

# THE ROLE OF RECOMMENDATIONS OF THE FINANCIAL ACTION TASK FORCE (FATF) IN THE REGULATION OF VIRTUAL ASSETS

GANNA VOIEVODINA

National Aviation University, Faculty of International Relations, International law  
E-mail: anna.v@manimama.eu

---

**Abstract** - The article examines the contents of the updated Recommendations of the Financial Action Task Force (FATF) and their impact on the fight against money laundering and terrorist financing, regarding the regulation of virtual assets and the activities of service providers with them. The following were analyzed: Guidance Financial Action Task Force on Money Laundering for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (VASPs) and the Law of Ukraine "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". The results of the study indicate the importance of the Group's Recommendations on the development of financial measures in the fight against money laundering in the field of virtual assets.

---

**Keywords:** Virtual Assets, Financial Action Task Force (FATF), Virtual Asset Service Providers, Anti-Money Laundering, Anti-Terrorist Financing, Risk-Based Approach.

---

## I. INTRODUCTION

Virtual assets have become quite popular in recent years with the growing use of internet technologies and the digital economy. These assets are used as an alternative to traditional money and financial systems, which emphasizes the special need for their legal regulation. The possibility of conducting operations with virtual assets remotely via the Internet and the anonymity of operations with them are one of the reasons for using virtual assets for money laundering and terrorist financing [1, c. 2]. Vandesande noted that money laundering and terrorist financing is one of the biggest risks for the development of the virtual assets market [2, c. 2].

Analysis of recent research and publications. Ukrainian and foreign representatives of legal science, such as H. Pavlidis, I.M. Gaevskiy, N. Vandesande, L. Haffke, M. Fromberger, P. Zimmermann dealt with the issues of combating money laundering and terrorist financing in the context of virtual assets. However, the issue of comprehensive analysis of the international standards of the Financial Action Task Force on Money Laundering (FATF), in particular their Recommendations, was not considered in the domestic scientific literature. The above confirms the relevance of the chosen topic and the expediency of the analysis of the raised issue. The purpose of the study. The purpose of the study is to analyze the Recommendations of the FATF and to determine the impact of the Recommendations on combating money laundering and terrorist financing in the context of the regulation of virtual assets. To achieve this goal, the following tasks are set:

1) analyze the 40 Recommendations of the Group on the development of financial measures to combat money laundering in the context of the regulation of virtual assets.

2) investigate the impact of the FATF's Recommendations on the development of financial measures to combat money laundering in the field of virtual assets and determine their significance in the context of regulation of this segment at the international level.

## II. THE MAIN MATERIAL

In the context of the regulation of virtual assets, an important role is played by the Financial Action Task Force on Money Laundering (hereinafter - FATF), an international organization created in 1989 by the Ministers of member countries. The FATF is a global body for combating money laundering and terrorist financing.

In accordance with its mandate, the FATF sets standards and promotes the effective implementation of legal, regulatory and operational measures to combat money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, as well as other threats to systems of financial integrity. The FATF also works with other international stakeholders to identify vulnerabilities at the national level in order to protect the international financial system from illicit use [3]. As a policy-making body, the FATF works to ensure that there is the necessary political will for national legislative and regulatory reforms in these areas. Today, it includes 38 members: 36 countries and 2 organizations, as well as 26 observers: 25 organizations and 1 country [4]. More than 200 countries and jurisdictions have committed to implement FATF international standards. One of the key tools of the FATF for carrying out the tasks assigned to the organization are recommendations, generally recognized international standards for combating money laundering (hereinafter - "AML") and combating the financing of

terrorism (hereinafter - "CFT"). As of 2023, there are 40 main recommendations that are designed to provide a comprehensive action plan needed for AML and 9 special recommendations that are designed to address CFT issues. They help authorities trace the funds of criminals involved in drug trafficking, human trafficking and other crimes. The FATF is constantly analyzing AML and CFT technologies, so its standards are not static, but change to ensure a response to new threats, such as the regulation of virtual assets, which are proliferating with the growing popularity of crypto-assets[5].

