“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=393

2026-yil
10-son
oktabr
ISSN 3093-8546



Inviolability of diplomatic premises, archives and correspondence in the digital age: the limits of applicability of the 1961 Vienna Convention to cyberspace

Azimjon Saidov,
Institute of State and Law
Independent Researcher
e-mail: saidovazimjonakmalovich@gmail.com

Аннотация. Maqolada 1961-yilgi Diplomatik munosabatlar to‘g‘risidagi Vena konvensiyasi bilan kafolatlangan diplomatik binolar, arxivlar va yozishmalarning daxlsizligi kibermakonga qay darajada tatbiq etilishi o‘rganiladi. Konvensiyaning 22, 24, 27, 30 va 40-moddalari, shartnomalarni talqin qilish usullari, Xalqaro sud amaliyoti, Tallin qo‘llanmasi 2.0 va BMT Hukumat ekspertlari guruhlarining hisobotlari tahlil qilinadi. Arxivlar va aloqa vositalari raqamli shaklidan qat’i nazar Konvensiya matni bilan himoyalanishi, binolar va diplomatik pochta tushunchalari hamda ma’lumotlarning chet el serverlarida joylashishi esa sezilarli noaniqlik tug‘dirishi asoslanadi. O‘zbekiston qonunchiligi, jumladan Konsullik nizomi va Kiberxavfsizlik to‘g‘risidagi Qonun baholanib, takliflar beriladi.

Калит сўзлар. diplomatik daxlsizlik, diplomatik arxivlar, kibermakon, Diplomatik munosabatlar to‘g‘risidagi Vena konvensiyasi, Tallin qo‘llanmasi 2.0, kiberayg‘oqchilik, ma’lumotlar elchixonasi, shartnomalarni talqin qilish, O‘zbekiston.

Аннотация. В статье исследуется, применяется ли и в каком объёме неприкосновенность дипломатических помещений, архивов и корреспонденции, гарантированная Венской конвенцией о дипломатических сношениях 1961 года, к киберпространству. Анализируются статьи 22, 24, 27, 30 и 40 Конвенции, методы толкования договоров, практика Международного Суда ООН, Таллинское руководство 2.0 и доклады Групп правительственных экспертов ООН. Обосновывается, что архивы и сообщения защищены текстом Конвенции независимо от их цифровой формы, тогда как понятия помещений и дипломатической почты, а также местонахождение данных на иностранных серверах порождают существенную неопределённость. Оценивается законодательство Узбекистана, включая Консульский устав и Закон о кибербезопасности, и предлагаются меры по его совершенствованию.

Ключевые слова. дипломатическая неприкосновенность, дипломатические архивы, киберпространство, Венская конвенция о дипломатических сношениях, Таллинское руководство 2.0,

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

кибершпионаж, посольство данных, толкование договоров, Узбекистан.

Annotation. The article examines whether and to what extent the inviolability of diplomatic premises, archives and correspondence guaranteed by the 1961 Vienna Convention on Diplomatic Relations applies to cyberspace. It analyses Articles 22, 24, 27, 30 and 40 of the Convention, the methods of treaty interpretation, the case law of the International Court of Justice, the Tallinn Manual 2.0 and the reports of the UN Groups of Governmental Experts. The author argues that archives and communications are protected by the text of the Convention irrespective of their digital form, whereas the concepts of premises and diplomatic bag, as well as the location of data on foreign servers, reveal significant uncertainty. The legislation of Uzbekistan, including the Consular Charter and the Law on Cybersecurity, is assessed and reforms are proposed.

Keywords. diplomatic inviolability, diplomatic archives, cyberspace, Vienna Convention on Diplomatic Relations, Tallinn Manual 2.0, cyber espionage, data embassy, treaty interpretation, Uzbekistan.

Introduction. The 1961 Vienna Convention on Diplomatic Relations was drafted in an era of paper files, safes, couriers and telegrams [1]. Today a diplomatic mission operates through email, encrypted messaging, cloud storage, remote servers located in other jurisdictions and networks whose traffic is routed across the territories of several States. The question is whether the guarantees that the Convention attaches to the premises, archives and correspondence of a mission continue to protect these digital assets, and if so where the boundaries of that protection lie. The question is not academic. Intrusions into the information systems of foreign ministries and embassies have been repeatedly reported, and the answer determines whether such conduct is merely an unfriendly act or a breach of a treaty obligation that triggers State responsibility.

