БЪЛГАРСКА НАРОДНА БАНКА

# НАСОКИ ЗА БАНКИТЕ ОТНОСНО МОНИТОРИНГ НА ТРАНСАКЦИИ И „СКРИНИНГ“ (ПРОВЕРКА) ЗА СЪОТВЕТСТВИЕ С ЦЕЛЕВИТЕ ФИНАНСОВИ САНКЦИИ ЗА ФИНАНСИРАНЕТО НА ТЕРОРИЗМА И НА РАЗПРОСТРАНЕНИЕТО НА ОРЪЖИЯ ЗА МАСОВО УНИЩОЖЕНИЕ

Кредитните институции следва да съобразят настоящите насоки при осъществяването на мониторинг за съмнителни операции и скрининг на трансакциите за съответствие с целевите финансови санкции за финансирането на тероризма и на разпространението на оръжия за масово унищожение.

Настоящите Насоки са приети от Управителния съвет на Българската народна банка на основание чл. 73, ал. 4, във връзка с чл. 73, ал. 1, т. 11 от Закона за кредитните институции, и във връзка с чл. 14а, ал. 2, т. 1 буква „а“, от Закона за мерките срещу финансирането на тероризма и на разпространението на оръжия за масово унищожение, както и насока 4.4.9, буква „б“, т. 124 и 125 от Насоки на ЕБО за рисково базиран надзор (EBA/GL/2021/16).

07.2025 г.

**Съдържание**

## 1. Въведение

### 1.1. Цел и приложно поле

Целта на настоящите насоки е да подпомогнат разбирането и ефективното изпълнение от страна на кредитните институции на техните законови задължения и очакванията на надзорния орган по отношение на извършването на мониторинг на трансакциите и скрининг за нарушаване или заобикаляне на санкционни режими на ООН или ЕС за ФТ/ФП (финансиране на тероризма/финансиране на разпространението на оръжия за масово унищожение (финансиране на пролиферацията), както и за установяване на съмнителна дейност, свързана с ИП/ФТ.

В настоящите насоки се вземат предвид стандартите и насоките, издадени от FATF[1] , Насоки на ЕБО, най-добрите практики в отрасъла и индикатори „червен флаг“. Те не са изчерпателни и не определят ограничения за мерките, които трябва да бъдат предприети за изпълнение на законовите задължения на банките, съгласно действащата правна и регулаторна рамка.

Насоките преминаха предварително обсъждане с банките в България и Асоциацията на банките в България в рамките на „Форум за рисковете от изпирането на пари и финансирането на тероризма между БНБ и банките“ (AML Форум).

### 1.2. Съкращения

| Термини | Описание |
|---|---|
| БИС | Банкова информационна система |
| ДВ | Държавен вестник |
| ДПУ | Доставчик на платежни услуги по смисъла на чл. 3 от Закона за платежните системи и платежните услуги |
| ИП | Изпиране на пари |
| МС | Министерски съвет |
| МТ | Мониторинг на трансакциите |
| НОР | Национална оценка на риска от ИП/ФТ/ФП |
| САД-ФР на ДАНС | Специализирана административна дирекция „Финансово разузнаване“ на държавна агенция „Национална сигурност“ |
| СОР | Собствена оценка на риска от ИП/ФТ/ФП |
| УСО | Уведомление за съмнителна операция или сделка |
| ФП | Финансиране на пролиферацията/финансиране на разпространението на оръжия за масово унищожение |
| ФТ | Финансиране на тероризъм |
| ЦФС | Целеви финансови санкции |
| ЮЛ | Юридически лица |
| AML | Anti-money laundering / Превенция от изпирането на пари |
| CDD/КПК | Customer due diligence / Комплексна проверка на клиента |

[1] 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.), и с финансиране на пролиферацията (2008 г.).

| | |
|---|---|
| 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.), и с финансиране на пролиферацията (2008 г.) |
| ISIN | International Securities Identification Number / Международни идентификационни номера на ценни книжа |
| KYC | Know your customer / Опознайте клиента си |
| OCR | Optical Character Recognition / Оптично разпознаване на символи |
| TFS | Targeted financial sanctions |

### 1.3. Основание за издаване на насоките

По отношение на наблюдението на трансакциите банките следва да имат разработени вътрешни политики и процедури за осъществяване на контрол, съизмерими с естеството и размера на тяхната стопанска дейност, които да са одобрени от висшето им ръководство. Банките следва да въведат индикатори/показатели, които могат да се използват за идентифициране на подозрителни сделки и други дейности. Що се отнася до скрининга на санкциите и на лицата по чл. 4б от ЗМФТ, банките са задължени редовно да проверяват своята клиентска база (вкл. действителни собственици и пълномощници на клиенти и техни контрагенти) и операции/сделки срещу списъците за наложени санкции за тероризъм или финансирането му с регламент на Съвета на Европейския съюз (консолидиран списък на ЕС), списъци, издадени от съответните комитети към Съвета за сигурност на ООН (консолидиран списък на ООН) или списъка на МС (местния списък със санкционирани лица), както и незабавно, когато бъдат уведомени за всякакви промени в тези списъци.

С промените в ЗМФТРОМУ, обнародвани в бр. 49 на „ДВ“ от 2025 г., се въвежда аналогично изискване за ФП (нови точки 4 и 5 на чл. 4б от закона за лица от списъци, касаещи ФП от ЕС и СС на ООН).

## 2. Мониторинг на трансакциите

Ефективната програма за мониторинг на трансакциите позволява на банките да откриват, проверяват и докладват съмнителни сделки/операции/трансакции в съответствие с относимата правна и регулаторна рамка, както и да гарантират, че клиентите и сделките, реализирани чрез банките, не превишават рамката на склонността им към риск. Следователно ефективният МТ зависи в голяма степен от информацията, получена чрез прилагането на мерки за комплексна проверка на клиента (CDD)/Опознайте клиента си (KYC) мерки, включително, но не само, информация относно видовете сделки, в които обикновено се очаква клиентът да участва.

Получаването на достатъчно разбиране за своите клиенти и естеството и целта на деловите взаимоотношения с клиентите, заедно с текущия анализ на действителното поведение на клиента и поведението на техните партньори/контрагенти, позволява на банката да придобие информация/знание за нормалната или очакваната дейност за клиента, спрямо която могат да бъдат идентифицирани необичайни или потенциално подозрителни сделки. Служителите, които отговарят за обработване на трансакциите, трябва да следят за коректно въвеждане/пренасяне

от друга система на информацията и при установени пропуски или неточности в съответната информация за клиента или действителния собственик или пропуски или проблеми с качеството или обема на платежните детайли на операциите или сделките да предприеме приоритетно действия за решаването на проблема или неговото ескалиране към звеното, което има правомощия за отстраняването на проблема.

**Ефективната програма за МТ се състои от следните основни елементи:**

- Поддържане на политики и процедури, които представляват вътрешнобанковата рамка по отношение на борбата с ИП/ФТ рисковете, в които ясно и в пълнота са формализирани основните задължения на банката и разпределение на отговорностите на служителите, както и има разписани работните процеси (вкл. по ескалация на казуси) и описание на контролните механизми и тяхната приложимост.

- Добре калибрирана рамка, основана на риска: рисковете, пред които са изправени банките са динамични и сделките/операциите, които извършват, могат да бъдат разнообразни, сложни по характер и големи по обем. Поради това всяка банка следва да преразглежда и подобрява своята рамка за управление на МТ редовно и при настъпване на определени „задействащи събития“, като например съществени промени в стопанската дейност или рисковия си профил или в правна и регулаторна среда, в която работи, за да се гарантира, че те остават в рамките на приетите рискове от банката. Използването на информация и придобития опит на служителите, които обработват сигналите към системата МТ, е от съществено значение за по-доброто калибриране и настройка.

- Въвеждащо и продължаващо обучение и осведоменост за рисковата експозиция на банката: За да се гарантира правилното функциониране и изпълнение на техните програми за управление на МТ, банките следва да гарантират, че служителите с отговорности по МТ разполагат с подходящ експертен опит и получават специфично за функцията обучение относно политиките за МТ, процедурите и рисковете, както и за работа със системите.

- Ефективна интеграция на програмата за борба с изпирането на пари и финансирането на тероризма: банките следва да гарантират, че техните системи и рамки за МТ се развиват и са разглеждани като част от контрола, свързан с БИП/БФТ. Ефективният МТ зависи от качеството и пълнотата на данните, извлечени от клиентските и трансакционните системи и бази данни на банките. Едновременно с това резултатите от МТ следва да се ползват за оформяне на разбирането и управлението на рисковете от ИП/ФТ, включително чрез извършване на прегледи на клиенти извън предвидения периодичен преглед и прилагане на засилен контрол или допълнителен контрол по отношение на клиенти, които носят по-висок риск от ИП/ФТ.

- Активен вътрешен контрол: Висшето ръководство на банката следва да има активна роля в осъществяване на ефективен контрол над изпълнението на програмите за МТ и текущото подобряване на системите въз основа на идентифицираните рискове на институцията. Когато резултатите от МТ са компрометирани от фактори като неподходящо калибриране, неефективност на

процесите, проблеми с персонала или неизправности на системата, е необходимо висшето ръководство да бъде своевременно информирано за тези въпроси, за да се гарантира, че проблемите се отстраняват своевременно и по подходящ начин. Висшето ръководство следва да има ангажимент за информиране на служителите за склонността на банката към приемане на риск и да определя предотвратяването, разкриването и докладването на незаконни или подозрителни трансакции като главен приоритет. Процесът на осигуряване на качеството на функционалностите на системите също следва да играе решаваща роля в програмата за МТ чрез валидиране на прегледа от гледна точка на точността и детайлността. Всички промени във функционалностите на системите/контролни механизми, които имат отношение към БИП/БФТ, следва да се свеждат до знанието на висшето ръководство.

### 2.1. Политики и процедури

Банката за да подсигури пълното, правилното и навременното прилагане на законовите изисквания за проследяване на съмнителна дейност в областта на ИП/ФТ рисковете и докладване на компетентните органи, следва да има ефективни политики, процедури и контроли. В тази връзка тя трябва да има действащи вътрешни процедури и инструкции, в които ясно и в пълнота да са формализирани основните задължения на банката и разпределение на отговорностите на служителите.