Since 2014, the FATF has been actively developing anti-AML standards in transactions with virtual assets, which are supplemented and updated almost annually. Thus, in June 2014, the FATF published Virtual Currencies Key Definitions and Potential AML/CFT Risks [6]. In addition, in June 2015, the FATF published Guidance on a Risk-Based Approach to Virtual Currencies (2015 Guidance on Virtual Currencies) as part of a phased approach to addressing AML and CFT risks associated with virtual asset payment products and services [7].

It should be noted that the 2015 Guidance on Virtual Currencies focus on areas where virtual asset activity intersects with the traditional regulated financial system, including virtual asset exchanges. However, in recent years the field of virtual assets has expanded to include many new products and services, business models, activities and interactions, including transactions between different types of virtual assets.

The FATF revised its Guidelines in October 2018 to specify that they also apply to financial activities involving virtual assets and added two new definitions to its Glossary: "virtual asset" and "Virtual Asset Service Provider", hereinafter - "VASP"). Revised Recommendation 15 requires VASPs to be regulated for anti-money laundering, anti-terrorist financing and anti-proliferation purposes, licensed or registered, and subject to an effective monitoring and oversight system.

In June 2019, the FATF adopted an Explanatory Note to Recommendation 15 to clarify how the FATF's requirements should apply to virtual assets and VASPs, particularly regarding the application of a risk-based approach (hereinafter - RBA) to virtual asset activities and transactions and to VASPs; supervision and monitoring of VASP for AML/CFT purposes; licensing and registration; preventive measures such as due diligence of the client, record keeping and reporting of suspicious transactions; sanctions and other law enforcement methods; as well as international cooperation [8].

Also in June 2019, the FATF adopted Guidance on the application of a risk-based approach to virtual

assets and VASPs. The guide was updated in October 2021. It is intended to assist national authorities to understand and develop regulatory and supervisory arrangements for virtual asset activities and VASPs, as well as for private sector businesses wishing to engage in virtual asset activities to understand their AML/CFT obligations and how they can meet these requirements [8].

The Guidelines emphasize the need for countries, VASPs and other businesses involved in virtual asset activities to be aware of the AML/CFT risks associated with their activities and to take appropriate measures to address these risks. As such, the Guidelines provide examples of risk indicators that should be considered separately in the context of virtual assets and highlight factors that may further confuse transactions or impede VASPs' ability to identify customers [8].

It is noted that the FATF Recommendations are a key element in defining and regulating activities with virtual assets and VASPs, as well as in combating AML/CFT risks related to virtual assets and VASPs. Almost all of the FATF Recommendations are simultaneously concerned with understanding how countries should use public authorities and international cooperation to counter AML/CFT risks related to virtual assets and VASPs, while other Recommendations are less directly or explicitly related with virtual assets and VASP, although they remain relevant and applicable [8].

To determine the role of a particular FATF Recommendation in the regulation of virtual assets, each FATF Recommendation should be considered in more detail to understand how they affect legal regulation.

Thus, Recommendation 1 [9] requires countries to take measures to prevent their associated AML/CFT risks, in particular to increase requirements for high-risk activities with virtual assets, such as P2P transactions and VASP activities. Due to the high anonymity and entanglement of financial flows in the field of virtual assets, due diligence measures and the application of monitoring may be necessary where appropriate, depending on the country context. Recommendation 1 also states the need to identify and assess risks in order to take effective measures to mitigate these risks. Countries can achieve these goals through cooperation between the public and private sectors [8].

