



БЪЛГАРСКА
НАРОДНА БАНКА

**Насоки за банките относно превенция на изпирането на пари и финансирането на
тероризма и финансирането на пролиферацията, във връзка с извършването на
дейности с виртуални активи (криптоактиви)**

Настоящите Насоки са приети от Управителния съвет на Българската народна банка с Решение № 606 от 8.12.2025 г. на основание чл. 73, ал. 4, във връзка с ал. 1, т. 11 от Закона за кредитните институции, като са относими към чл. 108, ал.6, т.1, б. а) от ЗМИП, чл. 14а, ал. 2, т. 1 буква „а“, от Закона за мерките срещу финансирането на тероризма и на разпространението на оръжия за масово унищожение, Насоки относно рискови фактори ИП/ФТ (ЕВА/GL/2024/01), Секторна оценка на рисковете от ИП/ФТ, свързани с виртуални активи.

Декември 2025 г.

Съдържание

Съкращения.....	3
I. Въведение.....	4
1. Цел и обхват	4
2. Рамка (международна и национална).....	4
3. Ключови дефиниции.....	6
II. Идентифициране и оценка на рисковете, свързани с криптоактиви	9
1. Обхват на дейностите по регламента MiCA.....	9
2. Рисковобазирен подход.....	9
III. Мерки за комплексна проверка	11
1. Идентификация и проверка на идентификацията.....	11
2. Събиране на информация и оценка на целта и характера на деловите взаимоотношения.....	11
3. Изясняване на произхода на средствата и източника на имуществено състояние	12
4. Текущо наблюдение.....	12
5. Мерки за опростена комплексна проверка	15
6. Мерки за разширена комплексна проверка	15
IV. Съхраняване на информацията, разкриване на информацията и обучение	17
1. Съхраняване на информация	17
2. Обучение.....	17
3. Установяване и докладване на съмнителни операции	18
Приложение 1 – Рискови индикатори (червени флагове) за ИП/ФТ/ФП с КА	19
Приложение 2 - Полезна информация по въпроси, касаещи прехвърлянията на КА и смекчаващи мерки за риска от ИП/ФТ/ФП при прехвърляне на КА - Прехвърляния на криптоактиви / правила за пътуване / travel rule.....	20
Библиография на документи (насоки, мнения, доклади)	21

Съкращения

БИП/БФТ	Борба с изпиране на пари/Борба с финансиране на тероризма
БНБ	Българска народна банка
ВА/КА	Виртуален актив (термин, използван в международния стандарт) / криптоактив (термин, използван в законодателството на ЕС); еквивалентността на термините е посочена в т. I (т.1 и т.3)
ВПЛ	Видна политическа личност
Директива (ЕС) 2015/849	Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20 май 2015 година за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма, за изменение на Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета и за отмяна на Директива 2005/60/ЕО на Европейския парламент и на Съвета и на Директива 2006/70/ЕО на Комисията
ДУВА/ДУКА	Доставчик на услуги за виртуални активи/Доставчик на услуги за криптоактиви; еквивалентността на термините е посочена в т. I (т.1 и т.3)
ЕБО	Европейски банков орган
ЗКИ	Закон за кредитните институции
ЗМИП	Закон за мерките срещу изпирането на пари
ЗМФТ / ЗМФТРОМУ	Закон за мерките срещу финансирането на тероризма / Закон за мерките срещу финансиране на тероризма и на разпространението на оръжия за масово унищожение
ЗПКА	Закон за пазарите за криптоактиви
ЗПУПС	Закон за платежните услуги и платежните системи
ИП/ФТ	Изпиране на пари и финансиране на тероризма
Регламент (ЕС) 2024/1624	Регламент (ЕС) 2024/1624 на Европейския парламент и на Съвета от 31 май 2024 година за предотвратяване на използването на финансовата система за целите на изпирането на пари или финансирането на тероризма
ЦФС за ФТ и ФП	Целеви финансови санкции за финансиране на тероризъм и финансиране на пролиферацията
DLT/ТДР	Distributed ledger technology / Технология на децентрализирания регистър
FATF	Financial Action Task Force / Група за финансови действия срещу изпирането на пари - Международна организация, учредена по инициатива на Г7 през 1989 г., която разработва и следи за прилагане на политики за борба с изпирането на пари; в последствие мандатът ѝ е разширен и за борба с финансирането на тероризма (2001 г.), с финансиране на пролиферацията (2008 г.)
MiCAR	Регламент (ЕС) 2023/1114 на Европейския парламент и на Съвета от 31 май 2023 година относно пазарите на криптоактиви и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на директиви 2013/36/ЕС и (ЕС) 2019/1937
TFR	Регламент (ЕС) 2023/1113 на Европейския парламент и на Съвета от 31 май 2023 година относно информацията, придружаваща преводите на средства и прехвърлянията на определени криптоактиви, и за изменение на Директива (ЕС) 2015/849

I. Въведение

1. Цел и обхват

Понятията за „виртуални валути“ и потенциалните рискове от изпиране на пари/финансиране на тероризъм (ИП/ФТ), свързани с тях, са въведени от FATF през 2014 г.¹ През 2018 г.² в речника на FATF се въвеждат две нови дефиниции: „виртуален актив“ и „доставчици на услуги за виртуални активи“ – ВА и ДУВА и се прави допълнение в Препоръка 15 на FATF.

Понятията криптоактиви (КА) и доставчици на услуги за криптоактиви (ДУКА) са въведени през 2020 г. във връзка с работата по проекта на европейската законова рамка (MiCAR и TFR)³, приложима за държавите-членки на ЕС, официално публикувана през 2023г.

Съображение 10 от Преамбюла на TFR⁴ извежда еквивалентност на понятията КА и ВА, както и ДУКА и ДУВА, въведени от препоръките на FATF и европейската законодателна рамка.

Препоръките на FATF имат за цел да послужат като глобална рамка, която страните трябва да прилагат за борба с ИП/ФТ/ФП. С новата законодателна европейска рамка MiCAR и TFR от 2023 г. и т.нар. нов ИП/ФТ пакет от 2024 г. ЕС въвежда термина криптоактив (cryptoasset (CA)) и изискване за лицензионен режим за ДУКА. Услугите за КА, дефинирани в MiCAR, се припокриват с услугите за ВА, дефинирани от FATF, като в обхвата на лицензионния режим по регламента е добавена и услугата „предоставяне на съвет за криптоактиви“ (за която не се изисква лиценз/регистрация при FATF).

Насоките са с фокус към банки, които имат намерение да разширят лиценза си с предоставяне на услуги, свързани с криптоактиви, както и банки, които имат/ще имат клиенти, които са ДУКА.

2. Рамка (международна и национална)

2.1. Групата за финансови действия срещу изпирането на пари (FATF)

В настоящия документ са взети предвид стандартите и насоките, издадени от FATF, добри практики в отрасъла и индикатори за съмнителна дейност.

През 2019 г. FATF е извърши актуализация на стандарта за ВА и ДУВА съгласно Препоръка 15, за да се определи и изясни начинът, по който да се прилагат изискванията за превенция на ИП/ФТ по отношение на виртуалните активи и доставчиците на услуги за виртуални активи⁵.

¹ Транспонирани в ЕС с 5-та ИП/ФТ Директива (Директива (ЕС) 2015/849) и ЗМИП от 2019 г.

