BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 4, Number 386 (2020), 21 – 26 https://doi.org/10.32014/2020.2518-1467.99

UDC 004.343.3/.7

Elena A. Antonyan, Olga S. Rybakova

Federal State Budgetary Educational Institution of Higher Education
"Moscow State Law University named after O.E. Kutafina". Moscow, Russia.
E-mail: antonyaa@yandex.ru, orro21@yandex.ru

BLOCKCHAIN TECHNOLOGIES FOR SECURITY AGAINST CYBER ATTACKS

Abstract. The article deals with new technologies for countering cyber attacks that can be aimed at destabilizing public order, large-scale disruption of communication systems, intimidation by imposing one's will, including on power structures, and, in general, pose an increased threat to the national and information security of the state. Particular attention is paid to blockchain technology, which allows to hide funds aimed at financing criminal, including terrorist activities, including in the information space. Also in the article, the authors present generalized research results as part of the implementation of the RFBR scientific project No. 18-29-16175 "Blockchain technology to counter the risks of cyberterrorism and cyber extremism: a criminal-legal study".

Modern cybercrime dictates new challenges to the state, which can no longer be responded to within the space of a single state. Today, the issue of legislative regulation of the interaction of states to prevent cybercrime with the use of new technologies is an acute issue.

The most important aspect of the new forms of countering cybercrime is the decentralization of users of anonymous proxy server systems. And if earlier security agencies still had available "loopholes" for direct access to the user's IP address, now everything has become much more complicated and a comprehensive analysis of the traffic of a particular user is necessary.

Scientists also point out that network attacks can contain malicious embedded code, the use of backdoors and much more. Such attacks can be triggered from anywhere in the world because of a computer with a masked IP-address. A new type of warfare, even cyber warfare, is changing the landscape of war itself.

This type of war eliminates the need to have physically capable armed forces and requires the need for forces with strong technical capabilities, such as computer skills.

Many countries, including Russia, have come to understand that this is a problem and are actively pursuing policies to address it in order to mitigate threats.

Key words: blockchain technology, Information Security, cybersecurity, counteraction, cybercrime, cyber terrorism, National security, cyberattack, financial security of Russia, VPN server, SORM - 3, cryptocurrency, Bitcoin, Litcoin, IP-address.

Introduction. The main task for modern states is the problem of creating a secure cyberspace, which can be achieved through the coordinated activities of international organizations, international regional organizations, and individual states. Scientists and scholars focus on the need to develop new approaches to ensuring the security of cyberspace, as well as examining modern technological threats of cybercrimes that can destabilize technological systems, lead to information leaks, and cause irreparable damage to state security [Antonyan & Aminov, 2019; Rybakov & Rybakova, 2019; Stepanenko et al, 2019; Bliznets et al, 2018; Polyakova et al, 2019].

Unauthorized access to data, programs, and other network resources is widespread today. Despite the use and use of various well-known methods, including law enforcement services, to protect online data, cybercriminals are finding new ways to penetrate the network. Nowadays it is not uncommon, in particular, in the United States (2018), when a mass cyber-attack affected 150 million people in a day, whose personal data was accessed through certain files in web applications. Another example, when in September 2018, already in Russia, the Aeroflot server was attacked by hackers, which led to the leak of a

large part of the source code. This data was freely available on GitHub. Despite the fact that due to the rapid response to the incident, the data was deleted quickly enough, they still managed to spread over the network, which made it possible to download them. Modern cyber-attacks are characterized by complexity, branching locations and a significant amount of damage, which makes it necessary to search for new means of ensuring the security of technological systems.

All this means that any leaks of information quickly become public, and, therefore, the data must be protected safety.

One of the reasons for existing cyber-attacks is their partial decentralization.

In this case, blockchain technologies can be used not only to protect personal data from possible cyber-attacks, but also to improve cybersecurity on various platforms in general. The introduction of blockchain technology will completely decentralize content, increasing cybersecurity in the storage chain of a large number of nodes, which will make it almost impossible for cyber-attacks. Blockchain technology is an opportunity to increase the cybersecurity of data storage and transportation, primarily due to the distributed data storage system on the computers of all network participants, and the absence of a central administrator [Nakamoto, 2008].