In Recommendation 2 [9], the issue of the requirement for national cooperation and coordination between regulators, supervisory authorities, financial intelligence units and law enforcement agencies is considered. In particular, regulators should create cooperation and coordination mechanisms for the

development and implementation of effective policies and regulations aimed at addressing AML/CFT risks and the financing of the proliferation of weapons of mass destruction (hereinafter - "WMD") related to activities with virtual assets and VASP. National cooperation is important due to the high mobility and cross-border nature of virtual assets, as well as the variety of regulatory authorities that may be responsible for their regulation. In addition, national cooperation regarding the issuance of virtual assets is necessary to investigate and solve problems in the cyber and/or virtual asset ecosystem [8].

According to Recommendation 3 [9], the crime of money laundering should cover any type of property, including virtual assets, that represents criminal proceeds, regardless of their value. Therefore, countries should expand their measures against AML crimes to criminal proceeds that include virtual assets. Similarly, Recommendation 4 [9] deals with confiscation and provisional measures that apply to various types of property, including virtual assets. In a similar way, as described in Recommendation 5 [9], CFT offenses should be extended to "any funds or other assets", including virtual assets, whether from a legal or illegal source [8].

Recommendations 6 and 7 [9], which are similar to each other, relate to ensuring security by regulating virtual assets, in particular, countries should freeze funds and other assets, including virtual assets, of specified persons and institutions in the context of targeted financial sanctions that are related to terrorism and CFT. These measures are aimed at preventing the access of certain persons and institutions to frozen funds and other assets [8].

Recommendation 8 [9] concerns the protection of non-profit organizations from their use for the purpose of financing terrorism, including when the secret non-targeted transfer of funds to terrorist organizations includes virtual assets [8].

Recommendation 9 [9] aims to ensure that secrecy laws do not impede the implementation of FATF recommendations. As with financial institutions, the country must ensure that secrecy laws do not impede the implementation of FATF VASP, although Recommendation 9 does not directly refer to VASP [8].

Recommendation 10 [9], aimed at developing a process of performing customer due diligence for VASPs and other entities dealing with virtual assets. This process should assist in the assessment of AML/CFT risks associated with activities involving virtual assets, business relationships or transfers exceeding the threshold amount in accordance with the Explanatory Note to Recommendation 15 paragraph 7(a) this amount is 1000 USD/EUR. The

process includes identifying the customer and the beneficial owner, verifying the customer's identity for risk and reliable documentation, and understanding the objective and predictable nature of the business relationship. As stated in the Explanatory Note to Recommendation 10, there are conditions when the risk of AML/CFT is increased and when enhanced (Customer Due Diligence, hereinafter - «CDD») is required. In the context of virtual asset and VASP activities, countries should consider specific geographic risk factors. For example, whether the VASP is located in, or the transaction with virtual assets takes place with participation in, a country that presents a potentially increased risk of AML/CFT (Explanatory Note to Recommendation 10, paragraph 15(b)).

Recommendation 11 [9] requires states to ensure that VASPs maintain and store records of all CDD operations and activities during the past five years. Such storage of records should help in the reconstruction of individual operations and the rapid forwarding of the necessary elements to the competent authority [8].

Recommendation 12 [9] requires states to implement measures that require accountable entities, in particular VASPs, to have appropriate risk management systems in place to determine whether customers or beneficial owners are politically exposed persons (PER) ) or related to foreign PEP. If so, they should take additional steps beyond the usual CDD to determine whether they have a business relationship with them, including identifying sources of funding if necessary [8].

Recommendation 13 [9] stipulates that countries should require financial institutions to take certain measures in addition to normal CDD measures when entering into cross-border correspondent relationships. Correspondence applies to VASPs and means the provision of VASP services to one VASP to another VASP or to a financial institution. Correspondent relationships in the VASP sector may have characteristics similar to cross-border correspondent banking relationships and should include measures to reduce the ML/TF risks associated with such relationships. Such activities include gathering information about the other VASP or interacting financial institution, assessing AML/CFT controls, obtaining senior management approval for establishing new cross-border correspondent relationships, and conducting CDDs on customers of the other VASP or financial institution using accounts or custodians wallets for conducting business in the client's own name [8].

