Ministerstwo Finansów

ANEKS NR 3
SCENARIUSZE RYZYKA FINANSOWANIA TERRORYZMU

1. Obszar – bankowość

Tabela nr 1

Rodzaj wykorzystanych usług, produktów finansowych	rachunek bankowy
Ogólny opis ryzyka	wykorzystanie rachunku bankowego do gromadzenia i transferowania pieniędzy na cele działalności terrorystycznej
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Gromadzenie na rachunku bankowym środków pozyskiwanych w różny sposób (ze źródeł legalnych, jak i nielegalnych), celem dalszej ich wypłaty w gotówce (często w krajach graniczących z krajami, w których działają organizacje terrorystyczne) lub transferowania, najczęściej na rachunki w instytucjach kredytowych, ulokowanych w jurysdykcjach nieprzestrzegających międzynarodowych standardów i rekomendacji z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (PPP/PFT). 2. Wyprowadzanie aktywów z kontrolowanej przez sympatyków organizacji terrorystycznej spółki, która następnie ogłasza bankructwo. Aktywa, w tym przypadku środki pieniężne, są transferowane poprzez łańcuch rachunków bankowych należących do powiązanych podmiotów, celem ich wypłaty w gotówce. 3. Korzystanie z rachunków bankowych osób fizycznych powiązanych z terrorystami (rodzina oraz inne bliskie osoby) w celu dokonania wpłat gotówkowych, a następnie przelewów transgranicznych. 4. Otwieranie rachunków bankowych na potrzeby zagranicznej osoby prawnej (zarejestrowanej w szczególności w raju podatkowym), a następnie wykorzystanie tych rachunków do przekazywania środków na rzecz podmiotów gospodarczych znajdujących się na obszarze o dużej aktywności organizacji terrorystycznych. 5. Otwieranie rachunków bankowych przez osoby fizyczne na podstawie fałszywego dowodu tożsamości. Wykorzystanie rachunku do przekazywania środków osobom powiązanym z działalnością terrorystyczną. 6. Samofinansowanie się terrorystów (zwł. "samotnych wilków") z własnych środków, zgromadzonych na rachunku bankowym (często z legalnych źródeł - zarobki, kredyty/pożyczki, stypendia, datki od rodziny). 7. Transfer środków przeznaczonych na cele działalności terrorystycznej z banku umiejscowionego w Azji na rachunek w instytucji kredytowej w Europie. Rachunek należy do członka lub zwolennika organizacji terrorystycznej, lub też podmiotu przez niego kontrolowanego, a transfer środków odbywa się za pośrednictwem banków-korespondentów umiejscowionych w Ameryce Płd., co utrudnia identyfikację i weryfikację danych zleceniodawcy transferu. 8. Wykorzystywanie rachunku bankowego przez podmiot, którego beneficjentem rzeczywistym jest osoba znajdująca się na międzynarodowych listach sankcyjnych bądź powiązana z organizacją terrorystyczną lub też z nią sympatyzująca.
Poziom podatności	2

Uzasadnienie dla poziomu podatności	Otwarcie rachunku bankowego, jak i dokonywanie transakcji - również o międzynarodowym charakterze - za jego pośrednictwem jest stosunkowo łatwe. Istotny jest dostęp do rachunku za pośrednictwem elektronicznych kanałów łączności (w szczególności przez Internet), który umożliwia ukrycie danych rzeczywistych zleceniodawców transakcji - przy wykorzystywaniu tzw. słupów czy przedsiębiorstw symulujących do otwarcia rachunku. Zgodnie z opracowaniem Narodowego Banku Polski (NBP) p.t. *Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r.,* liczba rachunków bankowych w Polsce wciąż rośnie (w 2017 r. wzrosła w stosunku do danych za 2016 r. o ponad o 6,6%, czyli o 4,5 mln rachunków).[1] Łączna ich liczba na 1 mieszkańca wynosi 1,9 i jest wyższa niż dla całej Unii Europejskiej (UE)[2]. Także łączna liczba transakcji zrealizowanych za pomocą kart płatniczych, czeków, poleceń zapłaty i przelewów wyniosła ponad 6,51 mld w 2017 r.[3] Przy czym w przypadku liczby poleceń przelewów na 1 mieszkańca Polska plasuje się powyżej średniej w UE, a w przypadku liczby poleceń zapłaty na 1 mieszkańca znacznie poniżej średniej w UE. Wszystkie podmioty oferujące ww. produkty/usługi są instytucjami obowiązanymi (IO). Te podmioty stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Posiadają świadomość swoich obowiązków z zakresu PPP/PFT.[4] Efektywnie analizują transakcje – najwięcej STR[5]/SAR[6], przekazywanych do Generalnego Inspektora Informacji Finansowej (GIIF), pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych (w 2017 r. było to ok. 94,9% SAR-ów od IO i ok. 97,8% STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka prania pieniędzy oraz finansowania terroryzmu (PP/FT) w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	4

[1] Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r., NBP, grudzień 2018 r, s. 7, na: https://www.nbp.pl/home.aspx?f=/systemplatniczy/obrot_bezgotowkowy/obrot_bezgotowkowy.html.
[2] Tamże, s. 8.
[3] Tamże, s. 32.
[4] Jakkolwiek podczas wszystkich przeprowadzonych w 2018 r. przez Urząd Komisji Nadzoru Finansowego (UKNF) kontroli (m. in. w 12 bankach komercyjnych i 3 bankach spółdzielczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 4 na 5 kontroli banków przeprowadzonych w latach 2017-2018 ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.
[5] Skrót od angielskiego pojęcia *suspicious transaction report* (tj. raport o podejrzanej transakcji).
[6] Skrót od angielskiego pojęcia *suspicious activity report* (tj. raport o podejrzanej aktywności).

Uzasadnienie dla poziomu zagrożenia	Finansowanie terroryzmu poprzez założone rachunki bankowe, zarówno rachunki firmowe, jak i rachunki osób fizycznych, jest jedną z najprostszych w wykorzystaniu metod. Rachunki mogą być zasilane zarówno legalnymi środkami, jak i pochodzącymi ze źródeł nielegalnych. Sposób ten ze względu na dobrze rozwinięty system bankowy jest szeroko dostępny i jego zastosowanie niewiele kosztuje. Samo dokonywanie transakcji na rachunkach bankowych nie wymaga specjalistycznej wiedzy ani umiejętności. Wykorzystanie systemu bankowego, a przede wszystkim rachunków bankowych, ze względu na możliwości dokonywania za ich pośrednictwem szybkich transakcji uznaniowych i obciążeniowych, jest łatwe, nie wymaga skomplikowanego planowania. Jeśli organizacja terrorystyczna stworzy system fikcyjnych podmiotów posiadających rachunki bankowe w kraju i za granicą, może dokonywać przelewów i płatności pomiędzy tymi podmiotami, które to transakcje z punktu widzenia uzasadnienia ekonomicznego nie będą podejrzane i bardzo trudne do zakwestionowania. W dużej ilości legalnych transakcji relatywnie łatwo jest ukryć prawdziwe przeznaczenie środków, zwłaszcza w przypadku transakcji o relatywnie niskich wartościach. GIIF dysponuje informacjami, że ten *modus operandi* może być wykorzystywany do finansowania terroryzmu. WNIOSEK: Wykorzystanie rachunku bankowego do gromadzenia i transferowania pieniędzy na rzecz terrorystów stwarza bardzo wysokie zagrożenie finansowaniem terroryzmu.

Tabela nr 2

Rodzaj wykorzystanych usług, produktów finansowych	pożyczki i kredyty
Ogólny opis ryzyka	zaciąganie pożyczek lub kredytów w instytucjach finansowych bez zamiaru spłaty powstałych zobowiązań
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zaciąganie przez osoby fizyczne pożyczek krótko- lub długoterminowych, pozwalających na finansowe wsparcie terrorystów, w szczególności na wyjazd do strefy konfliktu w celu walki w szeregach zagranicznych bojowników terrorystycznych.
Poziom podatności	2

Uzasadnienie dla poziomu podatności	Dostęp do kredytów i pożyczek udzielanych przez banki jest prosty, jakkolwiek istnieją pewne ograniczenia związane przede wszystkim z posiadaniem przez klienta zdolności kredytowej i odpowiednich zabezpieczeń. Z ich powodów możliwość wykorzystania słupów lub przedsiębiorstw symulujących do zaciągania kredytów i pożyczek jest utrudniona. Spłaty kredytów i pożyczek można dokonywać również poprzez realizację transakcji o charakterze międzynarodowym, również przy wykorzystaniu osób lub podmiotów trzecich. Zgodnie z informacjami ze strony Biura Informacji Kredytowej (BIK) w 2018 r. stwierdzono wzrost udzielonych kredytów zarówno w ujęciu liczbowym, jak i w wartościowym. W 2018 r. banki oraz spółdzielcze kasy oszczędnościowo-kredytowe udzieliły łącznie 7,5 mln szt. kredytów konsumpcyjnych, tj. o 2,8% więcej niż w 2017 r. (w ujęciu wartościowym – wzrost wyniósł 6,7% w stosunku do roku poprzedniego).[7] Wzrost odnotowano także w liczbie i wartości udzielonych kredytów mieszkaniowych (odpowiednio o 10,3% i 20,1% więcej niż w 2017 r.). Niewielki spadek odnotowano jedynie w liczbie wydawanych kart kredytowych (o ok. 0,6% w stosunku do 2017 r.), jednak wartość ich limitów była o ok. 2,2% większa od wartości limitów kart kredytowych w 2017 r.[8] Wszystkie podmioty oferujące ww. produkty/usługi są IO. Te podmioty stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Posiadają świadomość swoich obowiązków z zakresu PPP/PFT.[9] Efektywnie analizują transakcje – najwięcej STR/SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych (w 2017 r. było to ok. 94,9% SAR-ów od IO i ok. 97,8% STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Zaciąganie pożyczek lub kredytów w instytucjach finansowych bez zamiaru spłaty powstałych zobowiązań może być postrzegane w Polsce jako dosyć atrakcyjna metoda sfinansowania przestępstwa o charakterze terrorystycznym. Dotyczy to zwłaszcza kredytów i pożyczek konsumpcyjnych, a zdecydowanie mniej kredytów hipotecznych. Uproszczone procedury otrzymywania takich kredytów czy pożyczek, duża gama banków i firm pożyczkowych wpływa na atrakcyjność tego *modus operandi*. Nie wymaga to od członków organizacji terrorystycznej lub osób ich wspierających specjalistycznej wiedzy, planowania czy unikalnych umiejętności. W niektórych przypadkach konieczne może jednak być sfałszowanie dokumentacji. Informacje o wykorzystaniu tego *modus operandi* do finansowania terroryzmu pochodzą przede wszystkim z zagranicy. WNIOSEK: Zaciąganie pożyczek lub kredytów w instytucjach finansowych bez zamiaru spłaty powstałych zobowiązań stanowi wysokie zagrożenie finansowaniem terroryzmu.

