security activities refer to the protection of guarded facilities, as well as activities aimed at ensuring access control and maintaining internal security regimes at protected facilities of legal entities. It should be noted that the concepts of “security” and “security activities” are distinct and should not be treated as synonymous, as such an approach is unjustified from both theoretical and practical perspectives.[1] In this regard, it would be appropriate to introduce a separate legal definition of the term “security” into the Law of the Republic of Uzbekistan No. ZRU-778 “On Security Activities.”First, the current version of the Law provides a definition only for the concept of “security activities,” which denotes a specific set of actions and service-related processes. In other words, security activities constitute practical measures aimed at protecting guarded facilities and ensuring compliance with access-control procedures and internal security regimes. Therefore, this concept primarily reflects an organizational and operational process.

Based on the analyses presented in the preceding sections concerning the civil-law regulation of contracts related to ensuring the cybersecurity of protected facilities, it can be concluded that national legislation currently relies on general civil-law provisions to regulate such legal relations. However, the highly technological nature of cybersecurity services, the specific characteristics of digital assets, and the global nature of cyber threats have given rise to a number of legal gaps in this area. In particular, although the concept of protected facilities and their categories are recognized under national legislation, the legal status of a “protected

cyber object" remains undefined. Unlike the objects involved in traditional security relationships, cybersecurity relations may involve servers, databases, digital platforms, and other digital assets as objects of protection. In such circumstances, the legal nature of a security contract may also undergo significant transformation. A further issue is that the concept of a "protected cyber object" is not provided for in the current legislation at all, which gives rise to a number of legal uncertainties. The absence of a clear legal definition and regulatory framework for protected cyber objects creates difficulties in determining the subject matter of cybersecurity contracts, the scope of the parties' rights and obligations, and the allocation of liability for failures to ensure cybersecurity.

First, it remains unclear which digital resources may constitute independent objects of a security contract. For example, current legislation does not provide a clear answer as to whether a website, domain name, cryptocurrency wallet, or artificial intelligence model may be recognized as an object of protection under a security agreement.

Second, the scope of obligations imposed on the provider of security services remains uncertain. This is because the protection of a tangible object and the cybersecurity protection of digital infrastructure represent fundamentally different types of activities in terms of their nature, methods, and objectives.

Third, where damage is caused to a protected cyber object, determining the subject matter of civil liability and the composition of damages becomes considerably more complex. For instance, assessing losses resulting from the destruction of a database, the theft of crypto-assets, or unauthorized interference with an artificial intelligence model requires, as a preliminary matter, the establishment of the legal status of the relevant object. Without a clearly defined legal framework governing protected cyber objects, the proper determination of liability and the calculation of damages may give rise to significant legal challenges.

From this perspective, it is necessary to establish the digital object of security relations as a separate legal category within the legislation.

Therefore, it is proposed to supplement Article 3 (“Basic Definitions”) of Law No. ZRU-778 with the following new definition: “Protected cyber object” means an information system, information resource, database, server, digital platform, website, cloud infrastructure, digital asset, crypto-asset, artificial intelligence system, or any other object of the digital environment that is created, stored, processed, or transmitted through information and communication technologies; that constitutes an object of property or other legal rights in accordance with the legislation; and that is subject to protection against unauthorized access, use, modification, destruction, blocking, or other cyber threats.

Based on the proposed definition, it may be concluded that a protected cyber object is a digital asset, information resource, or information and communication infrastructure that possesses economic or social value as an object of civil rights and requires protection through special cybersecurity measures aimed at ensuring its confidentiality, integrity, and availability.

The incorporation of the above-mentioned provision into the legislation would contribute to clarifying the modern scope of objects subject to security activities and to determining the legal nature of cybersecurity services.

Another legal gap in Law No. ZRU-778 is the absence of provisions identifying entities authorized to provide cybersecurity services. Article 9 of the Law recognizes state security units, departmental security services, and militarized security units as subjects of security activities. While this approach may be sufficient for the physical protection of tangible objects, it is inadequate for the legal regulation of cybersecurity services that have emerged in the context of the digital economy. The essence of the problem lies in the fact that ensuring the cybersecurity of protected facilities requires specialized knowledge, advanced technical tools, and highly qualified professionals, which fundamentally distinguishes such activities from traditional security services. In particular, Article 9 of the Law does not envisage organizations operating in the field of cybersecurity as subjects of security activities. At the same time, despite the significant role

currently played by the State Institution “Cybersecurity Center” in the field of cyber protection, as well as its cooperation with the Ministry of Digital Technologies of the Republic of Uzbekistan, there is no clearly established legal framework enabling these entities to provide cybersecurity services on an outsourcing basis. The Cybersecurity Center performs a number of important functions, including monitoring and analyzing information security threats, studying methods used by offenders in cyberspace, certifying hardware and software products, assisting public authorities in developing and implementing information security policies, ensuring the security of state information systems and resources, and providing timely notifications to users regarding cybersecurity threats. This legal gap is particularly evident in two key areas.