Recommendation 14 [9] directs countries to register and license individuals and legal entities that provide services for the transfer of funds or valuables and to

ensure their compliance with relevant AML/CFT measures. However, the registration and licensing requirements of Recommendation 15 [9] apply to all VASPs, even those involved in money or value transfer services (for example, domestic entities that provide as business-converted services exchange of virtual assets between virtual and fiat currencies in the jurisdiction) [8].

FATF Recommendation 15 [9] plays a significant role in the regulation of virtual assets. The Recommendation requires countries to manage and mitigate the risks arising from virtual assets and to ensure VASP regulation for AML/CFT purposes, their licensing or registration; supervision or monitoring; preventive measures such as CDD, record keeping and reporting of suspicious transactions; sanctions and other law enforcement measures; as well as international cooperation [8].

Recommendation 16 [9], also known as the "travel rule", applies to all bank transfer providers. This includes VASPs that provide services or engage in activities such as virtual asset transfers that are functionally similar to bank transfers. The FATF requires VASPs and financial institutions that transfer virtual assets to collect necessary and accurate information about the sender and necessary information about the beneficiary and to share it with counterparties of VASPs or financial institutions during or before the transaction. The requirements of Recommendation 16 apply to VASPs when their transactions, whether in fiat currency or virtual assets, include: a traditional wire transfer, a transfer of virtual assets between a VASP and another obligated entity (for example, a VASP or between a VASP and another by an obligated entity, for example, a bank or other FI, or the transfer of virtual assets between a VASP and an unobligated entity (for example, a non-hosting wallet) [8].

As previously noted, the FATF recommends that countries adopt a minimum threshold of USD/EUR of 1,000 for virtual asset transfers. For virtual asset transfers below the threshold amount, VASPs must collect: the name of the sender and beneficiary (recipient), the virtual asset wallet address for each, or a unique transaction reference number. Such information does not need to be verified if there is no suspicious AML/CFT activity. For transfers exceeding the minimum threshold, VASPs must collect: the sender's name; the sender's account number, when such an account is used to process the transaction; sender's address, or national identification number, or customer identification number, or date and place of birth; the name of the beneficiary and the beneficiary's account number when such an account is used to process the transaction [8]. According to the FATF Targeted Update on the Implementation of the FATF Standards on Virtual Assets and VASPs, as of

March 2022, 29 out of 98 jurisdictions reported that they had adopted "travel rule" legislation, while only 11 jurisdictions had begun to implement enforcement and supervisory measures [10].

Recommendation 17 [9] enables countries to allow accountable entities to rely on third parties, including VASPs, to conduct business and/or perform part of the CDD processes, including customer identification and verification. In the context of third-party VASPs states and accountable entities should consider the risks that third parties may pose, the nature of business activities and operations, the customer base or target market of the third-party VASPs and, where appropriate, their business partners.

Recommendation 18 [9] obliges countries to require accountable entities, such as VASPs, to have internal control mechanisms to ensure the effectiveness of policies and processes, as well as AML/CFT, as well as high-quality risk management during operations. Internal control should include appropriate governance mechanisms where AML/CFT responsibility is clearly allocated and the responsible person is appointed at board level; integrity control of personnel, which is implemented in accordance with current national legislation; continuous training of personnel; and independent audits (external or internal) to verify the system.

Recommendation 19 [9] obliges countries to require accountable entities, such as VASPs, to apply Enhanced due diligence (hereinafter - EDD) measures for business relationships and transactions conducted with natural or legal by individuals from high-risk countries, which include countries for which FATF requires EDD measures to be taken. This is particularly important for virtual asset activities and VASPs, given the cross-border nature of their activities.

Recommendation 20 [9] requires all financial institutions and VASPs that suspect or have reasonable grounds to believe that funds are proceeds of crime or related to the financing of terrorism to immediately report their suspicions to the appropriate financial intelligence unit. To do this, VASPs must submit suspicious transaction reports to the Financial Intelligence Unit.

