

R.A.Gafarov
master, Azerbaijan State University of Economics
gafarov.r@icloud.com

ANALYSIS OF FINANCIAL MONITORING TOOLS AND TECHNIQUES USED IN DIFFERENT JURISDICTIONS

Resume

This article examines the tools and techniques employed for financial monitoring and anti-money laundering (AML) across different jurisdictions, focusing on the United States, United Kingdom, European Union, and Japan. It compares regulatory frameworks, real-time transaction monitoring systems, blockchain forensic analytics, and Know Your Customer (KYC)/AML practices in these regions. The findings indicate that each jurisdiction adopts a distinct approach: the US leverages robust Bank Secrecy Act reporting and extensive Suspicious Activity Reporting (SAR) regimes, the UK combines regulatory innovation with proactive oversight (including in the crypto sector), the EU harmonizes standards via AML Directives across member states, and Japan enforces strict compliance especially by licensing cryptocurrency exchanges. A table of original data and an illustrative figure are included to compare key metrics such as reporting volumes. The author provides insights and recommendations on enhancing the effectiveness of AML monitoring through advanced technologies and improved international cooperation.

Keywords: *financial monitoring, anti-money laundering, blockchain analytics, KYC, cryptocurrency regulation.*

Introduction

Financial monitoring for anti-money laundering (AML) is a critical component of safeguarding the integrity of the global financial system. Money laundering, estimated to equal between 2% to 5% of global GDP, undermines economic stability and facilitates criminal activity (Basel Institute on Governance, 2023). In response, international standards – primarily those set by the Financial Action Task Force (FATF) – urge jurisdictions worldwide to implement robust AML frameworks and monitoring tools. Over time, regulators and financial institutions have developed a spectrum of tools ranging from traditional rule-based transaction monitoring systems to advanced analytics and artificial intelligence solutions. New technologies have demonstrated the potential to enhance the speed, quality, and efficiency of AML measures (Financial Action Task Force, 2021). However, jurisdictions differ significantly in their regulatory approaches and technology adoption, especially as emerging challenges such as cryptocurrency proliferate. Large economies like the United States, United Kingdom, European Union members, and Japan offer instructive case studies in how different jurisdictions deploy tools and techniques to detect and deter financial crime.

Each of these jurisdictions has built an AML regime shaped by its legal environment and risk exposure. The United States enforces long-standing laws such as the Bank Secrecy Act (BSA) and USA PATRIOT Act, which mandate comprehensive reporting of suspicious activities to the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN). The United Kingdom, guided by the Proceeds of Crime Act and Money Laundering Regulations, operates a Financial Intelligence Unit (UKFIU) under the National Crime Agency to manage SARs, and has updated its framework post-Brexit while aligning with international standards. The European Union continually updates its AML Directives to unify member states' responses – for example, the EU's 5th and 6th AML Directives expanded requirements for customer due diligence and incorporated cryptocurrency service providers into the regulated sector. Japan, learning from high-profile cases and FATF evaluations, has strengthened its AML laws (such as the Act on Prevention of Transfer of Criminal Proceeds) and requires strict oversight of financial institutions and crypto-asset

exchanges by the Japan Financial Services Agency (JFSA) in coordination with the Japan Financial Intelligence Center (JAFIC).

Despite these robust frameworks, money laundering remains a global concern. Key performance indicators, such as the number of suspicious transaction reports filed, have been rising in many jurisdictions, reflecting both enhanced monitoring and possibly an increase in detected illicit activity. At the same time, questions linger about the efficiency of current systems – for instance, it is estimated that less than 1% of worldwide illicit financial flows are ultimately seized by authorities (Pol, 2020). This paper provides a comparative analysis of financial monitoring tools and techniques in the US, UK, EU, and Japan, with a particular focus on innovations related to cryptocurrency. We analyze how regulatory frameworks shape monitoring practices, examine the use of real-time transaction monitoring and blockchain analytics, and compare outcomes such as reporting trends and enforcement results. Through this analysis, we offer insights into best practices and recommend ways to enhance AML effectiveness across jurisdictions.

