e-ISSN(Online) 2709-1201

МЕЖДУНАРОДНЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

ENDLESS LIGHT IN SCIENCE

NO 1
31 ЯНВАРЯ 2026
Астана, Казахстан

lrc-els.com

МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ «ENDLESS LIGHT IN SCIENCE»

INTERNATIONAL SCIENTIFIC JOURNAL «ENDLESS LIGHT IN SCIENCE»

International scientific journal «Endless Light in Science», includes reports of scientists, students, undergraduates and school teachers from different countries (Kazakhstan, Tajikistan, Azerbaijan, Russia, Uzbekistan, China, Turkey, Belarus, Kyrgyzstan, Moldova, Turkmenistan, Georgia, Bulgaria, Mongolia). The materials in the collection will be of interest to the scientific community for further integration of science and education.

Международный научный журнал «Endless Light in Science», включают доклады учёных, студентов, магистрантов и учителей школ из разных стран (Казахстан, Таджикистан, Азербайджан, Россия, Узбекистан, Китай, Турция, Беларусь, Кыргызстан, Молдавия, Туркменистан, Грузия, Болгария, Монголия). Материалы сборника будут интересны научной общественности для дальнейшей интеграции науки и образования.

31 января 2026 г.
Астана, Казахстан

https://doi.org/10.5281/zenodo.18523809
УДК 343.2

CYBERCRIME: THE PROBLEM AND SOME WAYS TO SOLVE IT

WU DI
Graduate student of the educational program 7M04202 – Jurisprudence
International Taraz University named after Sherhan Murtaza, Taraz

Scientific supervisor – **GAZAYEV ASKHAT**
Head of the Department of Civil and Criminal Law, Doctor of Criminology
International Taraz University named after Sherhan Murtaza, Taraz

Annotation. *The article examines the theoretical foundations of interaction between international and national law in combating cybercrime. It analyzes the nature and specific features of legal norms regulating this area, as well as mechanisms of their interaction and mutual influence. The article emphasizes the importance of a comprehensive approach and effective cooperation in countering cybercrime in the context of globalization.*

Keywords: *cybercrime, internet, internet fraud, IT sector, digital environment, computer software.*

The world is undergoing a constant process of development of society and the state as a whole. Thanks to scientific and technological progress, a digital world has emerged in people's lives, where the Internet is no longer merely a tool for meeting people, but also serves as a medium for sharing knowledge, cultures, and traditions of different states, while bringing together people from diverse countries who aim to connect with each other, discuss any topics of interest, which remain relevant today. Over recent years, the number of Internet users has increased manyfold and continues to grow. According to statistics from the Digital 2022 Global Overview Report, as of January 2024, the global number of Internet users rose to 4.95 billion, accounting for 62.5% of the world's population. These figures indicate that over the last year alone, there was an increase of 192 million Internet users. However, given the emergence of COVID-19, actual growth trends might have been considerably higher than initially reported[1]. From this, we can conclude that the number of computer users has increased dramatically in 2024 and continues to rise due to the popularity of the Internet, even during the coronavirus pandemic, user numbers continued to grow. States are evolving by leveraging ongoing advancements in science, developing numerous projects aimed at enhancing the digital landscape to improve the quality of life for their citizens. However, criminal activity does not stand still either, especially among Internet users. Advances in technology allow criminals to devise novel ways of earning money and circumventing security systems, thereby eluding detection of their misconduct. Not only do they commit illegal acts, but they also enhance their influence on public consciousness. With the increasing number of users, two factors come into play: 1) Society becomes dependent on information technologies, and this dependency cannot be eliminated; and 2) Internet users become victims of cybercriminals. Committing cybercrimes requires minimal effort—only a computer and access to the Internet are needed. However, perpetrators, including hackers, are becoming increasingly cunning and resourceful every day, inventing new tools to carry out their illicit deeds: This includes the creation of artificial intelligence programmed to commit crimes at its creator's request, the development of computer viruses used to launch hacking attacks on various organizations and banks with the intent of stealing funds, as well as the theft of classified documents and research created by specific scientists containing state secrets and monetary value.

Furthermore, the Internet facilitates the distribution of narcotics and psychotropic substances, the promotion of terrorism and extremism aimed at overthrowing government authority, the dissemination of pornography, human trafficking, organization of prostitution, and coercion into it, among others. All socially harmful acts carried out using information and telecommunication

technologies fall into two categories: 1) Acts involving interactions between humans and technology (for example, thefts facilitated by software and hardware); and 2) Acts involving technologically mediated interactions between one person and another (group of persons)[2]. It is specifically the second group of crimes that poses a very serious threat to the safety of individuals, society, and the state, known as cybercrime. Cybercrime refers to socially harmful acts committed via the Internet, causing damage not only to individuals but also to the state itself. Ten to twenty years ago, this phenomenon was known only to specialists in the IT field, whereas today it represents a problem of global magnitude. The origins of cybercrime date back to the 1990s, since it was during this period that computers became widely available throughout society. Initially, most cybercrimes were largely humorous in nature, but nowadays they are committed primarily for profit, intimidation, warfare, and similar purposes. Current legislation in countries aims to curb this type of crime, yet as laws evolve, so too do the methods of committing these crimes. For instance, the damage caused by crimes utilizing computer technologies could amount to approximately 165 billion rubles for Russia in 2024. According to statistical data, the total loss from cybercrimes exceeded around 150 billion rubles in 2023. During 2023, there were 518,000 cybercrimes recorded, which is 1.4 times greater than the previous year's indicators and almost 1.9 times more compared to 2019. As noted by Eugene Tsarev, CEO of RTM Group[3], During 2023, the number of cyberattacks increased by one-third, or 35%. This trend is linked to telephone fraud and the use of emerging computer technologies, with expected annual growth rates remaining steady at a minimum of 30%. The cumulative damage for the entire year could reach 165 billion rubles. From this, we can deduce that the number of cybercrimes increases annually, resulting in substantial economic losses nationwide. This situation arises because criminals develop new methods of committing crimes, engage in fraudulent activities involving bank cards, and employ popular tactics for stealing funds, such as computer viruses and phishing attacks. Experts predict that cybercriminals will become even more active, with their tools for perpetrating illegal acts becoming ever more sophisticated. They will continue engaging in cyberattacks because current criminal law regulations are insufficiently adapted to deal with such types of crimes. Furthermore, virtual space allows for the creation of new computer programs designed specifically for committing criminal acts.

In our view, the gravest form of cybercrime involves the theft of personal data, considering nearly everyone globally uses social networks and registers on websites where required—for instance, banking sites, governmental platforms, online stores, etc. Today, the issue of cybercrime in cyberspace gains greater relevance, necessitating thorough research and meticulous efforts toward resolving this problem. Nations strive to prevent such threats. Nevertheless, it must be remembered that we live in an era characterized by informational wars, wherein many countries wage such conflicts to destabilize the internal order of rival nations. In such scenarios, the country possesses its own cyberdefenders. To illustrate this point vividly, I would like to describe the case of the WannaCry virus [4]. The WannaCry virus was a ransomware program whose primary function was to exploit vulnerabilities in Windows operating systems and leave a message instructing users to transfer 300 dollars to a specified account in order to regain access to their devices. First detected in Spain, the virus quickly spread to Ukraine, Russia, India, and other regions, causing significant damage.

According to reports, the vulnerability exploited by WannaCry had previously been identified by the U.S. National Security Agency (NSB), and the information about it was stolen by the hacker group Shadow Brokers and then publicly released. Among those suspected of creating the virus is the North Korea-linked hacker collective Lazarus Group.

One of the most severe cyber-attacks occurred in September 2023, when hackers compromised servers connected to life support equipment in a university hospital in Germany, leading to the death of a patient due to temporary device failure. Additionally, Russian hacker group Sandworm infiltrated NSB email servers, exploiting a vulnerability discovered in June 2022 in the Exim mail agent.

These examples highlight the growing sophistication and danger of cyber-criminals, reinforcing the need for stronger defensive strategies and enhanced collaboration among nations to combat these threats [5]. This hacker group, known as Sandworm, enables attackers to send a malicious email to a

server and immediately obtain the ability to remotely execute their own code on the target system. The group has also been accused of involvement in political events in Ukraine and Georgia, as well as interference in elections in France.

As a result of thorough research on cybercrime in cyberspace, it can be concluded that this issue remains highly relevant today. While complete elimination of cybercrime appears impossible, mitigation measures can substantially reduce its impact. One key solution lies in establishing a filtering system that carefully screens articles, posts, and other forms of textual content on the Internet. Additionally, setting up a specialized agency dedicated to monitoring criminally oriented websites and implementing registration systems for social media platforms, with mandatory identification requirements and strict anti-fake policies, could prove beneficial. Such initiatives aim to enhance online security and minimize opportunities for cybercriminals to exploit vulnerable users. Additionally, to combat cybercrime in the realm of information technology, it is crucial to enhance and develop existing systems addressing crimes in this domain comprehensively. Efforts should integrate responses to cybercrime across all dimensions, encompassing both established and emerging forms of criminality. Here are some additional strategies to tackle cybercrime:

Strengthen Penalties: Drawing inspiration from legislative practices abroad, penalties for cybercrimes should be strengthened. For instance, U.S. federal law imposes harsher sentences for large-scale computer-related fraud, potentially reaching up to 20 years imprisonment, contrasting with Russia's limit of 10 years.

Enhance Collaboration Between Agencies: Improved coordination among law enforcement bodies, judicial authorities, and cybersecurity experts will facilitate quicker response times and more effective investigations.

Investment in Cyber Infrastructure: Upgrading digital infrastructures to incorporate advanced encryption protocols and multi-layered defense mechanisms can deter potential offenders.

Public Awareness Campaigns: Educating the public about safe online behaviors and recognizing signs of cyber threats empowers individuals to avoid becoming victims.

By adopting these measures, along with ongoing innovations in cybersecurity technologies, we can create a safer digital ecosystem. [6].

In China, a new form of punishment called “mass inconvenience” has been introduced instead of fines and prison terms. This penalty essentially amounts to social isolation in a country where mobile payments dominate everyday transactions, spanning everything from public transportation to grocery shopping, utility bills, healthcare services, and tourism. Introduced as part of the fight against organized criminal gangs involved in selling, renting, and credit-lending of bank accounts and mobile SIM cards tied to citizen IDs, this measure punishes convicted individuals by depriving them of the ability to make mobile or bank card payments for five years. Instead, they are forced to rely solely on cash transactions.

Reactions to this drastic measure have varied, with one commentator on Chinese social platform Weibo describing it as a form of “social death,” stating, “It's really too cruel.” Despite criticism, supporters argue that such harsh punishments serve as a powerful deterrent against financial crimes, particularly those enabling larger criminal enterprises [7].

Moreover, introducing new legislation to regulate societal relations in the sphere of information technology is imperative. This regulatory framework should focus on preventing actions that compromise the confidentiality, integrity, and availability of computer systems, networks, and data. By doing so, the level of cybercrime will gradually decrease, although complete eradication remains challenging. Implementing clear guidelines and enforceable sanctions can help establish boundaries and consequences for violations, discouraging potential offenders. Additionally, fostering international cooperation and shared expertise will contribute to building resilient cyber-defense mechanisms globally.