Recommendation 21 [9] deals with disclosure and confidentiality measures applicable to financial institutions and VASPs. Accordingly, VASP, its directors, officers and employees shall be protected by law from criminal and civil liability for violations of any disclosure provisions and prohibitions against disclosure of suspicious transaction reports.

Recommendations 24 and 25 [9] state that states should take measures to prevent the use of legal

entities, including VASPs, for AML/CFT, and consider implementing measures that facilitate access to beneficial ownership information and the exercise of control over VASPs.

Recommendations 26 and 27 [9], paragraph 5 of the Explanatory Note to Recommendation 15 states that VASPs are subject to appropriate AML/CFT regulation and supervision or monitoring. Supervision or monitoring under VASP should be carried out by competent authorities, not self-regulatory bodies, which should conduct risk-based supervision or monitoring. Supervisory authorities should have adequate powers to supervise VASPs and ensure compliance with AML/CFT requirements, including the power to conduct inspections, inspect books and records, require information, impose disciplinary and economic sanctions, including the power to revoke, limit or suspend a VASP license or registration.

Recommendation 29 [9] states that suspicious transaction reports sent to the VASP under Recommendation 20 [9] should be referred to the Financial Intelligence Unit. In addition, FIUs should have access to additional information from reporting entities within their jurisdiction (including VASPs), and they should have timely access to financial, administrative and law enforcement information that FIUs may request to properly perform their functions. Recommendation 30 [9] applies to virtual asset activities and VASPs to the extent that it covers all terms relating to money or value such as "property", "income", "funds", "money and other assets", as well as other "equivalent value", which include virtual assets. States should ensure that competent authorities are responsible for promptly identifying, tracking and taking measures to freeze and seize property related to virtual assets that can be confiscated or are suspected of being the proceeds of criminal activity.

Recommendation 31 [9] states that States and competent authorities should have access to all necessary documents and information, including the power to use coercive measures, to draw up reports maintained by VASPs. They must have effective mechanisms to detect whether a natural or legal person, such as a VASP, maintains or controls virtual asset accounts or wallets, and mechanisms to ensure that competent authorities have operational processes in place to detect assets, including virtual assets, without prior notification to the owner.

Recommendation 32 [9] that jurisdictions should consider in their RBAs whether VASP activities and virtual asset activities fall within the parameters of the transportation of physical monetary instruments and how they will work in practice in terms of declarations and systems to detect cross-border movements of assets, and how they will reduce AML/CFT risk in their jurisdiction.

Recommendation 33 [9] specifies that countries should keep statistics on reports of suspicious transactions in the context of virtual assets, as well as on frozen, seized and confiscated property related to criminal activities. For better investigation and financial analysis, countries should consider updating suspicious transaction reports and statistics with indicators related to virtual assets.

Recommendation 34 [9] is an important part of States' approach to identifying and addressing AML/FT risks associated with virtual asset activities and VASPs, as well as virtual assets themselves. The relevant competent authorities should develop guidance and provide feedback to assist VASPs in the application of national AML/CFT measures, including the detection and reporting of suspicious transactions – regardless of whether the transaction is virtual/fiat or virtual/virtual assets.

Recommendation 35 [9] requires states to introduce a range of effective, proportionate and dissuasive sanctions (criminal, civil or administrative) against individuals or legal entities subject to Recommendations 6 and 8-23 and who fail to comply with the necessary requirements of the AML/ FT. According to paragraph 6 of the Explanatory Note to Recommendation 15, countries should similarly have sanctions in place to deal with VASPs (and other accountable entities involved in virtual asset activities) who fail to meet their AML/CFT obligations. As with financial institutions and specified non-financial institutions and professions, and other natural and legal persons, similar sanctions apply not only to VASPs, but also to their directors and officers, where appropriate.