The blockchain is a multi-functional and multi-level digital system consisting of separate distributed registries, in which all transactions performed on an ongoing basis are tracked. Information stored in the blockchain is organized as a chain of individual blocks (hence the name "block ", "chain"), each subsequent block is linked to the previous one thus any changes to it automatically changes all subsequent blocks, and since the chain of blocks is stored on the computers of all users (owners) of this database, the changes cannot be unnoticed (Sukhodolov et al, 2019). Thus, once a transaction is made, it is impossible to execute it, since each transaction is recorded in the Ledger constantly in order, i.e. in chronological order. The database stores the entire history of transactions made within the chain, which is available to all users. When a new data block is created, the registry is updated simultaneously on all computers in the network, which eliminates the possibility of data distortion by one of the participants [Antonyan, 2020].

Thanks to these features, the system is transparent and reliable. In this case, a group of blocks together forms a blockchain network. Each block contains basically three values: the data itself; the previous hash value of the block; and the current value of the hash block. The hash value of the previous block is always zero in the Genesis block, since this is the very first block created. The hash function values for each block are generated using the hash function itself. The hashing technique briefly includes: a decentralized storage platform for secure transactions; strictly chronological order; immutability; no intermediaries; simple fraud identification; and data stability.

Methodology. We used a general scientific method of analysis that allowed us to argue the authors' positions on the use of blockchain technology for specific forms of cyber threats, to differentiate and update blockchain technology as a universal condition for preventing cyber-attacks and cybercrimes in the information technology environment. A comparative legal private method of studying the problems posed has proved acceptable for the correlation of the possibilities of using blockchain technology on various information platforms in order to increase cybersecurity. The method of abstraction allowed us to focus on certain extremely relevant properties of the blockchain technology, which is shown in individual examples of this technology from various spheres of professional and public activity (monetary transactions, supply chain management system, elections, etc.).

Research result. The biggest advantage of using blockchain to ensure the security of cybersystems is that when a cybercriminal tries to hack a separate block, the entire system analyzes each block of data to find one that is different from the rest. As a result, the system eliminates this type of block and identifies it as false.

In blockchain, if a node needs to update a specific part of the data in a transaction to a block, it must add a new transaction on top of the previous one in the block. Because even a small dot or comma is added to the data, the value of the hash function changes. Using this technique, the system easily detects which block contains incorrect or false data.

The most important aspect of the new forms of countering cybercrime is the decentralization of users of anonymous proxy server systems. And if earlier security agencies still had available "loopholes" for direct access to the user's IP address, now everything has become much more complicated and a comprehensive analysis of the traffic of a particular user is necessary.

In the Russian Federation, the main tool for combating cybercrime is the system SORM – 3 (the System of operational search measures – 3), which provides control of part of VPN servers, listens in real time to satellite communications, messengers, stores metadata about calls and Internet sessions, and allows you to get data from the operator's internal systems. Experts point out some difficulties in using SORM, for example, when cybercriminals use encryption programs for data packets, which makes it difficult or impossible to obtain computer information as evidence of criminal acts (Petrov & Makarov, 2020). The blockchain system is able to solve this problem. The absence of a single node that the attack is aimed in can ensure that the cyber-attack is decentralized across different blocks, thereby reducing the effectiveness of criminal influence. We believe that the use of blockchain will allow detecting traces of cybercrime that will be visible in the block chain and it will be almost impossible to mask them, which will negate illegal transactions and significantly complicate the activities of terrorist and extremist organizations. The ability to prevent cyber-attacks is inherent in the very principle of a decentralized block chain system, which not only provides a decentralized network for storing information, but also guarantees its security due to the resistance to hacking of hashed and encrypted blocks [Antonyan & Aminov, 2019].

Blockchain can become the technology that will significantly reduce the scale of criminal processes. Enabling cryptographic functions is used as a hash in each block, making it difficult for cybercriminals to access the blockchain network and change entries stored in the register. The most popular cryptographic hashing function is SHA256 / SHA512, which generates a unique hash value each time.

Discussion of the research results. A consensus algorithm is used to reach an agreement on the reliability of a single data value in a distributed network where untrusted nodes are present. A 51% consensus is required to accept a valid transaction. The consensus algorithm supports many real-world systems, including Google PageRank, smart grids with load balancing, clock synchronization, and drone management.

Currently, there is a positive practice of using blockchain technologies in various areas.

Monetary operation. One of the most important applications of blockchain is the transfer of money and storage of information without the help of banks. The digital currency is growing rapidly and is attracting the attention of major financial institutions. This cryptocurrency has been called "memory" in the literature on monetary Economics. Bitcoin is a peer-to-peer electronic money system in which no one controls or has a linked printed currency. Bitcoin allows anonymity in peer-to-peer electronic currency systems. Some argue that major benefits are lost if a trusted third party is needed to prevent double spending. The technical infrastructure of this decentralized digital currency is based on several cryptographic technologies.

