SPECIFICS OF INTERNATIONAL COOPERATION IN THE CYBERCRIMES INVESTIGATION PROCESS

DOI: 10.63407/611037

Sabyrbaeva Aynura

Abstract: *International cross-border crime poses a threat to the whole world, and information and communication technologies and networks make the main contribution to its spread. Cybercrime has become one of the global problems of our millennium, which is developing rapidly, as confirmed by both world statistics and the extent of damage inflicted on entire states in terms of economics and politics. The emergence of the terms "cyberwarfare", "cyberterrorism", and "cyber espionage" also indicates the scale of threats and the need to unite to counter cybercrime.*

Keywords: *cybercrime, cyber threat, international cooperation, international document, international inquiry, cross-border crime.*

In today's world, cybercrime seriously threatens global security and economic stability. As A. A. Bessonov noted, "Modern cybercrime is a serious threat both for individual states and the entire world community"[1]. Unlike traditional crimes, which are often limited by geographical boundaries, cyberattacks can be carried out anywhere and exploit vulnerabilities in a country's digital infrastructure. To counter cybercrime, it is necessary to establish cooperation between law enforcement agencies in different countries. However, achieving practical international cooperation is challenging due to various obstacles, such as legal differences, jurisdictional issues, technological challenges, and geopolitical tensions.

[1] Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерных преступности – Территория науки. № 2. С. 231–237. 2013.

As Klevtsov K. K. rightly noted, " Most law enforcement agencies in the investigation of cybercrime intentionally or without intent resort to obtaining evidence that is physically located on the territory of other states, independently, without obtaining the consent of these states. This is done by remote connection in real time to the subscriber device of the criminally prosecuted person or by seizing such a device from the victim or witness located in the territory of the state whose law enforcement agencies are conducting proceedings on a cybercrime case, with subsequent inspection to find information relevant to the case, as well as by using other legal methods." [2] However, for this issue to be resolved without violating national sovereignty, it is necessary to establish international cooperation, but this issue is still open for several reasons. According to Hazel Diez Castaño, head of the information security office at Banco Santander, " Cybercriminals have an advantage on the battlefield: it is easier to attack than to defend, since protection requires more effort and resources. Therefore, the public and private sectors must work together to develop collective information on cyber threats and share detection, security, and technology tools, and coordinate incident response mechanisms. By combining our efforts and creating concrete cooperation channels, we can achieve a decisive shift in the fight against cybercrime "[3].

International cooperation in the fight against cybercrime is complicated by the divergent positions of various states of the world, due to fundamental differences in approaches to defining concepts, the lack of a clear understanding of the boundaries between multiple phenomena that require different mechanisms of cooperation, the difference in approaches to

[2] Клевцов К.К. 2022. «Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам». Вестник Санкт-Петербургского университета. Право 3: 678–695. https://doi.org/10.21638/spbu14.2022.306

[3] Hazel Diez Castaño, Chief Information Security Officer at Banco Santander. Annual Meeting on Cybersecurity. 2023. https://www.weforum.org/agenda/2023/10/cybercrime-violent-crime/

ensuring the security of personal data, and the general level of mutual distrust, which makes collaboration on cross-border procedural partnership impossible. For this reason, the UN rejected the draft of the Global Convention on Cybercrime, which Russia and China proposed in 2010. [4]However, more than a decade later, the world is on the verge of signing the Convention on Combating Cybercrime (the draft Convention was approved by the UN and submitted for discussion at the 79th session of the UN in September 2024). After its signing, each country will be able to ratify it and apply it in its legislation, but time will tell how this Convention will work.

There is a paradox regarding cybercrime: on the one hand, States are forced to cooperate to combat such a transnational threat, but on the other hand, such cooperation affects the sovereignty of the state and restricts it in the fields of criminal law and information protection. Therefore, cooperation is successful in regions with a high level of political trust between countries, as in the European Union "[5].