REFERENCES:

1. Ten Loudest Cyber Attacks of the 21st Century // Cybersecurity – 2024.
2. China Invented an Alternative to Fines and Prison Sentences. It's Called "Social Death" // Kadara.ru. 2024.
3. Potential Damage from Cybercrime Estimated at ₽165 Billion in 2024 // Rambler.
4. United States Code // Legal Information Institute.
5. Tips for Protecting Against Cybercriminals // Kaspersky.
6. Sikach A. S. Combating Computer Crimes. The Issue of Eradicating Crime Among Internet Users // Current Issues in Solving and Investigating Crimes Committed Using the Internet: Proceedings of the All-Russia Scientific-Practical Conference. Belgorod, September 23, 2025 / Ed. N. A. Zhukova. Belgorod: ID "BelGU" NIU "BelGU", 2025. P. 179.
7. Digital Trends of 2024: All the Latest Statistics Every Marketer Needs to Know // PiN-UP. 2024.

https://doi.org/10.5281/zenodo.18523831
УДК 346

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ВОПРОСЫ ВЗАИМОДЕЙСТВИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И КРИПТОБИРЖ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ОТМЫВАНИЮ ДЕНЕГ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА

ТАЙЖАНОВ АРМАН КАИРГЕЛЬДИНОВИЧ
магистрант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

Аннотация. *В настоящей статье исследуются организационно-правовые аспекты взаимодействия правоохранительных органов с криптобиржами в контексте борьбы с отмыванием денежных средств (ПОД/ФТ). Проводится детальный анализ существующих механизмов регулирования и контроля, а также рассматриваются основные проблемы и перспективы межсекторного сотрудничества. Особое внимание уделяется международным стандартам и рекомендациям.*

Ключевые слова: *криптобиржи, правоохранительные органы, противодействие отмыванию денег (ПОД), финансирование терроризма (ФТ), регулирование, контроль, международное сотрудничество, международные стандарты, ПОД/ФТ.*

АҚШАНЫ ЖЫЛЫСТАТУҒА ЖӘНЕ ТЕРРОРИЗМДІ ҚАРЖЫЛАНДЫРУҒА ҚАРСЫ ІС-ҚИМЫЛ САЛАСЫНДАҒЫ ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫ МЕН КРИПТОВАЛЮТА БИРЖАЛАРЫНЫҢ ӨЗАРА ІС-ҚИМЫЛЫНЫҢ ҰЙЫМДАСТЫРУШЫЛЫҚ-ҚҰҚЫҚТЫҚ МӘСЕЛЕЛЕРІ

Аңдатпа. *Бұл мақалада құқық қорғау органдарының криптовалюта биржаларымен ақшаны жылыстатумен (АЖ/ТҚҚ) күресу тұрғысында өзара әрекеттесуінің ұйымдастырушылық-құқықтық аспектілері қарастырылады. Қолданыстағы реттеу және бақылау тетіктеріне егжей-тегжейлі талдау жүргізіледі, сондай-ақ салааралық ынтымақтастықтың негізгі проблемалары мен перспективалары қарастырылады. Халықаралық стандарттар мен ұсыныстарға ерекше назар аударылады.*

Түйінді сөздер: *криптовалюта биржалары, құқық қорғау органдары, ақшаны жылыстатуға қарсы іс-қимыл, терроризмді қаржыландыру, реттеу, бақылау, халықаралық ынтымақтастық, халықаралық стандарттар, ақшаны жылыстатуға және терроризмді қаржыландыруға қарсы іс-қимыл*

ORGANIZATIONAL AND LEGAL ISSUES OF INTERACTION BETWEEN LAW ENFORCEMENT AGENCIES AND CRYPTO EXCHANGES IN THE FIELD OF COUNTERING MONEY LAUNDERING AND TERRORIST FINANCING

Annotation. *This article examines the organizational and legal aspects of law enforcement agencies' interaction with crypto exchanges in the context of combating money laundering (AML/CFT). A detailed analysis of the existing regulatory and control mechanisms is carried out, as well as the main problems and prospects of intersectoral cooperation are considered. Special attention is paid to international standards and recommendations.*

Keywords: *crypto exchanges, law enforcement agencies, anti-money laundering (AML), terrorist financing (FT), regulation, control, international cooperation, international standards, AML/CFT.*

Введение

Тема нашего исследования, несмотря на её актуальность, остается недостаточно освещенной в казахстанских научных трудах. В контексте анализа историографии данной проблематики следует выделить работы таких авторитетных исследователей, как Карабеков К.О. [1], Искаков З.Д., Рахымжанов А.А. [2], Нургазиев С.Б., Карымсаков Р.Ш. [3], Сериков Д. [4] и другие. Их вклад в изучение вопроса является значительным и представляет собой фундаментальную основу для дальнейших исследований.

В научном сообществе стран СНГ данная тематика частично отражена в трудах таких ученых, как Курилов С.И., Осипов И.В. [5], Пушкарев В.В. и Техеров А.Ю. [6]. Их работы вносят важный вклад в теоретическое осмысление проблемы и предоставляют ценные эмпирические данные для анализа.

Как верно отмечает А. П. Фильченко [7], в условиях стремительного прогресса информационно-телекоммуникационных и цифровых технологий, а также появления инновационных платежных средств, основанных на криптографических принципах, значительно возросли риски, связанные с осуществлением незаконных финансовых операций, включая легализацию преступных доходов и финансирование террористической деятельности. Высокая степень анонимности, характерная для субъектов высокотехнологичной преступности, вынуждает правительства и регулирующие органы корректировать существующие подходы к контролю за оборотом виртуальных активов, а также разрабатывать новые управленческие, правовые и экономические механизмы, направленные на выявление, предотвращение и минимизацию последствий неправомерных финансовых операций.

С учетом вышеуказанных факторов возникает настоятельная необходимость в проведении фундаментальных научных исследований и последующей оценке организационного опыта различных государств в области регулирования оборота виртуальных активов. Преимущества, которые виртуальные активы предоставляют для осуществления незаконной деятельности, требуют адекватного противодействия путем расширения контрольных функций государственных органов, что включает в себя введение нормативно-правовых санкций и внедрение системы комплаенса, обеспечивающей их соблюдение как для физических, так и для юридических лиц, участвующих в создании и обороте виртуальных активов.

Таким образом, комплексное научное исследование данной проблематики является критически важным для формирования эффективных стратегий противодействия финансовым преступлениям в цифровом пространстве.

Целью настоящего исследования является анализ организационно-правовых аспектов взаимодействия правоохранительных органов и криптовалютных бирж в контексте противодействия отмыванию денег и финансированию терроризма.

Актуальность темы обусловлена стремительным ростом популярности криптовалют и значительным увеличением объема операций на криптовалютных биржах. Эти тенденции требуют адекватного усиления мер по противодействию финансовым преступлениям в цифровой среде.

Основная часть

В условиях глобализации и цифровизации финансовых систем вопросы противодействия легализации преступных доходов (AML, Anti-Money Laundering) и финансированию террористической деятельности (CFT, Combating the Financing of Terrorism) приобретают первостепенное значение. Эти вызовы требуют комплексного подхода, включающего взаимодействие государственных органов, финансовых институтов и участников криптовалютного рынка.

Криптовалюты, основанные на технологии блокчейн, открывают новые горизонты для проведения финансовых транзакций, однако их децентрализованный и анонимный характер создает благоприятные условия для злоупотреблений. В связи с этим возникает потребность в разработке и внедрении эффективных механизмов комплаенса и регулирования,

направленных на минимизацию рисков отмывания денег и финансирования преступной деятельности в сфере цифровых активов.

Основу мер по противодействию в Республике Казахстан составляют такие правовые акты, как Закон Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [8], «О противодействии терроризму» [9], «О противодействии экстремизму» [10].

В современный период фундамент государственной системы по рассматриваемой отрасли представляет комплекс, состоящий из традиционного правоохранительного блока и специализированного финансового мониторинга, представляемого Агентством финансового мониторинга Республики Казахстан.

Современные цифровые технологии и процессы глобализации инициировали трансформацию финансового ландшафта, что привело к возникновению нового класса финансовых инструментов — цифровых активов, обладающих юридической значимостью. Этот класс охватывает широкий спектр цифровых объектов, включая криптовалюты, токены, смарт-контракты и другие формы цифровых ценностей.

Классификационная структура цифровых активов включает следующие подкатегории:

1. Криптовалюты, такие как Bitcoin и Ethereum, представляют собой виртуальные активы, обеспеченные криптографическими алгоритмами и функционирующие на платформе блокчейн-технологий. Они обладают уникальными характеристиками децентрализации, анонимности и прозрачности транзакций.

2. Токены, включая утилитарные и security-токены, являются цифровыми активами, предоставляющими определенные права на материальные или нематериальные блага, услуги или доступ к конкретным сервисам. Утилитарные токены используются для получения доступа к продуктам или услугам, в то время как security-токены обеспечивают инвесторам права на долю в капитале компании или другие финансовые активы.

3. Невзаимозаменяемые токены (NFT) обозначают уникальные цифровые объекты, которые не могут быть заменены другими идентичными единицами. Примерами NFT могут служить произведения искусства, коллекционные предметы, игровые активы и другие цифровые объекты, обладающие высокой степенью уникальности и ценности.

4. Цифровые права в распределенных реестрах также входят в категорию цифровых активов. Эти права могут быть закреплены в виде записей в блокчейн-системе, что обеспечивает их неизменяемость и прозрачность.

Смарт-контракты представляют собой программные алгоритмы, автоматизирующие исполнение сделок при выполнении заранее заданных условий. Они функционируют на основе децентрализованных платформ, таких как Ethereum, и позволяют существенно снизить транзакционные издержки и минимизировать риски, связанные с человеческим фактором.

Правовое регулирование цифровых активов представляет собой сложную и многоаспектную задачу, варьирующуюся в зависимости от юрисдикции. Законодательные инициативы направлены на обеспечение безопасности, стабильности и легитимности рынка цифровых активов, а также на защиту прав участников этих рынков.

Республика Казахстан, нацеленная на укрепление своего экономического потенциала и повышение конкурентоспособности на международной арене, уделяет пристальное внимание регулированию правоотношений, связанных с цифровыми активами. Закон Республики Казахстан от 6 февраля 2023 года № 193-VII «О цифровых активах в Республике Казахстан» [11] представляет собой основополагающий нормативно-правовой акт, направленный на формирование правовой базы для эффективного регулирования цифровой экономики.

Регулирование криптоактивов в Казахстане можно условно разделить на несколько этапов:

1. Начало формирования регулирования (запрет на обращение с 2020 по 2022 годы)

2. Пилотная фаза нового механизма (с августа 2022 года по ноябрь 2023 года включительно)

3. Введение законодательного регулирования оборота криптовалют на территории МФЦА в сотрудничестве с казахстанскими финансовыми институтами (ноябрь 2023 года - настоящее время)

В рамках нового правового регулирования на криптовалютном рынке появились новые категории участников, включая криптоброкеров, криптодилеров и инвестиционные компании. Помимо традиционных операций по инвестированию средств в цифровые активы, закон разрешил проведение таких сложных финансовых инструментов, как криптостейкинг, маржинальная торговля и криптолендинг (привлечение фиатных средств под залоговое обременение цифровых активов).

Республика Казахстан в настоящее время сталкивается с рядом значимых вызовов в сфере правового регулирования цифровых активов, что обусловлено стремительным развитием данной отрасли и её интеграцией в глобальные экономические процессы. В условиях динамично меняющегося правового ландшафта необходимо обеспечить соответствие национального законодательства международным стандартам, что является ключевым аспектом для успешной интеграции Казахстана в глобальный финансовый рынок.

Одной из первоочередных задач является установление оптимального баланса между мерами регулирования и стимулированием инновационных процессов, что предполагает разработку и внедрение механизмов регулирования, которые, с одной стороны, обеспечат защиту прав участников рынка и минимизацию потенциальных рисков, а с другой стороны, будут способствовать развитию цифровой экономики и привлечению инвестиций.

Особое внимание следует уделить созданию эффективных механизмов защиты прав инвесторов. В условиях цифровизации финансовых рынков возрастает риск мошенничества и недобросовестной деятельности, что требует разработки и внедрения комплексных мер по обеспечению безопасности инвесторов, что включает в себя как правовые, так и технические аспекты, направленные на предотвращение и своевременное выявление мошеннических схем.

Обеспечение транспарентности и подотчётности в сфере цифровых активов является ещё одним важным направлением. Прозрачность операций и подотчётность участников рынка способствуют повышению уровня доверия со стороны инвесторов и регуляторов, что является необходимым условием для устойчивого развития цифровой экономики.

Для успешного преодоления существующих вызовов необходимо консолидированное взаимодействие государственных органов, представителей бизнес-сообщества и экспертного сообщества. Только при условии комплексного подхода и координации усилий различных заинтересованных сторон можно обеспечить эффективное регулирование и развитие данной отрасли, что будет способствовать её интеграции в мировую экономику и повышению конкурентоспособности Казахстана.

Международный Валютный Фонд (МВФ) для нивелирования рисков, ассоциированных с криптоактивами, предлагает комплексную стратегию, основанную на принципах экономической стабильности, правового регулирования и международного сотрудничества [12].

Международная организация комиссий по ценным бумагам (IOSCO) в 2019 году опубликовала «Методологические принципы» для государственных регуляторов, охватывающие ключевые аспекты регулирования криптовалютной торговли, хранения и передачи цифровых активов. В данном документе IOSCO сформулировала ряд рекомендаций, направленных на обеспечение эффективного и безопасного регулирования криптовалют без ущерба для интересов пользователей [13].

16 ноября 2023 года IOSCO представила финальный вариант рекомендаций по политике регулирования криптоактивов, разработанный группой экспертов организации. Документ охватывает шесть ключевых областей, включающих 18 рекомендаций, направленных на минимизацию конфликтов интересов, предотвращение манипулирования рынком, борьбу с инсайдерской торговлей и мошенничеством, управление трансграничными рисками,

обеспечение безопасного хранения клиентских активов, а также оценку операционного и технологического рисков [14].