The article proceeds from the hypothesis that the Convention is neither obsolete nor fully adequate. Its text contains broadly worded provisions, such as the inviolability of archives and documents “wherever they may be” and the freedom of communication by “all appropriate means”, which can accommodate technological change. At the same time, other provisions are tied to physical concepts, namely premises, entry, the diplomatic bag and its external marks, and these resist straightforward transposition. The study uses treaty interpretation, analysis of the case law of the International Court of Justice, the Tallinn Manual 2.0 as a restatement of expert opinion, and a review of the legislation of Uzbekistan, with particular attention to texts available on the official portal lex.uz.

The textual baseline: what the Convention protects. The Convention establishes five relevant layers of protection. First, Article 22 declares the premises of the mission inviolable and provides that agents of the receiving State may not enter them without the consent of the head of the mission; paragraph 2 imposes a special duty on the receiving State to take all appropriate steps to protect the premises against any intrusion or damage and

to prevent any disturbance of the peace of the mission or impairment of its dignity; paragraph 3 exempts the premises and their contents from search, requisition, attachment or execution [1, Art. 22]. Premises are defined in Article 1(i) as buildings or parts of buildings and the land ancillary thereto used for the purposes of the mission [1, Art. 1(i)]. Second, Article 24 provides that the archives and documents of the mission are inviolable at any time and wherever they may be [1, Art. 24].

Third, Article 27 guarantees the free communication of the mission for all official purposes. The mission may employ all appropriate means, including diplomatic couriers and messages in code or cipher, but may install and use a wireless transmitter only with the consent of the receiving State. Official correspondence, defined as all correspondence relating to the mission and its functions, is inviolable, and the diplomatic bag may be neither opened nor detained [1, Art. 27]. Fourth, Article 30(2) extends inviolability to the papers, correspondence and property of the diplomatic agent [1, Art. 30(2)]. Fifth, Article 40(3) requires third States to accord official correspondence and other official communications in transit, including messages in code or cipher, the same freedom and protection as the receiving State [1, Art. 40(3)]. The Vienna Convention on Consular Relations of 1963 contains parallel guarantees for consular premises, archives and communications in Articles 31, 33 and 35 [2].

Two features of this text are important for the digital context. The Convention itself anticipated technological change in communications, since Article 27(1) already regulated wireless transmitters and coded messages, which shows that the drafters treated the means of communication as open-ended. And Article 24 attaches protection to the archives themselves rather than to a location, with the words “wherever they may be”, which the standard commentary reads as ensuring that protection does not depend on where the documents are physically held [3]. These textual hooks are the basis of the argument that digital archives and correspondence are covered.

Interpretation: how far can a 1961 text evolve? The Vienna Convention on the Law of Treaties requires a treaty to be interpreted in good faith in accordance with the ordinary meaning of its terms in their context and in the light of its object and purpose, taking into account subsequent agreements and subsequent practice [4, Art. 31]. The International Court of Justice has accepted that where the parties have used generic terms in a treaty, aware that the meaning of the terms is likely to evolve over time, and the treaty has been entered into for a very long period, the terms are presumed to have the evolving meaning [5, para. 66]. The International Law Commission reached a similar conclusion in its 2018 conclusions on subsequent agreements and subsequent practice [6]. The expressions “archives and documents”, “official correspondence” and “all appropriate means” are generic in this sense, and the Convention is a treaty of unlimited duration. The evolutive reading is therefore well founded for these terms.

The same method, however, shows the limits of extension. The concept of “premises” is defined in Article 1(i) by reference to buildings and land, and the prohibition in Article 22(1) is framed as a bar on entry by agents of the receiving State. These formulations are not generic and imply a spatial notion. Interpretation cannot replace a physical concept by a virtual one without exceeding the ordinary meaning of the words. Moreover, the International

Court in the Tehran Hostages case described the rules of diplomatic law as a self-contained regime that provides the receiving State with its own remedies against abuse, namely the declaration of a diplomat as persona non grata or the severance of relations [7, para. 86]. This characterisation suggests that the content of diplomatic inviolability should be determined mainly from within the regime and that its extension to new technologies should be justified by the Convention's own logic, not by analogy with other branches of law.