Политиките, процедурите и контролите на банката следва да обхващат най-малко:

- Какви контроли банката е въвела с цел установяването на съмнителни операции (това например може да включва описание на различни технологични решения, вкл. специализиран софтуер);
- Описание на работния процес и разпределение на отговорностите на служителите при обработка и документиране на анализа на получените сигнали за съмнителна дейност (това може да включва както сигнали, които са генерирани от система, така и сигнали от служители или външни трети страни), така и нива на контрол при обработката на сигнали;
- Процеси и нива на ескалация при установени по-сложни казуси или проблеми с данните/системите;
- При използването на (автоматизирани) системи за мониторинг – потребителско ръководство за работа със системите, както и информация за системите, с които системата за мониторинг си взаимодейства; какви данни, с каква честота и от кои системи се зареждат в нея, функционалности и сценарии/филтри/контроли, които са заложени в нея;
- процеси, гарантиращи, че политиките, процедурите и контролите са съизмерими с идентифицирания риск от ИП/ФТ;
- процеси, гарантиращи, че политиките и процедурите за мониторинг на трансакции:
    - редовно се преразглеждат;

- редовно се изменят и актуализират, когато и където е необходимо;
- се прилагат ефективно; и
- разработени са по начин, който им позволява да задействат необходимите действия, след като бъдат установени недостатъци.

Така описаните работни указания могат да са част от вътрешните правила на банката по чл. 101 от ЗМИП или отделен вътрешнобанков документ.

**Добра практика:**
- Банката има разписан процес за установяване на свързани операции.
- Разписан във вътрешнобанков документ е процесът на обработка на сигналите, регламентиращ разпределението на отговорностите, срок за обработка, нивата на компетентност във връзка с потвърждаване/отхвърляне на съмнение от ИП/ФТ.
- Процесът на допълнителна проверка и ескалация може да включва: изискване за допълнителни действия от служителите на фронт офис, за получаване на информация от клиента (в ситуации, когато наличната в банката информация не е достатъчна за вземане на решение); преглед от по-старши служител/ ръководител, отговарящ за БИП/БФТ/ служител от друго звено, който може да има отношение към операцията/сделката.

## 2.2. Оценка на риска

Разработването на програмата за МТ следва да бъде базирано на резултатите от собствената оценка на риска на банката, така че контролът на МТ да се прилага за целия набор от рискове, на които е изложена институцията, и да е засилен в областите с идентифициран най-висок риск. Оценката на риска на банката следва да включва най-малко оценка на рисковите фактори, свързани с клиентите, продуктите и услугите, механизмите за доставка и географската експозиция, и идентифициране на рисковите фактори, които носят най-висок риск от изпиране на пари (ИП), финансиране на тероризма (ФТ) и финансиране на пролиферацията/разпространението на оръжия за масово унищожение (ФП), както и влиянието на въведения контрол за смекчаване на тези рискове. Оценката на риска служи за редица цели, включително, но не само, да позволи на банката (респективно ръководството) да:

- разбира вида на риска, свързан с бизнес отношенията и сделките;
- разработи политики, процедури и контрол, основани на риска;
- вземе информирани решения по отношение на ресурсите и набирането на персонал;
- приложи допълнителни проверки в дейностите/услуги/процеси, където е идентифициран повишен риск; и
- гарантира, че остатъчните рискове са в рамките на риска, който банката може да поеме.

Оценката на риска следва да се актуализира периодично (поне веднъж годишно), а също и при настъпването на съществени промени в стопанската дейност или рисковия профил на банката или в правната и регулаторната среда.

**Добри практики:**

- При промени в собствената оценка на риска от ИП/ФТ/ФП, особено когато промените са настъпили вследствие на отразяване на резултатите от НОР/секторни оценки на риска, преценка относно необходимостта от актуализация на системите за мониторинг.
- Разписване във вътрешнобанков документ на начина, по който резултатите от собствената оценка на риска от ИП/ФТ/ФП се използват за актуализация на системите за мониторинг.

### 2.3. Въвеждане на контролни механизми за наблюдение на трансакциите

МТ може да включва процеси на ръчно наблюдение и/или използване на автоматизирани и основани на проучване на данните/информацията системи за мониторинг. Във всички случаи подходящият вид и степен на наблюдение следва да съответства на идентифицираните рискове от ИП/ФТ/ФП на клиентите, продуктите и услугите на институцията, механизмите за доставка и географската експозиция и следователно могат да варират в зависимост от стопанските дейности или звената на банката, когато е приложимо. Програмите за МТ трябва да бъдат калибрирани според размера, естеството и сложността на всяка институция. Очаква се банки с по-голям мащаб на операциите да разполагат с автоматизирани системи, способни да се справят с рисковете от увеличен обем и сложност на сделките/операциите. Банките, използващи автоматизирани системи, следва да извършват оценка на типологията, за да разработят подходящи процеси и контроли за автоматизирано наблюдение, основани на правила или сценарии. Въпреки че по-малките банки могат да разчитат на по-малко автоматизирани системи за мониторинг, те все пак следва да гарантират, че създадената организация и процеси изпълняват по подходящ начин законовите им ангажименти за справяне с рисковете от ИП/ФТ/ФП.

Примери за автоматизирани инструменти включват специализирани автоматизирани системи за наблюдение на подозрителни дейности, основани на правила или сценарии, автоматизирани системи за следене на измамно поведение, системи за наблюдение на сделки по търговско финансиране, сделки с ценни книжа, автоматизирани инструменти за мониторинг на отрицателни новини и др.

Примерите за ръчно наблюдение включват докладване на необичайна дейност или необичайни сделки или операции от служители на фронт офис или от бизнес звената (включително, но не само, служители връзка с клиента (relationship manager) или такива, които по друг начин изпълняват функции, насочени към обслужването на клиенти), докладване на потенциално съмнителна дейност от служители на банката (включително вътрешно докладване от лица, сигнализиращи за нередности), ръчни прегледи на сделки, основани на документи (като сделки за търговско финансиране, сделки с ценни книжа или заеми), ръчна проверка за наличие на негативна информация и периодични или основани на събития прегледи на КПК.

Прилагането на автоматизирани системи за наблюдение не пречи за ползването и на ръчни способи за проверка и обратно.

Когато се използват изцяло ръчни способи за проверка, банките следва да провеждат по-често специализирано обучение относно политиките и процедурите за управление, за да се гарантира, че персоналът се придържа към вътрешните процеси за установяване и докладване на потенциално подозрителна дейност. Банките следва да гарантират, че тяхната програма за мониторинг на съмнителната дейност включва процеси във връзка с подаване на вътрешни сигнали за по-нататъшни проверки при необходимост. Независимо дали за извършване на МТ се използват автоматизирани или ръчни прегледи (или комбинация от двете), банката носи отговорност да докаже (например пред компетентен орган), че програмата за мониторинг е ефективна и се основава на подходящите за нея контролни механизми за смекчаване на рисковете.

**Добри практики:**

- В ситуации с установен по-висок риск от ИП/ФТ, банката прилага принципа на 4-те очи, комбинирано с извършване на последващ преглед на качеството на обработката на част от останалите сигнали (“alerts”)(извадка от сигнали).
- Резултатите от собствената оценка на риска от ИП/ФТ/ФП се използват за актуализация на системите за мониторинг, включително при създаване/актуализация на сценариите.
- Въз основа на резултатите от собствената оценка на риска от ИП/ФТ/ФП се преценява:
  - възможността за използване на системите за мониторинг за смекчаване на риска, установен за отделните продукти/услуги, като се отчитат техните характеристики и се обръща внимание на тези, оценени с по-висок риск, и
  - какъв вид мониторинг (в реално време и/или последващ) е най-подходящ за съответния продукт/услуга.
- В съответствие с подхода, основан на риска, банките определят рисково претеглени оценки на сигналите от МТ, за да приоритизират сигналите с по-висок риск за ускорен преглед и анализ. Въвеждането на този процес на приоритизиране може да бъде особено полезен за банки, при които автоматизираните системи за МТ генерират голям обем от сигнали.

## 2.4. Идентификация и управление на данните

Банките следва да разполагат с подходящи процеси, за да се гарантира, че данните за клиентите и трансакционните данни, подавани в тяхната програма за МТ (независимо дали се използват ръчни или автоматизирани процеси, или и двете) отговарят на установените стандарти за качество на данните, че данните подлежат на изпитване и валидиране на интервали, основани на риска, и че установените проблеми, свързани с качеството и пълнотата им, се отстраняват своевременно.

Банките следва да идентифицират и документират всички източници на данни, които служат като входящи данни в тяхната програма/система за МТ. Източниците на данни за МТ могат да включват както вътрешни клиентски бази данни, данни от основни банкови системи или други системи за обработка на трансакции/клиентски данни, така и външни източници, като например данни за съобщения на Society for Worldwide Interbank Financial Telecommunication (SWIFT). Когато се използват (автоматизирани) системи за МТ, банките следва да въведат документиране на процеси за зареждане и извличане на данни, за да се гарантира пълно, точно и напълно проследимо прехвърляне на данни от източника им към системите за МТ. Банките следва също така да гарантират, че правата на достъп на персонала до системите и данните (системите, от които се получават данни, така и до системите за мониторинг) са съизмерими с

техните функции и отговорности, така че да се гарантира, че съответният персонал може да изпълнява ефективно своите задължения и че достъпът не се предоставя на неоправомощени лица или на лица, които вече не се нуждаят от достъп до системата/данните.

За гарантиране на качеството на информацията/документите, генерирани като резултат от извършения мониторинг на трансакциите, следва да има определени служители, чиито основни задължения включват извършването на анализ на сигналите във връзка с мониторинга, както и да има разписани процедури/работни инструкции относно извършването на анализ и неговото документиране.

Банките следва да въведат подходящи механизми за контрол, които да им позволяват откриването на нови тенденции, рискове, както и за установяване на необичайно функциониращи контроли или сценарии за МТ и да се гарантира, че всички такива нередности, причинени от непълнотата или други проблеми с качеството на данните, се установят и отстраняват по подходящ начин. Когато е целесъобразно, следва да се извършва анализ на първопричините и всички констатации и препоръчани коригиращи действия следва да бъдат ескалирани към висшето ръководство, за да се реши своевременно основният проблем.