Комитет по платежам и финансовой инфраструктуре (CPMI) Банка международных расчетов (BIS) совместно с Международной организацией комиссий по ценным бумагам (IOSCO) в июле 2022 года представил Руководство по применению принципов инфраструктуры финансового рынка к системно значимым экосистемам стейблкоинов (Application of the Principles for Financial Market Infrastructures to stablecoin arrangements) [15].

Данный документ является важным шагом в реализации принципа «риск-ориентированного регулирования» применительно к системно значимым стейблкоиновым экосистемам, используемым в платежных системах. Он также вносит значительный вклад в реализацию программы трансграничных платежей Группы двадцати (G20).

Международная ассоциация свопов и деривативов (ISDA, International Swaps and Derivatives Association), ведущая организация в области финансовых деривативов, в сентябре 2021 года предложила разработать унифицированные стандарты для регулирования торговли криптодеривативами с целью повышения эффективности и минимизации рисков в данном сегменте [16].

В мае 2022 года ISDA опубликовала документ под названием «Риски криптоактивов и анализ хеджирования», в котором рассматривается возможность использования фьючерсов и биржевых фондов (ETF) для хеджирования рисков, связанных с криптоактивами.

Группа разработки финансовых мер борьбы с отмыванием денег (FATF, Financial Action Task Force) представляет собой межправительственную организацию, занимающуюся разработкой и продвижением международных стандартов в области противодействия отмыванию денег (ПОД), финансированию терроризма (ФТ) и финансированию распространения оружия массового уничтожения (ФРОМУ). В рамках своей деятельности ФАТФ рассматривает криптовалюты как «виртуальные» активы, требующие особого внимания и регулирования [17].

Согласно отчетам взаимной оценки ФАТФ, США демонстрируют наиболее продвинутый уровень регулирования провайдеров услуг по виртуальным активам (ПУВА). В США действует законодательство, обязывающее криптовалютные биржи, владельцев криптовалютных кошельков и провайдеров услуг по передаче виртуальных активов проходить процедуру регистрации и лицензирования. Кроме того, в стране функционирует множество органов регулирования, осуществляющих надзор за соблюдением установленных правил и стандартов.

ФАТФ, как ведущая международная организация в сфере противодействия отмыванию денег (ОД), финансированию терроризма (ФТ) и финансированию распространения оружия массового уничтожения (ФРОМУ), выдвигает рекомендации, направленные на гармонизацию национальных подходов к регулированию рынка ВА. В частности, FATF акцентирует внимание на необходимости реализации системного риск ориентированного подхода, предусмотренного 15-й Рекомендацией, который включает в себя создание условий для регистрации и лицензирования ПУВА, а также установление строгих требований к их деятельности.

Кроме того, ФАТФ подчеркивает важность проведения периодических национальных и секторальных оценок рисков ОД/ФТ/ФРОМУ с участием представителей сектора ВА. Данные оценки должны учитывать корпоративные риски, связанные с деятельностью ПУВА, и способствовать выработке эффективных мер по минимизации выявленных угроз. В случае отсутствия полноценного регулирования ВА, FATF рекомендует применять полный запрет на их оборот, что свидетельствует о признании критической значимости эффективного контроля над данным сегментом финансового рынка.

Таким образом, международные финансовые институты акцентируют внимание на необходимости глобальной координации усилий и комплексного подхода к регулированию рынка криптоактивов. Рекомендации ФАТФ и других авторитетных организаций направлены

на создание прозрачной, безопасной и устойчивой среды для функционирования данного сегмента, что в конечном итоге способствует снижению рисков ОД/ФТ/ФРОМУ и повышению уровня финансовой безопасности на глобальном уровне.

В настоящее время около 180 государств мира внедряют рекомендации в области противодействия отмыванию денег (ПОД) и финансированию терроризма (ФТ), разработанные Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ). Соблюдение стандартов ФАТФ является ключевым элементом для обеспечения национальной безопасности, экономической стабильности и устойчивого развития, а также для интеграции в глобальное финансовое сообщество.

Результаты оценки соответствия данным стандартам оказывают значительное влияние на финансовую стабильность государства, поскольку способствуют поддержанию чистоты финансовой системы и снижению рисков, связанных с использованием финансовых ресурсов в незаконных целях. Кроме того, они повышают инвестиционную привлекательность страны для иностранных инвесторов и оказывают мультипликативный эффект на её позиции в международных рейтингах, таких как Организация Объединённых Наций (ООН), Организация экономического сотрудничества и развития (ОЭСР), Международный валютный фонд (МВФ), Всемирный банк, Transparency International и другие.

Проведение данной оценки позволяет казахстанскому бизнесу осуществлять упрощённый контроль трансграничных финансовых операций, что, в свою очередь, способствует повышению инвестиционной привлекательности не только Международного финансового центра «Астана» (МФЦА), но и всей страны в целом.

«Республика Казахстан продемонстрировала эффективные меры по противодействию отмыванию преступных доходов. Данный факт способствует реализации поручений Главы государства, — отметил исполняющий обязанности управляющего директора регуляторного офиса МФЦА, директор департамента по борьбе с отмыванием денег Валихан Гусманов» [18].

Касым-Жомарт Токаев в своем Послании народу Казахстана обозначил разгосударствление и создание открытой конкурентной экономики как ключевые аспекты стратегии развития страны на ближайшие годы. Президент неоднократно подчеркивал важность критериев прозрачности и открытости в проведении всех запланированных реформ.

МФЦА применяет модель риск ориентированного подхода в надзорной деятельности, разработанную на основе классических принципов управления рисками с учетом специфики бизнеса участников МФЦА. Данная модель обеспечивает эффективное распределение ресурсов для применения мер, рекомендованных ФАТФ. МФЦА систематически проводит анализ уязвимостей в сфере противодействия отмыванию денег и финансированию терроризма (ПОД/ФТ), используя разработанную риск ориентированную модель регулирования и надзора. В рамках создания эффективной системы ПОД/ФТ налажен постоянный обмен информацией с Агентством по финансовому мониторингу Республики Казахстан (АФМ РК), что способствует эффективному взаимодействию.

На этапе регистрации и авторизации (лицензирования) осуществляется проверка компаний и их собственников, анализ структуры бенефициарного владения с использованием открытых источников, международных и национальных баз данных, а также санкционных списков Казахстана и Совета Безопасности ООН. После прохождения всех необходимых процедур компании переходят под надзор кураторов финансового центра.

Таким образом, режим противодействия отмыванию денег и финансированию терроризма обеспечивается за счет многоуровневой системы надзора и контроля, основанной на оценке рисков. Данная система позволяет применять превентивные меры, повышать прозрачность и доступность информации о бенефициарной собственности юридических лиц и образований, а также обеспечивать международное сотрудничество.

В 2023 году ФАТФ включила Казахстан в список стран с повышенным риском финансовых преступлений в онлайн-гемблинге [19].

В июне 2024 года Казахстан вышел на стандартный мониторинг, успешно пройдя второй раунд взаимной оценки ФАТФ. Результаты процедуры показали, что в стране формируется эффективная государственная система, соответствующая стандартам организации [20].

АФМ РК активно работает над усилением международного присутствия страны в глобальной сети ФАТФ, в том числе в сфере современных технологий. Например, в июне 2024 года АФМ вошло в Контактную группу ФАТФ по вопросам рисков цифровых активов, что позволило Республике Казахстан предлагать решения вопросов эффективной борьбы с использованием криптовалют в противоправных целях [21].

Заключение

Республика Казахстан демонстрирует последовательную стратегию регулирования рынка криптовалют, направленную на минимизацию рисков и стимулирование его легализации. С 2020 года страна эволюционировала от полного запрета на операции с криптовалютами до внедрения комплексного законодательного регулирования в рамках Международного финансового центра «Астана» (МФЦА), которое вступило в силу в ноябре 2023 года. Закон «О цифровых активах» легализовал криптовалютные транзакции.

Республика Казахстан демонстрирует высокий уровень эффективности в реализации стратегий по борьбе с отмыванием преступных доходов. Данные меры строго соответствуют указаниям Главы государства и требованиям международных стандартов, что подтверждает высокий уровень институционального развития в данной области.

Риск-ориентированный подход Международного финансового центра «Астана» (МФЦА) способствует повышению уровня соблюдения нормативных требований (комплаенса) и минимизации рисков, связанных с финансовыми преступлениями.

Национальная система противодействия легализации доходов, полученных преступным путем, и финансированию терроризма в Республике Казахстан базируется на многоуровневом подходе, включающем процессы регистрации, авторизации и постоянного обмена информацией с Агентством по финансовому мониторингу Республики Казахстан (АФМ РК). Данная система обеспечивает комплексный и интегрированный контроль за финансовыми потоками.

Республика Казахстан активно участвует в глобальных инициативах ФАТФ, включая работу Контактной группы по вопросам рисков, связанных с цифровыми активами, что способствует укреплению международного сотрудничества и обмену передовыми практиками в области противодействия финансовым преступлениям.

В 2023 году Республика Казахстан была включена в список стран с повышенным риском в секторе онлайн-гемблинга. К июню 2024 года страна успешно прошла второй раунд взаимной оценки ФАТФ, что свидетельствует о формировании эффективной национальной системы противодействия легализации доходов, полученных преступным путем, и финансированию терроризма.

Агентство по финансовому мониторингу продолжает укреплять международное присутствие Республики Казахстан в глобальной сети ФАТФ, что способствует обмену опытом и внедрению передовых международных практик, а также повышает уровень национальной безопасности в сфере финансовых отношений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Карабеков К.О. Актуальные вопросы исследования киберпреступности в Российской Федерации и Республике Казахстан // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2022. № 22–2. С. 25–27;
2. Искакова З.Д., Рахымжанова А.А. О финансовом мониторинге и казахстанская модель финансового мониторинга // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 4. – С. 219-222;

3. Нургазиев С.Б., Карымсаков Р.Ш. О вопросах правового регулирования оперативно-розыскной деятельности, связанной с криптовалютными преступлениями // Вестник науки №12 (81) том 4. С. 808 - 818. 2024 г. ISSN 2712-8849;
4. Сериков Д. Как криптобиржи борются с киберпреступлениями: схемы и инструменты. Интервью inbusiness.kz с экспертом по кибербезопасности биржи Binance Ярек Якубчек. [Электронный ресурс] - Режим доступа: https://inbusiness.kz/ru/news/kak-kriptobirzhi-boryutsya-s-kiberprestupleniyami-shemy-iinstrumenty (дата обращения: 06.03.2025).
5. Курилов С.И., Осипов И.В. Об актуальности организации внутреннего и внешнего взаимодействия органов предварительного следствия, дознания и экспертно-криминалистических подразделений в процессе расследования преступлений с использованием криптовалют // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации: сборник научных статей по материалам международной научно-практической конференции, Москва, 21 мая 2021 года / под ред. Ю. В. Гаврилина, Ю. В. Шпагиной. Москва: Академия управления МВД России, 2021. С. 178–186;
6. Пушкарев В. В., Техеров А. Ю. Преступления с использованием криптовалюты: актуальные вопросы уголовного преследования // Алтайский юридический вестник. 2021. № 1(33). С. 122–127;
7. Фильченко А. П. Использование режима санкций и системы комплаенс в снижении рисков незаконных операций с виртуальными активами: зарубежный и российский опыт / А. П. Фильченко, В. Ю. Жандров // Правовое государство: теория и практика. – 2022. – № 3(69). – С. 171-183. – DOI 10.33184/pravgos-2022.3.25. [Электронный ресурс] - Режим доступа: https://www.elibrary.ru/item.asp?id=49750857 (дата обращения: 22.11.2025).
8. Закон Республики Казахстан от 28 августа 2009 года № 191-IV «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изменениями и дополнениями по состоянию на 01.07.2025 г.) Режим доступа: https://online.zakon.kz/Document/?doc_id=3046690815 (дата обращения 10.10.25)
9. Закон Республики Казахстан от 13 июля 1999 года № 416-I «О противодействии терроризму» (с изменениями и дополнениями по состоянию на 06.07.2025 г.) Режим доступа: https://online.zakon.kz/Document/?doc_id=1013957 (дата обращения 10.10.25)
10. Закон Республики Казахстан от 18 февраля 2005 года № 31-III «О противодействии экстремизму» (с изменениями и дополнениями по состоянию на 20.08.2024 г.) Режим доступа: https://online.zakon.kz/Document/?doc_id=30004865 (дата обращения 10.10.25)
11. Закон Республики Казахстан от 6 февраля 2023 года № 193-VII «О цифровых активах в Республике Казахстан» (с изменениями и дополнениями от 07.01.2025 г.) Режим доступа: https://online.zakon.kz/Document/?doc_id=33689356&show_di=1 (дата обращения 10.10.25)
12. Доклад: IMF-FSB Synthesis Paper: Policies for Crypto-Assets (2023). Режим доступа: https://www.fsb.org/uploads/R070923-1.pdf (дата обращения 10.10.25)
13. Доклад: Issues, Risks and Regulatory Considerations Relating to CryptoAsset Trading Platforms Consultation Report (2019). Режим доступа: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD627.pdf (дата обращения 10.10.25)
14. Финальный доклад: Policy Recommendations for Crypto and Digital Asset Markets Consultation Report (2023). Режим доступа: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf https://www.iosco.org/library/pubdocs/pdf/IOSCOPD755.pdf (дата обращения 10.10.25)
15. Доклад: Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions, Application of the Principles for Financial Market Infrastructures to stablecoin arrangements (2022). Режим доступа: https://www.bis.org/cpmi/publ/d206.pdf (дата обращения 10.10.25)