[7] https://media.bik.pl/informacje-prasowe/420017/perspektywy-rynku-kredytowo-pozyczkowego-na-rok-2019, data odczytu 14.06.2019 r.

[8] https://media.bik.pl/publikacje/read/420072/newsletter-kredytowy-bik-grudzien-2018-r-i-podsumowanie-roku-kredytowe, data odczytu 14.06.2019 r.

[9] Jakkolwiek podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 12 bankach komercyjnych i 3 bankach spółdzielczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 4 na 5 kontroli banków przeprowadzonych w latach 2017-2018 ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Tabela nr 3

Rodzaj wykorzystanych usług, produktów finansowych	anonimowe karty przedpłacone – nośniki pieniądza elektronicznego wydawane przez podmioty zagraniczne – instytucje pieniądza elektronicznego oferujące swoje produkty w Polsce na podstawie paszportu europejskiego
Ogólny opis ryzyka	korzystanie z anonimowych kart przedpłaconych w celu utrudnienia identyfikacji osób dokonujących transakcji związanych z finansowaniem terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Środki przeznaczone na finansowanie terroryzmu są przekazywane pomiędzy osobami fizycznymi z wykorzystaniem kart przedpłaconych zapewniających anonimowość zarówno nabywcy karty, jak i beneficjentom środków na niej zgromadzonych. 2. Sponsorowanie działalności o charakterze terrorystycznym poprzez kupno anonimowych kart przedpłaconych o międzynarodowym zasięgu (także kart do międzynarodowych połączeń telefonicznych, do gier w Internecie) i przekazywanie numeru karty osobom powiązanym z terrorystami. Karta (dokładnie jej opis i numery) jest sprzedawana przez ww. osoby, a uzyskane środki zostają wykorzystane do finansowania działalności przestępczej. 3. Środki, którymi anonimowe karty przedpłacone są zasilane przez różne osoby, są następnie transferowane na różne rachunki posiadane lub kontrolowane przez terrorystów lub wypłacane w gotówce. 4. Wykorzystanie przez terrorystów portfeli pieniądza elektronicznego do gromadzenia środków pieniężnych pod różnymi tytułami, w tym na cele charytatywne, a następnie zasilanie nimi kart płatniczych (w tym anonimowych kart przedpłaconych), z których pieniądze są pobierane w gotówce.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do kart przedpłaconych będących nośnikiem pieniądza elektronicznego jest stosunkowo łatwy (poprzez Internet). Głównym źródłem ryzyka finansowania terroryzmu są anonimowe karty przedpłacone oferowane w Polsce, ale wydawane przez emitentów z innych krajów UE. Istnieje możliwość wydawania zgodnie z prawem pieniądza elektronicznego (zapisanego na karcie przedpłaconej lub na serwerze), bez identyfikowania i weryfikowania klienta, jakkolwiek w tym zakresie istnieją limity kwot przechowywanych na instrumencie płatniczym, a także limity kwot transakcji określone w dyrektywie 2018/843[10]. Pieniądz elektroniczny i karty przedpłacone mogą być używane do realizacji transakcji o charakterze międzynarodowym. Z uwagi na sprawowanie nadzoru nad zagranicznymi instytucjami pieniądza elektronicznego oferującymi swoje produkty i usługi w Polsce przez władze kraju macierzystego należącego do UE należy zakładać, że posiadają one i stosują się do obowiązujących procedur w zakresie przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu (warto jednak pamiętać, że nie są one instytucjami obowiązanymi w myśl polskich przepisów, o ile nie działają one poprzez oddział ustanowiony w Polsce). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia[11] i analizowania informacji, jednak w dużej mierze jest w tym zakresie uzależniony od informacji uzyskanych od zagranicznych jednostek analityki finansowej. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.

[10] Tj, *dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającą dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającą dyrektywy 2009/138/WE i 2013/36/UE* (Dz. Urz. UE L 156 z 19.06.2018 r., str. 43).

[11] Zgodnie z artykułem 53 ust. 1 dyrektywy 2015/849, w przypadku gdy dana jednostka analityki finansowej otrzyma raport o transakcji podejrzanej, dotyczący innego państwa członkowskiego UE (np. Polski), niezwłocznie go przekazuje jednostce analityki finansowej tego państwa członkowskiego.

Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Banki krajowe wydają jedynie karty przedpłacone będące rodzajem kart debetowych. Anonimowe karty przedpłacone - nośniki pieniądza elektronicznego są wydawane przez instytucje pieniądza elektronicznego z innych krajów UE i oferowane klientom w Polsce. Należy zakładać, że ryzyko finansowania terroryzmu może dotyczyć przede wszystkim tych kart, które są nabywane przez osoby fizyczne. Wymaga to od sprawców wiedzy na temat oferty zagranicznych instytucji pieniądza elektronicznego. Są informacje pochodzące głównie z zagranicy o wykorzystywaniu tego *modus operandi* do FT. WNIOSEK: Wykorzystanie anonimowych kart przedpłaconych w celu utrudnienia identyfikacji osób dokonujących transakcji związanych z finansowaniem terroryzmu jest aktualnie w Polsce na niskim poziomie zagrożenia.

Tabela nr 4

Rodzaj wykorzystanych usług, produktów finansowych	transfery środków pieniężnych
Ogólny opis ryzyka	wykorzystanie transferów do przekazywania środków do innych jurysdykcji
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie transferów środków pieniężnych do przekazywania środków pod fikcyjnym tytułem (m.in. na rzecz pomocy rodzinie). Środki przekazywane są do banków ulokowanych w krajach graniczących z miejscem działalności organizacji terrorystycznych. 2. Pracownik banku, współpracujący z terrorystami, przyjmuje od nich lub ich zwolenników środki pieniężne, które następnie za pośrednictwem bezgotówkowych transferów przekazuje na wskazane przez nich rachunki bankowe, ukrywając ich źródło oraz przeznaczenie.
Poziom podatności	2

Uzasadnienie dla poziomu podatności	Zlecanie transferów środków pieniężnych za pośrednictwem banków jest stosunkowo łatwe. Część banków świadczy również usługi przekazów pieniężnych w imieniu zagranicznych instytucji płatniczych. Istnieje ograniczona ilość produktów ułatwiających dokonywanie anonimowych transakcji (ewentualnie jest to możliwe w przypadku dokonywania sporadycznych transakcji poniżej progu równowartości 1 tys. EUR lub w przypadku posłużenia się słupem albo przedsiębiorstwem symulującym). Transfery środków pieniężnych mają często charakter międzynarodowy. Zgodnie z opracowaniem NBP p.t. *Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r.,* łączna liczba przelewów wyniosła w 2017 r. ok. 2,62 mld.[12] Przy czym w przypadku liczby poleceń przelewów na 1 mieszkańca Polska plasuje się powyżej średniej w UE. Wszystkie podmioty oferujące ww. produkty/usługi są IO. Te podmioty stosują środki bezpieczeństwa finansowego, choć wciąż ujawniane są podczas kontroli braki w tym obszarze. Posiadają świadomość swoich obowiązków z zakresu PPP/PFT.[13] Efektywnie analizują transakcje – najwięcej STR/SAR, przekazywanych do GIIF, pochodzi od banków/oddziałów instytucji kredytowych/oddziałów banków zagranicznych (w 2017 r. było to ok. 94,9% SAR-ów od IO i ok. 97,8% STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej mierze zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Finansowanie terroryzmu poprzez wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji jest jedną z najczęściej spotykanych metod. Sposób ten ze względu na dobrze rozwinięty światowy system bankowy jest szeroko dostępny i jego zastosowanie stosunkowo niewiele kosztuje. Zlecanie transferów nie wymaga wiedzy o systemie bankowym ani specjalistycznych umiejętności, jednakże realizacja tego *modus operandi* jest wtedy stosunkowo bezpieczna, gdy bank ze względu na charakter transakcji bądź miejsce transakcji nie jest zobowiązany do stosowania wzmożonych środków badania klienta. Ominięciem tego niebezpieczeństwa jest np. pozyskanie do współpracy pracownika banku. Jeśli organizacja terrorystyczna stworzy system fikcyjnych podmiotów posiadających rachunki bankowe w kraju i za granicą, może dokonywać przelewów i płatności pomiędzy tymi podmiotami, które to transakcje z punktu widzenia uzasadnienia ekonomicznego nie będą podejrzane i bardzo trudne do zakwestionowania. Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji w systemie bankowym jest łatwe, nie wymaga skomplikowanego planowania ani specjalistycznej wiedzy ani umiejętności. WNIOSEK: Wykorzystanie transferów do przekazywania środków finansowych do innych jurysdykcji na cele działalności terrorystycznej stwarza wysokie zagrożenie finansowaniem terroryzmu.

[12] Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2017 r., NBP, grudzień 2018 r, s. 32, na: https://www.nbp.pl/home.aspx?f=/systemplatniczy/obrot_bezgotowkowy/obrot_bezgotowkowy.html.