S. Brenner noted that " as is well known, it is possible to effectively counteract cybercrime only by joining forces. This is exactly the path taken by the world's largest Internet service providers, who in 2005 announced the conclusion of a global anti-hacking alliance, within which an early warning system for hacker attacks on the Internet was created". In addition, an International Cybersecurity Alliance was established in London in 2011 to combat cybercrime globally [6]

Despite various attempts by countries or individual organizations to gain an advantage over cybercriminals, their efforts remain futile, as confirmed by the study's results: " In

[4] Brenner S. Cyberthreats and the Decline of the Nation-State. Routledge, 2014.
[5] Атнашев В.Р., Яхъеева С.Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом. Право. 2022. С. 38
[6] Акопов Г.Л. Правовая информатика: современность и перспективы: учеб. пособие. Ростов н/д, 2005. С.218

2023, the number of ransomware attacks increased by 160% compared to the previous year "[7]

As some scholars have noted, "the legal analysis of international cooperation and national legislation of various states indicates that there is no unified practice in combating cybercrime"[8]This is despite the existence of several multilateral treaties on this issue, which, of course, negatively affect this area of state activity [9]

Many challenges are associated with international cooperation and developing global guidelines for combating cybercrime. Identifying criminals across borders anywhere in the world, conducting investigations, and securing electronic evidence is daunting, as Russell L. G. Smith noted," one of the essential outcomes of the very few successful cases is an unprecedented demonstration of multi-faceted international cooperation between law enforcement agencies, the exchange of information and techniques for collecting evidence, identifying violators and arresting them. However, this level of collaboration is the exception rather than the rule"[10]

Many problems arise in the implementation of international cooperation in the fight against cybercrime:

1. Difficulties in determining which State has criminal jurisdiction over a particular cybercrime. The reason for this is the lack of virtual borders and the inability to assess jurisdiction based on the traditional principle of territoriality (this opinion is

7 Аналитический отчет компании F.A.C.C.T. «Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023–2024 гг.».
https://ict.moscow/research/kiberprestupnost-v-rossii-i-sng-2023-2024/
8 Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and cybercrime:
9 An analysis of the nature of groups engaged in cybercrime". International of Journal of Cyber Criminology 8 (1): P.2.
10 Многие законодательные и правоприменительные проблемы, с которыми сталкиваются различные государства в борьбе с киберпреступностью, обобщены в докладе Генерального секретаря ООН на 74-й сессии Генеральной Ассамблеи ООН, озаглавленном «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Дата обращения 1 мая, 2020.

shared by Grant Christensen[11], Maillart John-Baptiste[12]) and the principle of extraterritoriality (this opinion is shared by Kimberly Ferzan[13], Frédéric Maigret[14], Christopher Soler[15]. Shmatkova L. P., Volevodz A. G. pointed out "contradictions between states on cooperation procedures that affect the principle of sovereignty"[16]. E. L. Anselmo noted that "attempts to manage the Internet based on the old territorial principle are a temporary solution that the international legal system must overcome"[17], calling for abandoning the use of the Internet as a whole. the use of traditional designations of territorial borders applies to virtual space. The same opinion was shared by E. Verhelst and J. Wouters[18]. However, this issue is controversial, because the absence of virtual borders will allow countries to interfere in all information processes and areas in foreign countries, such as, for example, accusations against the Russian Federation about interference in the US elections.

2. Difficulties due to bureaucratic red tape in the framework of sending an international request for legal

11 Grant, Christensen. 2019. "Te extraterritorial reach of tribal court criminal jurisdiction". Hastings Constitutional Law Quarterly 46 (294): 1–18. http://dx.doi.org/10.2139/ssrn.3231533

12 Maillart, Jean-Baptiste. 2019. "Te limits of subjective territorial jurisdiction in the context of cybercrime".

13 Ferzan, Kimberly. 2020. "Te reach of the realm. Criminal law". Philosophy 14: 335–345

14 Megret, Frederic. 2020. "Do not do abroad what you would not do at home? An exploration of the rationales
for extraterritorial criminal jurisdiction over a state's nationals". Canadian Yearbook of international Law

15 Soler, Christopher. 2019. "Aut Dedere Aut Judicare". Te global prosecution of core crimes under international law, 319–401. Te Hague, T. M. C., Asser Press.