16. First Steps to Crypto Derivatives Standards (2022). Режим доступа: https://www.isda.org/2021/09/30/first-steps-to-crypto-derivatives-standards/ (дата обращения 10.10.25)
17. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2021). Режим доступа: https://www.fatfgafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets2021.html (дата обращения 10.10.25)
18. Алиев Р. О финансах – прозрачно. Режим доступа: https://kazpravda.kz/n/o-finansah-prozrachno/ (дата обращения 10.10.25)
19. FATF взяла Казахстан на мониторинг из-за высокого риска финансовых преступлений в онлайн-гемблинге. Режим доступа: https://www.sports.ru/betting/1115628899-fatf-vzyala-kazaxstan-na-monitoring-iz-za-vysokogo-riska-finansovyx-pr.html (дата обращения 10.10.25)
20. Делегация РК принимает участие в работе Пленарного заседания ФАТФ в Париже. Режим доступа: https://kzaif.kz/society/delegaciya-rk-prinimaet-uchastie-v-rabote-plenarnogo-zasedaniya-fatf-v-parizhe (дата обращения 10.10.25)
21. Делегация Казахстана принимает участие в работе Пленарного заседания ФАТФ в Париже. Режим доступа: https://www.gov.kz/memleket/entities/afm/press/news/details/870655?lang=ru (дата обращения 10.10.25)

https://doi.org/10.5281/zenodo.18523840
ӘОЖ 343.344

ҚАРУ МЕН ЖАРЫЛҒЫШ ЗАТТАРДЫҢ ЗАҢСЫЗ АЙНАЛЫМЫ ҮШІН ЖАУАПКЕРШІЛІК: ЗАҢНАМАДАҒЫ ОЛҚЫЛЫҚТАР

ЕРМУХАМЕДОВ АЛИБИ БОЛАТОВИЧ
М.Әуезов атындағы Оңтүстік Қазақстан зерттеу университетінің заң факультетінің 2 курс студенті.

Ғылыми жетекші- PHD доктор, профессор **ЖАНИБЕКОВ АҚЫНҚОЖА ҚАЛЕНОВИЧ**
Шымкент қаласы, Қазақстан Республикасы

Аңдатпа: *Қару-жарақ пен жарылғыш заттардың заңсыз айналымы зорлық-зомбылықтың, ұйымдасқан қылмыстық құрылымдардың және террористік белсенділіктің өсуіне ықпал ете отырып, қоғамдық қауіпсіздік пен мемлекеттің тұрақты дамуына елеулі қауіп төндіреді. Осы қылмыстардың алдын алуға және жолын кесуге бағытталған қылмыстық-құқықтық нормалардың болуына қарамастан, құқық қолдану практикасы қылмыстық-құқықтық қарсы іс-қимылдың тиімділігіне теріс әсер ететін заңнамадағы бірқатар олқылықтар мен қайшылықтарды анықтайды.*

Мақалада қару-жарақ пен жарылғыш заттардың заңсыз айналымы үшін жауапкершілікті құқықтық реттеудің өзекті мәселелері қарастырылады, тұжырымдамалық аппараттың кемшіліктері, қылмыстардың аралас құрамдарын ажырату мәселелері және тиісті әрекеттердің біліктілік ерекшеліктері талданады. Қылмыстық жазалардың пропорционалдылығы және қылмыс құрамының жекелеген элементтерін дәлелдеудің күрделілігі мәселелеріне ерекше назар аударылады.

Зерттеу нәтижелері бойынша құқықтық сенімділік деңгейін арттыруға, сот практикасының біркелкілігін қамтамасыз етуге және қылмыстық жауаптылықтың алдын алу әлеуетін күшейтуге бағытталған қылмыстық заңнаманы және құқық қолдану практикасын жетілдіру бағыттары ұсынылады.

Кілт сөздер: *қару-жарақтың заңсыз айналымы, жарылғыш заттар, қылмыстық жауапкершілік, заңнамадағы олқылықтар, қоғамдық қауіпсіздік, қылмыстардың біліктілігі.*

Кіріспе

Жаһандану және трансұлттық қылмыстың өсуі жағдайында қару-жарақ пен жарылғыш заттардың заңсыз айналымы мәселесі ерекше өзекті болып отыр. Қаруды заңсыз тарату мемлекеттің тұрақтылығы мен азаматтардың өміріне қауіп төндіре отырып, зорлық-зомбылық қылмыстарының, террористік актілердің және қоғамдық қауіпсіздікке өзге де қол сұғушылықтардың деңгейін арттыруға ықпал етеді. Қазіргі әлемде қарудың заңсыз айналымы трансшекаралық сипатқа ие, бұл оны анықтау мен жолын кесу процестерін қиындатады.

Қазақстан Республикасы үшін, басқа мемлекеттер сияқты, осы қатерлерге қарсы іс-қимыл Ұлттық қауіпсіздік пен құқықтық тәртіпті қамтамасыз етуге бағытталған қылмыстық саясаттың аса маңызды міндеті болып табылады. Мемлекет нормативтік-құқықтық базаны жетілдіру және құқық қорғау органдарының қызметін күшейту жөнінде шаралар қабылдайды, алайда қолданыстағы тәжірибе осы қылмыстарға тиімді қарсы тұру үшін қабылданып жатқан шаралардың жеткіліксіз екендігін айғақтайды.

Қару мен жарылғыш заттардың заңсыз айналымы үшін жауапкершілікті белгілейтін қылмыстық-құқықтық нормалардың болуына қарамастан, оларды қолдану практикасы заңнамада елеулі олқылықтар мен қайшылықтардың бар екендігін айғақтайды. Бұл олқылықтар терминологияның екіұштылығынан, қылмыстардың құрамын ажыратудың нақты

критерийлерінің болмауынан, сондай-ақ іс-әрекеттің сипаты мен қоғамдық қауіптілік дәрежесіне байланысты қылмыстық жауапкершілікті саралаудың жеткіліксіздігінен көрінеді.

Сонымен қатар, қылмыстарды саралау және субъективті жағын дәлелдеу, атап айтқанда адамның ниетін және оның қару-жарақ пен жарылғыш заттарды иеленудің заңсыздығы туралы хабардарлығын анықтау кезінде қиындықтар туындайды. Бұл жағдайлар сот практикасының біркелкілігіне және қылмыстық қудалаудың тиімділігіне теріс әсер етеді.

Осы баптың мақсаты қару мен жарылғыш заттардың заңсыз айналымы үшін жауапкершілікті құқықтық реттеудің негізгі проблемаларын анықтау, заңнаманың бар олқылықтарын талдау, сондай-ақ қылмыстық заңнаманы және оны қолдану практикасын жетілдіру бойынша теориялық негізделген және іс жүзінде маңызды ұсыныстарды тұжырымдау болып табылады.

Қару мен жарылғыш заттардың заңсыз айналымының түсінігі мен құқықтық сипаттамасы.

Қару мен жарылғыш заттардың заңсыз айналымы заңнамада белгіленген тиісті рұқсатсыз қаруды, оқ-дәрілерді және жарылғыш заттарды дайындауға, қайта жасауға, сатып алуға, сақтауға, тасымалдауға, алып жүруге, беруге, өткізуге және пайдалануға байланысты құқыққа қайшы әрекеттердің жиынтығын қамтиды. Бұл әрекеттер қоғамдық қауіпсіздікке қол сұғады және азаматтардың өмірі мен денсаулығына үлкен қауіп төндіреді.

Қару-жарақ пен жарылғыш заттардың заңсыз айналымының ерекшелігі оның жаппай зиян келтіру мүмкіндігіне байланысты қоғамдық қауіптілігінің артуы болып табылады. Қоғамдық тәртіпке қарсы басқа қылмыстардан айырмашылығы, бұл әрекеттер ауыр және қайтымсыз салдарға әкелуі мүмкін, бұл оларды қатаң қылмыстық-құқықтық реттеу қажеттілігін тудырады.

Негізгі проблемалардың бірі-қылмыстық заңнамада "қару", "оқ-дәрі", "жарылғыш заттар" және "жарылғыш құрылғылар" ұғымдарының бірыңғай және нақты анықтамаларының болмауы. Кейбір жағдайларда бұл санаттар заңға тәуелді нормативтік құқықтық актілерде, ведомстволық нұсқаулықтарда және техникалық регламенттерде ашылады, бұл құқықтық сенімділік деңгейін төмендетеді және заңдылық принципіне қайшы келеді.

Тұжырымдамалық аппараттың түсініксіздігі сол әрекеттерді біліктілікте әртүрлі тәсілдерге әкеледі. Сонымен, іс жүзінде жекелеген заттарды атыс қаруына немесе конструктивті ұқсас өнімдерге жатқызу, сондай-ақ жарылғыш заттар мен жарылғыш құрылғыларды ажырату кезінде қиындықтар туындайды. Бұл сот практикасының біркелкілігіне теріс әсер етеді және орындаудағы қателіктер үшін алғышарттар жасайды.

Біліктілік мәселелері және қылмыстық заңнамадағы олқылықтар.

Қылмыстық заңнаманың Елеулі олқылығы қару мен жарылғыш заттардың заңсыз айналымының әртүрлі нысандары үшін қылмыстық жауаптылықты жеткіліксіз саралау болып табылады. Заң шығарушы бұл әрекеттердің қоғамдық қауіптілігінің әртүрлі дәрежесіне және олардың ықтимал салдарына қарамастан, қаруды сақтау, тасымалдау және өткізу үшін ұқсас санкцияларды жиі белгілейді.

Қару-жарақтың заңсыз айналымын және терроризм, бандитизм және экстремистік әрекеттер сияқты қылмыстардың аралас құрамдарын ажырату әсіресе проблемалы болып табылады. Осы құрамдар арасындағы айырмашылықтың нақты критерийлерінің болмауы объективті белгілері бойынша бірдей әрекеттер құқық қолданушының субъективті қалауына байланысты әртүрлі қылмыстық-құқықтық баға алатын жағдайға әкеледі.

Адамдар тобы немесе ұйымдасқан қылмыстық құрылымдар құрамында жасалған қылмыстарды саралау кезінде қосымша қиындықтар туындайды. Заңнама әрдайым әр қатысушының рөлін барабар ескеруге мүмкіндік бермейді, бұл қылмыстық жауапкершілікті даралау принципіне теріс әсер етеді.

Қылмыстың субъективті жағын дәлелдеу мәселесі ерекше назар аударуға тұрарлық. Тікелей немесе жанама ниетті, адамның қаруды немесе жарылғыш заттарды иеленудің заңсыздығы туралы хабардарлығын, сондай-ақ олардың шығу көзін анықтау сотқа дейінгі

тергеу барысында айтарлықтай қиындықтар туғызады. Бұл қылмыс тақырыбының ерекшелігіне де, осы әрекеттерді тергеу әдістерінің жеткіліксіз дамуына да байланысты.

Заңнаманы және құқық қолдану практикасын жетілдіру бағыттары.

Қару мен жарылғыш заттардың заңсыз айналымына қарсы іс-қимылдың тиімділігін арттыру мақсатында негізгі дефинцияларды тікелей Қылмыстық кодексте бекіте отырып, қылмыстық заңнаманың ұғымдық аппаратын нақтылау орынды болып көрінеді. Бұл құқық қолданудың біркелкілігін қамтамасыз етуге және құқықтық сенімділік деңгейін арттыруға мүмкіндік береді.

Сондай-ақ, іс-әрекеттің сипаты мен қоғамдық қауіптілік дәрежесін, кінә нысанын, қылмыс жасаудағы адамның рөлін және туындаған салдарларды ескере отырып, қылмыстық жауапкершілікті неғұрлым нақты саралау қажет. Санкцияларды саралау әділеттілік, гуманизм және жазаны даралау принциптерін жүзеге асыруға ықпал етеді.