First, there is no unified legal mechanism governing the licensing, accreditation, and registration of cybersecurity service providers in the state register. As a result, uniform requirements concerning the qualifications, technical capabilities, and liability of organizations engaged in the protection of information systems have not been established.

Second, although Article 5 of the Law assigns responsibility for implementing a unified technical policy in the field of security systems and technical means of protection, it remains unclear which authority is responsible for developing and coordinating such a policy in the field of cybersecurity. In practice, these functions are divided among several institutions, including the Ministry of Digital Technologies, the Cybersecurity Center, and the Security Department under the Ministry of Internal Affairs. Such fragmentation of authority may lead to overlapping functions, duplication of responsibilities, and inefficiencies in the implementation of cybersecurity measures.

In light of these circumstances, it appears both legally and practically preferable for the Security Department to enter into outsourcing agreements with specialized state bodies and organizations in the field of cybersecurity rather than attempting to ensure the cybersecurity of protected facilities independently. Cybersecurity is a highly specialized field in which threats evolve continuously,

while protective technologies require constant updating and improvement. Given that the primary function of the Security Department is the organization of physical security, independently performing all cybersecurity-related functions may result in excessive financial and organizational costs. Accordingly, the involvement of specialized cybersecurity institutions through contractual outsourcing arrangements would contribute to improving the quality, effectiveness, and sustainability of cybersecurity protection for guarded facilities.

Under an outsourcing agreement, the Ministry of Digital Technologies and the Cybersecurity Center may perform a range of functions, including continuous monitoring of the information systems of protected facilities, early detection of cyber incidents and prompt incident response, conducting information security audits, assessing the level of protection of servers and databases, ensuring the security of artificial intelligence technologies used within security systems, providing cyber protection for video surveillance and alarm systems, and facilitating the rapid exchange of information concerning cyber threats.

The legal significance of such cooperation lies in the fact that an outsourcing agreement enables the clear allocation of rights and obligations among the parties, the establishment of service standards and quality indicators, the determination of liability in the event of cyberattacks, and the specification of requirements for ensuring data confidentiality. As a result, a comprehensive protection mechanism integrating both the physical security and cybersecurity of protected facilities can be established.

In this regard, it would be appropriate to supplement Law No. ZRU-778 with the following provision: *"For the purpose of ensuring the cybersecurity of protected facilities, the Security Department may conclude outsourcing agreements with the Ministry of Digital Technologies, the Cybersecurity Center, and cybersecurity service providers accredited in accordance with the established procedure. Such agreements may provide for the monitoring of protected cyber objects, the detection and mitigation of cyber incidents, the conduct of information security audits, and the provision of other cybersecurity services."*

This approach would, on the one hand, preserve the core functions of the Security Department and, on the other hand, enable the effective utilization of the existing cybersecurity capacity of the state. More importantly, it would facilitate the development of a comprehensive approach to the security of protected facilities, whereby physical and digital protection systems are integrated within a single legal framework. Such an approach would contribute to the formation of a modern model of security activities in the context of digital transformation. At the same time, it would be necessary to amend the list of entities specified in Article 9 of Law No. ZRU-778. In particular, it would be appropriate to include the Ministry of Digital Technologies of the Republic of Uzbekistan and the State Institution "Cybersecurity Center" among the entities authorized to conduct security activities in their capacity as providers of cybersecurity services for protected facilities.

Furthermore, the Regulation on the Security Department under the Ministry of Internal Affairs of the Republic of Uzbekistan (hereinafter referred to as the "Regulation"), approved by Resolution No. PQ-360 of the President of the Republic of Uzbekistan dated 28 November 2025 "On Measures for the Effective Organization of the Activities of Internal Affairs Bodies in the Field of Security," identifies among the Department's principal tasks the implementation of a unified technical policy in the field of security systems and technical means of protection, as well as the introduction of modern information and communication technologies and artificial intelligence technologies.[2] The Regulation also provides for the use of video surveillance systems, access control systems, hardware and software complexes, unmanned devices, and other digital technologies at protected facilities. In addition, it assigns responsibility for taking measures to ensure the cybersecurity of implemented information systems. However, a comprehensive analysis of the Regulation demonstrates the existence of several independent legal gaps in the regulation of relations associated with ensuring the cybersecurity of protected facilities.