Supply chain management system. More than a hundred years ago, supply chains were relatively simple because trade was local, but they have become incredibly complex. Throughout the history of supply chains, there have been innovations such as the shift to transporting goods by truck rather than rail, or the advent of personal computers in the 1980s, which led to dramatic shifts in supply chain management. It is incredibly difficult for buyers or buyers to truly evaluate the value of products because there is no transparency in the existing system. Similarly, it is extremely difficult to investigate supply chains when illegal or unethical practices are suspected. They can also be extremely inefficient, as suppliers try to combine opinions about who needs what, when, and how. Blockchain can increase the efficiency and transparency of supply chains and have a positive impact on everything from warehousing to delivery and payment.

Power strength. The blockchain can be used to transfer solar energy to neighbors. The app allows users to buy and sell a renewable energy resource by counting electrons and placing it on the blockchain.

Election. The traditional method of voting in the country is through a paper system or electronic voting, through a machine at a polling station, or online voting via a web browser. There is always a threat to the security of the voting system from potential attacks. Using the blockchain concept in the e-voting platform, transparency and additional verification of the elections for violations can be provided.

Blockchain technology is guaranteed to protect the system from forgery and fraud, which prevents terrorists and extremists from quickly and anonymously launching attacks and getting the information they need. The blockchain could be the basis of cybersecurity, in case the user data will be stored in its network. It protects your data from being hacked, stolen, or destroyed. If a hacker breaks into a traditional system, they can access thousands of objects, but if they break into a blockchain system, they will only get access to one block of information. This complicates the work of the criminal, since he will have to

decrypt each fragment separately to get all the information. Anti-terrorist groups in some countries already use supercomputers with advanced software, in particular blockchain technologies, to calculate the probability of cyber attacks, collect and analyze large amounts of data from the Internet, identify and recognize the location, movement and interpersonal relationships of cyberterrorists, as well as identify suspected individuals and control their criminal activities.

Scientists pay attention to the fact that network attacks can contain malicious embedded code, the use of backdoors, and much more. Such attacks can be initiated from anywhere in the world due to a computer with a masked IP address. A new type of war, even cyberwar, changes the landscape of war itself. This type of cyberwar eliminates the need to have a physically capable armed force and requires the need for forces with strong technical capabilities, such as computer science skills. Many countries, including Russia, have come to understand that this is a problem and are actively pursuing policies to address it in order to mitigate threats.

Conclusion. For cyberterrorists, there are a huge number of new tools and technologies available that allow them to commit criminal acts almost anywhere in the world. The tasks of ensuring cyberspace security are becoming an important element of state legal policy in modern States, and they are priority areas for ensuring national security, interstate cooperation, and the entire world community. The more technologically advanced a society is, the more it is interested in suppressing various types of cyber attacks and threats to technological systems that provide the state security system and other life-supporting digital platforms. The use of blockchain technologies in the security system will allow distributing a cyber-attack from a single node to different blocks of the blockchain system, which will ensure the stability of this system to counter cyber threats and attacks.

The research is performed with financial support RFBR, research project No. 18-29-16175 «Blockchain technology counter the risks of cyberterrorism and cyberactivism: of criminological and legal research».

Е. А. Антонян, О. С. Рыбакова

Федералдық мемлекеттік бюджеттік жоғары білім беру мекемесі
О. Е. Кутафин атындағы Мәскеу мемлекеттік заң университеті, Мәскеу, Ресей

КИБЕРШАБУЫЛ ҚАУІПСІЗДІГІ МӘСЕЛЕСІНДЕГІ БЛОКЧЕЙН ТЕХНОЛОГИЯЛАР

Аннотация. Мақалада қоғамдық тәртіпті тұрақсыздандыруға, байланыс жүйелерін ауқымды түрде бұзуға, өз еркіндігіне, соның ішінде билік орғандарына қысым көрсету арқылы қорқытуға және жалпы алғанда мемлекеттің ұлттық және ақпараттық қауіпсіздігіне үлкен қауіп төндіретін кибершабуылдарға қарсы тұрудың жаңа технологиялары қарастырылады. Қылмыстық, террористік әрекеттерді, соның ішінде ақпараттық кеңістікті қаржыландыруға бағытталған қаражаттарды жасыруға мүмкіндік беретін блокчейн технологиясына ерекше назар аударылған. Сондай-ақ мақалада авторлар РБДР № 18-29-16175 «Кибертерроризм мен киберэкстремизм қауіп-қатеріпе қарсы тұрудағы блокчейн технологиясы: қылмыстық-құқықтық зерттеу» ғылыми жобасын іске асыру аясында жалпыланған зерттеу нәтижелерін ұсынады.