Както преди първоначалното внедряване на система или процес за МТ, така и на времеви интервали, основани на риска след това, банките следва да тестват и валидират пълнотата, точността и качеството на данните, за да гарантират, че точните и пълни данни се зареждат в тяхната МТ програма. Проверката и валидирането на данните обикновено следва да се извършват най-малко на всеки 12 до 18 месеца, по целесъобразност въз основа на рисковия профил на банките, а честотата на тези дейности следва да бъде ясно определена и документирана в политиките и процедурите им. При изпитването може също така да се използват количествени и качествени стандарти за качеството/количеството на данните или референтни показатели за проследяване на качеството и количеството на данните във времето

**Добра практика:**

- Зареждане на събираните клиентски данни в системата за мониторинг в машинночетим формат с цел данните да се използват при анализа относно генерирането и обработката на сигнали.
- Своевременно (поне в рамките на същия ден) и автоматично (или поне с минимална човешка намеса) прехвърляне на данните за клиенти и операции към софтуера за мониторинг.
- Актуализирането на данните за клиенти и операции, налични в тестовата среда на софтуера (ако такава е налична), се извършва регулярно и своевременно, с оглед поддържане на актуалност на сценариите/филтрите.
- Залагане на срок за извършване на регулярна проверка за съвместимост/коректност на данните в използваните софтуери за мониторинг.

и да се определи праг или обхват, над който нередностите в данните или други проблеми, свързани с качеството на данните, изискват (незабавни) коригиращи действия.

### 2.5. Вътрешна организация за осъществяване на мониторинг на трансакции

Банките следва да използват сценарии/критерии/филтри с цел да идентифицират потенциално подозрителни или незаконни сделки/операции, които да подлежат на последващ по-задълбочен преглед и анализ. Банките, използващи автоматизирани системи, следва да

извършват оценка на типологиите за съмнителна дейност, за да разработят подходящи възможности и процеси за автоматизирано наблюдение, основани на бизнес модела им. Сделките/операциите могат да бъдат подозрителни поради индивидуалните им характеристики (като тяхната стойност, източник, местоназначение или използване на посредници) или защото, заедно с други сделки/операции, те образуват модел, който се отклонява от очакваната или обичайната трансакционна дейност или по друг начин може да бъде показателен за незаконна дейност, включително заобикаляне на изискванията за докладване или водене на документация.

На база идентифицирания риск от ИП/ФТ (собствената оценка на риска по чл. 98 от ЗМИП) банката следва да:

- прецени кои рискове ще наблюдава в реално време и кои последващо. Обикновено автоматизираните системи за мониторинг извършват проверка на минало трансакционно поведение с различен обхват – дневно, седмично, месечно, по-дълъг период или при изпълнение на определени критерии, но не е изключено и да се извършва мониторинг в реално време - особено при идентифицирани по-високи рискове от ИП/ФТ;
- прецени сценариите/филтрите/контролите дали ще обхващат цялото трансакционно поведение на клиента или конкретна сметка/продукт/операция;
- кои продукти/услуги ще се наблюдават по-интензивно (например чрез дефинирани на сценарии/филтри/контроли, които наблюдават конкретни продукти/услуги – кредити, депозити, операции на АТМ и др.).

Правилата за МТ могат да бъдат автоматизирани или ръчни и следва да използват прагове и параметри, както от количествен, така и от качествен характер, които отчитат специфичните рискове и контекст на институцията, посочени в оценката на риска от ИП/ФТ/ФП, и конкретния продукт или услуга и вид клиент, участващ в сделката. За тази цел банките следва да съобразят характеристиките на сценариите/правилата с клиентите, продуктите и услугите, географията и механизмите за доставка и нивата на риск, които те носят за банката.

За да се установят моделите на потенциално подозрителна или незаконна дейност, обхващаща множество сделки, банките следва да групират отделните параметри и прагове на МТ в многофакторни рискови сценарии, за да се насочат по-точно моделите и поведението на трансакциите в съответствие с известните видове. Информация за типологии (повтарящ се модел или нова тенденция с единичен, но характерен случай и съответни специфични за типологията характеристики /индикатори) се извежда ежегодно от САДФР на ДАНС в годишните им отчети. Очаква се обаче банките с по-голям мащаб на операциите да разполагат с автоматизирани системи, способни да се справят с рисковете от увеличения обем и сложност на сделките. Във всички случаи следва да се поддържа документация, в която са описани сценариите, техните основни допускания, параметри и прагове.

При първоначалното въвеждане на (автоматизирани) системи за мониторинг или въвеждане на нови функционалности, банките следва да извършват предварително изпитване/тест на правилата и системата за мониторинг на трансакции, като използват по целесъобразност данни за трансакциите от минали периоди. Това изпитване следва да включва изпитване за интегриране на системата, за да се гарантира съвместимостта на системата за управление на МТ с другите системи на банката, с които тя ще си взаимодейства, както и изпитване от страна на ползвателите, за да се гарантира, че системата функционира, както се очаква в работна среда.

**Добри практики:**

- Банката извършва вътрешно сегментиране на клиентите и продуктите въз основа на риска, който е идентифицирала, и съобразява дефинираните сценарии и техните параметри с различните дейности.
- Когато е възможно и въз основа на риска, банките наблюдават сделките на ниво клиент или взаимоотношение, включително между финансови групи, а не само на база индивидуална сметка, за да получат пълна представа за профила на трансакциите на клиента в институцията.

### 2.6. Анализ на резултатите и отчетност

Банките следва да документират и проследяват резултатите от МТ, за да установят и решат всички технически или оперативни проблеми и да разберат основните рискове или тенденции. Нередностите в работата на системата за МТ, включително значителните промени в обема на сигналите, могат да бъдат показателни за проблеми, свързани с качеството или пълнотата на данните, или за необходимостта от прекалибриране на праговете или параметрите на сценариите/филтрите/контролите. Установените проблеми, свързани с качеството или пълнотата на данните, следва да бъдат ескалирани в рамките на банката (например до „собствениците“ на данните или на системите, от които се прехвърлят данните или до висшето ръководство) за предприемане на действия, а очевидните проблеми с калибрирането на заложените в системата правила (като напр. такива, които пораждат прекомерни обеми фалшиви положителни сигнали), следва да бъдат докладвани за настройка и оптимизация (към вендор, който предоставя системата или звеното, на което са вменени ангажименти за извършване на промени по функционалностите на системата).

Когато анализът на резултатите от МТ разкрива, че определени видове операции/сделки или модели са маркирани многократно от системата за мониторинг и след това последователно се изчистват като фалшиви положителни резултати, банката може да обмисли проверка на параметрите на сценариите си, използването на основана на риска логика за ограничаването им или друг процес на „бял списък“[2], за да се предотврати генерирането на сигнали за дейност, многократно считани за неподозрителни. Тези методи обаче не следва да се прилагат за по-рискови клиенти или видове сделки и следва да бъдат внимателно наблюдавани и да подлежат на периодично изпитване, настройка и валидиране.

[2] Банката може да обмисли създаването и поддържането на „бял списък“ с елементи от данни, които вече са уточнени и е установено, че не са носители на риск. Ако такива списъци се използват, банките следва да имат документирани процедури за управление и периодично преразглеждане и актуализиране на тези „бели списъци“, за да се осигури тяхната актуалност и отчитане на промяната в риска.

Освен това банките следва да гарантират, че висшето ръководство редовно се информира относно изпълнението и резултатите от тяхната програма за управление на МТ, включително чрез предоставяне на индикатори, тенденции и други доклади, генерирани от системите за МТ или изготвени от екипите за преглед и анализ на сигналите от МТ. Тези доклади може да включват анализ на броя на сигналите, генерирани от всяко правило, дела на сигналите, които са изчистени като фалшиви положителнисигнали, които изискват допълнителен преглед и анализ и които в крайна сметка водят до подаване на УСО. Докладването и анализът, свързани с МТ, следва да бъдат взети предвид при оценката на риска от ИП/ФТ/ФП, а ръководството на банката следва да използва тази информация, за да гарантира, че клиентите и техните сделки/операции остават в рамките на склонността на банката за поемане на риск и че дейност, надвишаваща склонността ѝ към риск, се преодолява чрез подходящи мерки за намаляване на риска, включително, но не само, използването на ограничения на дейността, продуктите или услугите.

**Добри практики:**

- Действията на служителя във връзка с обработката на сигнал за съмнение за ИП/ФТ (вкл. извършени проверки и събрана допълнителна информация/документи) и резултатите от извършения анализ се документират по надлежен начин в системата или ако това не е възможно, по алтернативен начин.
- Ако банката използва функционалност „бял списък“, е необходимо да е формализиран процесът по прегледа и актуализацията му, включително разпределянето на отговорностите и регулярност на прегледа.
- Регулярно (поне веднъж годишно) отчитане пред ръководния орган на резултатите от дейността, свързана с мониторинга на трансакции.

### 2.7. Тестване и валидиране след изпълнение

Периодично и в случай на съществени системни или оперативни нередности или въвеждане на нови функционалности банките следва да извършват повторна оценка на функционалността на системите и процесите на МТ, включително анализ за ефективността/релевантност на сценариите и калибрирането на характеристиките им. Както и при предварителното изпитване на изпълнението, изпитването след въвеждането следва да включва проверки за интеграцията на системата с другите системи на банката, качество на данните и оперативна функционалност и следва допълнително да включва тестване на въведените правилата за управление, за да се гарантира, че те остават актуални и ефективни при насочването към по-рискови сделки и дейности. Всяка предложена настройка или корекция на правилата за МТ, но особено при съществени промени във функционалностите и сценариите/контролите/филтрите, следва да бъде предмет на тестове преди внедряването им, като се използват данни от извадки от минали периоди, за да се гарантира правилното функциониране на новите или преразгледаните правила, и следва да бъде отразено в актуализираната документация за МТ.

Изпитването и валидирането на модела за МТ следва да се извършва от лица с достатъчен експертен опит и подходящо равнище на независимост от разработването и прилагането на модела. Като цяло валидирането следва да се извършва от лица, които не са отговорни за разработването или използването на модела за МТ, но това не следва да е пречка и потребителите на системата за мониторинг да извършват тестове на функционалностите на системата и дефинираните сценарии/филтри/контроли. Независимото тестване може да се извършва например от специализираната служба за вътрешен одит или от външен независим оценител. От практическа гледна точка някои дейности по валидиране могат да се извършват най-ефективно от разработчиците и/или ползвателите на системата и сценариите, но от съществено значение обаче е дейността по валидиране да подлежи на критичен преглед от независима страна, която следва да извършва допълнителни тестове, за да гарантира правилното валидиране. Всички дейности по валидиране на модела и установените проблеми следва да бъдат ясно документирани, а ръководството следва да предприеме незабавни действия за справяне с проблемите, свързани с модела.