16 Шматкова Л.П., Волеводз А.Г. 2017. Формирование и современный этап совершенствования правового регулирования противодействия киберпреступлениям в Европейском союзе. – Библиотека уголовного права и криминологии. № 3. С. 154-159

17 Ансельмо Э. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? // Экономические стратегии. - 2006. - №2. - С. 24-31

18 Верхелст Э., Ваутерс Я. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций. – 2020. – Т. 15. – № 2. – С. 141-172

assistance in a criminal case, obtaining the necessary information for the disclosure and investigation of cybercrime takes a long time, which leads to the loss of crucial evidentiary details.

Unfortunately, the Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters of January 22, 1993 (Minsk Convention) and October 7, 2002 (Chisinau Convention) work very slowly and do not produce effective results, particularly on cybercrime. According to these types of crimes, the countdown lasts for minutes and seconds. Cybercriminals redirect funds from one account to another to hide and obfuscate their tracks. At the same time, they do not transfer them abroad through crypto exchanges, where it is almost impossible to track transactions quickly. As a rule, money is not stored in the drop account for more than 1 hour, so you can avoid blocking cards if the ANTIFRAUD system detects them. However, when it comes to cybercrimes, there is so much red tape and bureaucracy involved — from drafting a formal request, sending it to the Investigative Directorate, then up to the Investigative Department, and eventually to the General Prosecutor's Office. This entire bottom-up process alone can take up to a month. And once the request reaches the relevant foreign state, the process goes top-down — from the General Prosecutor's Office to the actual law enforcement officer responsible for the case. It becomes nearly impossible to trace the stolen funds by the time that happens.

As R. Zhubrin correctly noted, "this is mainly due to the absence of an obligation in multilateral and bilateral documents to respond within a certain period"[19]. Because the Minsk Convention and the Criminal Procedure Code of the Republic of Uzbekistan do not regulate the deadline for executing a request for legal assistance to a foreign state. Although in the course of studying judicial and investigative practice, it was found that

19 Жубрин Р.В. 2018. «Сроки исполнения запросов о правовой помощи по уголовным делам».Законность 5: 12–14.

employees of the Investigative Department, as a rule, when sending requests received from a foreign state directly to performers*, indicate* the deadline for its execution within 15 days.

As Klevtsov. K noted, " it is necessary to optimize international cooperation in the field of criminal proceedings in the field of cybercrime, regulating at the national level the timely provision of responses to requests for legal assistance, since during pre-trial proceedings in this category of criminal cases, traditional mechanisms of cooperation prevail within the framework of multilateral or bilateral agreements or based on the principle of reciprocity "[20]. It is worth noting that using traditional forms of cooperation leads to the loss of important information and disclosure of cybercrime due to the lack of efficiency.

3. The impossibility of sending an international request during a pre-investigation check. Thus, according to the requirements of these Conventions, it is initially necessary to write an international request for legal assistance in a criminal case and then send it to the regional Investigation departments, since legal assistance is possible only within the framework of an initiated criminal case. That is, during a pre-investigation check, it does not make sense to write an international request.

4. Lack of a common understanding of the phenomenon of cybercrime. As S. Brener noted, "international cooperation in the fight against cybercrime is complicated by the divergent positions of various states of the world, due to basic differences in approaches to defining concepts, the lack of a clear understanding of the boundaries between various phenomena that require different mechanisms of cooperation"[21]. Countries

[20] Клевцов К.К. 2022. «Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам». Вестник Санкт-Петербургского университета. Право 3: 678–695. https://doi.org/10.21638/spbu14.2022.306

[21] Brenner S. Cyberthreats and the Decline of the Nation-State. Routledge, 2014

do not know how to respond if there is no common understanding of the problem. For example, it is difficult to agree on the definition of cybercrime, despite the controversy among experts and scientists, it has not been possible to come to a single definition of cybercrime, and the desire of different authors to give it a precise definition has led to inaccuracies in using these definitions outside their intended context. As a result, there is still no generally accepted definition of cybercrime. In addition, " there is no consensus on what should be the subject of a cybersecurity treaty. For example, Russia supports a cybersecurity treaty regulating cyber and information warfare, the United States actively promotes criminalizing acts against computer systems, and advocates international cooperation in mutual legal assistance and extradition. Suppose China proposes to ban certain information that may harm or damage the stability of state power under the national cybersecurity program. In that case, the United States assesses such activities as an obstacle to freedom of speech[22]. So, everyone pulls the reins in their direction, but the" cart " still does not move;