Қазірғі заманғы киберқылмыс мемлекет алдына жаңа міндеттерді алға тартады, оған енді бір мемлекет кеңістігінде жауап беру мүмкін емес. Бүгінгі таңда жаңа технологияларды қолдана отырып, киберқылмыстың алдын алу үшін мемлекеттердің өзара қатынасын заңнамалық тұрғыда реттеу өзекті мәселе саналады.

Киберқылмыспен күресудің жаңа нысандарының маңызды аспектісі – анонимді прокси жүйелерді қолданушыларды орталықсыздандыру. Егер бұрын қауіпсіздік орғандарына пайдаланушының IP-мекенжайы тікелей қолжетімді болса, қазір бәрі күрделене түсті және пайдаланушының трафиғіне кешенді талдау қажет.

Ғалымдар сонымен қатар желілік шабуылдарда зиянды ендірілген код, артқы есікті пайдалану немесе басқалай болуы да мүмкін екендіғі айтылған. Мұндай шабуыл әлемнің кез-келген нүктесінде жасырынған IP-мекенжайы бар компьютерге байланысты тууы мүмкін. Соғыстың жаңа түрі, тіпті киберсоғыстың өзі соғыс ландшафтын өзгертуде.

Соғыстың аталған түрі физикалық қабілетті қарулы күштер қажеттілігін жояды және компьютерлік шеберлік секілді қуатты техникалық мүмкіндікке ие күшті қажет етеді.

Көптеген елдер, оның ішінде Ресей де бұның күрделі мәселе екендігін түсініп, қауіпті азайту мақсатында шешу саясатын белсенді жүргізуде.

Түйін сөздер: блокчейн технологиясы, ақпараттық қауіпсіздік, киберқауіпсіздік, қарсы әрекет, киберқылмыс, кибертерроризм, ұлттық қауіпсіздік, кибершабуыл, Ресейдің қаржылық қауіпсіздігі, VPN сервері, ЖІШЖ – 3, риптовалюта, Биткойн, Литкоин, IP-мекенжайы.

Е. А. Антонян, О. С. Рыбакова

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный юридический университет им. О. Е. Кутафина», Москва, Россия

БЛОКЧЕЙН-ТЕХНОЛОГИИ В ВОПРОСАХ БЕЗОПАСНОСТИ ОТ КИБЕРАТАК

Аннотация. В статье рассматриваются новые технологии противодействия кибератакам, которые могут быть направлены на дестабилизацию общественного порядка, масштабное нарушение работы коммуникационных систем, устрашение путем навязывания своей воли, в том числе властным структурам и, в целом, представляют повышенную угрозу национальной и информационной безопасности государства. Особое внимание уделено блокчейн-технологии, которая позволяет скрыть средства, направленные на финансирование преступной, в том числе, террористической деятельности, в том числе в информационном пространстве. В статье представлены обобщенные результаты исследования в рамках реализации научного проекта РФФИ № 18-29-16175 «Блокчейн-технологии противодействия рискам кибертерроризма и киберэкстремизма: криминолого-правовое исследование».

Современная киберпреступность диктует новые вызовы государству, на которые уже нельзя реагировать в рамках пространства одного государства. Сегодня остро стоит вопрос законодательного регулирования вопросов взаимодействия государств по предотвращению киберпреступлений с использованием новых технологий.

Важнейшим аспектом новых форм противодействия киберпреступлениям является децентрализация пользователей анонимных систем прокси-серверов. И если раньше органы безопасности ещё имели доступные «лазейки» для прямого выхода на IP-адрес пользователя, то теперь всё стало намного сложнее и необходим комплексный анализ трафика того или иного пользователя.

Также ученые обращают внимание на то, что сетевые атаки могут содержать вредоносный встроенный код, использование бэкдоров и многое другое. Такие атаки могут быть инициированы из любой точки мира из-за компьютера с маскированным IP-адресом. Новый тип войны, даже кибервойны, меняет ландшафт самой войны.

Этот тип войны устраняет необходимость иметь физически дееспособные вооруженные силы и требует потребности в силах, обладающих сильными техническими возможностями, например, навыками информатики.

Многие страны, в том числе и Россия, пришли к пониманию того, что это проблема, и активно ведут политику для ее решения в целях смягчения угроз.