² Транспонирани в ЕС с MiCAR, TFR и новия ИП/ФТ пакет на ЕС, а на национално ниво с промени в секторното законодателство, вкл. нов ЗПКА и промени в специалните закони ЗМИП и ЗМФТРОМУ.

³ MiCAR (Markets in Crypto-Assets Regulation) - Регламент (ЕС) 2023/1114 на ЕС относно пазарите на криптоактиви; с него е приета и съпътстваща регулация - TFR (Transfer of Funds Regulation) - Регламент (ЕС) 2023/1113 на ЕС относно информацията, придружаваща преводите на средства и прехвърлянията на определени криптоактиви. Двата регламента са публикувани през 2023 г. и влизат в сила от 30.12.2024 г., които са транспонирани със Закона за пазарите на криптоактиви, **обнародван в ДВ 54/04.07.2025 г.**

⁴ Съответствие на определенията за криптоактиви в Регламент (ЕС) 2023/1114 и определенията за виртуални активи, съдържащо се в преработените препоръки на FATF; списъкът на обхванатите от посочения регламент услуги за криптоактиви и доставчици на услуги за криптоактиви обхваща и доставчиците на услуги за виртуални активи.

⁵ Ревизията на Препоръка 15 се отнася до текста на препоръката, тълкувателна бележка към нея и критерии по препоръката от Методологията за оценка: 15. 3 Оценката на риска и рисковобазирания подход; 15.4 Лицензиране/Регистриране на ДУВА; 15.5 Идентификация на физически/юридически лица, извършващи дейност като ДУВА; 5.9 Превантивни мерки за борба с изпирането на пари и финансирането на тероризма, включително „правилото за пътуване“ (Travel Rule); 15.8 ДУВА и висшестоящи служители на ДУВА са обект на пропорционални и разубеждаващи санкции, при неспазване на изискванията за ИП/ФТ; 15.10 Спазване на целеви финансови санкции; 15.6 Надзор и регулиране на ДУВА; 15. 11 Международно сътрудничество.

В библиографията към настоящите Насоки са описани документите по текущата работа на FATF по Препоръка 15 относно новите технологии и насърчаване на държавите за спазването на препоръката, като през 2025 г. е публикуван последният доклад за съответствие на препоръката от страна на юрисдикциите (предоставя и актуална информация за нововъзникващите рискове и развитието на пазара, свързани с използването на ВА за целите на ИП/ФТ и финансиране разпространението на оръжия (финансиране на пролиферацията)).

Превантивните мерки, посочени в препоръки 10-21 на FATF, се прилагат за ДУВА по същия начин като за финансовите институции, с две особености - определеният праг за случайни сделки, над който ДУВА са длъжни да извършват комплексна проверка, е 1 000 USD/EUR (а не 15 000 USD/EUR) и правилата за банкови преводи, посочени в препоръка 16 на FATF, се прилагат за ДУВА и прехвърляния на виртуални активи ("правилото за пътуване" – travel rule).

2.2. Европейска рамка

С Регламент (ЕС) 2023/1114 от 31.05.2023 г.⁶ г. се въвежда лицензионен режим за дружествата, които издават и предлагат публично или искат да бъдат допуснати до платформа за търговия на токени, обезпечени с активи (asset-referenced tokens (ART)) и токени за електронни пари (e-money tokens (EMT)), както и за извършването на дейност като доставчици на услуги за криптоактиви (Crypto assets service providers (CASP)). Регламентът допуска тези дейности да бъдат изпълнявани от кредитните институции, но дейностите за КА трябва да бъдат включени в банковия ѝ лиценз.

С цел да подпомогне прилагането на MiCAR, Европейският парламент и Съвета на ЕС приемат и Регламент за прехвърляне на средства (Transfer of Funds Regulation (TFR)). Този Регламент изисква от доставчиците на криптоактиви да идентифицират ясно своите клиенти чрез процеса „Опознай клиента си“ (Know your customer (KYC)), който е основополагащ за БИП/БФТ. Регламентът TFR се основава и на изискването за прозрачност на плащанията (Препоръка 16) или т.нар. „Travel Rule“ (TRP) на FATF. Основният ангажимент за задължените лица в съответствие с TFR е създаването на ефективни процедури за постигане на прозрачност на преводите на средства и прехвърлянията на криптоактиви, което включва проверка, получаване (при необходимост) и съхраняване на пълна информация за инициатора и бенефициера.

Тази законодателна рамка предвижда строги административни санкции, включително отнемане на лиценз за извършване на дейност като ДУКА, ако задълженото лице не разполага с ефективни системи, процедури и механизми за откриване и предотвратяване на ИП/ФТ в съответствие с Директива (ЕС) 2015/849.

2.3. Национално законодателство

В ЗМИП доставчиците на виртуални валути и на портфейли, които предоставят попечителски услуги⁷ са въведени първоначално като задължени лица от 2019 г. и са обект на регистрационен режим⁸, като с приемането на Закона за пазарите на криптоактиви (ЗПКА)⁹ режимът се трансформира в лицензионен. ЗПКА регламентира лицензионен режим на дейностите по издаване на токени, обезпечени с активи (asset-referenced tokens), токени за електронни пари (e-money tokens) и/или извършване на дейности като доставчици на услуги за криптоактиви.

⁶ В сила от 30.12.2024 г.

⁷ чл. 4, точки 38 и чл. 39.

⁸ Наредба № Н-9/07.08.2020 г. на МФ.

⁹ Обнародван на 04.07.2025 г. с ДВ, бр. 54.

Във връзка със ЗПКА измененията и допълненията в ЗМИП са свързани с въвеждането на новите понятия за „криптоактиви“, „издатели на криптоактиви“, „доставчици на услуги за криптоактиви“ и др.¹⁰. Контролът по прилагането на ЗМИП ще бъде извършван от Българска народна банка (за банки, чийто лиценз включва дейности по ЗПКА), Комисия за финансов надзор (за други дружества, лицензирани по ЗПКА, които не са банки) и дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“ (за всички доставчици на услуги за криптоактиви).

3. Ключови дефиниции

За целите на настоящите насоки в речника на термините по-долу са показани понятията, които използва FATF и тези, дефинирани в MiCAR (последните са залегнали и в местното законодателство (ЗПКА, ЗМИП, ЗКИ и др.)