Құқық қорғау органдары мен соттар үшін қылмыстарды саралау практикасын біріздендіруге, дәлелдемелерді бағалауға және қылмыс құрамының субъективті жағын анықтауға бағытталған әдістемелік ұсыныстарды дамыту және енгізу жетілдірудің маңызды бағыты болып табылады. Қару мен жарылғыш заттардың заңсыз айналымына байланысты қылмыстарды тергеу бөлігінде тергеушілер мен судьялардың кәсіби даярлық деңгейін арттыру ерекше маңызға ие.

Аталған шараларды іске асыру осы қылмыстарға қылмыстық-құқықтық қарсы іс-қимылдың тиімділігін арттыруға және қоғамдық қауіпсіздікті қамтамасыз ету жүйесін нығайтуға мүмкіндік береді.

Қорытынды

Қару мен жарылғыш заттардың заңсыз айналымы мемлекет тарапынан жүйелі және тиімді қылмыстық-құқықтық ден қоюды талап ететін қылмыстық қызметтің аса қауіпті нысандарының бірі болып табылады. Бұл қылмыстар қоғамдық қауіпсіздік негіздеріне қол сұғады, азаматтардың өмірі мен денсаулығына қауіп төндіреді, сондай-ақ терроризм мен ұйымдасқан қылмысты қоса алғанда, өзге де ауыр және аса ауыр қылмыстардың дамуына ықпал етеді.

Қылмыстық заңнама мен құқық қолдану практикасына жүргізілген талдау қару мен жарылғыш заттардың заңсыз айналымына қарсы күрестің тиімділігін төмендететін елеулі олқылықтар мен қайшылықтардың бар екендігін айғақтайды. Мұндай проблемалардың қатарына тұжырымдамалық аппараттың белгісіздігі, қылмыстарды саралаудың қиындығы, қылмыстық жауапкершіліктің жеткіліксіз сараланuы, сондай-ақ қылмыс құрамының субъективті жағын дәлелдеу қиындықтары жатады.

Анықталған кемшіліктерді құқықтық анықтамаларды нақтылау, негізгі ұғымдарды тікелей қылмыстық заңнамада бекіту, әрекеттердің қоғамдық қауіптілік дәрежесін және олардың салдарын ескере отырып, қылмыстық жауаптылықты саралау, сондай-ақ құқық қолдану практикасын жетілдіру жолымен жою осы қылмыстарға қылмыстық-құқықтық қарсы іс-қимылдың тиімділігін арттыруға ықпал ететін болады.

Бұдан басқа, бірыңғай сот практикасын дамыту және құқық қорғау органдары қызметкерлерінің кәсіби даярлық деңгейін арттыру маңызды мәнге ие, бұл біліктіліктегі қателіктерді барынша азайтуға мүмкіндік береді және заңдылық, әділдік және жазаны дараландыру қағидаттарын іске асыруды қамтамасыз етеді.

Жалпы, қылмыстық заңнаманы және оны іске асыру тетіктерін кешенді жетілдіру қоғамдық қауіпсіздікті нығайтудың және азаматтардың құқықтық қорғалу деңгейін арттырудың, сондай-ақ қазіргі жағдайда қару мен жарылғыш заттардың заңсыз айналымына қарсы тұрудың тұрақты жүйесін қалыптастырудың қажетті шарты болып табылады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Қазақстан Республикасының Конституциясы.
2. Қазақстан Республикасының Қылмыстық кодексі.
3. Қазақстан Республикасының Қылмыстық кодексіне түсініктеме / ред.К. А. Мами. - Астана, 2023.
4. Наумов А. В. қылмыстық 4.құқық. Жалпы бөлім. — М.: Норма, 2022.
5. Лопашенко н. А. қоғамдық қауіпсіздікке қарсы қылмыстар. - М.: Юрайт, 2021.
6. Кудрявцев в. н. қылмыстарды саралау мәселелері. — М.: Жарғы, 2020.

https://doi.org/10.5281/zenodo.18523862
УДК 342.951 / 340.5

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МОЛДАБАЕВА АЛЬБИНА АБАЕВНА
студент 1 курса магистратуры Тюменского государственного университета

Научный руководитель – к.ю.н, доцент **МОРОЗОВ В.И.**
Тюмень, Россия

Аннотация: *В статье анализируется сущность информационной безопасности, раскрывается её содержание и основные направления укрепления, а также исследуются ключевые вопросы, связанные с обеспечением информационной безопасности. Особое внимание уделяется мерам по её обеспечению, которые должны применяться с соблюдением прав и свобод человека и быть соразмерными существующим угрозам и возможным последствиям их реализации.*

Ключевые слова: *информационная безопасность, кибербезопасность, защита, риски, компьютерные сети, интернет, киберпреступность.*

Новые технологии и электронные услуги прочно вошли в повседневную жизнь современного общества. По мере того как возрастает зависимость от информационно-коммуникационных технологий, обеспечение их защиты и доступности приобретает критическое значение и становится важным элементом национальных интересов. В современных условиях кибербезопасность выступает необходимым условием развития информационного общества, охватывая широкий спектр вопросов безопасности и способов их решения — от технических механизмов защиты до правового и законодательного регулирования.

Проблема кибербезопасности является сравнительно новой и напрямую связана с появлением во второй половине XX века средств вычислительной техники, компьютерных сетей и современных средств связи [1, 10 с.].

На сегодняшний день данная проблема относится к числу наиболее актуальных в современном мире. Вместе с тем представляется необходимым разграничить понятия кибербезопасности и информационной безопасности, которые находятся в тесной взаимосвязи. При этом кибербезопасность следует рассматривать как составную часть, то есть подмножество, информационной безопасности.

Информационная безопасность по своей сути означает защиту данных и направлена на обеспечение их сохранности независимо от формы представления. Её ключевая задача заключается в предотвращении утраты, искажения и несанкционированного доступа к информации. Кибербезопасность, в свою очередь, представляет собой совокупность технологий, методов и процессов, обеспечивающих защиту программного обеспечения, сетевой инфраструктуры и данных от кибератак, то есть цифровых угроз.

Соблюдение базовых требований информационной безопасности позволяет обеспечить целостность и конфиденциальность цифровых данных, полностью исключая либо существенно ограничивая несанкционированный доступ к ним. Несмотря на значительное количество научных исследований, посвящённых феноменам информации и управления, в которых отражены различные подходы к их сущности и взаимосвязи, вопросы соотношения понятий «информационная безопасность», «защита информации», «кибербезопасность» и «киберзащита» остаются недостаточно разработанными. Особенно это касается исследований в контексте законодательства Республики Казахстан, что, в свою очередь, порождает определённые трудности в правовом регулировании общественных отношений, связанных с использованием информации и киберпространства [2, 17 с.].

В национальном законодательстве Республики Казахстан отсутствуют определения понятий «кибербезопасность» и «киберзащита». В действующих правовых актах используются лишь термины «информационная безопасность» и «защита информации». В частности, пункт 29 статьи 1 Закона Республики Казахстан «Об информатизации» содержит определение «защиты электронных информационных ресурсов», которое по своему содержанию соответствует понятию «защита информации» и трактуется как комплекс правовых, организационных и технических мероприятий, направленных на сохранность электронных информационных ресурсов и информационных систем, а также на предотвращение неправомерного доступа к ним, включая незаконные действия по получению, копированию, распространению, искажению, уничтожению или блокированию информации [3]. Что касается определения понятия «информационная безопасность», то в пункте 2 статьи 1 Закона «О национальной безопасности Республики Казахстан» «информационная безопасность – состояние защищенности государственных информационных ресурсов, а также прав личности и интересов общества в информационной сфере».

Закон РК «Об информатизации» не содержит как такового определения термина «информационная безопасность», но в пункте 11 статьи 1 данного Закона содержится отсылка к национальному оператору в сфере информатизации, которое представляет собой «юридическое лицо, созданное по решению Правительства Республики Казахстан, на которое собственником в лице государства возложены задачи по интеграции и обеспечению безопасности государственных информационных систем и государственных электронных информационных ресурсов».

В последние годы в Республике Казахстан проведён комплекс мероприятий по совершенствованию системы обеспечения информационной безопасности государства. В рамках Стратегии национальной безопасности была разработана и принята Концепция информационной безопасности, предусматривающая реализацию комплекса правовых, организационных и научно-технических мер, направленных на прогнозирование, выявление, предупреждение и пресечение угроз в сфере информационной безопасности. Современные тенденции информатизации всех сфер государственной и общественной жизни свидетельствуют о том, что существование независимого государства невозможно без обеспечения информационной безопасности всех звеньев государственных структур.

Анализ международного опыта показывает, что в последние годы произошло существенное качественное изменение в управлении на всех уровнях — от межгосударственных объединений до отдельных организаций, включая банки и коммерческие структуры [4, 105 с.]. Одновременно с этим усилилась опасность несанкционированного вмешательства в работу информационных систем с целью получения конфиденциальной информации и нарушения их функционирования. В этих условиях необходимы адекватные меры по предотвращению подобных последствий. Эффективное противодействие информационным угрозам возможно лишь при наличии хорошо организованной государственной системы обеспечения информационной безопасности, функционирующей на основе полного взаимодействия всех государственных органов, негосударственных структур и граждан Республики Казахстан.

Так за прошедший в 2023-2024 годы было отражено 2,2 млрд различных кибератак координационным центром информбезопасности. В настоящее время реализуется второй этап проекта «киберщит», который подразумевает запуск всей защитной инфраструктуры [5]. Где Первым этапом была подготовка нормативно-правовой базы и приобретение оборудования. Данная Концепция разработана в соответствии с Посланием Первого Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность» с учетом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30-ти самых развитых государств мира. Целью данной Концепции является достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от

внешних и внутренних угроз, обеспечивающего устойчивое развитие Казахстана в условиях глобальной конкуренции.

Согласно карте национальных обязательств по кибербезопасности Казахстан относится к категории стран со средней оценкой, которые разработали комплексные обязательства и участвуют в программах и инициативах по кибербезопасности. В настоящее время в республике имеется 336 критически важных объектов, включающих госорганы, промышленные предприятия, банки и другие крупные организации, атаки на которые могут иметь страновой или межгосударственный эффект. Еще в сентябре в этот список входило 219 объектов. Пополнение списка продолжается.

Во многих странах мира в целях пресечения факта информационного преступления в последние годы специалисты по компьютерной безопасности начали сотрудничество с психологами, которые составляют профиль так называемого хакера, то есть преступника в сфере компьютерной информации и техники, который позволяет выявить уровень его квалификации и технической подготовки. Но следует отметить, что хотя компьютерные специалисты и могут многое сказать о хакере и о методах его работы, но они никогда не смогут понять психологию его криминального мышления. Подобными вопросами занимаются клинические психологи, судебные эксперты и другие специалисты совместно с органами внутренних дел. Подобная практика активно используется в США, Европе и других странах, где киберпреступления широко развиваются. Некоторые ученые считают, что налаживание подобной практики и в нашей стране, где преступления в сфере информационных технологий пока неразвиты, позволит еще в зачаточной форме уничтожить основы киберпреступности [5]. Для этого необходимо активизировать потребность международного сотрудничества.

Но ввиду того, что в современных условиях значительная часть средств борьбы с киберпреступлениями, как и с другими преступлениями международного характера, принадлежит к внутренней компетенции каждого отдельного государства, необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласовывая его с международными нормами права и опираясь на существующий позитивный опыт.

В мире есть примеры достаточно эффективных систем противодействия совершению киберпреступлений. В настоящее время ведущие страны мира активно расширяют и создают в вооруженных силах и спецслужбах подразделения, которые должны обеспечивать развитие наступательных возможностей в киберпространстве. Например в Великобритании создана Группа безопасности электронной коммуникации при центре правовой связи при МИД, а также подразделение Министерства обороны по защите от виртуальных угроз; Индии был создан Аналитический и исследовательский отделы внешней разведки и разведывательное бюро внутренней разведки; в России : Управление «К» МВД и отделы «К» региональных управлений МВД.

Мировое сообщество активно участвует в формировании единого и безопасного информационного пространства, а также в противодействии одной из ключевых угроз международной информационной безопасности. В этой связи можно выделить пять групп международных и региональных документов, разработанных в рамках или под эгидой различных организаций: Совета Европы и Европейского союза, Содружества Независимых Государств и Шанхайской организации сотрудничества, межправительственных африканских структур, Лиги арабских государств, а также Организации Объединённых Наций. Эти документы взаимно дополняют друг друга, в том числе в части концептуальных подходов и положений, заложенных в Конвенции Совета Европы о компьютерных преступлениях.