Ключевые слова: блокчейн-технологии, информационная безопасность, кибербезопасность, противодействие, киберпреступность, кибертерроризм, национальная безопасность, кибератака, финансовая безопасность России, VPN-сервер, СОРМ – 3, криптовалюта, биткойн, литкойн, IP-адрес.

Information about the authors:

Antonyan Elena Aleksandrovna, professor of criminology department and criminal executive law of the Kutafin Moscow State Law University (MSAL), Doctor of law, Professor, Moscow, Russia; antonyaa@yandex.ru; https://orcid.org/0000-0003-4765-5111

Rybakova Olga Sergeevna, senior researcher of the Federal Budgetary Institution «Scientific Center of Legal Information», Ph.D. in Law, Moscow, Russia; orro21@yandex.ru; https://orcid.org/0000-0002-2870-4355

REFERENCES

[1] Antonyan E.A. (2020) Issues of using new technologies in combating cyberterrorism // Monitoring of Law Enforcement. 2020. N 1 (33). P. 51-55 (in Russ.).

[2] Antonyan E.A., Aminov I.I. (2019) Blockchain technology in countering cyber terrorism // Actual problems of Russian Law. 2019. N 6 (103). P. 167-177 (in Russ.).

[3] Atagimova E.I., Ramazanova I.M. (2014) Some aspects of the legislative level of ensuring information security in the Russian Federation // Legal informatics. 2014. N 2. P. 14-19 (in Russ.).

[4] Baranova E.K., Babash A.V. (2018) Information Security and Information Protection: Textbook. allowance / E.K. Baranova, A.V. Babash. 4th ed., Revised. and add. M.: RIOR: INFRA-M, 2018. 336 p. ISBN 978-5-369-01761-6.

[5] Bliznets I., Kartskhiya A., Smirnov M. (2018) Technology transfer in digital era: legal environment // Tarih Kültür ve Sanat Araştırmaları. 2018. T. 7. N 1. P. 354-363 (in Eng.).

[6] Lopatin V.N. (2017) Information security problems and intellectual property risks in the digital economy // Information Law. 2017. N 2 P. 8-16 (in Russ.).

[7] Nakamoto S. (2008) Bitcoin: A Digital Peer-to-Peer Cash System. Available at: in Russ., in Eng. // access mode: http://bitcoinwhitepapers.com/bitcoin_ru.pdf / (accessed: 04/28/2020).

[8] Polyakova T.A., Minbaleev A.V., Boychenko I.S. Conceptual approaches to the legal regulation of information security in the conditions of digitalization and transformation of law // Journal of the Ural Federal District. Information security. 2019. N 3 (33). P. 64-68.

[9] Polyakova T.A., Minbaleev A.V., Boychenko I.S. (2019) Conceptual approaches to the legal regulation of information security in the context of digitalization and transformation of law // Bulletin of the Urals Federal District. Security in the information field. 2019. N 3 (33). P. 64-68 (in Russ.).

[10] Maurice Dawson A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism. // access mode: URL: www.igi-global.com (accessed: 03/15/2020).

[10] Petrov I.V., Makarov E.A. (2020) An operational-search measure obtaining computer information as a way of countering extremism and terrorism in cyberspace (legal analysis) // Military Law. 2020. N 1 (59). P. 213-219 (in Russ.).

[11] Rybakov O.J., Rybakova O.S. (2019) Principles of information security of a child on the internet // Studies in Computational Intelligence. 2019. Vol. 826. P. 427-433 (in Russ.).

[12] Rybakov O.Y. (2017) Priorities for the development of the information society in Russia: legal support // Monitoring of enforcement. 2017. N 3 (24). P. 71-76 (in Russ.).

[13] Stepanenko R.F., Khazieva N.O., Khaziev A.K., Rybakov O.Y. (2019) Modern problems and hypotheses of general theory of law: succession and novation // Opcion. 2019. Vol. 35. Special Issue N 22. P. 1097-1107 (in Russ.).

[14] Sukhodolov A.P., Antonyan E.A., Rukinov M.V., Shamrin M.Y., Spasennikova M.G. (2019) Blockchain in digital criminology: statement of the problem // All-Russian Criminological Journal. 2019. Vol. 13, N 4. P. 555-563 (in Russ.).

[15] Tereshchenko L.K. (2015) Development of information and telecommunication legislation (Ch. 15, Section III) // Scientific Concepts of the Development of Russian Legislation: Monograph / Executive Editor T.Y. Khabrieva, Y.A. Tikhomirov; Institute of Legislation and Comparative Law under the Government of the Russian Federation. M.: Publishing House of Law, 2015. 544 p. ISBN 978-5-9516-0743-0.