**Добри практики:**
Процесът по преглед и актуализация на функционалностите на системата за мониторинг и характеристиките на сценариите/филтрите/контролите включва:

- Формално разписана (във вътрешнобанков документ) периодична регулярност за извършване на проверка на ефективността (например на годишна база);
- участие на бизнес звена;
- извършване и документиране на анализ на съответствието на правилата с бизнес модела на банката;
- документиране на предприетите действия и резултатите от прегледа;
- комбинация от количествен анализ и експертна преценка.

БНБ не извършва сертифициране и валидиране на софтуер/система/технологично решение на банка.

## 3. „Скрининг“ (проверка) за съответствие със санкциите

За изпълнение на целите на ЗМФТРОМУ[3] (чл. 2) от банките се изисква да идентифицират, предотвратяват и управляват рисковете от санкции (заобикаляне или неприлагане на ЦФС за ФТ и ФП). Това включва най-общо: да извършват проверки срещу приложимите санкционни списъци на своите клиентски бази от данни и проверка на операциите и сделките, които изпълняват.

**Ефективната програма за съответствие със санкциите се състои от следните основни елементи:**

- Поддържане на политики и процедури, които представляват вътрешнобанковата рамка по отношение на съответствието със санкциите, в които ясно и в пълнота са формализирани основните задължения на банката и разпределение на отговорностите на служителите, както и разписани работни процеси (вкл. по

[3] Въведени със ЗИД на ЗМФТ от 2025 г. (обн. в бр. 49 на „ДВ“ от 2025 г.)

ескалация на казуси) и описание на контролните механизми и тяхната приложимост.

- Добре калибрирана рамка, основана на риска: рисковете, пред които са изправени банките, са динамични и бизнесът, който осъществяват, зависи от много фактори, свързани с клиентската база, география на сделките и операциите, продуктите и услугите, механизмите за доставка. Поради това банките следва да оценяват рисковете, свързани със съответствието със санкции, да преразглеждат и подобряват своите рамки за съответствие със санкциите регулярно и при настъпване на определени „събития, водещи до възможни нарушения“, като например съществени промени в стопанската дейност или рисковия профил на банките или в правната и регулаторна среда, за да се гарантира, че те остават съобразени с рисковете от финансови престъпления на институцията.
- Ефективна интеграция на системите за скрининг на санкциите с останалите системи: ефективната програма за скрининг на санкциите зависи от качеството и пълнотата на данните, извлечени от клиентските и трансакционните системи и базите от данни на банките.
- Системите и процесите за проверка за съответствие със санкциите са от съществено значение, но са толкова ефективни, колкото е пълна, коректна и актуална информацията за клиента и информацията за сделките, използвана при сравняването с приложимите списъци със санкции. Поради това ефективността зависи критично от пълнотата и точността на информацията, получена чрез прилагането на мерки за комплексна проверка и съдържаща се в платежни инструкции и други полета за трансакционни данни.
- Въвеждащо и продължаващо обучение и осведоменост за рисковата експозиция: За да се гарантира правилното функциониране и изпълнение на техните програми за скрининг на санкциите, банките следва да гарантират, че служителите с отговорности по скрининга на санкциите разполагат с подходящ експертен опит и получават специално за функцията си обучение относно политиките, процедурите и рисковете на институцията за скрининг на санкциите, както и за работа със системите.
- Активен вътрешен контрол: Висшето ръководство на банките следва да има активна роля в осъществяване на ефективен контрол над изпълнението на програмите за скрининг на санкциите и да стимулира текущото подобряване на системите за скрининг на санкциите въз основа на рисковете, на които е изложена институцията. Когато резултатите от проверката на санкциите са компрометирани от фактори като неподходящо калибриране, неефективност на процесите, проблеми с персонала или неизправности на системата, е необходимо висшето ръководство (или комитет, определен от управителния съвет) да бъде своевременно информиран, за да се гарантира, бързо и по подходящ начин отстраняване на проблема. Висшето ръководство следва също така да дефинира ясно рисковия апетит в рамките на банката и да определи категорично, че прилагането на целевите финансови санкции е приоритет.

**Основните елементи на рамката за съответствие със санкциите включва:**

- избор на система/техническо или организационно решение, с която да се осъществяват проверките за съответствие със санкции, което да е адекватно и надеждно, за да се спазват ефективно задълженията;
- избор на сделките и операциите, които ще подлежат на проверки (вкл. кои платежни детайли ще подлежат на проверка) и как ще се извършват проверките на операциите и сделките (в реално време или последващ преглед);
- избор на клиентските данни и лица, които ще подлежат на проверки и на какви периоди.

### 3.1. Политики и процедури

Банката, за да подсигури пълното, правилното и навременното прилагане на приложимите санкции, следва да има ефективни политики, процедури и контроли. В тази връзка тя трябва да има действащи вътрешни процедури и инструкции, в които ясно и в пълнота да са формализирани основните задължения на банката и разпределение на отговорностите на служителите.

Политиките, процедурите и контролите на банката следва да обхващат най-малкото процеси гарантиращи, че:

- институцията разполага с цялата актуална информация относно приложимите санкции;
- списъците и изискванията на приложимите санкции се актуализират без забава след влизането им в сила;
- оценката на рисковата експозиция на санкциите остава актуална;
- е постигната съизмеримост с идентифицирания риск от нарушение на санкционните режими;
- политиките и процедурите за санкции:
    - редовно се преразглеждат;
    - редовно се изменят и актуализират, когато и където е необходимо;
    - се прилагат ефективно; и
    - разработени са по начин, който им позволява да се задействат необходимите действия, след като бъдат установени недостатъци.

Така описаните работни указания могат да са част от вътрешните правила на банката по чл. 101 от ЗМИП или отделен вътрешнобанков документ, като **следва да включват най-малко:**

- описание как са разпределени отговорностите във връзка със санкциите;
- действия по обработка на сигнали (“alerts”)за възможни съвпадения, вкл. при установяване на реално съвпадение - предприемане на мерките, предвидени в ЗМФТРОМУ;

- правила за документиране на процеса по извършване на анализа и решенията, взети по отношение на сигналите и документиране на действията, които са довели до тези решения (напр. изискана допълнителна информация, документи или извършени справки и резултатите от тях);
- какви мерки за комплексна проверка следва да се прилагат при обработката на сигнали (“alerts”): банката следва формално, във вътрешнобанков документ (напр. в работна процедура или указание), да е разписала процеса по обработка на сигналите (“alerts”), вкл. процес по ескалация относно ситуации, когато данните за лицето, които са налични в банката, не са достатъчни за отхвърляне или потвърждение на съвпадението.
- нива на преглед на обработката на сигналите (“alerts”) (например приложение на принципа на 4-те очи).

**Добра практика:**
- В ситуации, при които има потенциален по-висок риск от несъответствие със санкциите, банката прилага принципа на 4-те очи, което е комбинирано с извършване на последващ преглед на качеството на обработката на част от останалите сигнали (“alerts”) (извадка от сигнали (“alerts”)).
- Процесът по ескалация може да включва: служителите на фронт офис изискват допълнителна информация или документи от клиента, напр., когато е установено съвпадение в данните за контрагента или основанието за плащане; препращане на информацията за преглед към по-старши служител/до ръководителя, отговарящ за съответствието със санкции/ до служител от друго звено, което може да има отношение към операцията/сделката.

### 3.2. Оценка на риска

Съответствието със санкциите е комбинация от прилагането на подход, базиран на правило и рисков-базиран подход.

Подходът, базиран на правило, включва изпълнение на законовото изискване за пълно прилагане на ЦФС за ФТ и ФП и предвижда задължение за блокиране на финансови средства и други финансови активи или икономически ресурси и забрана за предоставяне на финансови услуги, финансови средства и други финансови активи или икономически ресурси на лица по чл. 4б от ЗМФТРОМУ.

Прилагането на рисково-базиран подход дава възможност на банките да гарантират, че техните политики, процедури и механизми за контрол на неизпълнение на санкциите са съизмерими на рисковата им експозиция, и по-конкретно да определят дали всички структурни звена разполагат с необходимите ресурси, за да осигурят ефективно им спазване. Рисково-базираният подход в превенцията на рисковете от санкции включва преценка кои клиентски данни или данни от операциите следва да се проверяват, кога/как с каква честота да се извършва скрининг и каква „размита логика“ („fuzzy logic“) да се заложи.

Вътрешнобанковите процедури и инструкции на банките следва да включват ангажимент за извършване на оценка на рисковата експозиция на банката за възможно неспазване/нарушаване/заобикаляне на санкциите, за да се разбере степента, в която всяка област от тяхната дейност е изложена на риска от неспазване или заобикаляне на санкциите и

за да могат да определят какви контролни механизми следва да въведат, за да са в съответствие със санкциите.

Банката следва да има предвид, че въпреки че в общия случай оценката на рисковете от изпирането на пари и финансирането на тероризма и оценката на рисковата експозиция за възможно несъответствие/заобикаляне със/на санкциите да включват оценка на един и същи елементи, то нивата на риск, които носят, могат да се различават.

Оценката на рисковата експозиция може да е част от собствената оценка на риска по чл. 98 от ЗМИП, може да е и отделен документ - по преценка на банката като се взима под предвид естеството и сложността на бизнес модела на банката, като същият следва да се одобрява от висшето ръководство. Тя следва да се актуализира периодично (поне веднъж годишно) или при настъпване на „събития на задействане“: като например съществени промени в стопанската дейност (например: преди предоставяне на нови продукти, предлагане на нови механизми за доставка, обслужване на нови групи клиенти, навлизане в нови географски райони) или рисковия профил на банката, в правната и регулаторната среда (такива може да са приемане на нови санкционни списъци и значителни промени в съществуващите такива) или установени недостатъци във вътрешната организация по спазването на санкциите (установяване на неприлагане и/или заобикаляне на санкции или установени недостатъци в съществуващата оценка на рисковата експозиция на санкциите, установени от банката или от надзорен орган).

Оценката на риска на банките следва да включва най-малко оценка на клиентите, продуктите и услугите, механизмите за доставка и географския риск, чрез които банката може да влезе в делови взаимоотношения (пряко или непряко) със санкционирани лица, групи и организации, както и степента на въведения контрол за смекчаване на рисковете от заобикаляне/неспазване на санкционни режими за ФТ/ФП.

Когато е част от **група**, банката следва да се увери, че изготвената оценка на рисковата експозиция от санкции, както и политиките и процедурите са в съответствие с груповите такива, дотолкова доколкото същите са в съответствие с местното законодателство и специфики. Банката трябва да има разписан и документиран процес за ескалация/информиране на дружеството майка при установено несъответствие на груповите политики и процедури с местни законови изисквания и изискване за даване на изключение (неприлагане на съответното правило от груповата политика, което е в противоречие с местното законодателство).