Recommendations 36-40 [9], concerning international cooperation and implementation of measures to combat criminal activities related to virtual assets and VASP. Recognizing that effective regulation, supervision and enforcement in the area of VASP requires a global approach and the level of regulatory systems in jurisdictions, States should, *inter alia*, have the tools necessary to cooperate with each other, provide mutual legal assistance (Recommendation 37); assist in investigations, freeze, recover and confiscate proceeds of crime and instruments that may be in the form of virtual assets as well as other traditional assets related to VASP activities (Recommendation 38); provide effective extradition assistance in the context of crimes involving virtual assets or actors outside the law engaging in illegal activities (Recommendation 39).

Therefore, almost all FATF Recommendations are directly related to virtual assets in one way or another. The Recommendations describe in detail how virtual assets and VASPs should be regulated, in particular, the Recommendations oblige VASPs to comply with

certain norms and requirements, which include registration and licensing, monitoring and supervision of financial transactions, identification of customers and tracking of their transactions, informing authorities about suspicious transactions, international cooperation.

It should be noted that FATF recommendations are "soft law", that is, they do not have binding legal force. Not transferring them to an international agreement was a deliberate step. This was done to avoid lengthy ratification procedures and facilitate the adaptation of the recommendations. However, they have a significant political influence on the formation and counteraction of the legalization of income obtained through criminal means [11, p. 119-125]. In practice, countries that do not comply with the Recommendations face serious financial and economic consequences. The FATF maintains a "black list" and a "grey list" of countries that do not comply with their Recommendations [12]. As countries update their AML/CFT regulatory systems in line with FATF recommendations and requirements, they are added to or removed from these lists. Given the regulatory risk associated with countries that do not comply with international compliance standards, financial institutions and VASPs should be aware of FATF blacklisted and graylisted countries and the implications of such classification. Inclusion on these lists often results in lower bond ratings and greater difficulty connecting to the international banking system, making international trade and inward investment more difficult. As a result, most countries are trying to implement these Recommendations as soon as possible.

FATF recommendations are guided by international organizations and governments of many countries around the world, implementing AML/FT standards in the field of virtual assets and the VASP sector. The leaders of the G20 countries, based on the results of the meeting on February 22-23, 2020, called on the states to apply the new FATF recommendations regarding virtual assets and relevant market operators [13]. The recommendations of the FATF became the reason for making changes to "Directive (EU) 2018/843 of the European Parliament and the Council of 30.05.2018 "On making changes to Directive (EU) 2015/849 on preventing the use of the financial system for the purposes of money laundering and terrorist financing and introducing amendments to Directives 2009/138/EU and 2013/36/EU" (hereinafter - 5AMLD) (clause 4) [14]. However, compared to the FATF recommendations, the scope of application of 5AMLD to virtual asset transactions is narrower. It is also stated in the Preamble of MiCA that the legislation of the European Union should contribute to the fight against AML/CFT. With this in

mind, any definition of "crypto-assets" should be consistent with the definition of "virtual assets" set out in the FATF Recommendations [15].

As already mentioned, the FATF Recommendations provide for bringing national AML/CFT systems into compliance with international standards. Ukraine is no exception, where legal regulation of the circulation of virtual assets in the direction of AML/CFT is its European integration obligation. Thus, in accordance with Article 20 of the Association Agreement between Ukraine and the EU, the European Atomic Energy Community and their member states, Ukraine undertakes to ensure the implementation of relevant FATF international standards and standards equivalent to those adopted by the EU [16]. In particular, in order to fulfill these requirements, on December 6, 2019, the Verkhovna Rada of Ukraine adopted a new version of the Law of Ukraine "On Prevention and Combating Legalization (Laundering) of Income." This Law, among other things, enshrines: The legal status of a virtual asset for the purposes of the AML, in particular, paragraph 13 of the first part of Article 1 defines "a virtual asset as a digital expression of value that can be traded in digital format or transferred and that can be used for payment or investment purposes" [17]. This very definition of a virtual asset is a literal translation of the definition proposed by the FATF [9].