Използвано определение	Дефиниции FATF	Дефиниции MiCAR/TFR
Виртуални активи/ Криптоактиви	Виртуални активи представляват цифрово представяне на стойност, която може да се търгува цифрово или прехвърляна и може да се използва за разплащане или за инвестиционни цели. Виртуалните активи не включват цифрово представяне на фиатни валути, ценни книжа и други финансови активи, които са обхванати на други места в препоръките на FATF. FATF Glossary	Криптоактиви - цифрово представяне на стойност или право, което може да бъде прехвърляно и съхранявано електронно посредством технология на децентрализирания регистър или друга подобна технология ¹¹ . Определения Дял I, чл. 3, ал. 1, т. 7 от Регламент (ЕС) 2023/1114
Доставчик на услуги за виртуални активи/ криптоактиви	Физическо или юридическо лице, което не е обхванато от други разпоредби на Препоръките и което в качеството си на предприятие извършва една или повече услуги за виртуални активи за или от името на друго физическо или юридическо лице. FATF Glossary	Юридическо лице или друго предприятие, чието занятие или предмет на стопанска дейност е предоставянето на професионална основа на една или повече услуги за криптоактиви на клиенти. Определения Дял I, чл. 3, ал. 1, т. 15 от Регламент (ЕС) 2023/1114
Услуги за виртуални активи/ криптоактиви	1) Обмен между виртуални активи и фиатни пари; 2) Обмен между една или повече форми на виртуални активи; 3) Прехвърляне на виртуални активи	1) Предоставяне на попечителство и администриране на криптоактиви от името на клиенти; 2) Управление на платформа за търговия с криптоактиви; 3) Обмен на криптоактиви срещу

¹⁰ В чл. 4, точки 38 и 39 от ЗМИП се заличават и се заменят с нова т.19 от същия член - доставчиците на услуги за криптоактиви, получили лиценз по ЗПКА, с изключение на дейността им по предоставяне на съвети относно криптоактиви; оценява се риска от ИП/ФТ прехвърляния на криптоактиви, насочени към или произхождащи от самостоятелно хостван адрес от ДУКА (чл.20а); въвеждат се изисквания за установяване на кореспондентски отношения, включващи извършването на услуги за криптоактиви (чл.44а) и др.

¹¹ В определението на криптоактивите се обхващат и токените за електронни пари, съгласно член 2, точка 2 от Директива 2009/110/ЕО (парична стойност, съхранявана в електронна, включително магнитна форма...").

Използвано определение	Дефиниции FATF	Дефиниции MiCAR/TFR
	¹²; 4) Съхранение и/или управление на виртуални активи или инструменти, позволяващи контрол върху виртуални активи; 5) Участие в и предоставяне на финансови услуги, свързани с предлагането и/или продажбата на виртуален актив от страна на емитент. FATF Glossary	средства; 4) Обмен на криптоактиви срещу други криптоактиви; 5) Изпълняване на нареждания, свързани с криптоактиви, от името на клиенти; 6) Пласиране на криптоактиви; 7) Получаване и предаване на нареждания, свързани с криптоактиви, от името на клиенти; 8) Предоставяне на съвет относно криптоактиви¹³; 9) Предоставяне на управление на портфейл, свързано с криптоактиви; 10) Предоставяне на услуги за прехвърляне на криптоактиви от името на клиенти. Определения Дял I, чл. 3, ал. 1, т. 16 от Регламент (ЕС) 2023/1114
Технология на децентрализирания регистър (ТДР)	Технологичен протокол, който позволява едновременен достъп, валидиране и актуализиране на цифров запис между множество компютри (и обикновено в множество обекти или местоположения) https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html FATF/OECD 2021	Технология, която позволява функционирането и използването на децентрализирани регистри (информационно хранилище за съхранение на записи на трансакции, което се споделя между мрежови възли, основани на ТДР и се синхронизира между тях на базата на механизъм за консенсус. Механизъм за консенсус означава правилата и процедурите, чрез които се постига съгласие между мрежови възли, основани на ТДР, за валидиране на трансакция, а мрежов възел, основан на ТДР означава устройство или процес, които са част от мрежа и които съдържат пълно или частично копие на записи за всички трансакции в децентрализиран регистър) Определения Дял I, чл. 3, ал. 1, т. 1, 2, 3 и 4 от Регламент (ЕС) 2023/1114
Стабилни криптопари/stablecoins	Основната отличителна черта на така наречените стейбълкойни е, че тяхната стойност е предназначена да бъде стабилна в сравнение с тази на	Когато даден криптоактив попада в обхвата на определението за токен, обезпечен с активи, или токен за електронни пари се прилага дял III

¹²Прехвърляне означава извършване на трансакция от името на друго физическо или юридическо лице, при която се прехвърля виртуален актив от един адрес или сметка за виртуални активи в друга.

¹³ДУКА, които предоставят само съвет относно КА, са обект на лицензионен режим в Р България на основание ЗПКА, но не са задължено лице по ЗМИП (§ 1, т. 33 от ДР на ЗМИП).

Използвано определение	Дефиниции FATF	Дефиниции MiCAR/TFR
	базов актив или бенчмарк. Стойността на стейбълкойн може да бъде обвързана например със стойността на фиатна валута или кошница от активи, която може да включва фиатни валути, цифрови валути, инвестиционни ценни книжа, стоки и/или недвижими имоти. Стейбълкойн може също да използва алгоритмични средства за стабилизиране на пазарната си стойност. FATF (2020), FATF Report to the G20, FATF, France, www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.htm	или IV MiCAR, независимо от начина, по който издателят възнамерява да проектира криптоактива, включително механизма за поддържане на стабилна стойност на криптоактива. Това се отнася и за т.нар. алгоритмични „стабилни криптопари“¹⁴, при които е налице стремеж стойността да се поддържа стабилна по отношение на официална валута или по отношение на един или няколко актива посредством протоколи, които водят до нарастване или свиване на предлагането на такива криптоактиви в отговор на промени в търсенето Съображение 41 от Преамбюла Регламент(ЕС) 2023/1114
Дигитална валута / digital currency	Цифрово представяне на виртуална валута (нефиатна) или електронни пари и поради това често се използва взаимнозаменяемо с термина виртуална валута https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf	Цифровите активи, които не могат да бъдат прехвърлени на други държатели, не попадат в обхвата на определението за криптоактиви. Поради това цифровите активи, които се приемат само от издателя или от предложителя и които е технически невъзможно да бъдат прехвърлени пряко на други държатели, следва да бъдат изключени от обхвата на настоящия регламент. Съображение 17 от Преамбюла Регламент (ЕС) 2023/1114
Токени, обезпечени с активи		Вид криптоактив, който не е токен за електронни пари и при който е налице стремеж за поддържане на стабилна стойност чрез обвързването ѝ с друга стойност или право, или комбинация от тях, включително една или повече официални валути Определения Дял I, чл. 3, ал. 1, т. 6 от Регламент (ЕС) 2023/1114
Токени за електронни пари		Вид криптоактив, който има за цел да поддържа стабилна стойност чрез обвързването ѝ със стойността на дадена официална валута (валута, която се емитира от централна банка

¹⁴ MiCAR засяга предимно емитентите на т.нар. „стабилни монети“.

Използвано определение	Дефиниции FATF	Дефиниции MiCAR/TFR
		или друг паричен орган Определения Дял I, чл. 3, ал. 1, т. 6 от Регламент (ЕС) 2023/1114
Самостоятелно хостван адрес / „self-hosted address“		Адрес в децентрализирания регистър, който не е свързан с никое от следните: а) доставчик на услуги за криптоактиви; б) субект, който не е установен в Съюза и предоставя услуги, подобни на тези, предоставяни от доставчик на услуги за криптоактиви Определения Дял I, чл. 3, ал. 1, т. 20 от Регламент (ЕС) 2023/1113

II. Идентифициране и оценка на рисковете, свързани с криптоактиви

1. Обхват на дейностите по регламента MiCA

MiCA се прилага за издаването, публичното предлагане и допускането до търговия на криптоактиви, както и за предоставянето на услуги, свързани с криптоактиви. Той разграничава следните видове криптоактиви: токени за електронни пари (криптоактиви, които стабилизират стойността си по отношение на единна официална валута); токени, обезпечени с активи (криптоактиви, които стабилизират стойността си по отношение на други активи или кошница от активи) и криптоактиви, различни от токени, обезпечени с активи, или токени за електронни пари.