5. The draft Convention "On Combating Cybercrime" has just been approved, and it will take time for its ratification and implementation in national legislation. Currently, there are several documents. Still, they cover only several countries that have signed it and, in principle, are one of the types of multilateral agreements (the EU Convention on Computer Information Crime, the Arab League Convention on Combating Information Technology Crimes, the Agreement on Cooperation of the CIS member States in Combating Information Technology Crimes). Computer information). The EU Convention is one of the most effective treaties for law enforcement officials in the framework of international

22 Орджи У.Д. Предотвращение кибертерроризма в глобальном информационном обществе: вопрос коллективной ответственности государств. Orji U. J. deterring cyberterrorism in the global information society: a case for the collective responsibility of states // defence against terrorism review. - Ankara, 2014

cooperation, as it assists in carrying out specific procedural and investigative actions on the territory of the countries participating in the Convention. As I. A. Khimchenko noted, "The Convention is the only recognized international treaty that ... contains the norms of substantive and procedural (procedural) law to counter cybercrime and protect freedom, security and human rights on the Internet"[23]. However, about 70 countries have signed this Convention. The central position of the opposition[24] to join this Convention is the reference to Article 32, which violates the sovereignty of States. Chapter 3 provides for providing cross-border access to stored computer data to another party based on the principle of reciprocity, with the ability to collect evidence and flow data online. However, it should be noted that despite their "openness", non-EU countries can join the Convention with the unanimous approval of other participants.

6. Many countries adhere to "traditional" methods of information exchange (sending letters, mail) due to the difficulty of maintaining and ensuring the confidentiality of the transmitted data. Unfortunately, law enforcement agencies are not as armed as criminals, and no one can guarantee that the letter will be intercepted. A clear example of this is hacking the Pentagon or NASA systems.

7. Differences between the legal framework of a particular country may hinder the prompt implementation of the request, as some countries still do not regulate the criminalization of certain types of criminal encroachments. In addition, there is no single concept of "electronic evidence", the procedure for their registration, the scope of their application, and subsequent recognition as evidence in the criminal case of a particular country that has signed this document.

23 Химченко И.А. Информационное общество: правовые проблемы в условиях глобализации: дис. ... канд. юрид. наук: 12.00.13 / И. А. Химченко. М., 2014. 66 с.
24 Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. - 2020. - № 1. - С. 261-269;

8. Political and geopolitical factors, i.e., disputes, conflicts, tensions at the state level, can lead to the fact that grassroots structures (law enforcement agencies, for example) cannot cooperate to combat cybercrime;

9. Due to the different legal frameworks, i.e., systems and standards of evidence, there are challenges in harmonizing laws for practical international cooperation. So, for example, in some countries, investigative actions do not exist in our country or where the prosecutor's permission is required to conduct an elementary inspection. In addition, there are problems regarding the qualification of cybercrime. For example, phishing in many countries of the world qualifies as fraud, but in the investigative and judicial practice of our country, it is considered theft (with the reference that the person clicking on the link did not know that he was transferring money to the attacker);

10. The lack of unified statistics on cybercrime does not allow us to recreate this socially dangerous phenomenon's full picture and scale. Some types of cybercrime are not considered crimes in some countries, so cybercriminals have quietly moved to countries such as the Philippines. In most countries, cybercrimes are classified as traditional types of crimes, such as phishing, which is theft or fraud. As N. I. Zhuravlenko and L. E. Shvedova correctly noted, "at present, neither relevant statistics reflect the real picture of the state of cybercrime, nor reliable methods for collecting such data"[25]. You cannot be sure that the statistics transmitted by countries are reliable (the same crime shelters).