Эффективная борьба с киберпреступностью требует тщательного анализа специфики факторов, способствующих её распространению. В целом преступные проявления имеют общий причинный комплекс, который формируется на фоне глубоких и острых деформаций в обществе на всех уровнях — от глобального до индивидуально-личностного. В основе этих деформаций лежат явления, которые, во-первых, отражают несправедливость социального

устройства и создают условия для произвола одних субъектов в ущерб другим; во-вторых, ограничивают права и свободы граждан; в-третьих, способствуют дегуманизации и снижению социального статуса и морального состояния части населения.

В то же время на сегодняшний день не существует универсального рецепта или единой стратегии, позволяющей полностью устранить риски кибератак. Государства мира продолжают разрабатывать и совершенствовать стандарты кибербезопасности, адаптируя их к меняющимся угрозам и реалиям цифровой среды.

Важным начальным шагом в снижении рисков кибератак является создание специализированного подразделения по управлению информационными рисками, задачей которого является оценка уровня киберрисков, с которыми может столкнуться организация, а также разработка политики их предотвращения и минимизации. Организация должна обеспечивать защиту информации и используемых информационных технологий, внедряя современные меры кибербезопасности и руководствуясь принципами корректной конфигурации и эксплуатации информационных систем. Сетевая инфраструктура любой организации нередко является наиболее уязвимым звеном в системе защиты, поэтому крайне важно правильно проектировать сеть и обеспечивать корректную настройку сетевых устройств в соответствии с принятыми стандартами безопасности.

Пользователю следует предоставлять только те привилегии, которые необходимы для выполнения его служебных обязанностей. Учетная запись системного администратора не должна быть доступна обычным пользователям. При этом необходимо обеспечивать контроль и мониторинг активности пользователей.

Исследуя проблему киберпреступности в современном мире, важно опираться на действующее законодательство и достижения современных исследователей для определения направлений правового и социального регулирования интернет-отношений с целью снижения уровня киберпреступности. К таким направлениям можно отнести защиту персональных данных и частной жизни в сети, регулирование электронной коммерции и других видов сделок с обеспечением их безопасности, защиту интеллектуальной собственности, противодействие распространению противоправного контента и незаконному поведению в интернете, правовое регулирование электронных сообщений, а также обеспечение личной безопасности каждого пользователя через соблюдение базовых мер информационной безопасности и т.д.

В заключение следует отметить, что кибербезопасность в современном мире имеет первостепенное значение. С момента появления компьютерных сетей они подвергаются атакам со стороны злоумышленников, и по мере расширения сетевой инфраструктуры угроза кибератак будет продолжать расти. Вместе с тем при наличии должного уровня подготовки специалистов и соответствующего технического оснащения возможно эффективно контролировать последствия атак, а также минимизировать и восстанавливать нанесённый ущерб.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Актуальные проблемы информационного права: учебник / Под ред. И. Л. Бачило, М. А. Лапина. – Москва: Юстиция, 2016. – 532 с.
2. Ахметов Е. «Киберпреступность в Казахстане» // Журнал «Законность и правовая статистика» 2019. - № 2 (11). – С. 15-20.
3. Закон Республики Казахстан «Об информатизации» от 24.11.2015 № 418-V. // Әділет. — Электронный ресурс. Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 05.01.2026)
4. Information Security: Global Trends and National Responses / Ed. A. Ivanov. — Almaty, 2023. — 212 p.
5. Кибербезопасность – хороший ресурс // http://www.goodnewsfinland.ru/arhiv/mesyaca/c703aa4e/c87e38d0/

https://doi.org/10.5281/zenodo.18523875
УДК 342.533

ПОЛНОМОЧИЯ ОДНОПАЛАТНЫХ ПАРЛАМЕНТОВ В КОНТЕКСТЕ РАЗДЕЛЕНИЯ ВЛАСТЕЙ (СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ)

САРТАЕВА НАТАЛЬЯ АБАЕВНА
главный научный сотрудник Отдела конституционного и административного законодательства
Института законодательства и правовой информации
Республики Казахстан,
доктор юридических наук, доцент
г.Астана, Республика Казахстан

Аннотация: *Работа над настоящей статьей проводилась в рамках фундаментального и прикладного научного исследования «Пределы конституционного правосудия в контексте конституционного принципа разделения властей» (данное исследование проводится в текущем году Отделом конституционного и административного законодательства Института законодательства и правовой информации Республики Казахстан).*

В статье проводится сравнительно-правовой анализ законодательства государств с однопалатными парламентами, таких как: Азербайджанская Республика, Кыргызская Республика, Литовская Республика и Туркменистан.

По результатам анализа сделан вывод о том, что общими для однопалатных парламентов являются полномочия, которые регулируют такие сферы общественных отношений как: законодательная, финансовая; международные отношения; назначения (освобождения) высших должностных лиц либо участие в таком назначении (освобождении); обороны и безопасности; амнистии; государственных наград, а также парламентский контроль.

Ключевые слова: *парламент, парламентское право, полномочия (компетенции).*

В юридической литературе различают три способа законодательного регулирования компетенций парламентов. Первый способ – абсолютное определение компетенции, когда в конституциях устанавливается точный перечень вопросов, являющихся объектом деятельности парламента. Такие парламенты не имеют права переступать границы своих полномочий. Второй способ предусматривает абсолютно неопределенные компетенции. В этом случае парламенты юридически располагают неограниченными полномочиями и имеют право издавать законы по любому вопросу. И третий способ характеризуется относительно определенной компетенцией, когда у парламентов относительная подвижность правовых границ, в пределах которых они осуществляют свои властные полномочия.

В рамках заявленной тематики научный интерес представляет зарубежный опыт законодательного регулирования полномочий однопалатных парламентов. Так, статья 94 Конституции Азербайджанской Республики [1] предусматривает, что Милли Меджлис устанавливает общие правила по следующим вопросам: пользования правами и свободами человека и гражданина, закрепленными в Конституции, государственных гарантий этих прав и свобод; выборов Президента Азербайджанской Республики, выборов в Милли Меджлис Азербайджанской Республики и статуса его депутатов; референдума; судоустройства и статуса судей; прокуратуры; адвокатуры и нотариата; судопроизводства, исполнения судебных решений; выборов в муниципалитеты и статуса муниципалитетов; режима чрезвычайного положения; военного положения; государственных наград; статуса физических и юридических лиц; объектов гражданского права; сделок, гражданско-правовых

договоров, представительства и наследования; прав собственности, в том числе правового режима государственной, частной и муниципальной собственности, прав интеллектуальной собственности; других вещных прав; обязательственного права; семейных отношений, в том числе попечительства и опеки; основ финансовой деятельности, налогов, пошлин и сборов; трудовых отношений и социального обеспечения; определения преступлений и иных правонарушений; установления ответственности за их совершение; обороны и воинской службы; государственной службы; основ безопасности; территориального устройства, режима государственной границы; ратификации и денонсации международных договоров; связи и транспорта; статистики, метрологии и стандартов; таможенного дела; торгового дела и биржевой деятельности; банковского дела, бухгалтерии и страхования.

Статья 80 Конституции Кыргызской Республики [2] устанавливает, что Жогорку Кенеш: вносит изменения и дополнения в Конституцию в порядке, установленном Конституцией; принимает законы и дает их официальное толкование; ратифицирует и денонсирует международные договоры в порядке, определяемом законом; решает вопросы об изменении государственных границ Кыргызской Республики; дает согласие на назначение Председателя Кабинета Министров, его заместителей и членов Кабинета Министров; утверждает республиканский бюджет; заслушивает ежегодный отчет Кабинета Министров об исполнении республиканского бюджета; рассматривает вопросы административно-территориального устройства Кыргызской Республики; издает акты об амнистии. Также Жогорку Кенеш: назначает выборы Президента; вносит Президенту предложения о проведении референдума в порядке, предусмотренном Конституцией; на основании предложения Совета по делам правосудия по представлению Президента не менее половиной голосов от общего числа депутатов Жогорку Кенеша избирает судей Верховного суда и Конституционного суда; в случаях, предусмотренных Конституцией и конституционным законом, освобождает их от должности по представлению Президента; не менее половиной голосов от общего числа депутатов Жогорку Кенеша дает согласие представленным Президентом кандидатам на назначение председателей Конституционного суда и Верховного суда из числа их судей сроком на 5 лет; дает согласие на освобождение от должности председателей Конституционного суда и Верховного суда по представлению Президента на основании предложения Совета судей в случаях, предусмотренных конституционным законом; утверждает состав Совета по делам правосудия в порядке, предусмотренном конституционным законом; избирает:

- по представлению Президента председателя Национального банка; освобождает его от должности в случаях, предусмотренных законом;
- членов Центральной комиссии по выборам и проведению референдумов: одну половину - по представлению Президента, другую половину - по собственной инициативе и освобождает их в случаях, предусмотренных законом;
-членов Счетной палаты: одну треть состава - по представлению Президента, две трети - по собственной инициативе; освобождает их от должности в случаях, предусмотренных законом;
- в случаях, предусмотренных законом, освобождает от должности Акыйкатчы (Омбудсмена); дает согласие на привлечение его к уголовной ответственности, а также освобождает от должности по представлению Акыйкатчы (Омбудсмена) его заместителей, дает согласие на привлечение их к уголовной ответственности.

Кроме того, по представлению Президента Жогорку Кенеш дает согласие на назначение, освобождение и привлечение к уголовной ответственности Генерального прокурора не менее чем половиной голосов от общего числа депутатов Жогорку Кенеша; одобряет большинством не менее двух третей голосов от общего числа депутатов Жогорку Кенеша инициативу одной трети от общего числа депутатов Жогорку Кенеша об освобождении от должности Генерального прокурора в случаях, предусмотренных законом; вводит чрезвычайное положение в порядке и случаях, предусмотренных конституционным законом; утверждает или

отменяет указы Президента по этому вопросу; решает вопросы войны и мира, введения военного положения, объявления состояния войны; утверждает или отменяет указы Президента по этим вопросам, решает вопрос о возможности использования Вооруженных Сил Кыргызской Республики за ее пределами при необходимости выполнения межгосударственных договорных обязательств по поддержанию мира и безопасности; устанавливает воинские звания, дипломатические ранги и иные специальные звания Кыргызской Республики; учреждает государственные награды, государственные премии и почетные звания Кыргызской Республики; заслушивает ежегодные: послания, информацию Президента и выступления представителей иностранных государств, международных организаций; доклады Акыйкатчы (Омбудсмена) и председателя Центральной комиссии по выборам и проведению референдумов; отчеты Генерального прокурора, председателей Национального банка, Счетной палаты.

Сейм, согласно статье 67 Конституции Литовской Республики [3], обсуждает и принимает поправки в Конституцию; издает законы; принимает постановления относительно референдумов; назначает выборы Президента Литовской Республики; учреждает предусмотренные законом государственные институты, а также назначает и освобождает их руководителей; одобряет или не одобряет кандидатуру Премьер министра, представляемую Президентом Республики; рассматривает представленную Премьер министром программу Правительства и принимает решение относительно ее одобрения; по предложению Правительства образует или упразняет министерства Литовской Республики; осуществляет контроль за деятельностью Правительства, может выражать недоверие Премьер министр или министру; назначает судей Конституционного Суда, судей Верховного Суда, председателей судов, а также выборы Советов самоуправлений; назначает и освобождает государственного контролера, председателя Банка Литвы; образует Главную избирательную комиссию и вносит изменения в ее состав; утверждает государственный бюджет и осуществляет контроль за его исполнением; устанавливает государственные налоги и другие обязательные платежи; ратифицирует и денонсирует международные договора Литовской Республики, рассматривает другие вопросы внешней политики; устанавливает административное деление Республики; учреждает государственные награды Литовской Республики; издает акты об амнистии; вводит прямое правление, военное и чрезвычайное положение, объявляет мобилизацию и принимает решение об использовании вооруженных сил.

Конституция Туркменистана, в соответствии со статьей 67 [4], к ведению Меджлиса относит: принятие и изменение Конституции и законов, их толкование; назначение выборов Президента, Меджлиса, халк векиллери; образование Центральной комиссии по выборам и проведению референдумов; одобрение программы деятельности Кабинета министров, выражение ему недоверия; одобрение или отклонение кандидатов на должность Председателя Верховного суда, Председателя Высшего хозяйственного суда, Генерального прокурора, а также представлений об их освобождении; утверждение бюджета Туркменистана и отчета о его исполнении; учреждение государственных наград, награждение государственными наградами Президента, присвоение ему почетных званий, воинских званий и отличий; определение соответствия Конституции и законам нормативных актов органов государственной власти и управления; иные вопросы, отнесенные к полномочиям Меджлиса Конституцией и законами.