Archives and documents. The text of Article 24 is the strongest basis for digital extension. There is no reason to distinguish between a paper file and a document stored electronically, since both are the documents of the mission. The Tallinn Manual 2.0 adopts this reading in Rule 41, which concerns the inviolability of electronic archives, documents and correspondence, and its commentary treats official correspondence as including both electronic and paper forms and concludes that cyber espionage against such materials violates the inviolability of archives and documents even though States engage in it [8, Rule 41; 9]. The weight of this conclusion should not be overstated, since the Manual is a non-binding restatement of expert opinion. Yet it is consistent with the text. On cyber espionage and international law more generally, see [10; 11].

The harder question is where the archives are held. The protection under Article 24 applies “wherever” the archives are, but the obligation to respect inviolability is addressed to States, and it is unclear which States. When data sit on servers of a private provider in a third State, the commentary records that the experts were divided on whether the duty to respect the inviolability of archives held on private servers, as distinct from archives merely in transit, applies to all States or only to the receiving State [9]. The textual position is that the receiving State is bound by Article 24, and that third States are bound as regards communications in transit by Article 40(3). Documents stored permanently in a third State fall between these two provisions, and the gap is real. Practical protection in such cases depends on whether the archives retain their character as archives of the mission, which in turn depends on the mission's control over them and on the clear identification of the data as official.

Communications and the third State problem. Article 27 protects official correspondence and the freedom of communication by all appropriate means, and the reference to messages in code or cipher shows that encryption is a recognised and protected means. For the receiving State the obligation is clear: it may not intercept, block or read the official correspondence of the mission. The more difficult scenario concerns the routing of internet traffic. Data packets between a mission and its capital will usually cross the territories of third States. Article 40(3) obliges third States to accord official communications in transit the same freedom and protection as the receiving State [1, Art. 40(3)]. The text makes no distinction between telegrams and data packets, and mass collection of transit traffic by a third State would therefore engage the Article if diplomatic traffic could be identified and was knowingly intercepted. The difficulty is evidentiary and technical, since the encrypted content of a packet does not reveal its diplomatic character, and a State conducting bulk collection may claim not to have known it.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Premises and the problem of remote intrusion. Where a server is physically located inside the premises of the mission, it is covered by Article 22 as part of the premises and its contents. An agent of the receiving State who enters the premises and accesses the server violates the Article. Remote intrusion into the same server, without physical entry, is more problematic under the letter of Article 22(1), which prohibits entry. However, paragraph 2 imposes on the receiving State the duty to protect the premises against “any intrusion”, a word whose ordinary meaning is not limited to physical entry, and the object and purpose of the guarantee is to secure the independence of the mission from interference by the receiving State. A systemic reading therefore supports the view that a remote intrusion by the receiving State into systems located in the premises should be regarded as a breach of the inviolability of the premises or, at a minimum, of the inviolability of the archives and correspondence stored in them. The point remains contested, and it illustrates the difference between the strong textual basis for archives and the weaker basis for premises.

The diplomatic bag. Article 27(3) and (4) provide that the bag may not be opened or detained and that packages constituting it must bear visible external marks of their character [1, Art. 27(3)-(4)]. The concept of a “digital bag”, meaning an encrypted data transmission treated as equivalent to a sealed bag, is attractive but has no basis in the treaty text, because a data transmission has no external marks. The International Law Commission's 1989 draft articles on the status of the diplomatic courier and the diplomatic bag also address only physical consignments [12]. For this reason, the protection of electronic communications is better grounded in Article 27(1) and (2), as correspondence, than in the regime of the bag, and the argument that the bag regime extends to data should not be relied upon.