[13] Jakkolwiek podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 12 bankach komercyjnych i 3 bankach spółdzielczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 4 na 5 kontroli banków przeprowadzonych w latach 2017-2018 ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

2. Obszar – usługi płatnicze (oferowane przez inne podmioty niż banki)

Tabela nr 5

Rodzaj wykorzystanych usług, produktów finansowych	przekazy pieniężne
Ogólny opis ryzyka	wykorzystanie dostawców usług z zakresu transferu środków pieniężnych do przekazywania wartości majątkowych przeznaczonych na finansowanie terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie przez osoby powiązane z terrorystami możliwości stosowania przez dostawców usług z zakresu transferu środków pieniężnych uproszczonych środków bezpieczeństwa finansowego przy niskich kwotach transakcji. Umożliwia to transfer środków w sposób utrudniający identyfikację zleceniodawcy i beneficjenta. Wpłata środków pieniężnych zostanie dokonana w Polsce a wypłata w krajach charakteryzujących się dużą aktywnością organizacji terrorystycznych. 2. Wykorzystanie przekazów pieniężnych do finansowego wsparcia zagranicznych bojowników terrorystycznych przebywających albo podróżujących do strefy konfliktu. 3. Korzystanie przez osoby finansujące terroryzm z usług dostawców działających na terenie Polski, lecz nie przekazujących informacji o transakcjach podejrzanych do polskiej jednostki analityki finansowej.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Usługi przekazów pieniężnych są stosunkowo łatwo dostępne. Istnieje ograniczona możliwość ukrycia danych identyfikacyjnych zleceniodawców i beneficjentów przekazów pieniężnych w przypadku dokonywania sporadycznych transakcji poniżej progu równowartości 1 tys. EUR lub w przypadku posłużenia się słupem albo przedsiębiorstwem symulującym. Transfery środków pieniężnych mają często charakter międzynarodowy. Prawie wszystkie podmioty oferujące te usługi są IO za wyjątkiem instytucji płatniczych z innych krajów UE świadczących usługi płatnicze na terytorium Polski za pośrednictwem agentów. IO z obszaru usług płatniczych Te podmioty posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[14] Przekazują one relatywnie niewiele SAR-ów i STR-ów (w 2017 r. - 0,58% wszystkich otrzymanych SAR-ów od IO i 0,034% wszystkich otrzymanych STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Przy transakcjach niskokwotowych dostawcy usług transferu środków pieniężnych mogą stosować uproszczone środki bezpieczeństwa finansowego. Przekazywane mogą być środki pochodzące z zupełnie legalnych źródeł. Aktualnie działalność terrorystyczna jest niskonakładowa (przykładowo koszt zamachu na przystanku autobusowym w Izraelu wynosi około 200 USD, a koszt zamachu w Madrycie w 2004 r. wyniósł nie więcej niż 10 000 USD). Występuje coraz częściej zjawisko samofinansowania się terrorystów. Otrzymanie jednego bądź kilku niskokwotowych przekazów pieniężnych jest jedną z często

[14] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 16 krajowych instytucjach płatniczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas wszystkich 3 kontroli instytucji płatniczych, przeprowadzonych w latach 2017-2018, ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

	używanych, znanych metod finansowania terroryzmu. Jest to sposób szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców jako atrakcyjny. Do realizacji tego typu transferu pieniądza nie jest potrzebne posiadanie przez płatnika rachunku płatniczego. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są słupy bądź rodzina. Wykorzystanie dostawców usług z zakresu transferu środków pieniężnych do przesyłania pieniędzy pochodzących z legalnych bądź nielegalnych źródeł wymaga minimalnej specjalistycznej wiedzy o systemie transferu środków, jest relatywnie niezbyt drogie pod kątem opłat i stosunkowo bezpieczne. WNIOSEK: Powyższe informacje oraz fakt przebywania w Polsce osób z państw i regionów podwyższonego ryzyka powoduje, że wykorzystanie schematu z dostawcami usług z zakresu transferu środków pieniężnych do transferowania pieniędzy – w formie przekazu pieniężnego – przeznaczonych na cele finansowania terroryzmu stwarza wysokie zagrożenie finansowaniem terroryzmu.

Tabela nr 6

Rodzaj wykorzystanych usług, produktów finansowych	internetowe usługi płatnicze
Ogólny opis ryzyka	korzystanie z internetowych usług płatniczych przez podmioty uczestniczące w procesie finansowania terroryzmu, w szczególności przez potencjalnych zagranicznych bojowników terrorystycznych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie internetowych usług płatniczych przez zagranicznych bojowników terrorystycznych do dokonywania zakupów w sklepach internetowych ekwipunku niezbędnego do przebywania w strefie konfliktu. 2. Korzystanie z omawianych usług przez osoby wpłacające środki na rzecz organizacji charytatywnych, uczestniczących w procesie finansowania terroryzmu. 3. Transferowanie środków pomiędzy poszczególnymi osobami zaangażowanymi w działalność terrorystyczną. 4. Wykorzystanie bezgotówkowych transferów środków pieniężnych (poniżej progu, od którego wymagana jest identyfikacja klienta) do przekazywania środków pod fikcyjnym tytułem (m.in. na rzecz pomocy rodzinie). Środki przekazywane są do agencji instytucji płatniczych ulokowanych w krajach graniczących z miejscem działalności organizacji terrorystycznych. 5. Agent instytucji płatniczej (względnie pracownik instytucji płatniczej), współpracujący z terrorystami, przyjmuje od nich lub ich zwolenników środki pieniężne, które następnie za pośrednictwem bezgotówkowych transferów przekazuje na wskazane przez nich rachunki bankowe, ukrywając ich źródło oraz przeznaczenie.
Poziom podatności	3

Uzasadnienie dla poziomu podatności	Internetowe usługi przekazów są stosunkowo łatwo dostępne - wystarczy mieć dostęp do Internetu. Istnieją możliwości ukrycia danych identyfikacyjnych osoby korzystającego z tego typu usług płatniczych (np. jeden z portali daje możliwość realizowania transakcji do określonej kwoty bez weryfikacji danych identyfikacyjnych, a sama weryfikacja danych identyfikacyjnych jest uproszczona - opiera się na przekazanym przez klienta skanie paszportu lub prawa jazdy, zdjęciu z kamery internetowej i danych geolokalizacyjnych klienta). Transfery środków pieniężnych mają często charakter międzynarodowy. Tylko część podmiotów oferujące te usługi jest IO. Nie są nimi instytucje płatnicze świadczące usługi płatnicze za pomocą internetowych platform, zarejestrowane w innych krajach. IO z obszaru usług płatniczych posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[15] Przekazują one relatywnie niewiele SAR-ów i STR-ów (w 2017 r. - 0,58% wszystkich otrzymanych SAR-ów od IO i 0,034% wszystkich otrzymanych STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystywanie internetowych usług płatniczych, które umożliwiają płatności *online* i transfer pieniędzy przez Internet, będących elektroniczną alternatywą dla tradycyjnych papierowych metod, takich jak czeki i polecenia zapłaty, jest w miarę atrakcyjną metodą finansowania terroryzmu. Przedsięwzięcia terrorystyczne należą do względnie tanich inwestycji, w stosunku do wywołanych strat oraz wzbudzonej paniki. Aktualnie w Polsce przebywają osoby z państw i regionów podwyższonego ryzyka, dla których oferowane usługi płatnicze umożliwiające przedsiębiorcom i konsumentom posiadającym adres *e-mail* wysyłanie oraz odbieranie płatności przez Internet są atrakcyjne. Ze względu na względnie niskie kwotowo przepływy pieniężne mogą one nie zostać odnotowane jako podejrzane, a ponadto są łatwe do zastosowania, choć wymagają planowania i wiedzy. WNIOSEK: Wykorzystywanie internetowych usług płatniczych stwarza wysokie zagrożenie finansowaniem terroryzmu.

Tabela nr 7

Rodzaj wykorzystanych usług, produktów finansowych	systemy transferów typu Hawala
Ogólny opis ryzyka	Wykorzystanie sieci Hawala lub innych nieformalnych systemów transferu wartości majątkowych do finansowania terroryzmu

[15] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 16 krajowych instytucjach płatniczych) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas wszystkich 3 kontroli instytucji płatniczych, przeprowadzonych w latach 2017-2018, ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wpłata środków pieniężnych w kraju X, charakteryzującym się wysokim zagrożeniem terrorystycznym, połączona z wypłatą na terenie Polski w celu sfinansowania działalności o charakterze terrorystycznym. Wykorzystanie nieformalnej sieci transferu środków o charakterze przestępczym w celu uniemożliwienia wykrycia przepływu środków. 2. Środki przekazane na finansowanie terroryzmu podlegają wymieszaniu z innymi przekazami pieniężnymi w ramach sieci Hawala w celu zatarcia śladu po dokonanych transakcjach. 3. Wykorzystanie podmiotów oferujących nielegalnie usługi płatnicze do transferu gotówki na rzecz terrorystów. M.in. osoba oferująca takie usługi wykorzystuje rachunki bankowe, na które wpłaca pieniądze pochodzące od swoich klientów. Środki są transferowane następnie na rachunki podmiotów prowadzących legalne usługi płatnicze. W ramach tych systemów stosowane jest m.in. złoto do clearingu rozrachunków. Jest ono łatwe do upłynnienia, zwł. w niektórych krajach azjatyckich i afrykańskich, gdzie są rozbudowane rynki obrotu tym metalem.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Usługi systemów typu Hawala znacznie ułatwiają dokonywanie szybkich i anonimowych transakcji, o międzynarodowym charakterze. Z uwagi na fakt, że świadczą je podmioty pozostające poza kontrolą państwa - brak jest danych na temat ilości i wartości transakcji realizowanych w ramach tego systemu w Polsce. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwości gromadzenia i analizowania informacji od tego typu podmiotów. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanego ryzyka nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	System transferów typu Hawala jest rodzajem nieformalnego systemu bankowego. Wykorzystywana jest w handlu międzynarodowym, często do transferowania środków na duże odległości. Ważnym elementem tego systemu nieformalnej bankowości jest możliwość zachowania pełnej anonimowości oraz wykorzystania kilku pośredników przy zlecaniu przekazu. Osoba wpłacająca gotówkę nie jest proszona o żaden dokument tożsamości i z reguły jest nieznana lub słabo znana danemu pośrednikowi. Podobnie wypłacający, który może odebrać przesłane środki finansowe podając jedynie ustalone hasło. W ten sposób podmiot oferujący usługi w zakresie systemu typu Hawala z reguły nie wie, od kogo, za co, i komu dokonuje transakcji. Najważniejsze jest zaufanie pomiędzy pośrednikami, którzy najczęściej stanowią grono członków jednej rodziny, przyjaciół lub osoby polecone i działają w kilku lub kilkunastu krajach. Ważne jest również to, że wpłacający i wypłacający pieniądze nie muszą wcale posiadać rachunku płatniczego w danym kraju (często, z uwagi na restrykcyjne, lokalne przepisy bankowe, nie mogą tego konta otworzyć w tym kraju). Nie jest znany rozmiar (wolumen) płatności poprzez ten nieformalny system. W Polsce nie mamy dużych liczebnie mniejszości etnicznych, w których system typu Hawala jest rozpowszechniony (jakkolwiek zauważono rosnącą liczbę cudzoziemców z państw podwyższonego ryzyka, przebywających w RP). Polskie służby odnotowały przypadki wykorzystania tej metody do transferu środków przeznaczonych na działalność terrorystyczną. WNIOSEK: Poziom zagrożenia z użyciem nieformalnego systemu bankowego Hawala do transferowania wartości majątkowych na cele działalności terrorystycznej stwarza średnie zagrożenie finansowaniem terroryzmu.