Банките следва да документират методологията си за провеждане и преглед на своите оценка на експозицията на ограничителни мерки и резултатите от тази оценка и да ги на компетентния орган при поискване.

### 3.3. Въвеждане на скринингови механизми за контрол на санкциите

Скринингът на санкциите може да включва използването на автоматизиран софтуер и системи за скрининг, както и ръчно наблюдение на клиентите и сделките с приложимите списъци със санкции. Във всички случаи подходящият метод за скрининг на санкциите и използваните критерии за проверка следва да бъдат съобразени с рисковете от заобикаляне/неспазване на санкционни режими за ФТ/ФП от страна на клиентите, продуктите и услугите на институцията, механизмите за доставка и географската експозиция, и следователно могат да варират в различните стопански дейности или звена на банката. Областите на повишен риск може да изискват допълнителни мерки за комплексна проверка,

свързани със санкциите, по-чести или по-интензивни ръчни прегледи на клиенти, контрагенти и техните сделки, засилен мониторинг на сделките или поведението, или специализирано обучение за персонала, отговарящ за спазването на санкциите.

Проверките за скрининг на санкциите следва също така да бъдат съобразени с размера, естеството и сложността на всяка институция. Очаква се банките с по-голям мащаб на операциите да разполагат с автоматизирани системи, способни да се справят с рисковете от увеличен обем и разнообразие на сделките. Въпреки че по-малките банки могат да разчитат на системи/технически решения за скрининг на санкции, които са по-малко автоматизирани, те следва също така да гарантират, че управляват по подходящ начин рисковете от нарушението/заобикалянето на санкции в ежедневната им трансакционна дейност.

Примерите за автоматизирани системи включват автоматизирани инструменти за проверка на имена, които сравняват клиентските бази данни с приложимите списъци със санкции, инструменти за филтриране на трансакции, които сравняват данните за платежни нареждания и трансакции с приложимите списъци със санкции преди изпълнението, както и инструменти за анализ на текст, които автоматично преобразуват документацията на хартиен носител в електронни данни (OCR технология), които след това могат да бъдат проверени в приложимите списъци със санкции.

Примерите за ръчен преглед включват ръчно докладване и ескалиране на потенциално свързана със санкции дейност (напр. от банкови служители, които отговорят за връзките с клиенти или служители, отговарящи за др. бизнес линии в банката), ръчни прегледи на трансакции, базирани на документи (като документални сделки за търговско финансиране или заеми) и/или периодични или основани на конкретни събития прегледи на клиентската база.

Независимо от това дали за извършване на скрининг на санкциите се използват автоматизирани или ръчни процеси (или комбинация от двете), задължение на банките е да докажат, че програмата за скрининг е ефективна и изборът ѝ е в съответствие с идентифицирания риск от нарушение/заобикаляне на санкциите.

### 3.4. Идентификация и управление на данните

Банките следва да разполагат и с подходящи процеси, за да гарантират, че данните за клиентите и трансакционните данни, използвани в тяхната програма за скрининг на санкциите (независимо дали използват ръчни или автоматизирани процеси, или и двете), отговарят на установените стандарти за качество и пълнота на данните, че данните подлежат на изпитване и валидиране на интервали, основани на риска, и че установените проблеми с качеството им се отстраняват своевременно. Международният стандарт (последна актуализация на Препоръка 16 на FATF от 18.06.2025 г., чиито изисквания следва да се прилагат от 2030 г.) и Регламент 2023/1113 (TFR) обръщат особено внимание на необходимостта платежните детайли на преводите на средства да се предават в пълнота по цялата платежна верига[4] и да са структурирани по начин, който да позволява еднозначното идентифициране на данните, относими за платеца и крайния получател на средствата, както и ДПУ на платец и ДПУ на получател и държавата, в която те осъществяват дейност[5].

[4] Пар. 6 от Препоръка 16 и чл. 10 от TFR.
[5] Пар. 4 и 7 от Препоръка 16 и чл. 7 от TFR.

Служителите, чиито основни задължения са свързани със спазването на санкциите, при установени пропуски или неточности в съответната информация за клиента или действителния собственик или пропуски или проблеми с качеството на данните в полетата за трансакции или за платежни съобщения, следва да предприемат приоритетно действия за решаването на установения проблем, за да гарантират правилното използване на видовете съобщения и спазването на изискванията за прозрачност на плащанията.

Банките следва да идентифицират и документират всички източници на информация, които служат като входящи данни в тяхната програма за скрининг на санкциите, включително приложимите клиентски бази данни и основните банкови или други системи за обработка на трансакции. Следва да е документиран собственикът на системата или основното звено, който/което отговаря за надзора върху качеството на изходящите данни и за решаването на установените проблеми с данните. Когато се използват (автоматизирани) системи за скрининг на санкции (които не са част от БИС), банките следва да гарантират, че интеграцията между БИС и системата за скрининг е успешна и няма забавяне или не са установени грешки при прехвърлянето на данни. Банките следва да гарантират, че правата на достъп на служителите както до системите, от които идва информацията (например счетоводна или БИС), така и до системите за проверка на санкциите, са съизмерими с техните роли и отговорности, така че съответните служители могат да изпълнява ефективно своите задължения и че достъпът не се предоставя на неоправомощени лица или на лица, които не се нуждаят от достъп до системата (този процес следва да включва и разграничение на ролите за достъп).

Както преди първоначалното въвеждане на система или процес за скрининг на санкциите, така и на интервали, основани на риска, след това, банките следва да тестват и валидират пълнотата, точността и качеството на данните, за да гарантират, че точните и пълни данни се ползват в тяхната програма за скрининг на санкциите. Изпитването и валидирането на данните обикновено следва да се извършват най-малко на всеки 12 до 18 месеца, по целесъобразност въз основа на рисковия профил на банката, а честотата и обхвата на тези дейности следва да бъдат ясно определени и документирани в политиките и процедурите.

Освен това банките следва да въведат подходящи механизми за контрол на установяването на проблеми, като например анализ на тенденциите, наблюдавани чрез данните от процеса на мониторинг, и изготвяне на доклади за изключения, за да се установи необичайно функционираща логика за скрининг на санкциите и да се гарантира, че всички такива нередности, причинени от качеството и пълнотата на данните или функционалности на системата, се установяват и отстраняват навременно и по подходящ начин. Когато е целесъобразно, следва да се извърши анализ на първопричините, а всички констатации и препоръчани коригиращи действия следва да бъдат ескалирани до висшето ръководство за своевременно решаване на основния проблем.

### 3.5. Вътрешна организация за осъществяване на скрининг

Политиките и процедурите на банката във връзка със спазването на приложимите санкции следва да съдържат документирана обосновка на рисково-базираните решения (или на база технологични ограничения), които банката е взела при преценката кои операции/сделки и каква част от клиентската база, как – в реално време или последващо, и автоматично или ръчно и кои детайли на операциите/сделки и клиентски данни да проверява срещу санкционните списъци.

Например, ако банката прецени да не проверява определени лица, операции/сделки или информация/данни срещу санкционните списъци, то следва този избор да е надлежно обоснован в изготвената оценка за рисковата експозиция за съответствието със санкциите.

По-надолу в Насоките терминът, който ще е се използва за процеса на проверката на клиентската база, е „скрининг на имена“.

Сигналите, генерирани от системата за скрининг, следва да съдържат информация за това в кой списък е установено възможното съвпадение (ако е приложимо) и данните за санкцията (напр., ако става въпрос за установено съвпадение със санкционирано лице, ако е приложимо, следва да има информация за всеки списък, в който е установено съвпадението и данните, с които лицето присъства в тези списъци).

При извършване на анализ на сигнала (“alert”), за да се установи дали системата е установила реално или фалшиво съвпадение, служителят, който обработва сигнала (“alert”), следва да има достъп до информацията, която банката е събрала при прилагане на мерките за комплексна проверка (вкл. идентификационни данни като идентификационен номер, дата и място на раждане, всички гражданства, които лицето притежава, адрес, данни за контакт и др.), на база която да прецени дали има реално съвпадение.

### 3.1.1. Скрининг на имена

При определяне на обхвата на скрининга на имена банката следва да вземе следните решения на база оценката за рисковата експозиция от нарушаване/заобикаля на санкции, които да са надлежно документирани и придружени с аргументация при прилагане на изключения:

- ***Кои лица да проверява***

Скринингът на имена следва да включва: (потенциални) клиенти, приходящи клиенти[6], действителни собственици на клиенти-ЮЛ, пълномощници, законни представители и други лица, подлежащи на идентификация във връзка с клиента, както и различни контрагенти, с които банката има делови взаимоотношения (например.: доставчици, наемодатели, наематели и др.)

- ***Кои данни да подлежат на преглед***

Обичайна практика е да се извършват проверки на имената на лицата, а другите налични данни за лицето, събрани във връзка с прилагането на мерките за комплексна проверка (идентификационен номер, дата и място на раждане, гражданство, адрес и др.), да се използват за потвърждение или отхвърляне на установеното съвпадение.

- ***Как да се извършват проверките***

Зависи от това какво решение за скрининг за санкции банката използва и респективно може да е ръчно или автоматично. Обичайна практика е лица, които не са регистрирани в системите на банката (например приходящи клиенти или контрагенти по случайни операции, лица във връзка с банкови гаранции или акредитиви, които не са клиенти и др.), да се проверяват ръчно, докато лицата, които са регистрирани в системите на банката, да подлежат на (полу)автоматична проверка.

[6] Приходящи клиенти – клиенти, които извършват случайни операции, и с които банката не влиза в трайни делови взаимоотношения

- ***Кога да се извършват проверките***

Проверката на имената (независимо дали е автоматизирана или ръчна) трябва да се извършва преди встъпване в делово взаимоотношение с клиента и/или преди извършване на случайна сделка и периодично през цялото времетраене на деловите взаимоотношения.

Времевите периоди, през които банката преценява да извършва периодичната проверка, следва да зависят от оценката от рисковата експозиция във връзка със съответствието със санкции.

Периодичният преглед може да е на фиксиран период (например всеки работен ден) или на база задействащи събития като:

- промяна в някои от санкционните списъци;
- при промяна на клиентските данни или при заявяване на нов продукт/услуга;
- при активност по сметките на клиента;
- ако са налице основателни причини за съмнение, че клиентът или всяко лице, което е упълномощено да действа от името на клиента, се опитва да заобиколи санкциите.