The counterpart duty and the abuse of inviolability. The same Convention imposes duties on the sending State. Article 41(1) requires persons enjoying privileges to respect the laws of the receiving State and not to interfere in its internal affairs, Article 41(3) prohibits the use of the premises in a manner incompatible with the functions of the mission, and Article 3(1)(d) confines the mission to ascertaining conditions and developments in the receiving State by “all lawful means” [1, Arts. 3(1)(d), 41]. Cyber operations conducted from a mission against the receiving State, for example by a signals collection unit that uses the premises, would therefore fall outside the lawful functions, and the receiving State has the remedies of the self-contained regime, namely declaring the persons concerned persona non grata under Article 9. Inviolability protects the mission from interference, but it does not authorise the use of the mission as a base for cyber operations, and this reciprocity is an important element of any balanced position.

Responsibility, attribution and practice. A breach of inviolability engages State responsibility under the general rules codified by the International Law Commission, which require that the conduct be attributable to a State, for instance as conduct of a State organ (Article 4) or of a person acting under its direction or control (Article 8) [13]. Attribution of cyber operations is technically and evidentially difficult, and this explains much of the gap between the apparent legal clarity of the rule and the weakness of its enforcement. A second consequence is relevant to countermeasures. Article 50(2)(b) of the Articles on State Responsibility provides that countermeasures may not affect

the inviolability of diplomatic or consular agents, premises, archives and documents [13, Art. 50(2)(b)]. An injured State cannot therefore respond to a cyber intrusion into its embassy by hacking the archives of the offending State's embassy, which demonstrates that the inviolability regime has priority even in a conflict between States.

State practice presents a mixed picture. The widely reported revelations of 2013 about alleged surveillance of diplomatic and international institutions provoked protests and were followed by the adoption by the UN General Assembly of resolution 68/167 on the right to privacy in the digital age, which expressed deep concern at the negative impact of surveillance and interception on human rights [14]. Yet, to the author's knowledge, States have only rarely characterised intrusions into their missions publicly as violations of the Vienna Convention, and intelligence collection of this type is reported to continue, which may be invoked as evidence that the rule is tolerated in practice. The legal significance of such practice is limited, because conduct that is concealed and denied does not usually generate a rule permitting it, and the denial itself implies recognition of the rule. Nevertheless the absence of explicit protest weakens the possibility of invoking subsequent practice to confirm the extension of the Convention.

The International Court of Justice has not yet addressed an intrusion into a diplomatic mission's systems, but its order in the case brought by Timor-Leste against Australia is instructive by analogy. After Australian agents seized documents and data from the premises of a legal adviser to Timor-Leste, the Court found plausible a right to conduct arbitration and negotiations free from interference, including the confidentiality of communications with legal advisers, linked it to the sovereign equality of States, and indicated measures requiring Australia not to use the material to the disadvantage of Timor-Leste, to keep it sealed, and not to interfere with communications between Timor-Leste and its advisers [15]. The order did not concern diplomatic premises as such, but it shows that the Court is prepared to protect the confidentiality of State documents and data on the basis of general principles.

In the field of cyber norms, the UN Group of Governmental Experts affirmed in 2015 and 2021 that international law, including the Charter, applies in cyberspace and recommended voluntary norms, among them that States should not knowingly allow their territory to be used for internationally wrongful acts using information technologies [16; 17]. The 2021 report of the Open-ended Working Group confirmed the same position [18]. These documents do not mention diplomatic inviolability specifically, but they support the proposition that established rules, including those of diplomatic law, are applicable to State conduct in cyberspace, and they provide a basis for expecting States to exercise due diligence in preventing the use of their territory for operations against foreign missions.

Cloud storage and the “data embassy” experiment. The practical response of some States to the vulnerability of centrally stored data has been to create an arrangement outside the framework of the Convention. In 2017 Estonia and Luxembourg signed a bilateral agreement under which Estonia operates a secure server room in Luxembourg for backups of government data, an arrangement widely described as a “data embassy”. The data stored include backups of non-sensitive government information and symbolically important

sites, while the most sensitive data remain in Estonia [19]. The agreement has been described as having “a strong flavor” of the Vienna Convention, but a legal expert quoted in the same source considered its enforceability somewhat doubtful, and Estonia chose a bilateral agreement over testing the application of the Convention itself [19].

The significance of this model for the present topic is twofold. It shows, first, that States do not consider the Convention sufficient to guarantee the protection of digital archives located abroad, since otherwise no special agreement would be necessary. A data embassy is not a mission, and its status derives from the consent of the host State, not from the Convention. It shows, second, that the most reliable method of closing the gap in the case of cloud and third-State storage is a treaty that specifies the status of the facility, the obligations of the host State, the access of the sending State and the conditions of any search or seizure. This conclusion matters for States such as Uzbekistan that are considering the localisation or backup of data of their institutions abroad.