3. Obszar - ubezpieczenia

Tabela nr 8

Rodzaj wykorzystanych usług, produktów finansowych	ubezpieczenia komunikacyjne
Ogólny opis ryzyka	wyłudzanie odszkodowań z ubezpieczeń w celu finansowania terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Celowe wywołanie kolizji drogowej w celu uzyskania odszkodowania, które zostanie przeznaczone na finansowanie terroryzmu.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Uzyskanie ubezpieczenia komunikacyjnego jest stosunkowo łatwe. Trudno jest ukrycie danych identyfikacyjnych ubezpieczonego czy uposażonego. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku, gdy klient polskiego towarzystwa ubezpieczeniowego jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwości gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wyłudzenia odszkodowania z ubezpieczeń może być jedną z form finansowania terroryzmu. Jednakże stopień skomplikowania procedury uzyskiwania odszkodowania, przygotowanie odpowiedniej dokumentacji oraz ryzyko kontaktu z organami ścigania powoduje nieatrakcyjność tej formy finansowania działalności terrorystycznej. W warunkach polskich brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla finansowania terroryzmu. Jest on trudny do zastosowania z uwagi na konieczność posiadania wiedzy specjalistycznej, a istnieją tańsze i łatwiejsze sposoby finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu wyłudzenia odszkodowania z ubezpieczeń w celu gromadzenia środków na finansowanie działalności terrorystycznej stwarza niskie zagrożenie finansowaniem terroryzmu.

Tabela nr 9

Rodzaj wykorzystanych usług, produktów finansowych	ubezpieczenia na życie
Ogólny opis ryzyka	przeznaczenie pieniędzy z polisy na finansowanie terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Likwidacja polisy ubezpieczenia na życie w celu uzyskania pieniędzy z wpłaconych wcześniej składek przed podróżą zagranicznych bojowników terrorystycznych do strefy konfliktu.
Poziom podatności	1

Uzasadnienie dla poziomu podatności	Uzyskanie ubezpieczenia na życie/dożycie jest stosunkowo łatwe. Trudno jest ukryć dane identyfikacyjne ubezpieczonego czy uposażonego. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku, gdy klient polskiego towarzystwa ubezpieczeniowego jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT, choć relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez towarzystwa ubezpieczeń na życie (w 2017 r. było to 0,12% wszystkich SAR-ów od IO i 0,16% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie środków finansowych pochodzących z likwidowanej polisy na życie może być jedną z form finansowania terroryzmu. Jednakże ten m*odus operandi* może być stosunkowo kosztowny z uwagi na możliwość utraty części środków (związaną z warunkami umowy ubezpieczenia), a przez to stopień atrakcyjności tej formy finansowania działalności terrorystycznej jest dosyć niski. W Polsce, gdzie nie odnotowano wielu przypadków podróży bojowników terrorystycznych do strefy konfliktu, brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla finansowania terroryzmu. Istnieją tańsze i łatwiejsze sposoby finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie środków finansowych ze zlikwidowanej polisy na życie w celu sfinansowania działalności terrorystycznej, zwłaszcza na podróż bojowników do strefy konfliktu, stwarza niskie zagrożenie finansowaniem terroryzmu.

4. Obszar – inne instytucje finansowe

Tabela nr 10

Rodzaj wykorzystanych usług, produktów finansowych	usługi na rynku walutowym FOREX
Ogólny opis ryzyka	wykorzystanie firmy brokerskiej działającej na rynku FOREX do oszustwa w celu pozyskania środków na działalność terrorystyczną

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Sprawcy rejestrują spółkę, która rozpoczyna działalność jako firma brokerska na rynku FOREX bez uzyskania odpowiedniego zezwolenia na prowadzenie działalności inwestycyjnej/maklerskiej. Oferta firmy jest dostępna w kilku językach i zachęca wysokimi zyskami. Dzięki temu oraz wykorzystaniu technik agresywnego marketingu budowana jest baza klientów, którzy dokonują wpłat na rachunek podmiotu z zamiarem zasilenia swojego konta maklerskiego. Inwestorzy nie zdają sobie sprawy, że transakcje, których dokonują są fikcyjne, a środki zostaną w pewnym momencie przywłaszczone przez nielegalnie działającą firmę inwestycyjną. W przypadku firm będących tzw. *market makerami*[16], istnieje także możliwość, że oferowane im będą gorsze warunki niż rynkowe, tak aby ponieśli straty, a pozyskane w ten sposób środki zasilą organizacje terrorystyczne. 2. Sprawcy rejestrują spółkę, która rozpoczyna działalność jako firma brokerska na rynku FOREX bez uzyskania odpowiedniego zezwolenia na prowadzenie działalności inwestycyjnej/maklerskiej. Sympatycy organizacji terrorystycznych, którzy przelewali środki zawierają niekorzystne dla siebie transakcje (zwłaszcza w sytuacji, gdy firma działa jako *market maker*) lub godzą się na wygórowaną prowizję lub też przepadek środków w momencie zakończenia działalności tego podmiotu. Pozyskane w ten sposób środki transferowane są do organizacji terrorystycznych.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Usługi na rynku FOREX są dostępne za pośrednictwem brokerów. Raczej trudno jest ukryć dane identyfikacyjne zlecającego transakcje na tym rynku za pośrednictwem licencjonowanego brokera. Mogą występować transakcje o charakterze międzynarodowym jedynie w przypadku, gdy klient jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego albo korzystka z usług podmiotu zagranicznego. Wszystkie podmioty oferujące te usługi są IO (domy maklerskie bądź banki posiadające w swoich strukturach biura maklerskie) - jakkolwiek klienci mogą korzystać z usług oferowanych przez Internet przez podmioty zagraniczne. IO z tego obszaru posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[17] Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez domy maklerskie (w 2017 r. było to 0,49% wszystkich SAR-ów od IO i 0,42% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	FOREX to międzynarodowy rynek wymiany walut, o charakterze hurtowym, w ramach którego banki, wielkie korporacje międzynarodowe oraz inwestorzy instytucjonalni z całego świata przeprowadzają operacje wymiany walut 24 godziny na dobę przy wykorzystaniu sieci telefonicznych, łączy informatycznych oraz systemów informacyjnych. Wykorzystanie legalnej – choć nieposiadającej odpowiedniego zezwolenia na prowadzenie działalności inwestycyjnej/maklerskiej i kontrolowanej przez przestępców – firmy działającej

[16] Podmiot, który wystawia i kwotuje instrumenty finansowe, jednocześnie występuje jako drugą stroną transakcji zawieranych przez klienta.

[17] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 6 domach/biurach maklerskich) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 1 kontroli domu maklerskiego, przeprowadzonej w 2017 r., ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

	na rynku FOREX jako brokera w modelu *market maker* jest mało atrakcyjną metodą pozyskania i przeznaczenia środków na działalność terrorystyczną. Ten *modus operandi* wymaga specjalistycznej wiedzy o rynku walutowym, umiejętności i planowania. W modelu *market maker* wykazywane przez inwestorów straty z udziału w rynku FOREX (w wyniku oszustwa czy świadomej działalności) są zyskiem brokera i mogą być transferowane do organizacji terrorystycznych. GIIF nie posiada informacji o zamiarze wykorzystania tego *modus operandi*. WNIOSEK: Wykorzystanie firmy brokerskiej działającej na rynku FOREX jako *market maker* do oszustwa w celu pozyskania środków na działalność terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu.

Tabela nr 11

Rodzaj wykorzystanych usług, produktów finansowych	jednostki funduszy inwestycyjnych (FI)
Ogólny opis ryzyka	obrót jednostkami uczestnictwa w funduszach inwestycyjnych w celu gromadzenia środków na działalność terrorystyczną
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Sprawcy regularnie kupują jednostki uczestnictwa w funduszach inwestycyjnych za niewielkie kwoty, aby następnie po ich skumulowaniu je odsprzedać, a środki wytransferować poza granice kraju.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do jednostek uczestnictwa w funduszach inwestycyjnych jest relatywnie łatwy. Trudno jest ukryć dane identyfikacyjne klientów funduszy inwestycyjnych. Mogą występować transakcje o charakterze międzynarodowym związane z kupnem i sprzedażą jednostek uczestnictwa jedynie w przypadku, gdy klient polskiego FI jest rezydentem innego kraju lub dokonuje transakcji finansowej za pośrednictwem rachunku zagranicznego albo jednostki uczestnictwa są kupowane od zagranicznego FI. Wszystkie podmioty oferujące te usługi są IO – jakkolwiek klienci mogą korzystać z usług oferowanych przez podmioty zagraniczne. IO z tego obszaru posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[18] Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez towarzystwa funduszy inwestycyjnych i FI (w 2017 r. było to 0% wszystkich SAR-ów od IO i 0,09% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Zakup i obrót jednostkami uczestnictwa w funduszach inwestycyjnych w celu gromadzenia środków na działalność terrorystyczną może być jednym z *modus operandi* dla finansowania terroryzmu. GIIF nie miał jednak informacji o inwestowaniu nielegalnych bądź legalnych środków finansowych w fundusze inwestycyjne w tym celu. Obrót jednostkami uczestnictwa w funduszach inwestycyjnych jest trudną do zastosowania formą działania z uwagi na konieczność posiadania wiedzy specjalistycznej o rynku kapitałowym, a istnieją tańsze i łatwiejsze sposoby finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie zakupu i obrotu jednostkami uczestnictwa w funduszach inwestycyjnych w celu gromadzenia środków na działalność

[18] Podczas wszystkich 3 przeprowadzonych przez GIIF kontroli towarzystw funduszy inwestycyjnych, przeprowadzonych w latach 2017-2018, ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

	terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu.

Tabela nr 12

Rodzaj wykorzystanych usług, produktów finansowych	rachunki papierów wartościowych i rachunki pieniężne służące do ich obsługi
Ogólny opis ryzyka	wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu gromadzenia środków na działalność terrorystyczną
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Sprawcy, za pośrednictwem firm utworzonych w szczególności w rajach podatkowych, lokują środki pozyskane z nielegalnych lub legalnych źródeł na rynku kapitałowym. Zakupione papiery wartościowe są następnie sprzedawane, a uzyskane środki służą do finansowania działalności terrorystycznej. 2. Na rachunek pieniężny służący do obsługi rachunku papierów wartościowych, należący do spółki zagranicznej, kontrolowanej przez zwolenników organizacji terrorystycznej, są przelewane środki z rachunku bankowego prowadzonego w innym kraju na rzecz osoby fizycznej pod fikcyjnym tytułem inwestycji w akcje spółki publicznej. Środki są następnie – w krótkim odstępie czasu – przekazywane na rachunek bankowy prowadzony w kraju trzecim, należący do ww. spółki pod tytułem zysku z obrotu papierami wartościowymi.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Otwarcie tego typu rachunków jest stosunkowo łatwe. Raczej trudno jest ukryć dane identyfikacyjne klientów. Występują transakcje o charakterze międzynarodowym. Wszystkie podmioty oferujące te usługi są IO. Posiadają one pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[19] Relatywnie niewiele informacji o podejrzanych transakcjach/podejrzanej działalności jest przekazywanych przez domy maklerskie (w 2017 r. było to 0,49% wszystkich SAR-ów od IO i 0,42% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu gromadzenia środków na działalność terrorystyczną może być jedną z form finansowania terroryzmu. Jednakże stopień skomplikowania rynku papierów wartościowych powoduje nieatrakcyjność tej formy finansowania działalności terrorystycznej. Brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla finansowania terroryzmu. Jest on trudny do zastosowania z uwagi na konieczność posiadania wiedzy specjalistycznej o rynku kapitałowym, a istnieją tańsze i łatwiejsze sposoby finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie rachunków papierów wartościowych i rachunków pieniężnych służących do ich obsługi w celu gromadzenia środków na działalność terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu.