Analysis

Regulatory Frameworks and Reporting Requirements. Jurisdictions vary in their regulatory architecture for AML compliance. In the **United States**, the BSA and related regulations obligate banks and other financial institutions to implement internal controls, conduct customer due diligence, and report suspicious activities. As a result, the U.S. has an extensive Suspicious Activity Report (SAR) filing system managed by FinCEN. In 2022, U.S. financial institutions filed over 3.6 million SARs – a record high, and a 57% increase from 2019 pre-pandemic levels (Financial Crimes Enforcement Network, 2023). This surge is partly attributed to improved detection of fraud during the COVID-19 era and stricter enforcement of reporting mandates. **United Kingdom** law similarly requires the filing of Suspicious Activity Reports (SARs) to the UKFIU. For the period 2021–2022, the UK received over 900,000 SARs, marking a 21% year-on-year increase (National Crime Agency, 2023). Notably, the UK’s regulatory regime has begun to encompass fintech and crypto firms as reporting entities, which contributed to the uptick in SAR volumes. The **European Union**, through its AML Directives, mandates that each member state operate a Financial Intelligence Unit and enforce customer due diligence, record-keeping, and reporting of suspicious transactions. While SAR statistics in the EU are compiled at the national level, major member states also report growing numbers – for example, Germany’s FIU saw STR filings rise from about 144,000 in 2020 to over 337,000 in 2022 (Basel Institute on Governance, 2023). This reflects intensified efforts in Europe to crack down on money laundering, including better detection of fraud and tax evasion. **Japan** has tightened reporting requirements under its legal framework; by 2022 the number of suspicious transaction reports in Japan exceeded 580,000, the highest ever recorded for the country (Japan Financial Intelligence Center, 2023). Japan’s regulators have particularly focused on risks from organized crime and, more recently, on transactions involving crypto-assets, leading to rigorous enforcement of know-your-customer rules at exchanges and other institutions.

Table 1. Comparison of suspicious transaction reporting in selected jurisdictions (showing STR/SAR filings and recent trends):

Jurisdiction	Annual STRs/SARs (latest)	Recent Trend
United States (2022)	3,620,000	+57% vs. 2019 (pre-pandemic)
United Kingdom (2022)	~900,000	+21% vs. prior year
Germany (2022) – as largest EU economy	337,000	+134% vs. 2020
Japan (2022)	583,317	+35% vs. 2020

As **Table 1** shows, the United States generates by far the highest volume of suspicious activity reports among the jurisdictions compared, reflecting the size of its financial system and the broad scope of entities required to file reports. The United Kingdom and Japan each produce on the order of half a million or more reports annually, while Germany (representative of EU jurisdictions) also shows hundreds of thousands of reports and a particularly steep increase in recent years. These trends indicate that reporting volumes are rising across the board, which could signal both better monitoring and a growing complexity of financial crime being detected. However, merely increasing the quantity of STR/SAR filings does not automatically equate to more effective AML outcomes, an issue discussed later in this analysis.

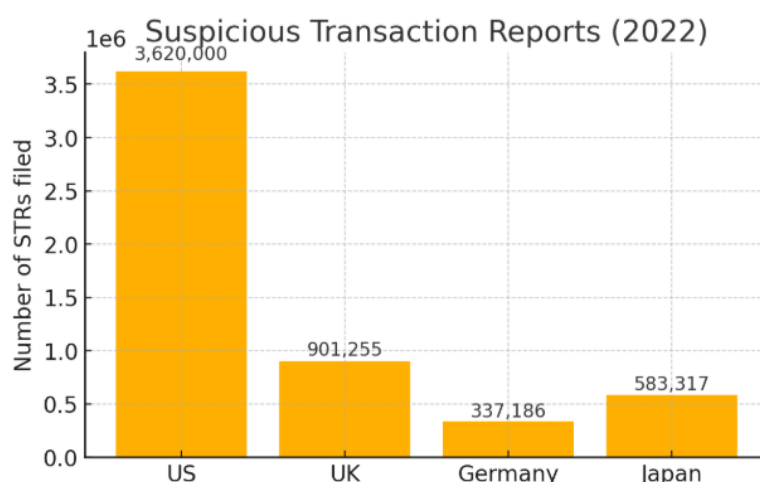


Fig. 1. Number of suspicious transaction reports filed in 2022 by jurisdiction.