Не се прилага за: криптоактиви, които са обхванати от други актове на ЕС в областта на финансовите услуги (напр. такива, които се квалифицират като финансови инструменти, пенсионни или застрахователни продукти) и криптоактиви, които са уникални и не са взаимнозаменяеми (non fungible tokens (NFT)), цифровите активи, емитирани от други публични органи, включително централни, регионални и местни администрации.

2. Рисковобазирен подход

В съответствие с Препоръка 1 на FATF държавите следва да идентифицират, оценяват и разбират рисковете от ИП/ФТ/ФП¹⁵, произтичащи от дейностите с ВА, дейностите или операциите на ДУВА.

Въз основа на тази оценка и собствената си оценка на риска от ИП/ФТ/ФП, задължените лица по законодателството за БИП/БФТ следва да прилагат рисковобазирен подход, за да гарантират, че мерките за предотвратяване ИП/ФТ/ФП са съизмерими с установените рискове.

¹⁵ Само по отношение на потенциално нарушение, неизпълнение или заобикаляне на ЦФС задължения, описани в Препоръка 7.

В случай че банка извършва дейности като ДУКА, тя следва да отчете рисковете от ИП/ФТ/ФП поради специфичните характеристики на този вид дейност и технологията, използвана като част от бизнес модела, което ѝ позволява незабавно да прехвърля криптоактиви по целия свят и да установява делови взаимоотношения с клиенти в различни юрисдикции, както и високата степен на анонимност на продуктите/ услугите, свързани с криптоактиви.

Допълнително, ако банка извършва дейности по MiCAR и въвежда нови продукти, услуги или бизнес практики, или ги променя значително, включително когато се въвежда нов механизъм за доставка или възприема иновативна технология като част от своите системи и механизми за контрол за борба с ИП/ФТ/ФП, следва да извърши оценка на ИП/ФТ/ФП рисковата експозиция преди въвеждането на тези продукти, услуги или бизнес практики (пар. 1.7 от Насока 1 и пар. 21.7 от Насока 21 „Секторни насоки за ДУКА“ от Насоки относно рисковите фактори, свързани с ИП/ФТ¹⁶).

Ако банка прецени да не осъществява дейност, свързана с криптоактиви, вкл. да не приема клиенти, които са ДУКА/да не изпълнява операции/сделки, свързани с криптоактиви, на база политика относно рисков апетит, то:

- в собствената оценка на риска се посочва, че ИП/ФТ/ФП рисковете при КА са неотнормими за нея и;
- създава вътрешна организация и контроли, които да подсикурат прилагането на практика на една такава забрана - т.е., че може да установява потенциални/съществуващи клиенти, които се опитват да заобиколят забраната.

В обхвата на деловите взаимоотношения с клиентите, вкл. и с клиенти ДУКА, банките следва да създават организация за извършване на регулярен преглед на клиентските данни и информация, както и текущ мониторинг на операциите и сделките, във времеви интервали в съответствие с определения рисков профил. Във връзка с Насока 2 (от Насоки относно рисковите фактори, свързани с ИП/ФТ), при определяне на индивидуалния рисков профил на клиент трябва да бъде отчетено дали клиентът или действителният му собственик е свързан със сектори, които се характеризират с по-висок риск от ИП/ФТ/ФП, например дружества, извършващи дейности по парични преводи, доставчици на услуги за криптоактиви, както е описано в пар. 9.20 и 9.21, казина или търговци на ценни метали (от цитираните Насоки).

През март 2023 г. бяха [публикувани](#)¹⁷ резултатите от първата Секторна оценка на риска при виртуалните активи, изготвена от постоянно действащата междуправителствена работна група по чл. 96 от ЗМИП. Оценката дава информация за извършваните дейности с виртуални активи в страната, тенденциите и секторите, които са засегнати, включително и банките, техните нагласи за приемане на клиенти, доставчици на услуги на виртуални активи. Анализът се базира на данни за периода 01.01.2021 – 30.06.2022 г., преди влизането в сила на европейското законодателство (MiCAR/TFR).

Неизчерпателен списък на рискови фактори (червени флагове) за ИП/ФТ/ФП с ВА е посочен в приложение 1.

¹⁶ ЕВА/GL/2024/01.

¹⁷ На интернет страницата на ДАНС <https://www.dans.bg/bg/78> в рубрика „Резултати от секторна оценка на риска при виртуалните активи“.

III. Мерки за комплексна проверка

1. Идентификация и проверка на идентификацията

В случай че клиент на банката е ДУКА или ФЛ/ЮЛ/ДПО, което извършва обмяна на криптоактиви за собствена сметка, банката прилага мерките за комплексна проверка (в частност идентификация и проверка на идентификацията) със степен и обем, отговарящи на определения индивидуален рисков профил на клиента, и според изискванията на Глава Втора от ЗМИП.

При делови взаимоотношения с клиенти ДУКА, част от процеса по идентификация и проверка на идентификацията следва да е събирането на информация за: използваното наименование (включително юридическо наименование и всяко друго търговско наименование); уникалният идентификационен код на ДУКА; уебсайтът, поддържан от този доставчик; адрес на електронна поща и телефонен номер за връзка; програмата за дейност, в която да бъдат включени видовете услуги, които ДУКА ще предоставя, вкл. къде и как ще се предлагат на пазара.

Част от проверката на идентификацията на клиент ДУКА следва да е и проверка в публичен регистър на ДУКА, поддържан от съответния пруденциален регулатор във връзка с издадения лиценз.

Когато банката е идентифицирала по-висок риск от ИП/ФТ/ФП при встъпване в делови взаимоотношения с клиенти ДУКА, мерки за разширена комплексна проверка, които могат да се приложат при идентификацията и проверката на идентификацията на клиента, са:

- проверка на предоставените идентификационни данни на клиента ДУКА и ФЛ, които са свързани с него във външни бази данни (напр. World check и др.) или чрез други надеждни и независими източници;
- проследяване на IP адреса на клиента/ проследяване от къде се достъпват средствата за отдалечен достъп, предоставени на клиента (напр. онлайн или мобилно банкиране)¹⁸;
- използване на продукти за извършване на специализиран анализ на операции/сделки, свързани с криптоактиви (блокчейн) и др.;
- FATF стандартът също така посочва, че въпреки че Препоръка 13 (кореспондентски отношения) не е приложима за местните ДУКА (регистрирани в Р България), при прилагане на мерките за комплексна проверка (в частност идентифициране и проверка на идентификацията на клиент ДУКА), на рисковобазирани подход, може да се прецени да се оценява и наличието и качеството на БИП/БФТ контролите им, тъй като преценката дали кореспондентските взаимоотношения с клиент ДУКА са местни или презгранични носи по-голямо предизвикателство.

2. Събиране на информация и оценка на целта и характера на деловите взаимоотношения

Когато банката извършва дейност като ДУКА, тя следва да събере информация за видовете, обемите и географията на сделките и операциите, които клиентът очаква да извърши.

¹⁸ Тази мярка може да се прилага и като един от способите за установяване на заобикаляне на санкции.