[19] Podczas wszystkich przeprowadzonych w 2018 r. przez UKNF kontroli (m. in. w 6 domach/biurach maklerskich) ujawniono nieprawidłowości i uchybienia w badanych obszarach (głównie w zakresie oceny ryzyka i stosowania środków bezpieczeństwa finansowego, a także organizacji procesu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przekazywaniu informacji do GIIF). Natomiast GIIF podczas 1 kontroli domu maklerskiego, przeprowadzonej w 2017 r., ujawnił nieprawidłowości w wypełnianiu obowiązków dot. przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

5. Obszar – wymiana walut

Tabela nr 13

Rodzaj wykorzystanych usług, produktów finansowych	gotówkowa wymiana walut
Ogólny opis ryzyka	wymiana waluty w celu utrudnienia identyfikacji przestępstwa finansowania terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Korzystanie przez osoby powiązane z organizacjami terrorystycznymi z wymiany walut w kantorach w celu utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych. Korzystanie z "zaufanych" kantorów, nieraportujących transakcji podejrzanych do właściwej jednostki analityki finansowej. 2. Wymiana zgromadzonych pieniędzy (np. zebranych od zwolenników) na wysokie nominały w innych walutach (powszechnie wymienianych na całym świecie, np. EUR) w kantorach, celem łatwiejszego ich transportowania przez granice państwowe.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do usług wymiany walut jest bardzo łatwy. Łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku realizacji takich transakcji przynajmniej częściowo w formie bezgotówkowej. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT.[20] Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[21] (w 2017 r. było to ok. 0,03% wszystkich SAR-ów od IO i ok. 0,0064% wszystkich STR-ów, co oznacza spadek w stosunku do danych za 2016 r., kiedy było to ok. 0,64% wszystkich SAR-ów i ok. 7,66% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wymiany waluty w celu utrudnienia identyfikacji przestępstwa finansowania terroryzmu jest sposobem stosunkowo łatwym do realizacji i szeroko dostępnym. Jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców raczej jako atrakcyjny, zwłaszcza że środki mogą pochodzić z zupełnie legalnych źródeł. Transakcje wymiany walut poniżej progu rejestracji z reguły nie wzbudzają podejrzeń. Wysoki wolumen obrotów kantoru pozwala ukryć wymianę nielegalnych bądź legalnych środków wśród zupełnie legalnych jednostkowych transakcji. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu wymiany waluty w celu utrudnienia identyfikacji przestępstwa finansowania terroryzmu stwarza średnie zagrożenie finansowaniem terroryzmu.

[20] W kontroli prowadzonych przez NBP udział przedsiębiorców prowadzących działalności kantorową, u których wykryto nieprawidłowości w zakresie realizacji obowiązków dotyczących PPP/PFT, w stosunku do wszystkich skontrolowanych przedsiębiorców prowadzących działalność kantorową był relatywnie niewielki, w 2018 r. wyniósł on 4,87%, w 2017 r. – 4,14%. Natomiast w przypadku wszystkich 3 kontroli przeprowadzonych przez GIIF w 2017 r. w IO zajmujących się wymianą walut, wykryto pewne nieprawidłowości.

[21] Abstrahując od usług świadczonych przez banki.

Tabela nr 14

Rodzaj wykorzystanych usług, produktów finansowych	wymiana pieniędzy w ramach jednej waluty
Ogólny opis ryzyka	wymiana pieniędzy o niskich nominałach na banknoty o wyższej wartości
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Wymiana banknotów EUR o niskich nominałach na banknoty o nominale 500 EUR w celu zmniejszenia objętości przenoszonych środków pieniężnych.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do usług wymiany walut jest bardzo łatwy. Łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku realizacji takich transakcji przynajmniej częściowo w formie bezgotówkowej. Wszystkie podmioty oferujące te usługi są IO. Posiadają one świadomość swoich obowiązków z zakresu PPP/PFT.[22] Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[23] (w 2017 r. było to ok. 0,03% wszystkich SAR-ów od IO i ok. 0,0064% wszystkich STR-ów, co oznacza spadek w stosunku do danych za 2016 r., kiedy było to ok. 0,64% wszystkich SAR-ów i ok. 7,66% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu wymiany pieniędzy o niskich nominałach na banknoty o wyższej wartości w celu finansowania terroryzmu jest sposobem szeroko dostępnym, a jego zastosowanie niewiele kosztuje. Może być on postrzegany przez sprawców jako atrakcyjny. Fizyczne przenoszenie banknotów przeznaczonych na cele finansowania terroryzmu nie powinno zwracać uwagi, a zmniejszenie objętości przewożonej gotówki zmniejsza zagrożenie jej wykrycia bądź przypadkowej utraty. Jednakże bezpieczeństwo tej metody wymaga zaplanowania, przestrzegania reguły dokonywania niskich kwotowo operacji. Bowiem wymiana pogniecionych, często brudnych banknotów o niskich nominałach może łatwo zwrócić uwagę. Najczęściej metoda ta wymaga współpracy pracowników zatrudnionych w instytucjach typu bank bądź kantor. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu wymiany pieniędzy o niskich nominałach na banknoty o wyższej wartości stwarza średnie zagrożenie finansowaniem terroryzmu.

Tabela nr 15

Rodzaj wykorzystanych usług, produktów finansowych	usługi podmiotów oferujących bezgotówkową wymianę walut
Ogólny opis ryzyka	bezgotówkowa wymiana waluty połączona z transferem środków

[22] W kontroli prowadzonych przez NBP udział przedsiębiorców prowadzących działalności kantorową, u których wykryto nieprawidłowości w zakresie realizacji obowiązków dotyczących PPP/PFT, w stosunku do wszystkich skontrolowanych przedsiębiorców prowadzących działalność kantorową był relatywnie niewielki, w 2018 r. wyniósł on 4,87%, w 2017 r. – 4,14%. Natomiast w przypadku wszystkich 3 kontroli przeprowadzonych przez GIIF w 2017 r. w IO zajmujących się wymianą walut, wykryto pewne nieprawidłowości.

[23] Abstrahując od usług świadczonych przez banki.

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Korzystanie przez osoby powiązane z organizacjami terrorystycznymi z bezgotówkowej wymiany walut w tzw. kantorach internetowych w celu utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych. Przykładowo - środki w PLN są transferowane na rzecz tzw. kantoru internetowego z rachunku bankowego prowadzonego w jednej instytucji ze zleceniem ich wymiany na USD i przekazania na rachunek prowadzony w innym banku, należącego w rzeczywistości do innego podmiotu niż zleceniodawca.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do usług wymiany walut jest bardzo łatwy. Łatwe jest ukrycie danych identyfikacyjnych dokonującego transakcji, zwłaszcza jeśli poszczególne transakcje są przeprowadzane w relatywnie niewielkich kwotach. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym w przypadku realizacji takich transakcji przynajmniej częściowo w formie bezgotówkowej. Wszystkie podmioty oferujące te usługi są IO. Posiadają one pewną świadomość swoich obowiązków z zakresu PPP/PFT.[24] Relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty zajmujące się wymianą walut[25] (w 2017 r. było to ok. 0,03% wszystkich SAR-ów od IO i ok. 0,0064% wszystkich STR-ów, co oznacza spadek w stosunku do danych za 2016 r., kiedy było to ok. 0,64% wszystkich SAR-ów i ok. 7,66% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w części zakresowi analizowanego ryzyka.[26]
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu bezgotówkowej wymiany walut w tzw. kantorach internetowych połączonej z transferem środków dla utrudnienia organom ścigania odtworzenia ścieżki transferu wartości majątkowych jest zidentyfikowaną metodą umożliwiającą finansowanie terroryzmu. Obecnie kantory internetowe nie są regulowane prawnie. Nie podlegają żadnej ustawie ani jednemu organowi, które by ustanowiły ich zakres działania. Według szacunków dostępnych w Internecie, w 2017 r. ok. 35% transakcji wymiany walut odbywało się w sieci.[27] Dynamicznie wzrasta wolumen obrotów kantorów internetowych, a pojedyncze transakcje sięgają już nawet kilku milionów złotych. Bezgotówkowa wymiana waluty połączona z transferem środków stosunkowo niewiele kosztuje i jako *modus operandi* może być postrzegana przez sprawców jako atrakcyjny i szeroko dostępny sposób dla finansowania terroryzmu. W warunkach dynamicznego wzrostu obrotu gospodarczego prowadzonego przez przedsiębiorstwa, zajmujące się eksportem bądź importem, transakcje wymiany bezgotówkowej w kantorach internetowych mogą być relatywnie niewidoczne dla nadzoru (zwłaszcza przy braku jasnych uregulowań prawnych). GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu bezgotówkowej wymiany walut w tzw.

[24] W przypadku wszystkich 3 kontroli przeprowadzonych przez GIIF w 2017 r. w IO zajmujących się wymianą walut, wykryto pewne nieprawidłowości.

[25] Abstrahując od usług świadczonych przez banki.

[26] Trwają prace nad projektem *ustawy o zmianie ustawy - Prawo dewizowe oraz niektórych innych ustaw*, w zakresie objęcia nadzorem podmioty wymieniające waluty bezgotówkowo. Zgodnie z jego założeniami „transakcje bezgotówkowej wymiany walut, dokonywane przez kantory internetowe oraz transakcje gotówkowo-bezgotówkowej wymiany walut" mają podlegać przepisom *ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych*. Jednak już teraz część podmiotów oferujących jednocześnie bezgotówkową wymianę walut i usługi płatnicze podlega nadzorowi KNF.

[27] Polacy wymieniają waluty w Internecie. Raport - trendy w wymianie walut pierwsze półrocze 2017 r., Xchanger i Fintek.pl, 2017 r., s. 2, na: https://fintek.pl/najnowszy-raport-kantorach-internetowych-polsce/.

	kantorach internetowych połączonej z transferem środków stwarza średnie zagrożenie finansowaniem terroryzmu.