As illustrated in **Fig. 1**, there is a stark disparity in STR/SAR volumes across jurisdictions: the US bar towers over others, with about four times as many reports as the UK and more than six times the reports of Japan. The UK, EU (exemplified by Germany), and Japan each report substantial numbers in the hundreds of thousands, but still an order of magnitude lower than the United States. This disparity highlights differences in financial sector size, regulatory scope, and possibly reporting thresholds or practices. It may also suggest that U.S. institutions cast a “wider net” in reporting, potentially due to stricter rules or fear of penalties, whereas some other jurisdictions might employ a more risk-based filtering of what gets reported. The visual comparison underscores the importance of not only having robust reporting frameworks but also the capacity to analyze and act on the millions of reports generated worldwide.

Real-Time Transaction Monitoring and Technology Adoption. A key tool in financial monitoring is real-time or near-real-time transaction monitoring systems. These automated systems flag unusual patterns or anomalies in transactions as they occur, enabling prompt investigation. The **United States** pioneered widespread use of rule-based monitoring software in banks after the BSA, and today U.S. institutions increasingly integrate advanced algorithms to reduce false positives. Large U.S. banks have invested in machine learning models that sift through transaction data to detect suspicious behavior that rule-based systems might miss, such as complex layering of funds or micro-structuring of deposits. The **UK** has similarly encouraged a proactive stance: banks and payment providers under UK regulation use screening and monitoring engines that run in real-time, often calibrated to risk scores. The UK’s regulator (formerly the Financial Services Authority, now split into the FCA and PRA) emphasizes a risk-based approach where high-risk customers and transactions get enhanced scrutiny. In the **EU**, the 4th AML Directive explicitly adopted a risk-based approach, prompting financial institutions to tailor their monitoring intensity to the risk profile of customers and geographies. Many European banks process transactions in batch and in real-time hybrids, with efforts underway to upgrade legacy systems to real-time analytics, sometimes with support from EU-wide initiatives. **Japan**, having a technologically advanced banking sector, also employs automated transaction monitoring;

Japanese banks work closely with the JAFIC to update typologies of suspicious behavior (e.g. transactions linked to yakuza-organized crime). One challenge noted in Asia and elsewhere is the slower adoption of cutting-edge AI tools in some institutions due to cost and expertise barriers (Financial Action Task Force, 2021). Nonetheless, advanced financial centers like Tokyo, London, and New York are piloting artificial intelligence for anomaly detection and entity resolution (e.g., identifying networks of related accounts) to enhance monitoring. According to industry studies, such AI-driven approaches have the potential to substantially reduce false alerts and improve the true positive rate of detecting illicit activity (Breslow et al., 2017). Indeed, regulators are cautiously supportive: FATF has highlighted that responsible use of innovation can strengthen AML effectiveness, as long as proper safeguards (like transparency and avoidance of bias) are in place (Financial Action Task Force, 2021).