При избор на периодичността за извършване на регулярна проверка, банката следва да се подсигури, че в приемлив времеви период (например: всяка седмица/на две седмици) цялата клиентска база на банката се проверява за съвпадания в санкционни списъци независимо дали са настъпили някои от дефинираните задействащи събития или не.

**Когато се задават времеви периоди за извършване на проверки трябва да се има предвид следното:**

- Методология на FATF: Задължените лица следва да имат създадени и работещи процедури и контроли за установяване дали техен (потенциален) клиент е санкционирано лице/организация. Това включва проверка на клиентите при встъпване в делови взаимоотношения и последващо при всяка промяна на санкционните списъци или промяна на клиентските данни. При чести промени в списъците, проверката трябва да се извършва всеки ден.
- В случаите когато банката следва да прилага Регламент (ЕС) 260/2012, е необходимо да се съобрази с периодичността на скрининга на незабавните преводи, съобразно чл. 5г от посочения регламент.

- ***Задължителни технически функционалности***

В системата за мониторинг за санкции следва да е заложена проверка не само за пълни съвпадения в санкционни списъци, но и за близък правопис или техники за размито съвпадение („fuzzy logic“), на база които да се генерират качествени сигнали.

Банката следва да подсигури данните на клиентите в системите за мониторинг да са налични на езика, на който са санкционните списъци, срещу които се проверяват. ). Съпоставяне на данни, които са изписани на различни езици (на кирилица и/или латиница), няма да доведе до валиден и коректен резултат относно възможно съвпадение със санкционни списъци.

### 3.1.2. Скрининг на трансакциите

При определяне на обхвата на скрининга на операциите банката следва да вземе следните решения на база оценката за рисковата експозиция от нарушаване/заобикаля на санкции, които следва да са надлежно документирани и придружени с аргументация при прилагане на изключения:

- ***Кои операции/сделки да проверява***

Скринингът във връзка с операциите/сделките включват решение кои типове операции да се проверяват (всички, само клиентски плащания, само плащания в чуждестранна валута, операции над определени прагове и др.). Обичайна практика е част от плащанията да са изключени от процеса на мониторинг за санкции от презумпцията, че доставчиците на платежни услуги, които участват в операцията, следва да спазват един и същи законови изисквания относно санкциите и в тази връзка тези сделки и операции носят по-нисък риск от неспазване/заобикаляне на санкции: например националните плащания или SEPA плащанията, както и вътрешнобанкови плащания – от презумпцията, че и двамата участници в операцията (получател и наредител) са клиенти на банката и тя извършва регулярни проверки на клиентските си бази от данни, което е допълнителна контрола.

Банките следва да имат предвид, че ЗМФТРОМУ не прави разграничение между видовете плащания, както и размера на сумата и в тази връзка всяко едно решение за изключване на операции/сделки от скрининга на операции е рисково-базирано решение на банката, което трябва да бъде документирано и придружено с анализ относно риска от нарушаване/заобикаляне на санкциите и което представлява приемане на определено ниво на риск от нарушаване на санкционните списъци с ограничителни мерки (ЦФС за ФТ и ФП) от страна на банката.

Банката следва да прецени и кои видове съобщения (message type in SWIFT) ще проверява за санкции на база преценка кои съобщения могат да имат атрибути, относими за скрининга за санкции. Обичайно се извършва проверка на тези съобщения, чрез които се прехвърлят средства (MT10X, MT20X)[7], като в някои случаи се проверяват и текстови съобщения (MT19X, MT9XX, MT7XX и др.) във връзка с банкови гаранции и акредитиви.

- ***Кои данни да подлежат на преглед***

Не всички елементи на данните са от значение за скрининга на санкциите. Когато определя кои референтни данни следва да бъдат проверявани, банката следва да идентифицира данните в рамките на своите операции и записите, които са от значение за риска от санкции, да определи и гарантира, че те са достатъчни за ефективен скрининг, и да ги разграничи от данните, които не са от значение или не са подходящи за скрининг. Данните, които трябва да бъдат да бъдат проверени, следва да включват най-малко:

- Информация за получател и наредител (данните в поле в SWIFT 50 и 59 – това включва не само имената на получателя и наредителя и сметките, но останалите данни в тези полета като адрес);
- Основание за плащане;

[7] Препоръка 16 на FATF (Пар. 13-19), която има отношение към скрининга за възможни съвпадения със санкционни списъци, I и TFR (чл. 2) предвиждат определени изключения в приложното поле като: когато платецът, така и получателят са доставчици на платежни услуги, които действат от свое име, операции, свързани със сетълмент и клиъринг, преводи на средства, представляващи поредица от операции (batch) и картови плащания.

- Детайли на доставчиците на платежни услуги, които участват в операцията/сделката (BIC, SWIFT code);
- Други данни.

Други данни, които са относими към операции и сделки, различни от трансфери:

- ISIN кодове или други свързани с риска идентификатори на продукти, включително тези, които се отнасят до идентифициране на секторни санкции в рамките на сделки, свързани с ценни книжа;
- Документация за търговско финансиране, включително:
    - Вносители и износители, производители, платци, нотифициращи страни;
    - Корабни дружества, имена на плавателни съдове и номера на Международната морска организация (ММО), имена на страните, свързани с плавателния съд (включително корабособственици, чартьори и капитани), и спедитори;
    - Посредници, като застрахователни дружества, агенти и брокери; и
    - Доставчици на платежни услуги, включително емитиращи, консултиращи, потвърждаващи, преговарящи, претендиращи, събиращи, възстановяващи и гарантиращи банки.
- Географски данни, включително:
    - Адреси, държави, градове, региони, пристанища и летища (например съдържащи се в полета 50 и 59 на SWIFT или придобити чрез запитвания за проследяване на плавателни съдове);
    - Телефонни или факс номера и уеб адреси, доколкото те съдържат географски или други релевантни данни;
    - Място на получаване, изпращане, доставка или крайно местоназначение;
    - Страна на произход, местоназначение и разтоварване на стоки или услуги;
    - Летище на заминаване или местоназначение и др.
- ***Как да се извършват проверките***

Зависи от това какво решение за скрининг за санкции банката използва. Обичайна практика е сделките, които са в електронна форма, да се проверяват автоматично. Насоките на ЕБО относно рисковите фактори, свързани с ИП/ФТ предвиждат банките, които обработват голям обем сделки или сделки с голяма честота, да обмислят въвеждането на автоматизирана система за наблюдение на сделките.

При някои видове трансакции обаче все още се разчита на документация в различни формати и различни методи на представяне на данни – например сделки за търговско финансиране като банкови гаранции и акредитиви, чекове, сделки с ценни книжа, които предполагат ръчни проверки.

- ***Кога да се извършват проверките***

Банката следва да проверява операциите/сделките за съответствие с приложимите ограничителни мерки по санкционни списъци преди изпълнение на превода независимо дали става въпрос за операция/сделка, която се изпълнява в рамките на делови взаимоотношения или като случайна операция/сделка на приходящ клиент, ссвен в случаите, предвидени в чл. 5г от Регламент (ЕС) 260/2012[8].

Сделки и операции, които са изключени от скрининга за санкции (в реално време), могат да се проверяват последващо (вкл. на извадков принцип).

- ***Задължителни технически функционалности***

В системата за мониторинг за санкции следва да е заложена проверка не само за пълни съвпадения в санкционни списъци, но и за близък правопис или техники за размито съвпадение („fuzzy logic“), на база които да се генерират качествени сигнали (“alerts”).

Банката следва да подсигури данните по операциите/сделките да са налични на езика, на който са санкционните списъци, срещу които се проверяват или т.нар. транслитерация на данните.

### 3.6. Управление на списъците

Банките следва да включат във вътрешнобанков документ информация за това кои санкционни списъци са приложими за тях на база оценката за рисковата експозиция, вкл.:

- как са разпределени отговорностите за проследяване на актуализации на приложимите списъци и за актуализиране на данните в системите, чрез които банката извършва проверки на клиентската база и на операциите и сделките.
- ако банката има вътрешни списъци, които имат отношение към санкциите (вкл. бели списъци), процес по включване, промяна или изтриване на записи в тях, както и периодичен преглед и актуализация.

Съгласно чл. 4б от ЗМФТРОМУ[9] списъците за проверка за съответствие със санкциите на банките трябва да включват всички имена в списъците, издадени от Съвета за сигурност на ООН и съответните комитети (консолидирания списък на ООН за ФТ и ФП); санкции за тероризъм или финансирането му, както и санкции за разпространение на оръжия за масово унищожение и финансирането му, наложени с регламент на Съвета на Европейския съюз (консолидиран списък на ЕС на ФТ и ФП); или от Министерския съвет на Република България (местния списък за ФТ). Процесите на проверка в санкционните списъци от страна на банките следва също така да включват търсене на субекти[10], които сами по себе си не са включени в санкционни списъци, но които са притежавани или контролирани основно или изцяло от включено в списъка лице (или т. нар. вторични санкции). Въпреки че поради самото си естество тези субекти/лица не са включени в санкционни списъци, банките могат да разработят вътрешни списъци на такива лица въз основа на собствената си комплексна проверка и разглеждане на външни източници, като например негативни медии новини.

[8] Регламент (ЕС) 260/2012 е за определяне на технически и бизнес изисквания за кредитни преводи и директни дебити в евро; чл.5г от него е за скрининг на ППУ от ДПУ, които предлагат незабавни кредитни преводи, за проверка дали ППУ е лице или образувание, на което са наложени конкретни финансови ограничителни мерки.
[9] Промени със ЗИД на ЗМФТ от 2025 г. влезли в сила с бр. 49 на ДВ от 17.06.2025 г.
[10] Юридически лица/други правни образувания, притежавани или контролирани от физически или юридически лица, групи или организации, посочени в санкционен списък на ЦФС за ФТ или ФП.