Таким образом, полномочия рассматриваемых парламентов закреплены абсолютно определенным способом, т.е. Конституция устанавливает исчерпывающий перечень полномочий (*Милли Меджлис Азербайджанской Республики, Жогорку Кенеш Кыргызской Республики, Сейм Литовской Республики)* либо относительно определенным способом, когда полномочия предусматривается не только в Конституции, но и в других законах *(Меджлис Туркменистана)*.

Также на основе проведенного анализа общими для однопалатных парламентов являются полномочия, которые регулируют такие сферы общественных отношений, как:

-законодательная, заключающаяся в том, что парламент единственный орган, в чью компетенцию входит внесение изменений в Конституцию, принятие законов и их толкование (*МеджлисТуркменистана, Жогорку Кенеш Кыргызской Республики);*

-финансовая - наличие полномочий по установлению налогов и других обязательных платежей;

-международные отношения, так как в полномочия парламента входит ратификация и денонсация международных договоров;

-назначения (освобождения) высших должностных лиц либо участие в таком назначении (освобождении);

-обороны и безопасности, поскольку парламенты имеют право объявлять войну и заключать мир, решать вопрос о вхождении страны в военные союзы, определяет условия призыва на военную службу; устанавливать военное или чрезвычайное положение;

-амнистии;

-государственных наград;

-парламентский контроль, который включает в себя утверждение государственного бюджета, заслушивание отчета Правительства, высших должностных лиц и другие.

Полагаем, что в контексте проводимой парламентской реформы при обсуждении полномочий Курултая целесообразно учесть зарубежный опыт законодательного регулирования полномочий однопалатных парламентов.

СПИСОК ЛИТЕРАТУРЫ

1. https://president.az/ru/pages/view/azerbaijan/constitution. Дата обращения 13 января 2026 года.
2. https://cbd.minjust.gov.kg/1-2/edition/1202952/ru. Дата обращения 15 января 2026 года.
3. https://www.lrs.lt/home/Konstitucija/Konstitucija_RU.htm. Дата обращения 18 января 2026 года.
4. https://saylav.gov.tm/ru/law?id=2. Дата обращения 20 января 2026 года.

https://doi.org/10.5281/zenodo.18523895
УДК 343.98:343.343.6

СОДЕРЖАНИЕ И СТРУКТУРА КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ТОРГОВЛИ ЛЮДЬМИ

НАЗАРОВ ТИМУР АМАНКОСОВИЧ
Магистрант Атырауского университета им. Х. Досмухамедова, Атырау, Казахстан

Научный руководитель – **ШАЯХМЕТОВА ЖАННА БЕКБОЛОВНА,** к.ю.н., ассоциированный профессор, Атырау, Казахстан

Аннотация. *В статье рассматривается торговля людьми как одна из наиболее опасных форм транснациональной организованной преступности и анализируются криминалистические особенности данного вида преступной деятельности. Обосновывается социальная опасность торговли людьми, раскрываются ее экономические и криминологические предпосылки, а также международно-правовые основы противодействия. Особое внимание уделяется понятию и структуре криминалистической характеристики торговли людьми как обязательного элемента частной методики расследования. Анализируются обстановка, способы совершения и сокрытия преступления, механизм торговли людьми, особенности маршрутов перемещения жертв, виды эксплуатации, а также личностные характеристики потерпевших и преступников. Рассматриваются типовые стадии совершения торговли людьми и источники следовой информации. В заключение формулируются выводы о структуре криминалистической характеристики торговли людьми и системе обстоятельств, подлежащих доказыванию с учетом элементов уголовно-правового состава преступления.*

Ключевые слова. *торговля людьми; транснациональная преступность; криминалистическая характеристика; методика расследования; эксплуатация; жертвы торговли людьми; механизм преступления; обстоятельства, подлежащие доказыванию.*

Торговля людьми – это глобальная проблема, которая затрагивает жизнь миллионов людей практически в любой стране мира и которая лишает их человеческого достоинства. Являясь одним из самых опасных преступлений в мире, торговля людьми вводит в заблуждение и превращает в жертв женщин, мужчин и детей из всех уголков мира и ежедневно заставляет их быть объектом эксплуатации.

Основным отличительным признаком торговли людьми как транснациональной организованной преступной деятельности является то, что в результате ее совершения физические лица выступают в качестве товара, то есть, приравниваются к неодушевленным предметам, которые могут быть объектами купли и продажи, дарения, передачи.

Многие исследователи отмечают, что торговля людьми – гораздо более прибыльный бизнес, чем торговля наркотиками и оружием. Наркотики или оружие можно продать только однажды, тогда как услуги женщины можно продавать вновь и вновь. Поэтому зарегистрированный рост организованной преступности и ее дальнейшая глобализация приводят и к распространению торговли людьми и их дальнейшей эксплуатации.

Мировые доходы от торговли людьми оцениваются миллиардами долларов США, что сравнимо лишь только с торговлей оружием и наркобизнесом. К примеру, доходы современных рабовладельцев только от продажи невольников составляют 7 млрд. долларов в год [1].

По данным ОБСЕ, ежегодно жертвами подобных противоправных деяний становятся 800-900 тысяч человек. Более 30% из них – дети и молодежь не старше 18 лет [2].

В соответствии со ст. 3 Протокола от 15 ноября 2000 г. к Конвенции ООН против транснациональной организованной преступности «О предупреждении и пресечении торговли

людьми, особенно женщинами и детьми, и наказании за нее» понятие «торговля людьми» означает осуществляемые в целях эксплуатации вербовку, перевозку, передачу, укрывательство или получение людей путем угрозы силой или ее применения или других форм принуждения, похищения, мошенничества, обмана, злоупотребления властью или уязвимостью положения либо путем подкупа, в виде платежей или выгод, для получения согласия лица, контролирующего другое лицо [3].

Одним из элементов любой частной криминалистической методики расследования преступлений является криминалистическая характеристика уголовно наказуемого деяния.

К сожалению, до настоящего момента среди ученых не выработано единой позиции по определению и структуре криминалистической характеристики преступлений.

В свете рассматриваемых проблем представляется, что наиболее точное определение, содержащее необходимые и основные признаки, изложено Л.Л. Каневским, который под *криминалистической характеристикой* понимает «взаимосвязанную совокупность индивидуальных особенностей определенной категории преступлений, характеризующих обстановку, способ и механизм совершения и сокрытия преступления, личность преступника и потерпевшего, которые имеют значение для выявления, расследования и раскрытия преступлений» [4].

В структуру криминалистической характеристики, кроме перечисленных, автором могут входить и другие элементы.

Принимая во внимание представленные замечания различных авторов, можно заключить, что криминалистическая характеристика преступления – это система индивидуальных особенностей преступлений определенного вида, характеризующих личность преступника и потерпевшего, обстановку, каким способом подготавливается, совершается преступление, его сокрытие, а также другие элементы криминальной деятельности, которые имеют значение для выявления, раскрытия и предупреждения преступлений.

С учетом изложенного, в структуре криминалистической характеристики общественно опасных деяний, связанных с торговлей людьми и эксплуатацией их рабского труда, целесообразно рассматривать следующие элементы: сведения об обстановке совершения преступления; сведения о способе совершения преступления; сведения о личности преступника и сведения о личности потерпевшего.

Как и другие виды преступного бизнеса, торговля людьми подчинена определенным закономерностям рыночных отношений и, в первую очередь, таким как законы спроса и предложения, развития, рентабельности, необходимости учета и рекламирования товаров и услуг.

Указанные факторы имеют важное криминалистическое значение, так как закономерно определяют тот или иной способ совершения преступления, а также характер отдельных его элементов.

Действие закона спроса и предложения предполагает необходимость учета уровня спроса на тот или иной вид эксплуатации в стране, где осуществляется вербовка жертв и соотнесение его с уровнем спроса на данный вид эксплуатации в стране, где осуществляется эксплуатация.

Высокий уровень предложения рабочей силы для целей эксплуатации закономерно порождается в регионах и странах с меньшим уровнем доходов населения и высоким уровнем безработного населения, а соответствующий спрос на данных лиц в странах с высоким уровнем экономического развития, где существует низкий уровень спроса на тяжелые, малопрестижные виды трудовой деятельности – строители, дворники, уборка урожая.

В связи с этим, типовые маршруты перемещения жертв торговли людьми пролегают из деревень, сел и поселков в крупные города, из стран с менее развитой экономикой в страны с более развитой.

В целях обеспечения нормального функционирования и количественного развития канала торговли людьми, их участники вынуждены систематически вовлекать в сферу торговли как можно большее количество новых жертв, а также увеличивать число потребителей их работ и услуг.

В этих целях участники каналов торговли людьми вынуждены использовать различные средства и приемы рекламирования.

В частности, такие средства и приемы включают распространение информации о возможности трудоустройства среди знакомых, случайным знакомым на улицах, в барах, ресторанах, клубах, дискотеках, помещение рекламных объявлений о трудоустройстве, либо оказании соответствующих услуг в средствах массовой информации.

При этом, в целях сокрытия преступных намерений, при рекламировании, участники каналов торговли людьми, как правило, применяют прием инсценирования предлагаемых услуг под правомерные виды деятельности.

Механизм совершения торговли людьми предполагает перемещение жертв после заключения в отношении них незаконных сделок, или в целях заключения таких сделок в другие регионы или страны, где они и подвергаются эксплуатации.

При этом, следуя к месту эксплуатации, жертвы торговли людьми могут перемещаться через один или несколько транзитных регионов, где они могут быть перепроданы, временно эксплуатированы или сокрыты в транзитных или перевалочных квартирах.

По своей сути, маршрут канала торговли людьми является его пространственной составляющей.

Структуру маршрута торговли людьми образуют следующие элементы:

1) регионы, а в случае транснациональной торговли людьми – страны, в которых пребывают жертвы в процессе подготовки, совершения и сокрытия преступления, в том числе:

а) регионы или страны, где потенциальные, а впоследствии, реальные жертвы были завербованы или похищены. Такие территориальные образования, согласно общепринятой международно-правовой терминологии, называются, соответственно, регионами или странами происхождения;

б) регионы, а в случае транснациональной торговли людьми – страны, на территорию которых лицо ввозилось для временного пребывания в целях облегчения дальнейшего незаконного или легального переезда в другую страну, временной эксплуатации, перепродажи, временного сокрытия и т.д. Согласно общепринятой международно-правовой терминологии, такие территориальные образования называются, соответственно, транзитными регионами или странами;

в) регионы, страны конечного следования, на территории которых осуществляется эксплуатация пострадавших. Согласно общепринятой международно-правовой терминологии, такие территориальные образования называются, соответственно, регионами или странами назначения.

2) направление перемещения потерпевшего в пространстве.

Маршруты торговли людьми можно классифицировать на:

- локальные и транснациональные;
- простые (однозвенные) и сложные (транзитные);
- импортные (ввозные);
- экспортные (вывозные) и импортно-экспортные (обоюдные).

Само событие перемещения пострадавшего в пространстве также порождает следовую информацию.

В информационных системах компаний, осуществлявших перевозку пострадавших, а также лиц, совершающих преступление хранятся сведения о личности данных лиц, дате и маршруте перемещения, фактах их посадки и реального нахождения на борту самолета или поезда (такая информация отражается посадочных талонах).

Во многих аэропортах, аэро и ж/д вокзалах установлены системы видеонаблюдения, которые также могут запечатлеть важную информацию о лицах, следующих совместно с пострадавшим.

Кроме того, в вышеуказанных местах возможно установление очевидцев перемещения пострадавших из числа работников указанных учреждений, водителей автобусов, проводников или бортпроводников, а также иных пассажиров.

Важное значение имеет и информация, образуемая вследствие перемещения жертв торговли людьми через государственную границу страны и иных государств.

Факт такого пересечения государственной границы фиксируется в базе данных пограничной службы Республики Казахстан, а перемещение отдельных предметов в таможенной службе.

Важным пространственным элементом преступления является материальная (вещная) обстановка мест совершения преступления. Как правило, вербовка жертв для целей эксплуатации, а также непосредственно эксплуатация осуществляются в офисных или жилых помещениях.

В результате контактного взаимодействия лиц, совершающих преступление, а также пострадавших с окружающей материальной обстановкой, в ней могут дактилоскопические, биологические, трасологические, запаховые следы, микроследы – наслоения или отслоения и другие традиционные криминалистические следы контактного взаимодействия одежды и самого пострадавшего с окружающей вещной обстановкой.