Blockchain Forensics and Crypto-Asset Monitoring. The rise of cryptocurrency has introduced new complexities and tools in financial monitoring. Unlike traditional bank transfers, crypto-asset transactions occur on blockchain ledgers that are public but pseudonymous. This has led to the development of **blockchain forensic tools** – specialized analytics that trace transactions through blockchain networks to identify patterns indicative of money laundering (e.g., funds moving through mixers/tumblers or multiple wallets in rapid succession). **U.S. authorities** have been at the forefront of leveraging blockchain analytics; agencies such as the U.S. Department of Justice, IRS Criminal Investigation, and FinCEN routinely partner with companies like Chainalysis, Elliptic, and CipherTrace to trace illicit crypto flows. These tools use techniques such as clustering analysis (linking addresses to the same owner) and referencing known illicit addresses (from dark web marketplaces, ransomware wallets, etc.) to flag suspect movements. The U.S. regulatory framework classifies cryptocurrency exchanges and wallet providers as Money Services Businesses subject to BSA/AML requirements since guidance issued in 2013, and this was reinforced with the Anti-Money Laundering Act of 2020. As a result, U.S.-based crypto exchanges implement KYC on their users and file SARs for suspicious crypto transactions, feeding crypto-related SARs into FinCEN’s database. In the **United Kingdom**, cryptocurrency exchanges must register with the Financial Conduct Authority (FCA) and comply with AML regulations. The UK’s NCA has established a dedicated “Combating Kleptocracy Cell” and a cryptoassets team to build expertise in tracing digital assets (National Crime Agency, 2023). British law enforcement has successfully used blockchain forensics in several cases, for example to track proceeds from cybercrime and fraud, resulting in asset seizures. The **European Union** through its 5AMLD and now the forthcoming Markets in Crypto-Assets (MiCA) regulation requires crypto-asset service providers to conduct KYC/AML and report suspicious activities. European authorities (such as Europol and national police agencies) also use blockchain analysis tools and cooperate through the Europol Cybercrime Centre to follow cross-border crypto laundering schemes. **Japan** was one of the first jurisdictions to regulate crypto exchanges, after events like the Mt. Gox exchange hack in 2014 exposed vulnerabilities. By 2017, Japan’s Payment Services Act required crypto exchange licensing and AML obligations, including verifying customer identities and reporting suspicious crypto transactions. This early integration of crypto into the AML regime means Japanese exchanges work closely with regulators; Japan’s National Police Agency has used blockchain analytics to uncover crypto laundering connected to organized crime and drug trafficking. A notable global initiative in this domain is the FATF’s “travel rule” extended to virtual assets – requiring that originator and beneficiary information travel with crypto transactions above a threshold. Implementation has varied: countries like the US, UK, and Japan have moved to implement travel rule compliance in their domestic regulations, while many other jurisdictions have been slower. As of 2022, FATF observed that a relatively small subset of member countries had fully implemented the travel rule and related supervision for virtual asset service providers (Financial Action Task Force, 2022). This uneven adoption creates loopholes that illicit actors can exploit by moving activities to less regulated exchanges. The use of blockchain forensic tools by the leading jurisdictions is helping to mitigate crypto-related risks, but it also underscores the need for international coordination. Crypto transactions often hop across borders; therefore, intelligence

sharing between countries (for example, through the Egmont Group of FIUs or bilateral law enforcement cooperation) is crucial to follow the money trail effectively.

KYC Procedures and AML Techniques in Practice. Fundamental to all financial monitoring is the Know Your Customer process and related customer due diligence measures. **Customer Identification** requirements are strict in all the jurisdictions studied, but with some differences in implementation. In the **US**, financial institutions must collect and verify identifying information for all customers (under the Customer Identification Program rules of the USA PATRIOT Act) and perform ongoing due diligence, including screening against sanctions and politically exposed persons (PEP) lists. The US has large databases and inter-agency programs (for instance, FinCEN's beneficial ownership registry being established under recent legislation) to facilitate transparency of corporate customers. In the **UK** and **EU**, regulations mandate a risk-based approach to customer due diligence: for standard-risk customers, basic verification of ID and address suffices, whereas high-risk customers (those from high-risk countries, PEPs, etc.) require enhanced due diligence such as source-of-funds checks and senior management approval. EU members also implement identity verification using national ID systems; some have pioneered e-ID and digital verification methods to streamline KYC. For example, many European banks leverage government-backed electronic IDs or licensed third-party digital identity services to satisfy KYC in online account opening. **Japan** requires financial institutions and crypto exchanges to verify customers' identity with government-issued ID and, in some cases, confirm the existence of a domestic bank account link or physical address as an additional verification step. A cultural aspect in Japan is the usage of in-person verification (through postal mail verification codes, etc.) historically, although online verification is now more common. All jurisdictions oblige institutions to keep detailed records of customer transactions and report any suspicious behavior promptly.