Legislation of Uzbekistan. Uzbekistan acceded to the Vienna Convention on Diplomatic Relations on 2 March 1992 [20]. Under Article 15 of the Constitution of 2023, international treaties form part of the legal system and, where their rules differ from those of a law, the rules of the treaty apply [21]. The Convention is therefore applicable in Uzbekistan as a treaty, both to Uzbek missions abroad and to foreign missions on its territory. The relevant domestic legislation is, however, scarce, and it is useful to assess the main acts that have been identified, which are summarised in Table 2.

The Consular Charter, adopted by Law No. ZRU-517 of 17 January 2019, is the only reviewed act that addresses the archives of missions expressly, and it does so in modern terms. Article 10 defines the consular archive as all documents, correspondence, books, audio and video materials, electronic data carriers and registers of the consular post together with ciphers and codes, seals and stamps, and requires consular officials to take measures to ensure the inviolability of the archive [22, Art. 10]. This definition recognises electronic data carriers as part of the archive and therefore follows the evolutive reading discussed above. However, the Charter concerns consular posts only, and the text reviewed contains no provisions on consular correspondence and ciphered communications, on the bag, or on information security at consular posts. Article 8 refers to privileges and immunities in general terms, and Article 5(4) provides that consular premises may not be used for purposes incompatible with consular functions [22, Arts. 5(4), 8].

The Law “On Cybersecurity” of 15 April 2022, No. ZRU-764, which entered into force on 17 July 2022, establishes the general system of protection of critical information infrastructure. The State Security Service is the authorised body (Article 11), state bodies must create backup copies of their systems and of critical information infrastructure objects, kept for not less than the last three months (Article 15), and critical information infrastructure objects are classified into three categories and entered in a unified register (Articles 25 to 31); the Law also provides that treaty rules prevail over those of the Law (Article 2) and permits the authorised body to share information on combating cybercrime with foreign States (Article 36) [23]. The text reviewed does not mention diplomatic missions, and it does not indicate whether the information

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

systems of foreign missions in Uzbekistan or of Uzbek missions abroad are to be treated as critical information infrastructure.

Several gaps follow from this analysis. First, no reviewed act addresses the inviolability of the electronic archives and communications of foreign diplomatic missions in Uzbekistan, which means that the protection depends exclusively on the direct application of the Convention. Second, the protection of the electronic archives of Uzbek diplomatic missions abroad is not regulated by a specific rule, since the Consular Charter covers consular archives only, and the Cybersecurity Law is silent on missions. Third, the Law does not address the location of backups, although its backup requirement could lead to the storage of data of Uzbek missions on foreign servers, where the uncertainty described above arises. Fourth, there is no rule on incident reporting that would link the Ministry of Foreign Affairs to the authorised body when a mission is targeted

Conclusions and recommendations. The analysis allows the following conclusions. First, the 1961 Convention is applicable to cyberspace in respect of archives, documents and official correspondence, because the text protects them regardless of form and location and uses generic terms that admit evolutive interpretation. Second, the concepts of premises and of the diplomatic bag are tied to physical features, and their extension is contestable; remote intrusion into systems located in the premises is best addressed through the duty to protect against “any intrusion” and through the inviolability of archives and correspondence. Third, the principal uncertainties are the status of data held on third-State servers and of traffic routed through third States, the enforcement difficulties created by attribution, and the tolerance of intelligence collection in practice. Fourth, Estonia's data embassy shows that bilateral agreements are the most effective instrument for filling the gaps.

The following measures are proposed. At the international level, States should consider adopting a joint interpretative declaration or a resolution of the General Assembly confirming that Articles 24, 27 and 40 of the Convention apply to electronic archives, documents and communications, which would constitute a subsequent agreement under Article 31(3)(a) of the Vienna Convention on the Law of Treaties and remove much of the existing uncertainty [4, Art. 31(3)(a)]. The International Law Commission could be invited to study the status of data held abroad and the question of the digital bag. At the bilateral level, Uzbekistan could conclude agreements modelled on the Estonian experience when it decides to host or back up data of its missions abroad.