6. Obszar - waluty wirtualne

Tabela nr 16

Rodzaj wykorzystanych usług, produktów finansowych	zdecentralizowane i wymienialne waluty wirtualne (tzw. kryptowaluty)
Ogólny opis ryzyka	wykorzystanie kryptowalut do transferowania wartości majątkowych na cele działalności terrorystycznej
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Upowszechnianie informacji o adresach kryptowalut, na które zwolennicy organizacji terrorystycznych transferują wartości majątkowe w zdecentralizowanych i wymienialnych walutach wirtualnych. 2. Gromadzenie środków od sympatyków organizacji terrorystycznych lub nieświadomych inwestorów pod pretekstem finansowania przygotowań emisji nowej kryptowaluty, która to emisja albo nie następuje, albo kończy się deprecjacją wyemitowanej waluty. Zgromadzone środki przekazywane są organizacji terrorystycznej. Dodatkowo może funkcjonować system poleceń mający służyć skutecznej rekrutacji nowych jej członków.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do tego typu usług jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych klientów (podmioty oferujące tego typu usługi dokonują identyfikacji klientów na odległość). Występują transakcje o charakterze międzynarodowym. Podmioty oferujące usługi w zakresie wymiany walut wirtualnych (w tym kryptowalut) czy udostępniania tzw. „*hot wallets*" są IO. Jakkolwiek w Internecie są dostępne oferty podmiotów zarejestrowanych poza granicami kraju, a także UE, które nie podlegają obowiązkom w zakresie przeciwdziałania PP/FT. Ponadto transakcje przy użyciu kryptowalut mogą być dokonywane bez pośrednictwa podmiotów trzecich. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwości gromadzenia i analizowania informacji dot. tego typu usług, jednak pochodzących od podmiotów będących IO albo udostępnionych przez zagraniczną jednostkę analityki finansowej. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają częściowo zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie walut wirtualnych do transferowania wartości majątkowych na cele działalności terrorystycznej z uwagi na ich cechy sprzyjające anonimizacji stron transakcji i utrudniające zarówno śledzenie transferów, jak ich zatrzymanie, może być jedną z metod finansowego wspierania terroryzmu. Jednakże zgodnie z analizą EUROPOL-u z dnia 19 września 2017 r. (*Risk Analysis on the use of Virtual Currencies for Terrorism Financing purposes*), chociaż waluty wirtualne zyskały na popularności ze względu na kluczowe cechy, takie jak dostępność globalna, łatwość dostępu, rzetelne i nieodwracalne transakcje, niski koszt i szybkość międzynarodowego transferu, rozwój ich popularności wśród organizacji terrorystycznych wydaje się być stosunkowo słaby w stosunku do rozwoju ich popularności w ponadnarodowych grupach przestępczości zorganizowanej, zwłaszcza tych związanych z cyberprzestępczością. Zostały zidentyfikowane przez zagraniczne służby przypadki wykorzystania walut wirtualnych do realizacji transakcji mających związek z finansowaniem terroryzmu, jakkolwiek ich liczba pozostaje relatywnie niewielka.[28] Użycie walut wirtualnych jest trudne do zastosowania, wymaga specjalistycznej wiedzy. WNIOSEK: Wykorzystanie walut wirtualnych do transferowania wartości majątkowych na cele działalności terrorystycznej stwarza średnie zagrożenie finansowaniem terroryzmu.

7. Obszar - usługi telekomunikacyjne powiązane z płatnościami mobilnymi

Tabela nr 17

Rodzaj wykorzystanych usług, produktów finansowych	płatności dokonywane za pomocą telefonu komórkowego
Ogólny opis ryzyka	nabywanie lub doładowanie kart SIM w celu przekazywania środków
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Korzystanie z mobilnych płatności, niestosujących w odpowiednim zakresie środków bezpieczeństwa finansowego, w celu finansowania terroryzmu w sposób utrudniający identyfikacje zleceniodawcy i beneficjenta transakcji, np.: zwolennicy organizacji terrorystycznej przekazują płatności mobilne (w debet swoich rachunków telefonicznych) na rzecz jednej osoby, która następnie wypłaca otrzymane pieniądze w gotówce w bankomacie, aby przekazać je na cele organizacji terrorystycznej.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Możliwość świadczenia tego typu usług, a także dostęp do nich jest relatywnie łatwy. Istnieje możliwość ukrycia danych identyfikacyjnych klientów (przy wykorzystaniu słupów lub ewentualnie zagranicznych numerów tel.). Mogą występować transakcje o charakterze międzynarodowym. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwość gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1

[28] Lakoniczną informację na ten temat można znaleźć w: „European Union Terrorism Situation and Trend Report 2019". s. 17-18 (na: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat).
Niektóre przypadki wykorzystania walut wirtualnych w celu finansowania terroryzmu zostały przedstawione w krajowej ocenie ryzyka finansowania terroryzmu USA: „National Terrorist Financing Risk Assessment 2018", s. 26-27 (na: https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf). Jakkolwiek zaznaczono w niej, że waluty wirtualne nie stanowią istotnego ryzyka finansowania terroryzmu.

Uzasadnienie dla poziomu zagrożenia	Nabywanie lub doładowanie kart SIM w celu przekazywania środków jest jednym z bezpieczniejszych i szybkich sposobów finansowania działań o charakterze terrorystycznym. Korzystanie z mobilnych systemów płatności, w których nie stosuje się w odpowiednim zakresie środków bezpieczeństwa finansowego, jest tanie i atrakcyjne. Wystarczy w aplikacji mobilnej uruchomić opcję transferów na numer telefonu lub przekazać środki beneficjentowi do wypłaty w bankomacie. W Polsce jednak brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi* dla celów finansowania działalności terrorystycznej. Ograniczeniem anonimowości jest wprowadzony w 2017 r. obowiązek rejestracji numerów *prepaid* tak, aby każdy numer telefonu miał swojego jasno określonego użytkownika. WNIOSEK: Wykorzystanie nabywania lub doładowania kart SIM w celu przekazywania/gromadzenia środków na działalność terrorystyczną stwarza niskie zagrożenie finansowaniem terroryzmu.

Tabela nr 18

Rodzaj wykorzystanych usług, produktów finansowych	usługi telekomunikacyjne dot. numerów o podwyższonej płatności
Ogólny opis ryzyka	wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności do gromadzenia środków na działalność terrorystyczną
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zawarcie umowy na świadczenie usług telekomunikacyjnych dot. rejestrowanych numerów o podwyższonej płatności (typu *Premium*) na rzecz osób podstawionych (tzw. słupów) celem zapewnienia anonimowości sprawców. Następnie za pomocą odpowiednich kodów wykonywanie są określone połączenia przez zwolenników organizacji terrorystycznej, za które pobierane są wysokie opłaty. Część uzyskanego zysku stanowi zapłata dla "słupa", a pozostała większość jest przekazywana na cele działalności terrorystycznej.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Możliwość świadczenia tego typu usług, a także dostęp do nich jest relatywnie łatwy. Istnieje możliwość ukrycia danych identyfikacyjnych klientów (przy wykorzystaniu słupów lub ewentualnie zagranicznych numerów tel.). Mogą występować transakcje o charakterze międzynarodowym. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF nie ma możliwość gromadzenia i analizowania informacji dot. tego typu usług. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności (usługi typu PREMIUM) do gromadzenia środków na działalność terrorystyczną jest jedną ze zidentyfikowanych metod finansowania terroryzmu. Chociaż w Polsce brak jest jednoznacznej informacji o wykorzystywaniu tego *modus operandi*, to ABW odnotowała w przeszłości przypadki angażowania się cudzoziemców z państw podwyższonego ryzyka w oszustwa telekomunikacyjne z użyciem numerów typu PREMIUM, z których dochody najprawdopodobniej przeznaczane były na działalność ugrupowań terrorystycznych. Dla celów finansowania działalności terrorystycznej sposób jest postrzegany jako stosunkowo atrakcyjny, rozproszone grono zwolenników lub osób popierających działania terrorystyczne może w łatwy sposób wspomagać/zasilać niskokwotowo podmiot prowadzący usługi telekomunikacyjne w zakresie numerów o podwyższonej płatności. Zyski z takiej działalności przeznaczane są na działalność terrorystyczną. Potrzebne jest planowanie, wiedza i umiejętności do zastosowania tego *modus operandi*. Nie jest to jednak sposób tani. WNIOSEK: Wykorzystanie usług telekomunikacyjnych w zakresie numerów o podwyższonej płatności (usługi typu PREMIUM) do gromadzenia środków na działalność terrorystyczną stwarza średnie zagrożenie finansowaniem terroryzmu.

8. Obszar - fizyczny przewóz wartości majątkowych

Tabela nr 19

Rodzaj wykorzystanych usług, produktów finansowych	kurierzy wartości majątkowych (tzw. z ang. *cash couriers*)
Ogólny opis ryzyka	wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Osoby fizyczne (czasami wynajmowane jedynie w celu jednorazowego przewozu wartości majątkowych) transportują te wartości przez granice w różny sposób: • przewożąc jednorazowo środki pieniężne poniżej progu wymagającego ich deklaracji, • deklarując przywóz/wywóz środki pieniężne o wartości powyżej ww. progu i wskazując fikcyjny cel ich przeznaczenia, • transportując/przemycając środki pieniężne o wartości znacznie powyżej progu wymagającego ich deklarację, ukryte w bagażu, w środku transportu, pod ubraniem. 2. Oprócz gotówki przewozowi mogą podlegać takie wartości majątkowe, jak kamienie i metale szlachetne, dzieła sztuki, karty płatnicze, karty prepaid, czeki itd. 3. Przewóz znacznych sum pieniędzy przez granice z jednoczesnym zgłoszeniem do deklaracji przywozu/wywozu kwoty pieniędzy trochę powyżej progu wymaganego przy deklaracjach dewizowych, która nie wzbudzi podejrzeń. Sprawcy liczą, że funkcjonariusze służby celnej lub straży granicznej poprzestaną na dopełnieniu obowiązku z przyjęciem deklaracji i nie będą szukać innych środków pieniężnych, przewożonych przez sprawców w o wiele większej kwocie.
Poziom podatności	4

Uzasadnienie dla poziomu podatności	Dostęp do usług przewozu wartości majątkowych jest bardzo łatwy - każdy może być takim kurierem. Podczas kontroli na granicach zewnętrznych UE nie jest możliwe ukrycie danych identyfikacyjnych kuriera. Jakkolwiek sam przewóz wartości majątkowych, a tym samym dane identyfikacyjne kuriera mogą nie zostać rozpoznane przez organy administracji publicznej na granicy. Podmioty oferujące te usługi nie są IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji (informacje przekazywane przez KAS i SG). Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	3
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe jest jedną z najczęściej spotykanych metod finansowania działalności terrorystycznej. Przewóz pieniędzy albo innych wartości majątkowych poprzez granice państwowe jest sposobem szeroko dostępnym, a jego zastosowanie relatywnie niewiele kosztuje i jest postrzegane przez sprawców jako atrakcyjne i stosunkowo bezpieczne. Zwłaszcza gdy przewożone sumy są poniżej progu obowiązkowej deklaracji przywozu. Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe nie wymaga posiadania specjalistycznej wiedzy o systemie bankowym ani specjalistycznych umiejętności, a zapewnia anonimowość dla grupy/organizacji, która organizuje proceder. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. Polskie służby odnotowały przypadki wykorzystania tej metody do transferu środków przeznaczonych na działalność terrorystyczną. WNIOSEK: Wykorzystanie osób fizycznych do przewozu pieniędzy poprzez granice państwowe stwarza wysokie zagrożenie finansowaniem terroryzmu.