Важное значение также имеют отдельные такие предметы и документы обстановки как тетради, дневники, клочки бумаги с записями, содержание которых имеет значение для дела, различная техника, предметы одежды и интерьера, средства принуждения и эксплуатации пострадавших, бланки типовых договоров и иных документов, визитки, кредитные карты, накладные, фотографии, личные документы потенциальных и вовлеченных в сферу торговли людьми жертв, продукция порнографического или иного содержания, указывающая на обстоятельства эксплуатации жертв торговли людьми.

Временная характеристика торговли людьми.

При этом с момента вовлечения пострадавшего до момента начала его эксплуатации проходит значительный период времени, как показывает практика от одного месяца до четырех. В это время пострадавшие уже находятся на территории другого региона или даже государства.

При этом, вследствие действия различных факторов, в частности, - физического или психического принуждения, ограничения свободы передвижения, перемещения в сопровождении охранников, запугивания привлечением к уголовной ответственности, нахождения в чуждой социальной среде без документов, пострадавшие во многих случаях не желают или не имеют возможности обратиться с соответствующим заявлением в правоохранительные органы.

Таким образом, с момента совершения преступления до момента его выявления и принятия правоохранительных мер проходит значительный период времени. И хотя в этот период времени появляются множество следов преступления, фактор времени положительно влияет и на их сокрытие.

Взаимодействие с очевидцами преступного события.

К очевидцам преступного события следует отнести лиц, которые в той или иной форме воспринимали процесс подготовки, совершения или сокрытия преступления в целом, либо отдельные его элементы, а также участвовали в нем, за исключением лиц, совершающих преступление, а также лиц на эксплуатацию которых были направлены преступные действия непосредственных жертв торговли людьми.

Очевидцев торговли людьми можно условно разделить на три категории:

1) лица, неосведомленно способствовавшие подготовке, совершению, сокрытию преступления или преступной деятельности.

К рассматриваемой категории лиц следует отнести:

а) дополнительных вербовщиков – лиц, которые неосведомленно за вознаграждение лично осуществляют вербовку жертв;

б) наемных работников туристических, модельных, брачных агентств, агентств по трудоустройству и иных компаний, созданных в целях инсценировки вербовочных действий для целей эксплуатации человека под правомерную предпринимательскую деятельность;

в) арендодателей жилых и нежилых помещений, в которых осуществляется вербовка, укрывательство или эксплуатация жертв торговли людьми, неосведомленных о целях использования предоставленных ими помещений;

г) лиц, неосведомленно обеспечивающих те или иные направления нормального функционирования вербовки, перевозки, сокрытия и эксплуатации жертв, в том числе – бухгалтера, официантки, бармены, водители, охранники и т.д.,

д) сотрудники компаний, занимавшихся оформлением виз или иных документов необходимых для перемещения пострадавшего к месту его эксплуатации.

2) Лица, воспринимавшие событие преступление или отдельные его элементы, однако не влияющие на ход его развития. В данную категорию могут войти:

а) лица, проживающие или работающие по соседству с помещением, где осуществляется вербовка, укрывательство или эксплуатация жертв торговли людьми;

б) очевидцы похищения человека, в отношении которого в дальнейшем было совершено преступление рассматриваемого нами вида;

в) лица, которых пытались завербовать для целей эксплуатации, однако они по тем или иным причинам отказались;

г) очевидцы перемещения прямых участников в пространстве - попутчики, стюардессы, проводники, водители автобусов и т.д.

3) Лица осведомленно или неосведомленно препятствовавшие или осложнявшие подготовку, совершение или сокрытие преступления.

К данной категории, в первую очередь, следует отнести лиц, состоящих в родстве или свойстве с пострадавшим.

Также к данной категории следует отнести лиц, которые в силу своих должностных обязанностей выполняют различные контрольные, правоохранительные и иные функции, направленные на противодействие торговле людьми.

Это сотрудники посольств и консульств, проводившие собеседование и принимавшие решение о выдаче въездных виз пострадавшим и торговцам людьми; сотрудники паспортно-визовой, пограничной и таможенной службы, осуществлявшие выдачу и проверку личных документов, а также досмотр багажа; участковые уполномоченные, осуществляющие охрану правопорядка и другие лица, которые прямо или косвенно в силу своих функциональных обязанностей осложняли или препятствовали совершению преступления.

Типовые способы совершения и сокрытия преступления.

Как показывает анализ следственной практики, способ совершения торговли людьми включает в себя следующие стадии:

1-я стадия. Приискание потенциальных жертв для целей торговли людьми. Решение данной промежуточной задачи осуществляется посредством совершения следующих действий:

- поиска жертв через друзей и знакомых;
- знакомств с потенциальными жертвами на улицах, в клубах, барах и других заведениях;
- размещения рекламных объявлений в печатных, электронных и иных средствах массовой информации - журналах, газетах, телевидении, глобальной сети Интернет;
- приискание потенциальных жертв в среде безработных на биржах труда;
- поиск жертв в определенных социальных группах, группах занимающихся определенной сферой деятельности, информационных системах специализированных учреждений, например, в среде лиц, занимающихся проституцией, в среде лиц, обладающих

здоровыми органами и тканями с использованием картотек медицинских учреждений, содержащих сведения об их здоровье и группе крови, среди новорожденных от которых отказались родители в родильных домах, среди душевнобольных или изувеченных лиц (лишенных конечностей или иных органов) для целей их эксплуатации в форме попрошайничества.

2-я стадия. Понуждение потенциальной жертвы к определенному поведению и вовлечение ее в сферу торговли людьми, либо насильственное завладение ею.

В ходе реализации этой задачи, торговцами людьми могут совершаться следующие действия:

- похищение потенциальной жертвы и подавление ее воли к сопротивлению посредством насильственного удержания в подконтрольном помещении, а также путем введения в организм веществ различного действия, тормозящих психические процессы;
- вербовка.

3-я стадия. Приискание контрагентов и заключение с ними незаконных сделок имущественного характера в отношении подконтрольных лиц.

Приискание контрагентов может осуществляться:

- через друзей и знакомых;
- посредством глобальной сети Интернет;
- через сотрудников компаний по трудоустройству, располагающих информационной системой данных о работодателях, нуждающихся в работниках;
- через лиц, осуществляющих эксплуатацию людей, например содержателей притонов для занятия проституцией, владельцев различных нелегальных или полулегальных производств;
- через сотрудников медицинских учреждений, связанных с трансплантацией органов и тканей, а также научными исследованиями в области медицины;
- через лидеров организованных преступных формирований, контролирующих те или иные виды криминального бизнеса, предполагающего эксплуатацию человека, например попрошайничество.

4-я стадия. Перемещение жертв к месту назначения и передача их контрагентам, осуществляющим эксплуатацию.

Решение данной задачи может осуществляться посредством совершения следующих действий:

- безтранзитной перевозки пострадавших из места происхождения в место назначения;
- перевозки пострадавших через одно или несколько транзитных стран или регионов.

Такое перемещение может преследовать следующие цели:

а) сокрытие маршрута перемещения жертв. При этом сокрытые пострадавшие могут некоторое время пребывать в перевалочных квартирах, после чего, направляются в место назначения;

б) накопления необходимого количества жертв, для их коллективной транспортировки в место назначения;

в) временной эксплуатации на территории транзитных государств;

г) перепродажи на территории транзитных государств;

д) перемещение жертв в страну назначения, в случаях, когда их прямое перемещение из страны происхождение представляется затруднительным.

В зависимости от форм участия торговцев людьми в процессе перемещения жертв, следует различать:

- самостоятельное добровольное перемещение пострадавших к месту назначения по маршруту, указанному торговцами людьми, без сопровождения, при котором лица, совершающие преступление осуществляют финансирование транспортировки, обеспечивают необходимыми подложными или легальными документами, организуют их встречу в месте назначения;

- добровольная перевозка пострадавшего в сопровождении курьера;
- принудительная перевозка пострадавшего, посредством насильственного подавления его воли к сопротивлению путем связывания, заточения в помещения транспортного средства, введения в организм веществ, тормозящих психические процессы и т.д.

5-я стадия. Применение мер воздействия в отношении пострадавших, в целях подавления их воли к сопротивлению, смирению со своим положением и обеспечения подконтрольности их поведения.

В целях решения указанных задач, торговцами людьми в отношении пострадавших могут быть применены следующие меры:

- обман;
- лишение пострадавшего документов, удостоверяющих личность. В отсутствие указанных документов пострадавшие фактически лишаются возможности вернуться в страну назначения, обращаться в правоохранительные органы, а некоторых случаях безопасно перемещаться по городу;
- психическое воздействие;
- физическое насилие и понуждение к определенному поведению. Данная форма принуждения может выражаться в систематическом или разовом нанесении пострадавшему побоев, причинение вреда здоровью различной степени тяжести, истязании, насильственном ограничении свободы перемещения, предполагающем помещение пострадавшего в запертое подконтрольное помещение, запрете его перемещения за пределами такого помещения без сопровождения охранников и т.д.;
- преднамеренное поставление пострадавшего в положение долговой кабалы или иное зависимое состояние. Например, пострадавшему после перемещения его к месту эксплуатации и сообщения о реальных условиях деятельности, предлагается отдать сумму денежных средств, затраченных на обеспечение его документами и переезд, либо отработать их в натуре в процессе эксплуатации. Как правило, заявляемая таким пострадавшим сумма во много раз превосходит реально понесенные затраты.

6-я стадия. Эксплуатация жертв торговли людьми.

Практике известны следующие виды эксплуатации:

- сексуальная эксплуатация, предполагающая систематическое использование эксплуатируемого лица в целях возмездного оказания услуг, связанных с удовлетворением сексуальных потребностей иным лицам;
- производственная эксплуатация. К ней относится систематическое использование чужого труда для производства материальных или иных благ или оказания услуг не связанных с удовлетворением сексуальных потребностей их потребителей. Производственная эксплуатация человека может иметь место в таких отраслях хозяйства, как строительство, полулегальное или не легальное производство различных товаров, сельском хозяйстве, например сезонные уборки урожая, в личном хозяйстве и других;
- попрошайничество;
- изъятие органов и тканей для целей трансплантации или проведения научных и иных опытов.

В результате анализа этих составных элементов структуры методики расследования торговли людьми можно сделать следующий вывод:

1) Содержание криминалистической характеристики торговли людьми составляют: характеристика исходной информации; характеристика обстановки совершения преступления; данные о способах совершения и сокрытия преступления; данные о механизме совершения торговли людьми; сведения о типичных личностных особенностях потерпевших; сведения о типичных личностных особенностях преступников; обобщенные данные о наиболее распространенных мотивах преступления; круг основных обстоятельств, подлежащих установлению.

2) Обстоятельства, подлежащие установлению, должны излагаться в виде основных обстоятельств, подлежащих доказыванию по уголовному делу, сгруппированных по элементам уголовно-правового состава торговли людьми: основные обстоятельства, относящиеся к объекту посягательства (на что направлено посягательство, чему причинен ущерб, его размер и др.); основные обстоятельства, относящиеся к объективной стороне посягательства (где, когда, каким образом, действиями одного человека или нескольких лиц, роль каждого, при каких обстоятельствах, каковы последствия, причиненный ущерб, причинная связь между деянием и последствиями, обстоятельства, способствовавшие преступлению и т.д.); основные обстоятельства, относящиеся к субъекту посягательства (кто совершил посягательство; данные, характеризующие его личность; если участвовала группа лиц, то кто они и какова роль каждого из них и так далее); основные обстоятельства, относящиеся к субъективной стороне посягательства (вина, ее форма, мотив и цель – при умышленной вине).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Торговля людьми приносит преступникам более 150 миллиардов долларов США в год // Центр новостей ООН. — URL: https://news.un.org/ru/story/2015/07/1266601 (дата обращения: 13.01.2026 г.).
2. По данным ОБСЕ, ежегодно жертвами торговли людьми становятся 800–900 тысяч человек // Podrobnosti.ua. — URL: https://podrobnosti.ua/147324-ezhegodno-zhertvami-torgovli-ljudmi-stanovjatsja-800-900-tysjach-chelovek.html (дата обращения: 13.01.2026 г.).
3. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime; adopted 15 November 2000, Article 3. United Nations. — URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons (дата обращения: 20.01.2026 г.).
4. Каневский Л. Л. Криминалистические проблемы расследования и профилактики преступлений несовершеннолетних. – Красноярск, 1991. - 74 с.

СОДЕРЖАНИЕ
CONTENT

ЮРИДИЧЕСКИЕ НАУКИ
LEGAL SCIENCES

ENDLESS LIGHT IN SCIENCE

Контакт
irc-els@mail.ru

Наш сайт
irc-els.com