Банката следва да събере информация за клиенти ДУКА (неизчерпателно изброени): видът на услугите за криптоактиви, които клиентът възнамерява да предоставя, включително къде и как тези услуги ще бъдат предлагани на пазара; видът криптоактиви, с които е свързана услугата за криптоактиви; дали ДУКА ще предоставя услуги от името и за сметка на свои клиенти – напр. попечителство, изпълнение на нареждания и др. информация за специфики на клиентската база (най-малко дали ще набира клиенти само в държавата, в която е лицензиран или ще предлага услугите си презгранично); дали ще извършва презгранична дейност; дали ще извършва презгранична дейност чрез представител, дистрибутор или друга подобна форма.

3. Изясняване на произхода на средствата и източника на имуществено състояние

Виртуалните активи могат да променят своята стойност бързо и в широк диапазон, поради което за установяване на произхода на средствата е от съществено значение осигуряването на информация за периода, в който са придобити или продадени, както и по какъв начин са придобити (например чрез покупка от крипто платформа, „изкопани“ и др.), като отношение имат:

- Децентрализацията при ВА/КА – част от прехвърлянията на криптоактиви се осъществяват без участие на посредници (peer-to-peer прехвърляния) или без участници, които са задължени лица във връзка с БИП/БФТ – например участие на самостоятелно хостван адрес или портфейл; в част от случаите прехвърлянията не са част от блокчейн и в тази връзка данните за прехвърлянето не са публични;
- Анонимизирането - използването на инструменти за прикриване на произхода на прехвърлянето като mixers, tumblers, tornados и др.

При идентифициран по-висок риск от ИП/ФТ/ФП, банката може да събере и допълнителна информация при изясняване на произхода на средства и източника на имуществено състояние при клиенти ДУКА или операции/сделки, свързани с криптоактиви:

- Информация за основанието на плащане и относими документи (фактури, договори и др.);
- Характеристиките, предназначението и крайната дестинация/краен получател на продукта/услугата, свързана с криптоактиви;
- Доказателства за собственост върху средствата (например екрани от профила на лицето на съответната платформа и др.);
- Краен бенефициент и наредител по прехвърлянето/сделката/операцията с криптоактиви и какъв е характерът на отношенията между тях и др.

4. Текущо наблюдение

Банката следва да поддържа коректна, пълна и актуална информация за клиентите (вкл. ДУКА), което включва периодична и при необходимост извънредна актуализация на базите от данни и клиентските досиета.

В съответствие с изменената Насока 4: Мерки за КПК от Насоки относно рисковите фактори, свързани с ИП/ФТ, банката, която извършва дейности с криптоактиви, следва да извърши преценка за начина на наблюдение на сделките на своите клиенти, в зависимост от сложността, обема и честотата на сделките.

Създаденият процес по мониторинг на операциите следва да бъде формално разписан във вътрешнобанков документ и да включва най-малко: кои сделки/операции/прехвърляния

са обект на мониторинг и как се осъществява той (ръчно/автоматично, в реално време/последващ), как са разпределени отговорностите, описание на работния процес и действията, които се предприемат, описание на възможните справки, информация и документи, които се извършват/събират и тяхното документиране.

Банките, които осъществяват дейност като ДУКА, следва да гарантират, че разполагат с подходящи и ефективни инструменти за наблюдение, включително инструменти за наблюдение на сделките и усъвършенствани инструменти за анализ. Обхватът на тези инструменти се определя от естеството и обема на дейностите, включително вида на криптоактивите, които се предоставят за търгуване или обмен. **Банките ДУКА** следва също така да гарантират, че съответните служители (фронт офис и специализирана служба по ЗМИП) получават специализирано обучение (въвеждащо и последващо регулярно), имат добро разбиране и познания за криптоактивите и рисковете от ИП/ФТ/ФП, на които е изложена банката.

Създадената организация¹⁹ следва да включва първоначален, периодичен и извънреден (ad-hoc) преглед на заложените правила/контроли за мониторинг (формално разписан и включващ най-малко: вменени ангажименти и описание на действията във връзка с процеса по преглед, промяна, одобрение на клиент/обработване на сделка/трансакция).

По отношение на мониторинга на сделки/операции/прехвърляния на криптоактиви, когато банки извършват дейност, свързана с криптоактиви, или е в делови взаимоотношения с клиенти ДУКА, следва да създадат вътрешна организация, която да им позволява да осъществяват мониторинг на прехвърлянията на криптоактиви, което включва най-малко:

- задълбочена проверка и анализ на прехвърлянията/сделките/операциите с криптоактиви (чл. 10, т. 5 от ЗМИП);
- навременно установяване на съмнение и/или знание за ИП/ФТ и незабавно уведомяване на САДФР-ДАНС и компетентните органи (чл. 72, ал. 1 от ЗМИП, респ. чл. 9 от ЗМФТРОМУ);
- спазване на ограничителните мерки за ФТ и ФП – ЦФС за ФТ и ФП, вкл. опити за заобикаляне на приложимите санкции.

За клиенти ДУКА банките следва да извършват текущо наблюдение върху установените делови взаимоотношения, както и анализ на сделките, операциите и прехвърлянията на криптоактиви, извършвани през цялото времетраене на тези взаимоотношения, за да се установи доколко те съответстват на определения рисков профил за клиента. Текущият мониторинг следва да включва установяването на промени в клиентския профил (напр. клиентско поведение на клиент ДУКА, използвани продукти и услуги, вид и размер на операциите/сделките/прехвърлянията) и идентифициране на операции/сделки/прехвърляния, които не му съответстват.

Банките, които предоставят дейности като ДУКА или ще приемат клиенти ДУКА, следва да обмислят възможността за използване на усъвършенствани инструменти за анализ, като инструменти за анализ на технологията на децентрализирания регистър (ТДР) или блокова верига с оглед на риска от ИП/ФТ/ФП, свързан със стопанската дейност на банката и с индивидуалните сделки на клиентите ДУКА.

¹⁹ Παρ. 275, Updated guidance for a risk-based approach virtual assets and virtual asset service providers, FATF, 2021.

Инструментите за мониторинг на блокови вериги за управление на рисковете или блокчейн софтуерите обикновено използват публични данни за блокчейн и предоставят налична негативна информация относно заплахи, като адреси на портфейли, свързани с финансиране на тероризма, измами, престъпления или санкции, за да се даде възможност на задължените лица да идентифицират сделките, свързани с тези данни. Освен това, инструментите за мониторинг на блоковите вериги позволяват на дружествата да проследяват трансакциите към и от адрес, свързан с хакерска атака, измами с NFT (Non-fungible token), дейност със софтуер за изнудване или други престъпни деяния, идентифицирани от правоприлагащите органи, правителствата или общността на КА.

По отношение на мониторинга за спазване на ЦФС за ФТ и ФП по отношение на КА, банките следва да извършват проверки на операциите/сделките/прехвърлянията, свързани с криптоактиви, както и на клиентите ДУКА, за спазване на ЦФС за ФТ и ФП.

