FUQAROLIK HUQUQI MUOMALASIDA KRIPTOGRAFIYA TUSHUNCHASI VA EVOLYUTSIYASI

КОНЦЕПЦИЯ И ЭВОЛЮЦИЯ КРИПТОГРАФИИ В КОНТЕКСТЕ ГРАЖДАНСКОГО ПРАВА

CONCEPT AND EVOLUTION OF CRYPTOGRAPHY IN THE CONTEXT OF CIVIL LAW

Imamnazarova-Hryshchenko Nafosatkhon
Toshkent davlat yuridik universiteti mustaqil izlanuvchisi (PhD)
missimamnazarova@gmail.com

Annotatsiya: Ushbu maqolada fuqarolik huquqi muomalasida kriptografiya tushunchasi va uning evolyutsiyasi o'rganiladi. Kriptografiyaning tarixi, zamonaviy qo'llanilishi va huquqiy tartibga solish masalalari tahlil qilinadi. Maqolada kriptografiyaning fuqarolik huquqidagi ahamiyati, xavfsizlik va maxfiylikni ta'minlashdagi roli, shuningdek, raqamli iqtisodiyot sharoitida uning rivojlanish istiqbollari ko'rib chiqiladi.

Kalit so'zlar: kriptografiya, fuqarolik huquqi, axborot xavfsizligi, raqamli iqtisodiyot, huquqiy tartibga solish

Аннотация: В этой статье исследуется понятие криптографии и ее эволюция в гражданско-правовом обороте. Анализируются история криптографии, ее современное применение и вопросы правового регулирования. В статье рассматривается значение криптографии в гражданском праве, ее роль в обеспечении безопасности и конфиденциальности, а также перспективы ее развития в условиях цифровой экономики.

Ключевые слова: криптография, гражданское право, информационная безопасность, цифровая экономика, правовое регулирование

Abstract: This article explores the concept of cryptography and its evolution in civil law circulation. The history of cryptography, modern applications and issues of

Legal Regulation are analyzed. The article examines the importance of cryptography in civil law, its role in ensuring security and privacy, as well as the prospects for its development in the context of the digital economy.
Keywords: cryptography, Civil Law, Information Security, digital economy, Legal Regulation

KIRISH

Kriptografiya - bu ma'lumotlarni shifrlash va deshifrlash orqali axborot xavfsizligini ta'minlash usuli bo'lib, uning tarixi qadimgi davrlarga borib taqaladi. Zamonaviy dunyoda kriptografiya fuqarolik huquqi muomalasida tobora muhim rol o'ynamoqda. Bu ayniqsa raqamli texnologiyalar va internet tarmog'ining keng tarqalishi bilan bog'liq. Kriptografiya nafaqat shaxsiy ma'lumotlarni himoya qilishda, balki elektron tijorat, raqamli imzolar va blokcheyn texnologiyalari kabi sohalarda ham qo'llanilmoqda [1].

Ushbu maqolaning maqsadi fuqarolik huquqi muomalasida kriptografiya tushunchasining evolyutsiyasini o'rganish, uning zamonaviy qo'llanilish sohalarini tahlil qilish va huquqiy tartibga solish masalalarini ko'rib chiqishdan iborat.

USULLAR VA ADABIYOTLAR TAHLILI

Ushbu tadqiqot asosan adabiyotlar tahlili va mavjud manbalarni o'rganishga asoslangan. Kriptografiya tarixi va evolyutsiyasi bo'yicha tarixiy manbalar, zamonaviy ilmiy maqolalar va huquqiy hujjatlar o'rganildi. Shuningdek, O'zbekiston va boshqa mamlakatlarning kriptografiyaga oid qonunchilik bazasi tahlil qilindi.

Tadqiqot jarayonida quyidagi asosiy manbalardan foydalanildi:

1. Singh S. (2000) "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography" [2] - kriptografiya tarixi va rivojlanishini o'rganish uchun.
2. Diffie W. va Hellman M. (1976) "New Directions in Cryptography" [3] - zamonaviy kriptografiyaning asosiy tamoyillarini tushunish uchun.
3. Narayanan A., Bonneau J., Felten E., Miller A. va Goldfeder S. (2016) "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction" [4] - blokcheyn va kriptovalyutalarda kriptografiyaning qo'llanilishini o'rganish uchun.
4. O'zbekiston Respublikasining "Elektron raqamli imzo to'g'risida"gi Qonuni (2022) [5] - milliy qonunchilikda kriptografiyaning o'rnini tahlil qilish uchun.