Tabela nr 20

Rodzaj wykorzystanych usług, produktów finansowych	paczki kurierskie, pocztowe; przewozy cargo
Ogólny opis ryzyka	wykorzystanie usług kurierskich i pocztowych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zwolennik organizacji terrorystycznej przekazuje zgromadzone na jej cele środki pieniężne w paczkach nadawanych na poczcie do osoby fizycznej, zamieszkałej w jednym z krajów sąsiadujących z rejonem działalności organizacji terrorystycznych, która następnie przekazuje otrzymane środki członkom tej organizacji.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Dostęp do usług kurierskich i pocztowych oraz przewozów cargo jest relatywnie łatwy. Istnieją możliwości ukrycia danych identyfikacyjnych zlecających i odbierających przesyłki. Paczki kurierskie, pocztowe oraz towary w ramach usług cargo są przekazywane pomiędzy osobami i podmiotami z różnych krajów. Tylko część podmiotów oferujących te usługi jest IO. Nie są nimi przewoźnicy oraz firmy spedycyjne. Organy administracji publicznej posiadają ograniczoną wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji (jedynie w ograniczonym zakresie. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne tylko częściowo odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie usług kurierskich i pocztowych do przekazywania organizacjom terrorystycznym pieniędzy na cele działalności terrorystycznej jest jedną ze zidentyfikowanych metod finansowania terroryzmu. Jest to sposób stosunkowo łatwy, szeroko dostępny, jego zastosowanie niewiele kosztuje i jest postrzegany przez sprawców raczej jako atrakcyjny. Wykorzystanie usług kurierskich bądź pocztowych z reguły nie wzbudza podejrzeń. Wysoki wolumen obrotów - jeśli chodzi o przesyłki międzynarodowe - pozwala ukryć wykorzystanie tych usług do przekazywania pieniędzy na cele działalności terrorystycznej. Zwłaszcza gdy nie są to jednorazowo sumy zbyt wysokie. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystywane są „słupy". Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o systemie przesyłek i umiejętności logistycznych. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu bezgotówkowej wymiany walut w tzw. kantorach internetowych połączonej z transferem środków stwarza średnie zagrożenie finansowaniem terroryzmu.

9. Obszar – gry hazardowe

Tabela nr 21

Rodzaj wykorzystanych usług, produktów finansowych	internetowe gry hazardowe
Ogólny opis ryzyka	środki pozyskane nielegalnie na cele promowania terroryzmu były prane przy pomocy internetowych gier hazardowych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Przestępcy "hakowali" karty kredytowe, a następnie środki ukradzione z rachunków tych kart prali przy pomocy gier hazardowych dostępnych on-line w celu przeznaczenia ich potem na płatności za strony internetowe, na których promowali walkę i "męczeństwo" terrorystów, a które były też wykorzystywane do kontaktów pomiędzy terrorystami oraz przekazywania informacji o sposobie produkcji bomb. 2. Wykorzystanie internetowych platform hazardowych do prania pieniędzy pochodzących z czynów zabronionych, takich jak oszustwa. Osoba wspierająca ugrupowania o charakterze terrorystycznym wpłaca środki na odpowiedni rachunek powiązany z platformą hazardową. Środki przekazywane są z powrotem do omawianego klienta platformy pod postacią "wygranej", a następnie wykorzystane w procederze finansowania terroryzmu.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Dostęp do internetowych gier hazardowych jest stosunkowo łatwy, bo wciąż pojawiają się w sieci nowe domeny z grami hazardowymi. W przypadku zagranicznych kasyn *online* łatwe jest ukrycie danych identyfikacyjnych gracza. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym, zwłaszcza w przypadku dokonywania transakcji finansowych, w przypadku gdy rachunki podmiotu prowadzącego internetowe gry hazardowe są ulokowane za granicą. Tym niemniej Krajowa Administracja Skarbowa (KAS) we współpracy z Komisją Nadzoru Finansowego (KNF) opracował zasady dotyczące ograniczenia wykorzystywania instrumentów bądź usług płatniczych oferowanych przez dostawców usług płatniczych w Polsce do dokonywania transakcji związanych z nielegalną grą hazardową. Hostingodawcy natomiast usuwają/blokują dostęp do zabronionych treści związanych z nielegalnymi grami online. W grudniu 2018 r. powstało w Polsce pierwsze (legalne) kasyno *online*. Płatności w nim można dokonywać jedynie poprzez przelewy online lub BLIKIEM. Wszystkie podmioty oferujące legalnie gry hazardowe są IO. Posiadają pewną

	świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[29] Relatywnie niewiele – w porównaniu z innymi IO – informacji o podejrzanych transakcjach/podejrzanej działalności przekazywanych jest przez podmioty prowadzące działalność w zakresie gier hazardowych (w 2017 r. było to 0,00% wszystkich SAR-ów od IO i 0,008% wszystkich STR-ów). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie internetowych gier hazardowych może być jedną z metod użycia nielegalnie pozyskanych środków na cele finansowania terroryzmu. Zgodnie jednak z polskimi przepisami urządzanie gier hazardowych przez Internet, z wyjątkiem zakładów wzajemnych i loterii promocyjnych jest objęte monopolem państwa. Przepisy prawne zakazują zarówno urządzania gier hazardowych przez sieć przez podmioty nieuprawnione, jak i uczestniczenie w takich grach. Działalność kontrolna KAS, utworzenie Rejestru domen służących do oferowania gier hazardowych niezgodnie z ustawą oraz blokowanie dostępu do zabronionych domen internetowych może negatywnie wpływać na możliwość użycia nielegalnie pozyskanych środków na cele finansowania terroryzmu. GIIF nie otrzymywał informacji o możliwości wykorzystywania w Polsce *modus operandi* polegającego na wykorzystaniu internetowych gier hazardowych dla finansowania terroryzmu. Sposób ten, z uwagi na uwarunkowania prawne, zdaje się być postrzegany przez sprawców jako mało atrakcyjny i stosunkowo ryzykowny, by legitymizować środki finansowe pochodzące z czynów zabronionych. Ponadto potrzebne jest planowanie, wiedza i umiejętności do zastosowania tego *modus operandi*. WNIOSEK: Wykorzystanie internetowych gier hazardowych stwarza niskie zagrożenie finansowaniem terroryzmu.

10. Obszar – organizacje typu *non-profit*

Tabela nr 22

Rodzaj wykorzystanych usług, produktów finansowych	działalność charytatywna
Ogólny opis ryzyka	wykorzystanie funduszy gromadzonych na cele charytatywne na finansowanie organizacji terrorystycznych

[29] W latach 2017-2018 w 6 na 10 kontrolach przeprowadzonych przez GIIF w podmiotach oferujących gry hazardowe stwierdzono nieprawidłowości w zakresie wypełniania obowiązków w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Wykorzystanie kontrolowanych przez terrorystów organizacji charytatywnych (zarejestrowanych i niezarejestrowanych) do gromadzenia i przekazywania pieniędzy na cele organizacji terrorystycznych. 2. Przeznaczenie środków na finansowanie terroryzmu przez osoby działające w ramach NPO - na etapie zbierania, tj. przed wpłaceniem środków na rachunek organizacji. 3. Zwolennik grupy terrorystycznej, mający dostęp do pieniędzy gromadzonych przez legalną organizację charytatywną jako jej pracownik, odpowiedzialny za ich księgowanie lub nadzór nad tym obszarem, ułatwia ich przekazanie na cele tejże grupy terrorystycznej. 4. Podszywanie się przez zwolenników grup terrorystycznych pod legalnie działające organizacje charytatywne i gromadzenie pieniędzy pod fikcyjnymi tytułami celem przekazania ich na cele tych grup. 5. W organizacji charytatywnej, kontrolowanej przez zwolenników grup terrorystycznych, fundusze gromadzone na potrzeby pomocy humanitarnej są mieszane ze środkami gromadzonymi na cele terrorystyczne, celem ich ukrycia i łatwiejszego transferowania na rzecz tych grup terrorystycznych. 6. Fundusze gromadzone na legalne cele charytatywne - po ich przesłaniu do miejsc docelowych w obszarach konfliktu lub w ich sąsiedztwie - są przejmowane przez organizacje terrorystyczne dla swoich celów. 7. Pobieranie przez dostawców z zakresu usług transferu środków pieniężnych "podatku" za przekazywanie środków pochodzących od tych organizacji w rejon docelowy. "Podatek" jest następnie przekazywany organizacji terrorystycznej prowadzącej działalność na danym terytorium. 8. Przesyłanie przez NPO środków od darczyńców do zagranicznego NPO, który przeznaczył otrzymane wartości majątkowe na finansowanie terroryzmu.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Założenie fundacji lub stowarzyszenia jest utrudnione (wymagane jest spełnienie konkretnych obowiązków, m.in. sporządzenie statutu, rejestracja w KRS, ponadto należy liczyć się z nadzorem organów administracji publicznej). Łatwe jest ukrycie danych identyfikacyjnych prawdziwych darczyńców i beneficjentów, zwłaszcza w przypadku gdy fundacja lub stowarzyszenie jest kontrolowane przez sprawców. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym. Fundacje i stowarzyszenia posiadające osobowość prawną są IO jedynie w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy płatność jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane. Ww. podmioty posiadają pewną świadomość swoich obowiązków z zakresu PPP/PFT, choć wciąż ujawniane są braki w ich wypełnianiu.[30] Nie przekazują lub przekazują relatywnie mało informacji o podejrzanych transakcjach/podejrzanej działalności do GIIF (w 2017 r.[31] nie było żadnych STR-ów lub SAR-ów od nich). Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

[30] W latach 2017-2018 w 3 na 3 kontrole przeprowadzone przez GIIF w fundacjach stwierdzono nieprawidłowości w zakresie wypełniania obowiązków w obszarze przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

[31] W tamtym czasie IO były wszystkie fundacje, bez względu na przyjmowanie lub dokonywanie płatności w gotówce, a także stowarzyszenia, posiadające osobowość prawną, przyjmujące płatności w gotówce o wartości równej lub przekraczającej równowartość 15 tys. EUR, również w drodze więcej niż jednej operacji.