Another technique in AML is the use of **watchlists and screening**. Banks globally use software to screen transactions and customer names against lists (sanctions lists, wanted criminals, adverse media). The US Office of Foreign Assets Control (OFAC) sanctions list is a global benchmark – US and international banks alike must ensure no transactions involve sanctioned entities. The EU and UK maintain their own sanctions lists; post-Brexit, the UK has an autonomous sanctions regime but coordinates closely with the US/EU. Japan implements UN sanctions and its own where applicable. Screening tools have evolved to use fuzzy matching and even natural language processing (for adverse media) to reduce false matches.

Effectiveness and Challenges – STR Utilization and Compliance Costs. While the tools and regulations have grown more sophisticated, a common challenge is ensuring that the deluge of data (such as millions of SARs/STRs) is effectively used by law enforcement. In the United States, for instance, only a fraction of SARs lead to investigative action, due in part to resource constraints – there are simply more reports than agencies can thoroughly analyze. A similar situation exists in the UK, where the National Crime Agency noted that about 83,000 of the ~900,000 SARs in 2022 were prioritized as needing consent or intervention, and the rest serve as intelligence for potential future analysis (National Crime Agency, 2023). The value of the SAR system is undeniable for intelligence gathering, but **quality over quantity** has become a focus. Regulators in the UK and EU have been encouraging better *targeted* reporting (to avoid defensive or low-value submissions) and have embarked on SARs reform projects to upgrade analytics capabilities within FIUs. On the other side of the equation, compliance costs for financial institutions are very high. Banks and companies must invest in compliance staff, training, and technology. Estimates show that globally, hundreds of billions of dollars are spent annually on AML compliance (Pol, 2020), yet the actual amount of illicit funds intercepted remains relatively small. Pol (2020) notably characterizes the global AML system as “the world's least effective policy experiment,” given that by some analyses, for each \$100 of laundered money, significantly less than \$1 is successfully confiscated. This critique underscores that despite the sophisticated tools and strict regulations now in place in the US, UK, EU, Japan and elsewhere, criminals continue to find gaps – whether by exploiting regulatory arbitrage between jurisdictions,

leveraging new technologies to obscure fund flows, or simply overwhelming the system with sheer volume (e.g., numerous small transactions below reporting thresholds).

At the same time, there have been **improvements and success stories**. International cooperation has increased, as seen in joint investigative teams that tackle money laundering networks spanning multiple countries. Large-scale enforcement actions, such as the exposure of the 1MDB scandal or European money laundering “laundromat” cases, were facilitated by better data sharing and more agile analysis of financial records. In Japan, coordination between JAFIC and local law enforcement has led to more STR-driven investigations of organized crime financing. In the UK, the use of Account Freezing Orders and Unexplained Wealth Orders (legal tools to seize assets from suspicious origins) demonstrates how intelligence from SARs can be turned into enforcement outcomes, recovering hundreds of millions of pounds in criminal assets. The United States has also ramped up penalties for AML compliance failures, prompting institutions to adopt more effective internal controls. For example, major banks have been fined for failing to detect obvious patterns of laundering, sending a clear message that merely filing SARs is not enough – they must also actively prevent abuse of their systems.

Overall, the comparative analysis reveals that **each jurisdiction has strengths and weaknesses** in its financial monitoring regime. The US benefits from scale and a data-rich environment, but faces the challenge of sifting through an enormous volume of reports. The UK and EU have been agile in updating rules (such as quickly bringing crypto businesses into scope) and emphasizing quality of reports, but must continue investing in technology and inter-agency coordination. Japan’s stringent approach, especially towards crypto exchanges and cash transaction reporting, has created a high compliance culture, yet it grapples with emerging threats that require continuous adaptation of tools.