First, Paragraph 10 of Chapter 2 of the Regulation provides that, upon request from state bodies and legal entities, the Department may develop, enhance,

and maintain software products. At the same time, the Regulation assigns responsibility for ensuring the cybersecurity of implemented information systems. However, the regulatory framework does not establish the criteria by which cybersecurity services should be evaluated, nor does it define service quality indicators such as minimum security requirements, information system availability levels, vulnerability remediation deadlines, or other measurable performance standards. This deficiency may create difficulties in assessing the extent to which a service provider has properly fulfilled its contractual obligations. Therefore, it is proposed that the Regulation establish specific service quality indicators for cybersecurity services provided to protected facilities, including information system availability rates, cyber incident response times, security update implementation periods, and other relevant technical performance metrics.

Second, although the Regulation establishes procedures for detecting, eliminating, and investigating violations at protected facilities, it does not provide a separate mechanism for responding to cyber incidents. For example, in cases involving unauthorized access to servers, theft of databases, or unlawful interference with video surveillance systems, the Regulation does not specify which authority or commission is responsible for conducting an investigation, how digital evidence should be collected and preserved, or which parties bear responsibility for incident response. Accordingly, it would be appropriate to introduce a provision requiring that, in the event of a cyber incident, an official investigation be conducted with the participation of representatives of the Department, the owner of the protected facility, and designated cybersecurity specialists, while ensuring that digital evidence is collected, documented, and preserved in accordance with the requirements of applicable legislation.

Third, the Regulation requires that inspectorate supervision and inspections include an assessment of technical security equipment and video surveillance systems. However, it contains no separate provision concerning cybersecurity audits. The absence of such a requirement increases the likelihood that protected facilities may continue operating with weak passwords, outdated software, or

inadequately secured networks. For this reason, the chapter governing inspectorate supervision and inspections should be supplemented with the following provision: “Cybersecurity audits of critically important and categorized facilities shall be conducted at least once annually.”

Fourth, the Regulation stipulates that the protection of facilities shall be carried out on a contractual basis. Nevertheless, several issues of fundamental importance in the field of cybersecurity remain unregulated, including responsibility for password management, accountability for maintaining backup copies of data, and liability for damage arising from third-party software. As a result, determining responsibility in the event of a cyber incident becomes significantly more complicated. In our view, the Regulation should require that contracts relating to the cybersecurity of protected facilities expressly define the responsibilities of each party regarding the protection of information assets, the allocation of cybersecurity risks, and the procedures for coordinated action in the event of a cyber incident. The implementation of these proposals would significantly strengthen the legal foundations of the Department’s activities in ensuring the digital security of protected facilities and would contribute to the development of a more effective and comprehensive cybersecurity governance framework.

An analysis of the Cybersecurity Strategy of the Republic of Uzbekistan for 2026–2030, approved by Presidential Decree No. PF-38 of 10 March 2026 “On Defining the Cybersecurity Strategy of the Republic of Uzbekistan and Improving the System for the Prevention of Cybercrime,” demonstrates that ensuring the stable and uninterrupted operation of critical information infrastructure facilities, monitoring cyber incidents, providing rapid responses to cyber threats, promoting public-private partnerships, and improving cybersecurity legislation have been identified as key priorities of the state cybersecurity policy.[3] The Strategy further emphasizes the necessity of developing legal mechanisms, alongside organizational and technical measures, to ensure the cybersecurity of state authorities and critical information infrastructure facilities. In light of these

strategic objectives, the civil-law improvement of contracts relating to the cybersecurity of protected facilities by the Security Department under the Ministry of Internal Affairs acquires particular relevance.

At the same time, the Strategy envisages the establishment of a national cyber incident response system, the development of mechanisms for the rapid exchange of information concerning cyber threats, and the expansion of cybersecurity outsourcing services. These objectives highlight the need to clearly define the actions and responsibilities of contractual parties in the event of a cyber incident.

In practice, existing security contracts generally provide for liability in cases involving physical intrusions or attacks against protected facilities. However, the rights and obligations of the parties remain insufficiently regulated in situations involving database breaches, unauthorized access to video surveillance systems, or the compromise of software and information systems. Consequently, the existing contractual framework does not fully address the legal challenges arising from contemporary cyber threats, thereby necessitating the development of more detailed contractual provisions governing cybersecurity-related incidents and liabilities.

The Strategy identifies the development of public-private partnerships and the involvement of the private sector in the field of cybersecurity as one of its key priorities. This development necessitates the adoption of a new civil-law approach to security relations. In particular, it gives rise to the need for a legal framework governing tripartite contractual relationships among the Security Department, authorized cybersecurity institutions, and entities providing outsourced cybersecurity services.