Като се има предвид динамичният характер на целевите финансови санкции, банките следва да създадат и прилагат процедури за управление на списъците със санкции, които дават възможност на програмата за скрининг на санкциите на институцията да се адаптира бързо към промените, публикувани от органите за налагане на санкции. От значение за ефективното управление на списъците е всеки от тях да се преразглежда редовно и това да се документира, за да се гарантира, че избраният от банките подход остава в съответствие със склонността към риск и в съответствие с приложимите правни изисквания:

- Избор на списък: Банката следва да определи кои списъци, имащи отношение към санкциите, са от значение за скрининга ѝ. Списъците трябва да включват най-малко всички лица, които са включени в чл. 4б от ЗМФТРОМУ: консолидираните списъци на ООН, ЕС и списъка на МС на Р България, но могат да се включват и други списъци от юрисдикции11, в които банката осъществява бизнес, както и вътрешни списъци с географски термини (като градове, региони и пристанища), банкови идентификатори (като BIC) и списъци на забранени стоки или забранени ценни книжа, когато е приложимо. Допълнителните списъци могат да бъдат използвани въз основа на преценката на банката за наличието на риск.
- Набавяне на списъци: обикновено изборът е между това списъците да се набавят директно от международния/националния орган, който издава съответния списък или от външен доставчик (напр. Worldcheck, Lexis Nexis, Dow Jones и др.). Основните преимущества на използването на надежден външен доставчик са: списъците може да са обогатени с транслитерация на имената на други езици, да има допълнени варианти на изписването на името и друга допълнителна информация и са в подходящ за използване/зареждане в система формат. Групата Wolfsberg дава като пример за преимущество и избягването на дублиращи записи (много често определени лица присъстват в повече от един списък), но следва да се има предвид, че за да се вземе информирано решение при възможно съвпадение, следва да е налична информация в кой списък е установено съвпадението. Основните преимущества на набавянето на списъците директно от международния/националния орган са: навременно набавяне на актуализираните списъци, избягване на възможни грешки при консолидиране на списъците и същото не е свързано със заплащане на определена такса за услугата.
- Поддръжка на списък: банката следва да формализира (разпише във вътрешнобанков документ) процесите за добавяне на записи и тяхното заличаване във вътрешните списъци, когато вече не се изисква скрининг или когато резултатът е в рамките на склонността на институцията към риск. Доколкото поддържането на вътрешен списък е по преценка на банката, следва да има и ясно формализиран процес по периодичен преглед на записите в него и преценка доколко основанието за „престой“ в него не е отпаднало. В тази връзка, банката следва да идентифицира и въведе подходящи мерки за контрол, за да се гарантира, че списъците остават актуални и че само оторизирани лица могат да добавят или премахват лица от списъците, ползвани в рамките на банката. Списъците, които се издават от международни/национални органи, следва да се поддържат актуални

[11] Напр. САЩ, Великобритания и други.

и коректни, като се прилага FATF стандарта за прилагане на санкциите „без забава“ (without delay[12]). Поддръжката на списъци следва да включва и извършване на тестове за коректност на данните, които се зареждат в системата, при всяко актуализиране на списъците (например: на извадков принцип).

- Подобряване на данните: банката следва да определи дали определени записи в списъците следва да бъдат изменени или актуализирани въз основа на събрана допълнителна информация.
- Включване в бял списък: банката може да обмисли създаването и поддържането на „бял списък“ (ако системата за мониторинг, която използва, има такава функционалност) с имена на клиенти или други елементи от данни, за които вече е установено, че са фалшиви съвпадения на база приложени мерки за разширена комплексна проверка. Тези „бели списъци“ могат да се използват за подобряване на процеса, свързан със скрининга, чрез използване на резултатите от извършена комплексна проверка и намаляване на броя на фалшивите положителни резултати. Въпреки това, банката не следва да разчита прекалено много на такъв списък и трябва старателно и непрекъснато да проверява записите в него при актуализации на списъците, срещу които банката извършва проверки за съответствие със санкциите. Банката следва формално да разполага с документирани процедури за управление и периодично преразглеждане и актуализиране на тези „бели списъци“, за да се отчете възможността лицата, включени в бял списък, по-късно във времето да бъдат включени в санкционен списък за ФТ/ФП евентуално от съответен орган за налагане на санкции. Процедурите за управление на списъците следва да бъдат документирани и да подлежат на периодичен преглед, за да се гарантира, че практиките за управление на списъците продължават да бъдат в съответствие с рисковия профил и склонността към риск на банката.

### 3.7. Анализ на резултатите и отчетност

Банките следва да документират и проследяват резултатите от скрининга на санкциите, за да установят и отстранят всички технически или оперативни проблеми и да разберат основните рискове или тенденции във времето. Нередностите в ефективността на системата за скрининг на санкциите, включително значителните промени в обема на генерираните възможни съвпадения в списъците със санкции с течение на времето, може да са показателни за проблеми, свързани с качеството на данните или пълнотата им, или за необходимостта от прекалибриране на логиката за търсене при скрининга на санкциите. Установените проблеми, свързани с качеството или пълнотата на данните, следва да бъдат докладвани на собствениците на данни в дадена банка[13], а проблемите с логиката на скрининга следва да бъдат докладвани за настройка и оптимизация.

[12] Пленарната сесия на FATF от февруари 2018 г. потвърди, че дефиницията на израза по отношение на прилагането на ЦФС означава „в идеалния случай в рамките на часове“, но практически се разбира „не повече от 24 часа“.
[13] Структурни звена в банката, които събират и създават данни за определена цел.

### 3.8. Тестване и валидиране на системата

Банките следва да определят как да калибрират настройките на (автоматизираната) система за скрининг, за да се постигне нужният баланс между качеството на сигналите (“alerts”) и същевременно да се гарантира спазването на санкциите (прилагане на санкционни списъци и ограничителни мерки). Въз основа на оценката на рисковата експозиция за санкциите и редовното тестване, банките следва най-малко да:

- а определят подходящите параметри на съвпадение, които е вероятно да генерират качествен сигнал, позволяващ на банките да изпълнят задължението си за спазване на санкциите, като проверят праговете на истински положителни сигнали (“alerts”), свързани с различни проценти на съвпадение. Калибрирането следва да бъде нито твърде чувствително, което води до голям брой фалшиви положителни съвпадения, нито недостатъчно чувствително, което да доведе до пропуски в генерирането на сигнали за реални съвпадения в санкционни списъци;
- при използване на (автоматизирана) система за скрининг, базирана на алгоритъм, според който функционалността на системата предвижда проверка не само за пълни съвпадения в санкционни списъци, но и близък правопис или техники за размито съвпадение (fuzzy logic).
- да осигурят процес по проверка на целостта и коректността на данните предвид че в общия случай в системите за скрининг се зареждат данни от различни източници и канали.

Банките следва периодично (например веднъж годишно) да преглеждат ефективността на системата за скрининг, за да гарантират, че тя остава ефективна и продължава да идентифицира надеждно възможни несъответствия/нарушения или заобикаляне на санкциите. Преглед следва да се извършва и извънредно при необходимост, ако банката има опасения, че системата може да не е в съответствие с приложимите санкции - в случай на установени съществени системни или оперативни нередности банките следва да извършват повторна оценка на функционалността на системите и процесите за скрининг на санкциите, включително настройките на праговете и правилата за скрининг, както и точността и пълнотата на данните, използвани в процеса на скрининг. Всички предложени съществени корекции на логиката за установяване при скрининг на санкциите следва да подлежат на тестване преди внедряване в реална среда /на работния процес, като при тестването следва да се използват примерни или исторически данни, за да се гарантира правилното функциониране на новата или преразгледаната логика, и да бъдат отразени в актуализираната документация за скрининг на санкциите.

Тестването и валидирането на модела за скрининг на санкциите следва да се извършва от лица с достатъчен експертен опит и подходящо равнище на независимост от разработването и прилагането на модела. Като цяло валидирането следва да се извършва от лица, които не носят отговорност за разработването или използването на модела за скрининг на санкциите. Независимостта може да бъде подкрепена от разделяне на линиите на докладване, напр. валидирането на модела се извършва от вътрешен/външен одит или консултант, като звено, което не е ангажирано с разработване и ползване на модела. От практическа гледна точка някои дейности по валидиране могат да се извършват най-ефективно от разработчиците и

БНБ не извършва сертифициране и валидиране на софтуер/система/технологично решение на банка.

ползвателите на системата, но същите след това следва да се валидират и от независима страна.

Всички дейности по валидиране на модела и установените проблеми следва да бъдат ясно документирани, а висшето ръководство следва да предприеме незабавни действия за справяне с проблемите, свързани с модела.

## 4. Управление и контрол

### 4.1. Роля на висшето ръководство

Висшето ръководство на банката следва да упражнява активен контрол върху основните рискове от ИП/ФТ/ФП и неприлагане на санкционните режими или тяхното заобикаляне и върху въведените контролни механизми за смекчаване на тези рискове, което неизчерпателно се изразява в:

- Носи крайната отговорност за въвеждането, одобрението и спазването на ясни и подходящи политики и процедури, които са пропорционални на рисковата експозиция на банката, както и че съществуват ефективни системи за осъществяване на мониторинг върху операциите за евентуална съмнителна дейност или възможно нарушение/заобикаляне на санкциите, подкрепени от подходящ вътрешен експертен опит и ресурси;
- Информира се за основните рискове и тенденции, идентифицирани в дейността на институцията, както и за цялостното изпълнение на контрола за борба с изпирането на пари, финансирането на тероризма и заобикаляне или избягване на санкциите;
- Редовно се информира относно изпълнението и резултатите от дейността, свързана с борбата с рисковете от ИП/ФТ/ФП и несъответствие със санкционните режими или тяхното заобикаляне;
- Наблюдава и следи чрез отчитане дейността на третата линия на защита: всеки одит, имащ отношение към дейността за превенция изпирането на пари и финансирането на тероризма, както и доклади от извършени надзорни проверки или резултати от външни одити;
- Регулярно оценява ефективното функциониране на функцията (функциите) за борба с ИП/ФТ и спазване на санкциите, включително вътрешните политики, процедури и контрол, както и целесъобразното разпределение на човешките и техническите ресурси.

### 4.2. Роля на вътрешния одит

Ангажиментите на Специализираната служба за вътрешен одит следва да включват регулярен преглед на следните елементи от организацията на банката за борба с ИП/ФТ и съответствието с приложимите санкции[14]:

- Дали действащите политики, процедури и други вътрешнобанкови документи са в съответствие с регулаторните изисквания и изпълнението на законовите ангажименти са документирани по подходящ начин и доколко същите се спазват;
- Да се оценят доколко предвидените контролни механизми са ефективни и съответстващи на риска, който е идентифициран;
- Да се оцени ефективността и ефикасността на техническия инструментариум, който банката ползва: оценката следва да се извършва от квалифицирани служители с подходяща техническа експертиза (с достатъчен технологичен опит и разбиране на рисковете и изискванията във връзка с БИП/БФТ/БФП/съответствие със санкции) и да включва най-малко: тестване и оценка на функционалните характеристики на системата, проверка на качеството на данните, ефективността и ефикасността на заложените контроли и параметрите на сценариите. Ако банката няма служители с нужната експертиза, за да извършват преглед на системите на банката във връзка с борба с ИП/ФТ/ФП и съответствието с приложимите санкции, може да се използва външен независим оценител.