Conclusion

In conclusion, the tools and techniques of financial monitoring for AML, as observed in the United States, United Kingdom, European Union, and Japan, have evolved into robust systems with common foundations but distinct characteristics. All these jurisdictions have implemented comprehensive regulatory frameworks mandating KYC, record-keeping, and the reporting of suspicious transactions. They have increasingly embraced technology – from real-time transaction monitoring software to sophisticated blockchain forensic tools – to contend with the scale and complexity of modern financial crime. The comparative analysis shows that jurisdictional differences, such as the legal definition of what must be reported and the aggressiveness of enforcement, lead to significant variability in outcomes (e.g., the volume of STRs filed or the types of cases detected). Each approach offers lessons: the U.S. system demonstrates the power of extensive data collection, the UK and EU highlight the benefits of a risk-based approach and adaptive regulations, and Japan underscores the importance of early action on emerging risks like cryptocurrencies.

Despite substantial progress, the current AML monitoring regimes face ongoing challenges. One clear insight is that simply generating large numbers of reports is not a guarantee of effectiveness unless those reports are actionable. Improving the **signal-to-noise ratio** is essential – in other words, raising the quality and relevance of reports so that law enforcement can concentrate resources on the most pertinent leads. To this end, the author recommends **enhancing analytical capabilities** within Financial Intelligence Units and among compliance teams. This includes investing in artificial intelligence and machine learning tools that can process vast datasets to identify high-priority suspicions, as well as employing data visualization and network analysis software to reveal hidden connections among suspects. Such tools can help regulators and banks move from a compliance mindset of “box-ticking” to a truly intelligence-led approach.

Another recommendation is to **strengthen international cooperation and standardization**. Money laundering is often a cross-border operation; thus, discrepancies between jurisdictions can be exploited by criminals. Greater harmonization of regulations (for instance, consistent enforcement of the FATF travel rule for cryptocurrency transactions across all major financial centers) would close off some of the loopholes. Information sharing can also be

improved: building on platforms like the Egmont Group and bilateral treaties, countries should share typologies and even specific red flag indicators in real time. The author's view is that collaborative initiatives – such as joint financial crime task forces that include personnel from multiple countries – are critical to pursuing complex cases that no single jurisdiction can fully investigate alone.

From a policy perspective, regulators should also **promote innovation in compliance**. Sandboxing initiatives, where financial institutions and fintech companies can test new AML solutions with regulatory guidance, have shown promise in the UK and could be expanded elsewhere. Similarly, public-private partnerships (like the UK's Joint Money Laundering Intelligence Taskforce) allow pooled expertise and intelligence to target the most serious threats, such as professional money laundering networks. The author recommends more frequent feedback loops wherein law enforcement informs banks about which types of SARs proved useful, thereby guiding banks to refine their monitoring criteria (and conversely, pointing out over-reported areas that yield little value).

Finally, there is a need to **balance compliance costs with benefits**. Banks and businesses in all surveyed jurisdictions spend enormous sums on AML compliance. Ensuring that this investment translates into meaningful disruption of illicit finance is a policy priority. This could involve reassessing thresholds and exemptions to reduce unnecessary filings (focusing efforts where risk is truly higher) and leveraging automation to cut manual compliance costs. The jurisdictions studied have begun moving in this direction with risk-based approaches, but continuous calibration is needed to respond to the ever-changing tactics of money launderers.

In summary, financial monitoring tools and techniques across different jurisdictions are becoming more advanced and aligned, especially with the shared adoption of technologies like real-time analytics and blockchain forensics. The US, UK, EU, and Japan – each in their own way – have tightened their nets around illicit finance. The author's analysis and comparisons affirm that no system is perfect; each country or region must remain vigilant and adaptable. By learning from each other's experiences and pursuing the recommendations above, these jurisdictions can collectively enhance the effectiveness of AML efforts. In turn, this will bolster the integrity of the international financial system, ensuring that it becomes ever harder for criminals to exploit and ever easier for legitimate commerce to thrive without the shadow of dirty money.