Банките трябва да създадат такава организация (контроли), позволяваща навременно (без забавяне) да:

- установяват клиенти (вкл. потенциални/случайни) дали са лица, включени в списък с ограничителни мерки за ФТ или ФП (*чл. 4б от ЗМФТРОМУ*) или дали лица от списъците за ЦФС-ФТ и ЦФС-ФП са свързани с операции/сделки/прехвърляния, които се изпълняват от банката, или с клиенти на банката (напр. контрагенти, съдлъжници, действителни собственици и др.);
- установяват операции/сделки/прехвърляния с КА, които са насочени към финансиране на тероризма или пролиферацията;
- прилагат мерките (блокиране и забрана за предоставяне на финансови услуги, средства и др. активи) (*чл. 3 от ЗМФТРОМУ*);
- уведомяват компетентните органи по *чл. 3 от ЗМФТРОМУ*²⁰ (за ФТ и ФП) и *чл. 9 от ЗМФТРОМУ*²¹ (за ФТ).

Банките са длъжни също да установяват опити за заобикаляне²² на ограничителните мерки – т.е. когато лице от санкционен списък за ЦФС-ФТ или ФП или свързано лице, с лице от санкционен списък се опитва да заобиколи ограничителните мерки като прикрие произхода на средствата, данните за бенефициера или инициатора и т.н.

Следва да се отчитат уникалните характеристики на криптоактивите²³, при прилагане на мерки по чл. 3 от ЗМФТРОМУ (в частност блокирането на криптоактивите), предвид:

- начина за ограничаване на възможността за разпореждане с криптоактивите (собственикът да няма достъп до средствата, чрез които криптоактивите могат да бъдат прехвърляни или до т.нар. private and public keys);
- волатилната стойност на криптоактивите и възможността да бъдат обезценени блокираните криптоактиви, особено при възникване на необходимостта блокирането да отпадне и те трябва да бъдат върнати на собственика им.

²⁰ Министърът на вътрешните работи, министърът на финансите, председателят на ДАНС и КПК.

²¹ Министърът на вътрешните работи, председателят на ДАНС и САДФР-ДАНС.

²² Например при използване на различни инструменти за прикриване на движението на ВА/КА и данните за инициатора и бенефициера като mixers, tumblers, tornados и др.

²³ Има се предвид различните начини за съхраняване на КА и средствата за достъпване на КА (private and public key).

Банките следва да предприемат действия, които да включват надлежно документиране на извършените проверки относно съответствието с ограничителните мерки (проверки на клиенти и свързани с тях лица и проверки на операции/сделки/прехвърляния) и резултатите от тях, като по въпроса ЕБО има Насоки ЕВА/GL/2024/14²⁴, които са приложими от 30.12.2025 г.

5. Мерки за опростена комплексна проверка

В ситуации с по-нисък ИП/ФТ/ФП риск, при които банката е установила в собствената си оценка на риска по чл. 98 от ЗМИП и доколкото е разрешено от националното законодателство, банките, извършващи дейности, свързани с криптоактиви, могат да прилагат опростени мерки за комплексна проверка на клиенти съгласно ЗМИП.

6. Мерки за разширена комплексна проверка

Когато банка установи завишен ИП/ФТ/ФП риск, свързан с делови взаимоотношения или случайна сделка при извършването на дейност като ДУКА или ако имат клиент ДУКА да се уверят, че клиентът прилага мерки за РКП, които могат да включват:

- Проверка на самоличността на клиента и на действителния собственик въз основа на повече от един надежден и независим източник;
- Идентифициране на всички физически лица, които са упълномощени да управляват сметка за криптоактиви или адрес в децентрализиран регистър от името на клиента или да дават инструкции за прехвърляне или обмен на криптоактиви или други услуги, свързани с тези криптоактиви;
- Допълване на информацията за клиента и за целта и характера на деловите взаимоотношения например: чрез извършване на търсене в публични източници или търсене на негативна информация в медиите или възлагане на доклад за проучване клиента от трета страна;
- Получаване на доказателства за източника на средствата, източника на богатството или източника на КА по отношение на тези сделки, които представляват по-висок ИП/ФТ/ФП риск;
- По-често или по-задълбочено оценяване на дейностите, извършвани чрез сметките за КА (на клиента-ДУКА), като се използват инструменти за разследване на криптоактиви;
- Увеличаване на честотата на наблюдение на IP адресите на клиентите и сравняването им с IP адресите, използвани от други клиенти и др.
- При встъпване в делови взаимоотношения и регулярно, банките следва да проверяват и съхраняват информация за лиценза на ДУКА с цел установяване на услугите, които предлага на своите клиенти и дали оперира на международно ниво;
- Събиране на информация и оценка на репутацията на ДУКА (или на техните действителни собственици или членовете на управленския орган) чрез надеждни (публични) източници²⁵;
- Оценка на превенцията от ИП/ФТ/ФП и контролните механизми на ДУКА (например чрез събиране на информация чрез въпросник и документиране на извършена оценка на така събраната информация), вкл. дали прилага правилата за пътуване (travel rule);

²⁴ Виж източник 18 от Библиографията: [Gls on restrictive measures \(EBA GL 2024 14 and EBA GL 2024 15\) BG COR.pdf](#)

²⁵ Справки във външни/вътрешни бази от данни, информация от надеждни публични източници, каквито например са интернет страниците на компетентни органи или международни организации и др.

- Събиране на информация и оценка на дейността на ДУКА, когато ДУКА действа като представител на трети страни и/или извършва дейност чрез дистрибуторска мрежа, „white labeling“ и др.

6.1 Мерки за разширена комплексна проверка във връзка с кореспондентски отношения

Ако банка установява кореспондентски отношения, включващи извършването на услуги, свързани с криптоактиви с лице-респондент от трета държава, което предоставя подобни услуги, включително прехвърляния на криптоактиви, е подходящо да:

- събере информация и да провери дали лицето-респондент е лицензирано или регистрирано за дейности, свързани с КА;
- събира достатъчно информация за лицето-респондент, позволяваща ѝ да разбере изцяло естеството на дейността на респондента, и въз основа на обществено достъпната информация да установи репутацията на това лице и качеството на надзора, който се упражнява спрямо него (пруденциален и ИП/ФТ);
- извършва оценка на механизмите за контрол на лицето-респондент във връзка с противодействието на изпирането на пари и финансирането на тероризма;
- получава одобрение от служител на висша ръководна длъжност, преди да установи нови кореспондентски отношения;
- документира съответните отговорности на всяка от страните по кореспондентските отношения;
- по отношение на кореспондентските сметки за криптоактиви да се увери, че лицето-респондент е проверило идентификацията и е извършило текуща комплексна проверка на клиентите с пряк достъп до сметките на ДУКА, и е в състояние да предоставя съответните данни от комплексната проверка на клиентите при поискване от банката.

При преустановяване на кореспондентските отношения по причини, свързани с политиката за борба с изпирането на пари и финансирането на тероризма, решението се документира и се прилага в съответното досие.

6.2. Мерки за разширена комплексна проверка при прехвърляния на крипто активи, насочени към или произхождащи от самостоятелно хостван адрес²⁶

Банките, които извършват дейност като ДУКА, прилагат една или повече мерки за ограничаване на риска, съобразно установеното ниво на риск:

- предприемане на основани на риска мерки за идентификация и проверка на идентификацията на инициатора или бенефициера на прехвърляне, извършено към или от самостоятелно хостван адрес, или на действителния собственик на такъв инициатор или бенефициер, включително посредством трети страни;
- изискване на допълнителна информация относно произхода и местоназначението на прехвърляните криптоактиви;
- извършване на разширено наблюдение на тези операции или сделки.