Установените проблеми, свързани с резултатите от проверките, следва да бъдат документирани и проследявани, а състоянието на коригиращите действия следва да се докладва редовно на висшето ръководство.

Така описаните ангажименти на Специализираната служба за вътрешен одит следва да се извършват регулярно, чиято периодичност следва да се определя въз основа на идентифицирания риск.

### 4.3. Използване на външни доставчици и трети страни

Банките могат да използват както вътрешни решения (системи), така и такива, предоставени от външен доставчик за осъществяване на мониторинг на операциите по отношение установяване на съмнителна дейност или във връзка спазването на санкционните режими. Изборът на техническо решение трябва да е основан на:

**Добра практика:**

- Ръководството на банката (или определеният от управителния орган на банката, член на УС, отговорен за спазването на относимите изисквания за БИП/БФТ) следва да получава редовни доклади за основните рискове и тенденции, както и за цялостната ефективност на контрола за борба с изпирането на пари и финансирането на тероризма, вкл. и за сценариите.

[14] Санкционни списъци с ограничителни мерки за ЦФС за ФТ и ФП.

- оценката на риска на банката за ИП/ФТ и оценката за рисковата експозиция към санкциите;
- размера, естеството и сложността на дейността на банката;
- преценката на банката относно обезпечеността ѝ откъм ресурси, необходими за ефективното ѝ създаване и/или внедряване;
- сложността на процеса по интеграцията с останалите системи на банката.

Ако се избере да се използва вътрешна разработка, ключово е да се оцени дали в рамките на банката съществуват необходимите ресурси, вкл. човешки и техническа експертиза за такова начинание (създаване, внедряване и поддръжка).

Освен използването на продукти (например системи за мониторинг), банката може да възложи и част от задълженията си по мониторинг на операциите/сделките на трета страна.

В този случай банката следва да спазва:

- изискванията на насоките на ЕБО за възлагане на дейности на външни изпълнители (EBA/GL/2019/02);
- изискванията на т. 4.2.6[15] от насоки на ЕБО - EBA/GL/2022/05, вкл.:
    - банката **носи крайната отговорност** за спазването на изискванията за борба с изпирането на пари и финансирането на тероризма и за санкциите дори когато използва външни доставчици или други трети страни;
    - правата и задълженията на банката и на доставчика на услуги да бъдат **ясно разпределени и изложени в писмено споразумение**;
    - банката носи **отговорност за упражняването на контрол и наблюдение върху качеството** на предоставяната услуга, вкл. оценява ефективността на услугите, обхванати от споразумението, и да предприема всички необходими смекчаващи мерки, включително предоговаряне на споразумението при необходимост;
    - **вътрешногруповото възлагане** на дейности е предмет на същата регулаторна рамка като възлагането на доставчици на услуги извън групата (и в съответствие с Насоки на ЕБО EBA/GL/2019/02);
    - стратегически решения във връзка с БИП/БФТ **не се възлагат** на външен изпълнител (например в Насоките е посочено: „одобряването на **критериите**, които следва да се използват от кредитната или финансовата институция **за откриване на съмнителни или необичайни сделки** за целите на нейното текущо наблюдение и/или за целите на докладването“).

[15] 4.2.6.Възлагане на външен изпълнител на оперативните функции на служителя, отговорен за нормативното съответствие във връзка с БИП/БФТ от Насоки относно политиките и процедурите, свързани с управление на нормативното съответствие, и ролята и отговорностите на служителя, отговорен за нормативното съответствие във връзка с БИП/БФТ, съгласно член 8 и глава VI от Директива (ЕС) 2015/849.

Банката трябва да въведе и прилага контролни механизми, за да гарантира, че използването на външни доставчици на услуги не ги излага на риск от нарушаване на законови изисквания във връзка с БИП/БФТ или съответствието със санкциите, да документира тези контроли в споразумението за възлагане на дейности на външни изпълнители, както и да

**Добра практика**

- При възлагане в рамките на Групата банката документира формално и подробно отговорностите на двете страни и извършва контрол над качеството на услугата, въпреки че двете банки са част от една и съща група, задължени лица, и се ръководят от едни и същи законови изисквания и вътрешнобанкови правила.

извършват регулярни прегледи на актуалността и ефективността на тези контроли.

### 4.4. Обучение

Законовите и подзаконовите изисквания във връзка с обученията по ИП/ФТ/ФП са уредени в:

- ЗМИП: чл. 101, ал. 2, т. 13 и 14, ал. 11;
- ППЗМИП: чл. 67;
- Насоки на ЕБО относно рисковите фактори, свързани с ИП/ФТ[16], Насока 6.

В допълнение, банките следва да осигуряват редовно обучение на служителите, чиито основни задължения са свързани със съответствието със санкционните режими, като обучението следва включва **запознаване с:**

- приложимите санкции и регулаторни изисквания във връзка със съответствието със санкции;
- резултата от оценката на рисковата експозиция на санкциите (например, общи типологии за ИП/ФТ/ФП, вкл. избягване/заобикаляне на санкции);
- политиките, процедурите и контролните механизми за спазване на приложимите санкции.

Банката не е задължително да провежда отделно (самостоятелно) обучение във връзка със спазването на санкционните режими - може да е част от друго обучение, но следва да осигури както въвеждащ, така и продължаващ процес на обучение по темата ИП/ФТ/ФП.

Обучението по борбата с ИП/ФТ/ФП и спазване на санкции следва да бъде **съобразено с нуждите** на служителите и вменените им задължения. То следва да бъде **навременно, адекватно и актуално**, за да може банката да спазва законовите изисквания във връзка с борбата с ИП/ФТ/ФП, и да включва **процедура за документиране** на преминаването на обучението от всеки един служител, който участва в него, **проследяване на качеството му** (вкл. **периодичното му актуализиране**) и дали всички служители, чиито основни задължения

[16] EBA/GL/2024/01, изменящи EBA/GL/2021/02.

са свързани с тази дейност, са го преминали **своевременно и успешно,** особено за продължаващите обучения.

Обучението за новопостъпилите служители, чиито основни задължения ще са свързани с мониторинг на операциите (за съмнителна дейност и спазването на санкциите), следва да включва и запознаване с **процедури или инструкции за използването на всякакви системи**[17] за проверка или **друга технология**, свързана с изпълняваните от него/нея функции. Продължаващо обучение относно системите за мониторинг може да се организира регулярно или при определени събития – например при **промяна на функционалностите** на системата или при установяване на **грешки/пропуски** при използването й.

В рамките на групата обучителният процес може да се изпълнява - изцяло или частично - от дружеството майка, но следва да се подсигури, че горепосочените изисквания са изпълнени и в този случай, както и че обучението е в съответствие с местните законови изисквания и разпоредби.

Банките следва да документират своя план за обучение и да документират и отчитат неговото изпълнение и да имат готовност да демонстрират, при необходимост, че обучението им е адекватно и ефективно пред компетентните органи.

**Добра практика**

- Банката провежда въвеждащо обучение за работа със системите за мониторинг.
- Обучението относно борбата с финансиране на тероризма и съответствието със санкции включва практически насочена информация.

### 4.5. Съхраняване на информация

Банките трябва да поддържат подробна документация, свързана с техните мерки за оценка и смекчаване на риска във връзка с ИП/ФТ/ФП/нарушаване на санкции, както и справки, документи, данни и статистическа информация за операциите/сделките, които изпълняват, както и всички събрани и изготвени по реда на ЗМИП, ЗМФТРОМУ и ППЗМИП документи, данни и информация. Това неизчерпателно може да включва: данни и документи получени чрез прилагане на мерките за комплексна проверка на клиентите, досиета във връзка с операции/сделки, търговска кореспонденция, копия на документи за самоличност, УСО, записи/копия от извършени справки и резултати от извършен анализ. Банките трябва да поддържат записите по структуриран начин, така че да позволяват анализ на данните, проследяване на финансовите трансакции.

[17] Насока 6.2, буква „г“ от Насоки относно рисковите фактори, свързани с ИП/ФТ (изменени с EBA/GL/2024/01).

Създадената организация на съхраняване на информацията следва да позволява и навременното изготвяне на справки, данни и информация по запитвания и предоставяне им на надзорни, правоохранителни и други органи и лица, които имат право да разполагат с нея, вкл.

**Добра практика**

- Извършваните проверки се документират, като е налична информация за предприетите действия;
- Събраните документи и извършените справки се документират в съответствие с чл. 55, ал. 3 от ЗМИП и чл. 35 от ППЗМИП;
- Съхраняването на информацията и документите позволява извършването на анализ на данните, проследяване на финансовите трансакции или навременното изготвяне на справки, данни и информация по запитвания.

при необходимост да се предоставят доказателства за наказателно преследване на престъпна дейност.

Законоустановеният срок на съхранение за всички записи е най-малко 5 години (чл. 67 от ЗМИП), считано от датата на приключване на сделката или прекратяване на деловите взаимоотношения с клиента[18], или годината следваща тази на изготвяне на документи, свързани с оценка на риска или уведомление за съмнителна информация.

### 4.6. Разкриване на информация

Редът за разкриване на информация във връзка със съмнение за изпиране на пари е уреден в глава четвърта от ЗМИП и за разкриване на информация във връзка със съмнение за финансиране на тероризма - чл. 3, ал. 2, чл. 9, ал. 1 и 3 от ЗМФТРОМУ.

В допълнение, когато банката е част от група, дружеството майка следва да се увери, че всяка една банка в групата има цялата необходима информация за ефективното управление на рисковете от ИП/ФТ/ФП и риска от неспазването на ЦФС за ФП , както и обмяна на всякаква друга релевантна информация (например: чл. 66, ал. 1, т. 4, чл. 80, ал. 3, чл. 101, ал. 2, т. 18 от ЗМИП, чл. 9, ал. 14 и 15 от ЗМФТРОМУ, чл. 39, т. 7 от ППЗМИП и др.), което следва да е надлежно формализирано.

**Добра практика:**

- Групата има създадена платформа/интранет страница/друго подобно технологично решение, до което имат достъп служителите на банките в групата и могат да обменят информация, която е относима за повече от едно дружество в групата, на база предоставяне на разрешение за достъп до информация.

[18] По писмено указание от САДФР на ДАНС срокът може да бъде удължен с не повече от 2 години.