11. Lack of a clear, unified apparatus for countering cybercrime. In each country, cybercrime detection or investigation is handled by different institutions. In some countries, specialized agencies are being set up, and in some,

25 Н.И. Журавленко и Л.Е. Шведова. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере. Уголовная политика: теория и практика. №3 (53). – Общество и право. – 2015. С. 69

they are being handled by "ordinary" law enforcement agencies investigating traditional crimes. For example, in the UK, a national cybercrime unit has been created, and we only have a cybercrime unit in 2022, but even among specialists of this department, there is no interaction within the country, so they do not know what actions they can take to investigate this or that type of crime;

12. Insufficient level of coordination of the departments ' activities in the investigation of cybercrime. Several scientists also mentioned this in their work[26]. In the case of cyberattacks, it is difficult to contact the law enforcement agencies of states to stop the crime from being carried out in their territory. For example, in criminal case No. 260001/2023-385 UM, an online loan was issued for citizen B. The IP address the criminals entered belonged to an Egyptian company; all operations were carried out from Ukraine, and the mailbox was registered in Kazakhstan. However, it is difficult to expose the criminal, and cooperation between the lower levels of law enforcement agencies is necessary. As Grimes noted, " justice for cybercriminals is challenging to achieve in court. It turned out that catching and bringing to justice modern cybercriminals is very difficult. Only one in 10,000 hackers is seen, and only one in 100 is successfully brought to trial [27]It should be noted that although the CIS member states signed the Minsk Convention [28]in our opinion, it will not work effectively without joint efforts on the part of the law enforcement agencies of the countries that signed this agreement. The European Convention on Computer Crimes, signed in Budapest on 23 November 2001, proved to be effective, as each of the parties undertook to designate a communication point available 24 hours a day, 7

26 Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and cyber crime:

27 Grimes, R. (2017). *Why it's so hard to prosecute cyber criminals*. *CSO Online*. Retrieved 23 August 2017, from http://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html

28 http://www.cis.minsk.by

days a week, to provide immediate assistance in the investigation or proceedings of criminal offences involving the use of computer systems or data, and in collecting evidence on criminal offences in electronic form [29]

13. There is low information exchange on cyber incidents between states. Notification of committed cybercrimes and the exchange of statistical data and methods to counteract them would allow us to respond and regulate the criminal situation quickly. So, for example, vishing attacks "about the alleged involvement of a relative in an accident and the need to transfer money to couriers" were distributed in other CIS countries, including the Russian Federation and Kazakhstan. However, in April 2024, there was a surge in this type of crime in the country, which led to huge losses.

14. Insufficient level of public-private cooperation. Now, most crimes are carried out through social networks, and Telegram is gaining particular popularity. Telegram, whose privacy conditions allow it to be used as a Darknet, although for the sake of good, it should be noted that the founder of this network, P. Durov, announced his readiness to legally transfer the necessary information about the user. Another problem is that most social messengers do not have licenses to operate in the territory of any country, so they may not be subject to the legislation of a particular country since they provide services outside the state where their servers are located.

15. There are no territorial borders in the virtual space, which leads to the withdrawal of funds through crypto-exchanges or international payment systems. Due to this, it is almost impossible to compensate for the damage.

"Taking into account the factor of globalization of computer crime, it becomes more obvious that today no state can counter this threat independently. At the same time, an essential role in such cooperation belongs to international legal

29 https://rm.coe.int. CETS 185- Conventuion on Cybercrime

mechanisms of regulation and interaction of law enforcement agencies on countering and investigating computer crimes" [30]

Thus, international cooperation is key to eliminating the legal vacuum between the development of information technologies and the legislative response to them. As experience shows, developing measures at the global level is a complex problem. However, this is the only way to protect against electronic attacks and effectively combat cybercrime reliably.

References:

1. Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерных преступности – Территория науки. № 2. С. 231–237. 2013.
2. Клевцов К.К. 2022. «Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам». Вестник Санкт-Петербургского университета. Право 3: 678–695. https://doi.org/10.21638/spbu14.2022.306
3. Hazel Diez Castaño, Chief Information Security Officer at Banco Santander. Annual Meeting on Cybersecurity. 2023. https://www.weforum.org/agenda/2023/10/cybercrime-violent-crime/
4. Brenner S. Cyberthreats and the Decline of the Nation-State. Routledge, 2014.
5. Атнашев В.Р., Яхъеева С.Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом. Право. 2022. С. 38
6. Акопов Г.Л. Правовая информатика: современность и перспективы: учеб. пособие. Ростов н/д, 2005. С.218
7. В Лондоне создан Международный альянс обеспечения кибербезопасности. URL: http://www.vesti.ru/doc.html?id=499251
8. Аналитический отчет компании F.A.C.C.T. «Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023–2024 гг.». https://ict.moscow/research/kiberprestupnost-v-rossii-i-sng-2023-2024/
9. Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and cybercrime:
10. An analysis of the nature of groups engaged in cybercrime". International of Journal of Cyber Criminology 8 (1): P.2.
11. Многие законодательные и правоприменительные проблемы, с которыми сталкиваются различные государства в борьбе с киберпреступностью, обобщены в докладе Генерального секретаря ООН на 74-й сессии Генеральной Ассамблеи ООН, озаглавленном «Противодействие использованию информационно-