5. Yevropa Ittifoqining "Elektron identifikatsiya va trast xizmatlari to'g'risida"gi Reglamenti (eIDAS) (2014) [6] - xalqaro miqyosda kriptografiyani tartibga solish tajribasini o'rganish uchun.

NATIJALAR

Adabiyotlar tahlili va mavjud manbalarni o'rganish natijasida quyidagi asosiy natijalar olindi:

Kriptografiya tarixi va evolyutsiyasi: Kriptografiya tarixi miloddan avvalgi 1900-yillarga borib taqaladi. Qadimgi Misr, Yunoniston va Rim imperiyalarida oddiy almashtirish shifrlari qo'llanilgan [2]. O'rta asrlarda kriptografiya asosan harbiy va diplomatik sohalarda ishlatilgan. 20-asr boshlarida mexanik va elektromexanik shifrlash qurilmalari paydo bo'ldi. Ikkinchi jahon urushi davrida kriptografiya yanada rivojlandi va kompyuter texnologiyalari bilan birlashdi [7].

1970-yillarda Diffie va Hellman tomonidan ochiq kalitli kriptografiya g'oyasi taklif qilindi, bu esa zamonaviy kriptografiyaning rivojlanishiga turtki bo'ldi [3]. 1990-yillardan boshlab internet va elektron tijoratning rivojlanishi bilan kriptografiya fuqarolik huquqi muomalasida keng qo'llanila boshladi.

Fuqarolik huquqi muomalasida kriptografiyaning zamonaviy qo'llanilish sohalari:

- Elektron raqamli imzolar: hujjatlarning autentifikatsiyasi va yaxlitligini ta'minlash uchun
- Elektron tijorat: xavfsiz onlayn tranzaksiyalarni amalga oshirish uchun
- Shaxsiy ma'lumotlarni himoya qilish: maxfiylik va ma'lumotlar xavfsizligini ta'minlash uchun
- Blokcheyn va kriptovalyutalar: markazlashmagan moliyaviy tizimlarni yaratish uchun
- Bulutli hisoblash: ma'lumotlarni xavfsiz saqlash va uzatish uchun
- IoT (Internet of Things) qurilmalari: qurilmalar o'rtasidagi aloqani himoya qilish uchun.

Kriptografiyani huquqiy tartibga solish: Ko'pgina mamlakatlarda kriptografiyani tartibga soluvchi qonunlar qabul qilingan. Masalan, O'zbekistonda "Elektron raqamli imzo to'g'risida"gi Qonun (2003) elektron raqamli imzolarning huquqiy maqomini belgilaydi [5]. Evropa Ittifoqida eIDAS reglamenti (2014) elektron identifikatsiya va trast xizmatlari uchun yagona bozorni yaratishga qaratilgan [6].

Biroq, kriptografiyani tartibga solishda bir qator muammolar mavjud:

- Milliy xavfsizlik manfaatlari va fuqarolarning maxfiylik huquqi o'rtasidagi ziddiyat
- Kriptografik texnologiyalarning tez rivojlanishi va qonunchilikni yangilash zarurati
- Turli mamlakatlar o'rtasida kriptografiyaga oid qonunchilikni muvofiqlashtirish masalasi

Raqamli iqtisodiyot sharoitida kriptografiyaning kelajak istiqbollari:

- Kvant kriptografiyasi: mutlaq xavfsiz aloqani ta'minlash imkoniyati
- Gomomorf shifrlash: shifrlangan ma'lumotlar ustida amallar bajarish imkoniyati
- Blokcheyn texnologiyalarining yanada rivojlanishi va keng qo'llanilishi
- Suniy intellekt va kriptografiyaning integratsiyasi
- Kriptografiyaning IoT va 5G texnologiyalarida qo'llanilishi

TAHLIL VA MUHOKAMA

Kriptografiyaning fuqarolik huquqi muomalasidagi ahamiyati tobora ortib bormoqda. Bu bir tomondan raqamli texnologiyalarning rivojlanishi va ularning hayotimizning barcha jabhalariga kirib borishi bilan bog'liq bo'lsa, ikkinchi tomondan kiberjinoyatchilik va ma'lumotlar xavfsizligiga bo'lgan tahdidlarning kuchayishi bilan izohlanadi.