References

1. Basel Institute on Governance. (2023). Basel AML Index 2023: 12th Public Edition – Ranking money laundering risks around the world. Basel Institute.
2. Breslow, S., Hagstroem, M., Mikkelsen, D., & Robu, K. (2017). The new frontier in anti-money laundering. McKinsey & Company White Paper.
3. Financial Action Task Force. (2021). Opportunities and challenges of new technologies for AML/CFT. FATF.
4. Financial Action Task Force. (2022). Targeted update on implementation of the FATF standards on virtual assets and VASPs. FATF.
5. Financial Crimes Enforcement Network (FinCEN). (2023). Suspicious Activity Reports (SARs) annual statistics, 2022. U.S. Department of the Treasury.
6. Japan Financial Intelligence Center (JAFIC). (2023). Annual Report 2022. National Police Agency of Japan.
7. National Crime Agency. (2023). UK Financial Intelligence Unit (UKFIU) Annual Report 2022. NCA Publications.
8. Pol, R. (2020). Anti-money laundering: The world's least effective policy experiment? Policy Design and Practice, 3(1), 73–90.

R.A.Gafarov
magistr, Azərbaycan Dövlət İqtisad Universiteti

MÜXTƏLİF YURİSDİKSİYALARDA MALİYYƏ MONİTORİNQİ ALƏTLƏRİ VƏ METODLARININ TƏHLİLİ

Xülasə

Maliyyə monitorinqi alətləri və metodlarının müxtəlif yurisdiksiyalarda tətbiqini təhlil edən bu məqalədə ABŞ, Birləşmiş Krallıq, Avropa İttifaqı və Yaponiya kimi böyük dövlətlərin təcrübələri müqayisə olunur. Qanunvericilik çərçivələri, əməliyyatların real vaxt rejimində izlənməsi, blokçeyn təhlili və Müştərinə Tanı (KYC) və Pulun Yuyulmasına Qarşı Mübarizə (AML) texnikalarındakı fərqlər araşdırılır. Tədqiqat nəticələri göstərir ki, hər bir yurisdiksiya özünəməxsus monitorinq yanaşmasına malikdir: ABŞ-da Bank Gizliliyi Aktı (BSA) əsasında geniş STR (Şübhəli Əməliyyatlar haqqında Hesabatlar) sistemi formalaşmış, Birləşmiş Krallıqda maliyyə kəşfiyyatı vahidi (UKFIU) kripto sektorunu da əhatə etməklə hesabatlılığı artırır, Aİ üzv ölkələri vahid AML Direktivlərinə uyğun risk-əsaslı nəzarəti tətbiq edirlər, Yaponiya isə kriptovalyuta birjalarının lisenziyalaşdırılması yolu ilə şəffaflığı təmin edir. Təhlildə real məlumatlar əsasında müqayisəli cədvəl və qrafik təqdim olunur. Müəllif əldə olunmuş nəticələrə əsasən, AML rejiminin səmərəliliyini artırmaq üçün innovativ texnologiyaların tətbiqi və beynəlxalq əməkdaşlığın gücləndirilməsi barədə tövsiyələr verir.

Açar sözlər: maliyyə monitorinqi, pulların yuyulması, AML, KYC, kriptovalyuta, tənzimləyici çərçivə.

Р.А.Гафаров

магистр, Азербайджанский Государственный Экономический Университет

gafarov.r@icloud.com

АНАЛИЗ ИНСТРУМЕНТОВ И МЕТОДОВ ФИНАНСОВОГО МОНИТОРИНГА В РАЗНЫХ ЮРИСДИКЦИЯХ

Резюме

В данной статье проведён сравнительный анализ инструментов и методов финансового мониторинга, применяемых в таких юрисдикциях, как США, Великобритания, Европейский союз и Япония. Рассматриваются нормативные рамки, системы мониторинга транзакций в реальном времени, использование блокчейн-аналитики, а также практика применения процедур «Знай своего клиента» (KYC) и противодействия отмыванию денег (AML). Представлены сравнительные таблицы и графики с использованием актуальных статистических данных. В работе подчёркивается важность международного сотрудничества и внедрения инновационных технологий для повышения эффективности финансового мониторинга. Автор делает вывод, что ключом к эффективной борьбе с отмыванием денег является комплексный подход, основанный на правовом регулировании, техническом обеспечении и аналитических возможностях финансовых учреждений.

Ключевые слова: финансовый мониторинг, отмывание денег, криптовалюта, KYC, AML, блокчейн-аналитика.