²⁶ Промени в Директива 2015/849, въведени с чл. 38 от TFR (изменения на Директивата), съответно отразени с новия чл. 20а от ЗМИП (бр. 54 на ДВ от 04.07.2025 г.).

IV. Съхраняване на информацията, разкриване на информацията и обучение

1. Съхраняване на информация

Международният стандарт²⁷ по отношение на съхраняване на информация за КА от ДУКА е транспониран в европейското²⁸ и българското законодателство²⁹ (секторни и специални закони), като предвижда съхраняване на информацията за поне 5 години от: прекратяване на отношения с клиент/кореспондентско отношение; при случайна операция/сделка (датата на извършване); при подадени уведомления до САДФР-ДАНС (от следващата календарна година); оценки на риска (от началото на следващата година), вкл. за данни, информация и документи, изготвени по реда на ЗМИП; вътрешните правила по ЗМИП и за дейността на специализираната служба се съхраняват през цялото времетраене на банковата дейност и 1 г. след това. Възможно е удължаване на този срок до 2 години с писмено указание на директора на САДФР-ДАНС. Тази информация следва да е на разположение на САДФР-ДАНС и БНБ, при поискване.

Начинът на съхраняване на информация за прехвърляния на криптоактиви следва да позволява извличане на данни (наредител, бенефициер, сума, вальор, основание и др.) за всяка една отделна трансакция в подходящ формат за извършване на анализ от страна на компетентните органи. Следва да се има предвид, че FATF стандартът счита разчитането само на блокчейн или друг тип технология на децентрализирания регистър като начин за съхраняване на информация по прехвърляния на криптоактиви като недостатъчно за изпълнение на Препоръка 11 на FATF (съхраняване на информация). Същият подход е наличен и в Насоките на ЕБО за ИП/ФТ рисковите фактори (Насока 21.16).

2. Обучение

Програмата за обучение по БИП/БФТ/БФП във всяка банка, която предлага услуги, свързани с КА, следва да гарантира, че служителите са наясно с рисковете, свързани с криптоактивите и услугите за криптоактиви, запознати са със задълженията по ЗМИП и са подготвени да прилагат подходящи контроли, основани на риска за дейностите с криптоактиви, вкл. използване на аналитични софтуери. Това следва да включва преминаване на въвеждащи и продължаващи обучения, както в областта на БИП/БФТ/БФП, така и във връзка със специфичните продукти и услуги, които банката ще предлага, като в годишните програми за обучение следва да е ясно документиран анализът на необходимостта от специализирани обучения – например, във връзка със специфичните технологии (блокчейн), които са релевантни при криптоактивите.

Като резултат от този процес, служителите трябва да могат да разпознават съмнителни или необичайни сделки и дейности, включително да използват усъвършенствани инструменти за анализ за наблюдение на сделките и деловите взаимоотношения и да тълкуват резултатите от тези системи и инструменти.

²⁷ П15 и тълкувателната ѝ бележка предвиждат прилагане на същите изисквания за ефективен надзор и спазване на мерките от ДУВА/ДУКА по отношение на ВА, подобно на финансовите институции и техните услуги и продукти, вкл. и за съхранение на информацията.

²⁸ чл. 68, ал.9 от MiCA, чл.78 от Регламент (ЕС) 2024/1624.

²⁹ чл.67-69 от ЗМИП.

3. Установяване и докладване на съмнителни операции

Международният стандарт³⁰ по отношение на подаването на уведомления при съмнение за ИП/ФТ с КА от ДУКА и от банки е транспониран в европейското³¹ и българското законодателство³², като тези уведомления се подават незабавно, а форматът им е по утвърден от директора на САДФР-ДАНС образец. Освен от специализираната служба по чл. 106, ал. 1 от ЗМИП, уведомлението може да се подаде и от други служители в банката.

Уведомление се изпраща независимо дали прехвърлянето/операцията е извършено/а или не, като приложимите изисквания за уведомяване на компетентните органи за съмнителна дейност се изпълняват, дори когато дейността е презгранична, в съответствие с приложимите законови изисквания в държавата по произход/приемаща държава.

³⁰ П15 и тълкувателната ѝ бележка предвиждат прилагане на същите изисквания за ефективен надзор и спазване на мерките от ДУВА по отношение на ВА, подобно на финансовите институции и техните услуги и продукти, вкл. и за подаване на уведомления при съмнение/знание за ИП/ФТ с ВА.

³¹ чл. 9 и чл. 11 от Регламент (ЕС) 2024/1624.

³² чл. 72 от ЗМИП и чл. 9 от ЗМФТРОМУ.

Приложение 1 – Рискови индикатори (червени флагове) за ИП/ФТ/ФП с ВА

Съгласно информационен материал на FATF за червени флагове за ИП/ФТ/ФП³³, свързани с ВА, същите се категоризират в³⁴:

- индикатори, свързани с анонимността:
 - ✓ ДУВА предоставя услуги като mixers/tumblers/bridges срещу комисионна, с което спомага да се прикрие източника на средства на клиентите си;
 - ✓ опериране на нелицензиран/нерегистриран уебсайт за peer-to-peer ВА;
 - ✓ прехвърляния на ВА, при които участват няколко типа ВА;
- географски индикатори:
 - ✓ дружество предоставя услуги, свързани с ВА, от държава, където няма законодателство по отношение на този тип услуги или все още е в начален стадий;
 - ✓ прехвърляне или закупуване на ВА от/към високорискови държави;
- индикатори, свързани с определени типологии трансакционно поведение:
 - ✓ нов клиент захранва сметката си с вноски на голяма стойност и в рамките на един ден прехвърля ВА към няколко различни ДУВА за закупуване на ВА;
 - ✓ закупуване на малки суми ВА от местен ДУВА от различни физически лица, които в кратък период ги прехвърлят към чуждестранен ДУВА, като физическите лица са с еднакъв адрес на местоживеене и адресите на ВА се достъпват от един и същи IP адрес;
 - ✓ входящи прехвърляния на ВА за малки суми от различни портфейли и в кратък срок цялата сума е прехвърлена към друг портфейл/адрес или е обменена за фиатна валута;
- индикатори, свързани с профила на изпращача или бенефициера:
 - ✓ през първите дни, след откриване на платежна сметка от физическо лице, сметката се захранва с входящи преводи с основание, предполагащо търговска дейност на физическото лице, от различни юридически лица и на голяма стойност;
 - ✓ прехвърлени ВА от/към портфейли/IP адреси, които са идентифицирани като съмнителни, свързани със санкционирани лица (за ФТ или ФП) или с измама (ИП);
 - ✓ откриване на няколко сметки под различни имена с цел да се заобиколят действащи ограничения (за ФТ или ФП);
 - ✓ разминаване на IP адреса, с който се идентифицира клиента, и IP адреса, от който се извършват прехвърляния на ВА;
 - ✓ клиентът често си сменя идентификационни данни/информация, вкл. имейл адрес;
- индикатори, свързани с произхода на средства и източника на имуществено състояние:
 - ✓ клиент предоставя фалшиви документи във връзка с КУС процедури с цел да прикрие източника на средствата от откраднати ВА;
 - ✓ множество карти, свързани с криптопортфейл, с които се теглят големи суми/множество по-малки прехвърляния.