[30] Бураева Л.А. Компьютерные преступления транснационального характера как глобальная угроза мировому сообществу // Бизнес в законе. Экономико-юридический журнал. – 2016

коммуникационных технологий в преступных целях». Дата обращения 1 мая, 2020. https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf
12. Russell G. Smith. "Investigating cybercrime: Barriers and Solutions" Association od Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney, 11 September 2003, p.2
13. Grant, Christensen. 2019. "Te extraterritorial reach of tribal court criminal jurisdiction". Hastings Constitutional Law Quarterly 46 (294): 1–18. http://dx.doi.org/10.2139/ssrn.3231533.
14. Maillart, Jean-Baptiste. 2019. "Te limits of subjective territorial jurisdiction in the context of cybercrime". *ERA Forum* 19: 375–390. https://doi.org/10.1007/s12027-018-0527-2.
15. Ferzan, Kimberly. 2020. "Te reach of the realm. Criminal law". Philosophy 14: 335–345. https://doi.org/10.1007/s11572-020-09541-w
16. Megret, Frederic. 2020. "Do not do abroad what you would not do at home? An exploration of the rationales for extraterritorial criminal jurisdiction over a state's nationals". Canadian Yearbook of international Law / Annuaire canadien de droit international 57: 1–40.
17. Soler, Christopher. 2019. "Aut Dedere Aut Judicare". Te global prosecution of core crimes under international law, 319–401. Te Hague, T. M. C., Asser Press. https://doi.org/10.1007/978-94-6265-335-1_13.
18. Шматкова Л.П., Волеводз А.Г. 2017. Формирование и современный этап совершенствования правового регулирования противодействия киберпреступлениям в Европейском союзе. – Библиотека уголовного права и криминологии. № 3. С. 154-159
19. Ансельмо Э. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? // Экономические стратегии. - 2006. - №2. - С. 24-31
20. Верхелст Э., Ваутерс Я. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций. – 2020. – Т. 15. – № 2. – С. 141-172
21. Жубрин Р.В. 2018. «Сроки исполнения запросов о правовой помощи по уголовным делам». Законность 5: 12–14.
22. Клевцов К.К. 2022. «Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам». Вестник Санкт-Петербургского университета. Право 3: 678–695. https://doi.org/10.21638/spbu14.2022.306
23. Brenner S. Cyberthreats and the Decline of the Nation-State. Routledge, 2014.
24. Орджи У.Д. Предотвращение кибертерроризма в глобальном информационном обществе: вопрос коллективной ответственности государств. Orji U. J. deterring cyberterrorism in the global information society: a case for the collective responsibility of states // defence against terrorism review. - Ankara, 2014. - Vol. 6, n 1. - P. 39. Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. 2017.
25. Химченко И.А. Информационное общество: правовые проблемы в условиях глобализации: дис. ... канд. юрид. наук: 12.00.13 / И. А. Химченко. М., 2014. 66 с.

26. Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. - 2020. - № 1. - С. 261-269;
27. Н.И. Журавленко и Л.Е. Шведова. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере. Уголовная политика: теория и практика. №3 (53). – Общество и право. – 2015. С. 69.
28. Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, Steve Chon. 2014. "Organizations and cyber crime:
29. Grimes, R. (2017). *Why it's so hard to prosecute cyber criminals*. *CSO Online*. Retrieved 23 August 2017, from http://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html
30. http://www.cis.minsk.by
31. https://rm.coe.int. CETS 185- Conventuion on Cybercrime
32. Бураева Л.А. Компьютерные преступления транснационального характера как глобальная угроза мировому сообществу // Бизнес в законе. Экономико-юридический журнал. – 2016. – №5. – С.225. https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-transnatsionalnogo-haraktera-kak-globalnaya-ugroza-mirovomu-soobschestvu