Accordingly, taking into account the priorities and objectives established by the Strategy, the improvement of contracts relating to the cybersecurity of protected facilities should focus on several key directions. These include transforming the subject matter of security relations into a comprehensive security model encompassing the protection of digital assets and information infrastructure,

clearly defining contractual obligations relating to cyber incident response, strengthening the legal status of cybersecurity outsourcing service providers, and introducing special civil-law mechanisms aimed at ensuring the cyber resilience of critical information infrastructure facilities.The implementation of these measures would facilitate the adaptation of security activities to the realities of digital transformation and contribute to the establishment of a modern contractual framework capable of effectively addressing emerging cybersecurity challenges.

The findings of the research demonstrate that the rapid development of the digital economy, together with the widespread use of information and communication technologies in public administration, the financial and banking sector, e-commerce, and other areas, has significantly influenced the legal nature of protected facilities. As a result, new forms of contractual relations have emerged that extend beyond the scope of traditional security arrangements and are aimed at protecting information systems, databases, servers, digital platforms, and other elements of digital infrastructure from cyber threats.

In practice, legal relations concerning the cybersecurity of protected facilities are currently regulated through the general provisions of the Civil Code governing contracts for services, contracts for work and labor (contracts for services and works), and mixed contracts. However, this approach does not adequately address the specific characteristics of cybersecurity relations. In particular, issues relating to the legal status of cyber objects, the legal nature of cybersecurity services, the grounds for liability arising from cyber incidents, the criteria for assessing cyber damage, the determination of fault and causation, as well as the allocation of risks among the parties, remain insufficiently regulated under national legislation.

The analysis has demonstrated that contracts relating to the cybersecurity of protected facilities differ from traditional security contracts in terms of their legal nature. Such agreements constitute complex mixed contracts that combine elements of service provision, information services, and technical support. Consequently, the regulation of these legal relations requires not only the

application of general contractual rules but also the development of specialized legal mechanisms tailored to the specific characteristics of cybersecurity services.

Furthermore, the fact that damage in the field of cybersecurity often manifests itself in an intangible form, the complexity of calculating losses arising from cyber incidents, and the possibility that such damage may become apparent only after a considerable period of time indicate the need to reconsider traditional concepts of civil liability. In particular, given that cybersecurity services constitute a professional activity involving a heightened degree of risk, it appears appropriate to introduce broader elements of risk-based liability into the regulation of these legal relations.

Based on the findings of this research, the following scientific conclusions may be drawn:

First, contracts relating to the cybersecurity of protected facilities should be recognized within civil law as an independent contractual arrangement or, at a minimum, as a distinct category of contracts requiring special legal regulation.

Second, the legal concepts of “cyber object,” “cyber incident,” “cyber damage,” and “cybersecurity service” should be formally incorporated into national legislation.

Third, it is advisable to establish, through special legal provisions, the legal status, professional obligations, and liability standards applicable to entities providing cybersecurity services.

Fourth, the institutions of contractual penalties and compensation for damages in the field of cybersecurity should be adapted to the specific characteristics of digital relations. In particular, a special legal framework should be introduced for the assessment and recovery of cyber-related damages.

Fifth, in order to establish an effective liability mechanism for contracts relating to the cybersecurity of protected facilities, it is appropriate to incorporate into national legislation elements of the presumption of fault, liability based on professional standards, and risk-based liability.

Accordingly, the improvement of the legal regulation of contractual relations concerning the cybersecurity of protected facilities constitutes an important prerequisite for ensuring information security in the context of the digital economy, effectively protecting the rights and legitimate interests of the parties, and facilitating the adaptation of civil law to contemporary digital relations. Furthermore, such developments would provide both the theoretical and practical foundations for the emergence of a specialized civil-law institution governing cybersecurity-related contractual relations in the future.

References:

1. Law of the Republic of Uzbekistan No. ZRU-778 “On Security Activities” of 15 June 2022. National Database of Legislation of the Republic of Uzbekistan, No. 03/22/778/0525, 16 June 2022; No. 03/24/1008/0988, 2 December 2024.

2. Resolution of the President of the Republic of Uzbekistan No. PQ-360 “On Measures for the Effective Organization of the Activities of Internal Affairs Bodies in the Field of Security” of 28 November 2025. National Database of Legislation of the Republic of Uzbekistan, No. 07/25/360/1110, 29 November 2025.

3. Decree of the President of the Republic of Uzbekistan No. PF-38 “On Defining the Cybersecurity Strategy of the Republic of Uzbekistan and Improving the System for the Prevention of Cybercrime” of 10 March 2026. National Database of Legislation of the Republic of Uzbekistan, No. 06/26/38/0219, 11 March 2026.