³³ Виж т.10 от Библиографията

³⁴ Повече информация е налична в източници 10 и 11 от Библиографията, както и в Насоките на ЕБО за рисковите фактори ЕВА/GL/2024/01, Насока 21 (Секторни насоки за доставчиците на услуги за криптоактиви (ДУКА)), които са приложими от 30.12.2024 г.

Приложение 2 - Полезна информация по въпроси, касаещи прехвърлянията на КА и смекчаващи мерки за риска от ИП/ФТ/ФП при прехвърляне на КА - Прехвърляния на криптоактиви / правила за пътуване / travel rule

TFR урежда законовата рамка относно информацията, придружаваща преводи на средства и прехвърляния на определени криптоактиви или т.нар. правила за пътуване (travel rule). В допълнение, ЕБО³⁵ изготви Насоки във връзка с прилагането на чл. 14 – 17 и чл. 19 – 22 от TFR – Правила за пътуване при прехвърляне на определени криптоактиви, които са приложими от 30.12.2024 г.³⁶

Международният стандарт³⁷, отразен в регионалното³⁸ и националното³⁹ законодателство, изисква при извършване на случайна операция/прехвърляне на ВА/КА на стойност равна или по-голяма от 1000 евро или тяхната равностойност в друга валута да се прилагат мерки за комплексна проверка.

Задълженията⁴⁰, предвидени в Регламента за проверка на точността и пълнотата на информацията за инициатора и бенефициера при прехвърляния на определени КА, се прилагат независимо от размера на прехвърлянето, както и независимо дали е вътрешно (национално) или презгранично прехвърляне. Изключение на горното изискване⁴¹ е предвидено в случай на прехвърляне към/от самостоятелно хостван адрес, за което е приложим праг на стойността на прехвърлянето равна или по-голяма от 1000 евро или тяхната равностойност в друга валута. Предвиден е и допълнителен ангажимент за ДУКА - да проверява дали неговият клиент притежава/контролира този самостоятелно хостван адрес.

Прехвърляния на криптоактиви, извършвани чрез АТМ за криптоактиви, когато ДУКА или междинният ДУКА на инициатора или на бенефициера е със седалище в Съюза, са в обхвата на приложното поле на TFR.

Технологичното решение, което банката реши да използва, за да спазва правилото за пътуване, следва да позволява по ефективен и ефикасен начин да извършва следните основни действия:

- а. идентифициране на ДУКА на бенефициера/междинен ДУКА;
- б. подаване на необходимата пълна и точна информация за инициатора и бенефициера в съответствие с изискването на Препоръка 16 на FATF и TFR;
- в. подаване на разумно голям обем трансакции към множество дестинации по ефективно стабилен начин;
- г. предаване на данни по сигурен начин, т.е. да защитава целостта и наличността на необходимата информация, за да улеснява воденето на отчетност;
- д. да защитава използването на такава информация от получаващите ДУКА или други задължени лица, както и да я защитава от неразрешено разкриване в съответствие с националните закони за защита на личните данни и поверителността;
- е. да предостави на ДУКА канал за комуникация, който да подпомага по-нататъшното проследяване на прехвърлянето и при необходимост осъществяване на контакт за предоставяне на допълнителни данни във връзка с:
 - извършване на надлежна комплексна проверка на контрагента ДУКА; и
 - изискване на информация за определена транзакция, за да се определи дали транзакцията включва високорискови или забранени дейности.

³⁵ В съответствие с чл. 36 от TFR

³⁶ Насоките бяха приети за прилагане от 30.12.2024 г. с решение на УС на БНБ от 07.11.2024 г.

³⁷ Тълкувателна бележка по П15 във връзка с П10 на FATF

³⁸ Чл. 14-16 от TFR

³⁹ Чл.11, ал.1, т.5 от ЗМИП

⁴⁰ В съответствие с т. 30 от Преамбюла на TFR

⁴¹ В съответствие с т. 39 от Преамбюла на TFR

Библиография на документи (насоки, мнения, доклади) и изявления на FATF и ЕБА във връзка с криптоактивите (списъкът не е изчерпателен)

FATF:

1. [The FATF Recommendations](#), октомври 2025 г.
2. [Targeted Update](#) on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, 26.06.2025 г.
3. [Virtual Assets](#): Targeted Update on Implementation of the FATF Standards on VAs and VASPs, 09.07.2024 г.
4. [Status](#) of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity, 23.03.2024 г.
5. [Virtual Assets](#): Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, 27.06.2023 г.
6. [Targeted Update](#) on Implementation of FATF's Standards on VAs and VASPs, 30.06.2022 г.
7. [Updated Guidance](#) for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 28.10.2021 г.
8. [Quick Guide](#): RBA for Virtual Assets & Virtual Asset Service Providers, 28.10.2021 г.
9. [Second](#) 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs, 05.07.2021 г.
10. Virtual Assets [Red Flag Indicators](#) of Money Laundering and Terrorist Financing (report), 14.09.2020 г.
11. Virtual Assets [Red Flag](#) - Virtual Asset Service Providers (in brief), 14.09.2020 г.
12. [12 Month Review](#) of Revised FATF Standards - Virtual Assets and VASPs, 07.07.2020 г.
13. [FATF Report](#) to G20 on So-called Stablecoins, 07.07.2020 г.
14. [Money laundering](#) risks from stablecoins and other emerging assets, 18.10.2019 г.

EBA:

15. [Crypto-assets explained](#) what MiCA means for you as a consumer, 06.10.2025;
16. [Warning](#) on crypto-assets, 06.10.2025;
17. Joint Report [Recent developments](#) in crypto-assets (Article 142 of MiCAR), 13.01.2025;
18. [Guidelines on internal policies](#), procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/GL/2024/14), 14.11.2023 г. (в сила от 31.12.2025 г.)
19. [Guidelines on information requirements](#) in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 (EBA/GL/2024/11), 04.07.2024 г.
20. The ML/TF Risk Factors Guidelines ([EBA/GL/2024/01](#)), 16.01.2024 г.
21. The Risk-Based Supervision Guidelines ([EBA/GL/2023/07](#)), 27.11.2023 г.

EU:

22. [Регламент \(ЕС\) 2023/1114](#) на Европейския парламент и на Съвета от 31 май 2023 година относно пазарите на криптоактиви и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на директиви 2013/36/ЕС и (ЕС) 2019/1937 (MiCA);
23. [Регламент \(ЕС\) 2023/1113](#) на Европейския парламент и на Съвета от 31 май 2023 година относно информацията, придружаваща преводите на средства и прехвърлянията на определени криптоактиви, и за изменение на Директива (ЕС) 2015/849 (TFR).

Национално законодателство:

1. Закон за пазарите на криптоактиви
2. Закон за мерките срещу изпирането на пари
3. Закон за платежните услуги и платежните системи
4. Закон за кредитните институции

Насоки на други надзорни органи:

1. [УКАЗАНИЯ](#) относно ефективното управление и намаляване на рисковете, свързани с доставчици и услуги за виртуални активи, март 2024 г.
2. [НАСОКИ](#) за прилагане на задълженията за мерките срещу изпирането на пари и финансирането на тероризма за доставчици, които предоставят услуги за виртуални активи, октомври 2024 г.