### III. CONCLUSION

Therefore, having analyzed all of the above, it can be stated that the Recommendations of the Financial Action Task Force on Money Laundering are a necessary tool for the effective regulation of virtual assets, and are also an important element of international cooperation in the fight against the financing of terrorism and other illegal activities. In its recommendations, the FATF defined the concept of "virtual assets", which is contained in international acts such as 5AMLD and MiCA, requiring member countries to establish a regulatory framework to regulate virtual assets and virtual asset service providers. And some countries have already introduced into their legislation norms that correspond to the main FATF Recommendations in the regulation of virtual assets.

### REFERENCES

- [1] FATF (2018). FATF Report to G20 Finance Ministers and Central Bank Governors, FATF, Paris, France. URL: [www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html](http://www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-fm-cbg-july-2018.html).
- [2] Vandezande N. Virtual currencies under EU antimoney laundering law. *Computer Law & Security Review*. 2017. p. 33. URL: <https://doi.org/10.1016/j.clsr.2017.03.011>.
- [3] FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems URL: <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html>.

- [4] Countries FATF URL: <https://www.fatf-gafi.org/en/countries/fatf.html>.
- [5] Guide for judges on combating money laundering (laundering), 2021. URL: [http://www.nsj.gov.ua/files/1630574896%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D1%89%D0%BE%D0%B4%D0%BE%20%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97%20%D0%B2%D1%96%D0%B4%D0%BC%D0%B8%D0%B2%D0%B0%D0%BD%D0%BD%D1%8E%20%D0%BA%D0%BE%D1%88%D1%82%D1%96%D0%B2%202021%20%D0%A0%D0%84\\_%D0%9D%D0%A8%D0%A1%D0%A3.pdf](http://www.nsj.gov.ua/files/1630574896%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D1%89%D0%BE%D0%B4%D0%BE%20%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97%20%D0%B2%D1%96%D0%B4%D0%BC%D0%B8%D0%B2%D0%B0%D0%BD%D0%BD%D1%8E%20%D0%BA%D0%BE%D1%88%D1%82%D1%96%D0%B2%202021%20%D0%A0%D0%84_%D0%9D%D0%A8%D0%A1%D0%A3.pdf).
- [6] Financial Action Task Force (FATF). Virtual Currencies Key Definitions and Potential AML/CFT Risks. 2014. 15 p. URL: <https://www.fatf-gafi.org/en/publications/Methodsandrends/Virtual-currency-definitions-aml-cft-risk.html>.
- [7] Guidance for a Risk-Based Approach to Virtual Currencies 2015. URL: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html>.
- [8] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>.
- [9] The FATF Recommendations URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>.
- [10] Targeted Update on Implementation of FATF's Standards on VAs and VASPs URL: <https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html>.
- [11] Gaevskiy I.M. European anti-money laundering legislation: formation and development. Scientific bulletin of public and private law. 2016. No. 3. P. 119-125. URL: <http://www.nvppp.in.ua/vip/2016/3/27.pdf>.
- [12] «Black and grey» lists FATF URL: <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>.
- [13] G20 Leaders support the FATF's work to address money laundering and terrorist financing risks 2020 URL: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/G20-riyadh-summit.html>.
- [14] Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU; Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. Official Journal of the European Union. 2018. Vol. 61. P. 43–74. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843>.
- [15] European Commission (2019) Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937 COM/2020/593 final URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>.
- [16] Association Agreement between the European Union and the European Atomic Energy Community and their member states, of the one part, and Ukraine, of the other part: International agreement dated June 27, 2014 No. 984\_011. URL: [https://zakon.rada.gov.ua/laws/show/984\\_011](https://zakon.rada.gov.ua/laws/show/984_011).
- [17] On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction (The Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2020, No. 25, Article 171). URL: <https://zakon.rada.gov.ua/laws/show/361-20>.

\*\*\*