Zamonaviy kriptografiya nafaqat ma'lumotlarni shifrlash, balki ularning yaxlitligi va autentifikatsiyasini ta'minlash imkonini beradi. Bu esa elektron tijorat, raqamli bankchilik va boshqa onlayn xizmatlarning rivojlanishi uchun muhim ahamiyatga ega. Elektron raqamli imzolar kriptografik usullar yordamida yaratiladigan bo'lib, ular an'anaviy imzolarga teng huquqiy kuchga ega bo'lishi mumkin [5].

Blokcheyn texnologiyalari va kriptovalyutalarning paydo bo'lishi kriptografiyaning yangi qo'llanilish sohalarini ochib berdi. Ular markazlashmagan va ishonchli tizimlarni yaratish imkonini beradi, bu esa moliya, logistika, intellektual mulk huquqi va boshqa sohalarda inqilobiy o'zgarishlarga olib kelishi mumkin [4].

Biroq, kriptografiyaning keng tarqalishi bir qator huquqiy va axloqiy muammolarni keltirib chiqarmoqda. Masalan, kuchli shifrlash usullaridan foydalanish jinoyatchilar va terroristlar tomonidan o'z faoliyatlarini yashirish uchun ishlatilishi mumkin. Bu esa davlatlar oldiga kriptografiyani qanday tartibga solish kerakligi haqidagi murakkab savolni qo'ymoqda.

Kriptografiyani tartibga solishda muvozanatni topish muhim: bir tomondan, fuqarolarning maxfiylik huquqini va biznesning manfaatlarini himoya qilish, boshqa

tomondan esa milliy xavfsizlik va huquq-tartibot organlarining samarali ishlashini ta'minlash zarur. Bu masala bo'yicha turli mamlakatlar turlicha yondashuvlarni qo'llamoqda, va xalqaro hamjamiyat oldida ushbu sohada umumiy standartlarni ishlab chiqish vazifasi turibdi [6].

Kelajakda kriptografiyaning yanada rivojlanishi va yangi texnologiyalar bilan integratsiyalashuvi kutilmoqda. Kvant kriptografiyasi va gomomorf shifrlash kabi ilg'or usullar ma'lumotlar xavfsizligi va maxfiyligini yangi darajaga ko'tarishi mumkin. Shu bilan birga, sun'iy intellekt va kriptografiyaning birlashishi yangi imkoniyatlar va xavf-xatarlarni keltirib chiqarishi mumkin.

XULOSALAR

1. Kriptografiya fuqarolik huquqi muomalasida tobora muhim rol o'ynamoqda, bu esa raqamli iqtisodiyotning rivojlanishi va axborot xavfsizligiga bo'lgan ehtiyojning ortishi bilan bog'liq.
2. Zamonaviy kriptografiya elektron raqamli imzolar, elektron tijorat, shaxsiy ma'lumotlarni himoya qilish, blokcheyn texnologiyalari va boshqa sohalarda keng qo'llanilmoqda.
3. Kriptografiyani huquqiy tartibga solish murakkab masala bo'lib, maxfiylik huquqi va milliy xavfsizlik manfaatlari o'rtasida muvozanatni topishni talab qiladi.
4. Kelajakda kvant kriptografiyasi, gomomorf shifrlash va boshqa ilg'or texnologiyalarning rivojlanishi kutilmoqda, bu esa fuqarolik huquqi muomalasida yangi imkoniyatlar va muammolarni keltirib chiqarishi mumkin.
5. Kriptografiya sohasidagi xalqaro hamkorlik va standartlashtirish jarayonlarini kuchaytirish zarur, bu esa global raqamli iqtisodiyotning barqaror rivojlanishiga hissa qo'shadi.

REFERENCES

1. Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 1996. Handbook of applied cryptography. CRC press.
2. Singh, S., 2000. The code book: the science of secrecy from ancient Egypt to quantum cryptography. Anchor.
3. Diffie, W. and Hellman, M., 1976. New directions in cryptography. IEEE transactions on Information Theory, 22(6), pp.644-654.
4. Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S., 2016. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

5. O‘zbekiston Respublikasining Qonuni, 12.10.2022 yildagi O‘RQ-793-son, https://lex.uz/docs/-6234904

6. European Union, 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union, L 257, pp.73-114.

7. Kahn, D., 1996. The Codebreakers: The comprehensive history of secret communication from ancient times to the internet. Simon and Schuster.