At the national level, three reforms are suggested. The Consular Charter, or a separate act on diplomatic missions, should extend the definition of archives in Article 10 to diplomatic missions and include provisions on the protection of official electronic correspondence and ciphered communications. The legislation should determine whether the information systems of missions abroad are critical information infrastructure and should set requirements for encryption, access control and location of backups. Finally, it is recommended that the competent authorities establish an incident reporting procedure between the Ministry of Foreign Affairs and the authorised body, and that Uzbekistan state clearly, in its position on cyber norms, that intrusions into the

systems of diplomatic missions constitute violations of the inviolability protected by the Vienna Convention. Such steps would align the national framework with the evolving international understanding and strengthen the protection of the sensitive communications on which diplomacy depends.

References:

1. Vienna Convention on Diplomatic Relations, 18 April 1961, 500 United Nations Treaty Series 95.

2. Vienna Convention on Consular Relations, 24 April 1963, 596 United Nations Treaty Series 261.

3. Denza E. Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations. 4th ed. Oxford: Oxford University Press, 2016.

4. Vienna Convention on the Law of Treaties, 23 May 1969, 1155 United Nations Treaty Series 331.

5. Dispute regarding Navigational and Related Rights (Costa Rica v. Nicaragua), Judgment, I.C.J. Reports 2009. P. 213.

6. Conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties. International Law Commission, 2018. UN Doc. A/73/10.

7. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment, I.C.J. Reports 1980. P. 3.

8. Schmitt M.N. (gen. ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Cambridge University Press, 2017.

9. Diplomatic and consular law // Tallinn Manual 2.0 online commentary, NATO Cooperative Cyber Defence Centre of Excellence. URL: https://cyberlaw.ccdcoe.org/wiki/Diplomatic_and_consular_law

10. Buchan R. Cyber Espionage and International Law. Oxford: Hart Publishing, 2018.

11. Ziolkowski K. Peacetime Cyber Espionage: New Tendencies in Public International Law // Ziolkowski K. (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE, 2013.

12. Draft articles on the Status of the Diplomatic Courier and the Diplomatic Bag not accompanied by Diplomatic Courier, with commentaries. International Law Commission, 1989 // Yearbook of the International Law Commission. 1989. Vol. II, Part Two.

13. Articles on Responsibility of States for Internationally Wrongful Acts, 2001. Annex to UN General Assembly resolution 56/83 of 12 December 2001.

14. The right to privacy in the digital age. UN General Assembly resolution 68/167 of 18 December 2013.

15. Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, Order of 3 March 2014, I.C.J. Reports 2014. P. 147.

16. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc. A/70/174, 22 July 2015.

17. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UN Doc. A/76/135, 14 July 2021.

18. Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc. A/75/816, 18 March 2021.

19. Diplomatic immunity for data: Estonia creates a virtual embassy // Microsoft EU Policy Blog. 14 December 2017. URL: https://blogs.microsoft.com/eupolicy/2017/12/14/diplomatic-immunity-data-estonia-creates-virtual-embassy/

20. Vienna Convention on Diplomatic Relations: status of treaty // United Nations Treaty Collection, Chapter III.3. (Uzbekistan: accession, 2 March 1992.) URL: https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20III/III-3.en.pdf

21. Конституция Республики Узбекистан (принята на референдуме 30 апреля 2023 г., вступила в силу 1 мая 2023 г.). URL: https://lex.uz/docs/6445145 (Constitution of the Republic of Uzbekistan, adopted by referendum on 30 April 2023.)

22. Закон Республики Узбекистан от 17 января 2019 г. № ЗРУ-517 «Об утверждении Консульского устава Республики Узбекистан». URL: https://lex.uz/acts/4167688 (Law of the Republic of Uzbekistan No. ZRU-517 of 17 January 2019 “On approval of the Consular Charter of the Republic of Uzbekistan”.)

23. Закон Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 «О кибербезопасности». URL: https://lex.uz/en/docs/6997403 (Law of the Republic of Uzbekistan No. ZRU-764 of 15 April 2022 “On Cybersecurity”.)