Uzasadnienie dla poziomu zagrożenia	Organizacje charytatywne mogą być wykorzystywane przez ugrupowania terrorystyczne do ich finansowania na różne sposoby. Może to polegać na bezpośrednim przekazywaniu części pozyskiwanych przez NPO środków na cele działalności terrorystycznej albo na przekazywaniu całości środków pozyskiwanych przez NPO, gdy organizacja ta jest tylko kamuflażem dla działalności terrorystycznej. Organizacja charytatywna może również prowadzić rzeczywistą działalność charytatywną, jednak pomoc udzielana jest przez komórki tej organizacji, które są kontrolowane przez członków związanych z ugrupowaniami terrorystycznymi. Prowadzi to do sytuacji, w której beneficjenci pomocy są przeświadczeni, że otrzymują wsparcie od organizacji terrorystycznej. Takie działanie przynosi spore korzyści propagandowe. NPO są wykorzystywane przez organizacje terrorystyczne, gdyż poprzez działalność charytatywną cieszą się one dużym zaufaniem społecznym. Przekazywane za pośrednictwem NPO treści mają duży wpływ na postawy ludzi, a ewentualne przeciwdziałanie organów państwowych może się spotkać z zarzutami o prześladowania, rasizm, łamanie praw człowieka. Samo stosowanie tego *modus operandi* jest postrzegane z ww. powodów za dosyć atrakcyjne i bezpieczne. Przygotowanie logistyki dla takich operacji to średni poziom przygotowania. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie organizacji charytatywnych dla finansowania terroryzmu w Polsce stwarza średnie zagrożenie finansowaniem terroryzmu.

11. Obszar – finansowanie społecznościowe

Tabela nr 23

Rodzaj wykorzystanych usług, produktów finansowych	finansowanie społecznościowe
Ogólny opis ryzyka	pozyskiwanie darczyńców środków na rzecz organizacji terrorystycznych przy wykorzystaniu nowoczesnych sieci komunikacyjnych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Organizowanie akcji poprzez platformę *crowdfundigową* w celu zbiórki środków na potrzeby działalności o charakterze terrorystycznym. Rzeczywisty cel zbiórki funduszy nie będzie bezpośrednio wskazywał na zamiar wykorzystania zgromadzonych środków do finansowania terroryzmu. 2. Zwolennicy organizacji terrorystycznej rozsyłają apele o fundusze poprzez media społecznościowe. Darczyńcy przekazują inicjatorom akcji datki w gotówce lub kupują międzynarodowe karty przedpłacone, których numery następnie im udostępniają.
Poziom podatności	4
Uzasadnienie dla poziomu podatności	Relatywnie łatwe jest rozpoczęcie akcji *crowdfundingowej*, np. za pośrednictwem mediów społecznościowych. Łatwe jest ukrycie danych identyfikacyjnych darczyńców i beneficjentów. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym. Teoretycznie każdy może prowadzić akcję *crowdfundingową*. Podmioty prowadzące takie akcje nie są IO. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji dot. tego typu akcji. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne nie odpowiadają zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Finansowanie społecznościowe stanowi alternatywne źródła finansowania, również dla działalności terrorystycznej. Jest formą finansowania różnego rodzaju projektów przez społeczność, która jest lub zostanie wokół tych projektów zorganizowana. Działalność terrorystyczna jako pewnego rodzaju

	przedsięwzięcie jest w takim przypadku finansowane poprzez dużą liczbę drobnych, jednorazowych wpłat dokonywanych przez osoby zainteresowane wspieraniem działalności terrorystycznej. Zazwyczaj jednak cel zbiórki pieniędzy nie jest przedstawiany wprost. *Crowdfunding* środków niewiele kosztuje i jako *modus operandi* może być postrzegany przez sprawców jako w miarę atrakcyjny i szeroko dostępny sposób dla finansowania terroryzmu, jednakże okupione jest to sporym ryzykiem. Z reguły akcja zbierania środków trwa jakiś czas, więc *crowdfunding* jest stosunkowo łatwy do namierzenia i może nie przynieść spodziewanych rezultatów, co wpływa na postrzeganie tej metody jako stosunkowo mało atrakcyjnej. GIIF otrzymywał bardzo nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie mechanizmu crowdfundingu stwarza średnie zagrożenie finansowaniem terroryzmu.

12. Obszar - handel dobrami o wysokiej wartości

Tabela nr 24

Rodzaj wykorzystanych usług, produktów finansowych	kamienie i metale szlachetne
Ogólny opis ryzyka	kamienie i metale szlachetne zagrabione przez terrorystów są przemycane do innych krajów w celu ich sprzedaży
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Na rachunek bankowy spółki C wpływały relatywnie duże kwoty pieniędzy od podmiotów zajmujących się obrotem diamentami. Pieniądze były następnie transferowane na Środkowy Wschód na korzyść obywatela jednego z krajów europejskich - osoby A, pochodzącego z Afryki. Część środków była transferowana przez rachunek jednego z dyrektorów spółki C. Pieniądze były wymieniane na EUR, a następnie przekazywane na rzecz pana B. Pan A i B skupowali diamenty od rebeliantów działających w 1. z krajów afrykańskich, a następnie przemycali je do Europy. 2. Zakup przez polską spółkę metali szlachetnych, takich jak złoto, od spółki zagranicznej, pośredniczącej w obrocie kruszcem. Metale szlachetne mogą pochodzić z terenu objętego działalnością grup terrorystycznych a fundusze uzyskane z ich sprzedaży mogą zostać przeznaczone na ich finansowanie.
Poziom podatności	3

Uzasadnienie dla poziomu podatności	O ile kupno i sprzedaż relatywnie niewielkich ilości tego typu towarów nie nastręcza większej trudności (np. w sklepach jubilerskich), to kupno/sprzedaż ich dużych/hurtowych już tak. Łatwo jest jednak uniknąć identyfikacji, zwłaszcza przy zakupie/sprzedaży towarów o wartości poniżej równowartości 15 tys. EUR. Istnieje możliwość kupowania/sprzedawania przez Internet, a tym samym realizowania transakcji o charakterze międzynarodowym (np. przy zakupie kamieni lub metali od podmiotu zagranicznego). Obecnie podmioty prowadzące działalność w zakresie obrotu metalami lub kamieniami szlachetnymi i półszlachetnymi nie są IO, o ile nie przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane. W Polsce istnieje możliwość zakupu złota w formie sztabek, a także złotych monet – tzw. monet bulionowych (bez wartości numizmatycznych). Oprócz tego monety bulionowe traktowane są jako legalny środek płatniczy, co zapewnia możliwość przewiezienia monet z kraju do kraju. Ponadto import, przetwarzanie oraz obrót diamentami nie jest w Polsce działalnością reglamentowaną prawnie. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie handlu kamieniami i metalami szlachetnymi zagrabionymi przez terrorystów jest jedną ze zidentyfikowanych metod finansowania terroryzmu. Kamienie bądź metale szlachetne są przemycane przez organizacje terrorystyczne ze stref wojny, gdzie działają te organizacje do innych krajów w celu ich sprzedaży na cele działalności terrorystycznej. Jest to jednak sposób finansowania częstokroć wymagający sporządzenia fałszywych certyfikatów pochodzenia dla sprzedawanych towarów. Nie jest całkiem bezpieczny, ponieważ może wzbudzić zainteresowanie służb kraju sprzedaży. Zastosowanie tego *modus operandi* wymaga znajomości lokalnego rynku, zaplanowania i specjalistycznej wiedzy na średnim poziomie. Brak jest informacji o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej w Polsce. WNIOSEK: Wykorzystanie mechanizmu zakupu kamieni i metali szlachetnych od osób związanych z działalnością o charakterze terrorystycznym do finansowania terroryzmu stwarza w Polsce niskie zagrożenie.

Tabela nr 25

Rodzaj wykorzystanych usług, produktów finansowych	antyki oraz dzieła sztuki
Ogólny opis ryzyka	zakup skradzionych antyków i dzieł sztuki od osób związanych z działalnością o charakterze terrorystycznym
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Zakup przez polskich kolekcjonerów dzieł sztuki oraz antyków pochodzących z obszarów objętych aktywnością organizacji terrorystycznych (np. Bliski Wschód). Zakupiony towar mógł zostać bezprawnie odebrany właścicielom przez organizację terrorystyczną w celu sfinansowania jej działalności.
Poziom podatności	3

Uzasadnienie dla poziomu podatności	Kupno/sprzedaż antyków czy dzieł sztuki jest relatywnie łatwa. Istnieje wiele firm handlujących tego typu towarami, na podstawie przepisów *ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców* (domy aukcyjne, antykwariaty). Łatwo jest uniknąć identyfikacji, zwłaszcza przy zakupie/sprzedaży towarów o wartości poniżej równowartości 15 tys. EUR. Istnieje możliwość kupowania/sprzedawania przez Internet, a tym samym realizowania transakcji o charakterze międzynarodowym. Obecnie domy aukcyjne czy antykwariaty nie są IO, o ile nie przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 tys. EUR, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja, czy kilka operacji, które wydają się ze sobą powiązane. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie mechanizmu zakupu skradzionych antyków i dzieł sztuki od osób związanych z działalnością o charakterze terrorystycznym jest jednym ze sposobów finansowania działalności o charakterze terrorystycznym. W Polsce apogeum narażenia na tego typu mechanizm wystąpił w czasie udziału polskich wojsk w operacji w Iraku. Jest to jednak metoda finansowania terroryzmu trudna do zastosowania. Wymaga sporych nakładów logistycznych, specjalistycznych ekspertyz, znajomości rynku dzieł sztuki, znajomości klientów gotowych zakupić towar na czarnym rynku, a każda operacja handlowa powinna pozostawać dyskrecjonalna. Częstokroć wymaga sporządzenia fałszywych certyfikatów pochodzenia dla sprzedawanych antyków i dzieł sztuki. Przeprowadzane operacje finansowe zawsze mogą wzbudzić podejrzenia co do ich legalności. Zastosowanie tego *modus operandi* wymaga zaplanowania i wysokospecjalistycznej wiedzy. Brak jest informacji o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej w Polsce. WNIOSEK: Wykorzystanie mechanizmu zakupu skradzionych antyków i dzieł sztuki od osób związanych z działalnością o charakterze terrorystycznym do finansowania terroryzmu stwarza w Polsce niskie zagrożenie.

13. Obszar – działalność gospodarcza (ogólnie)

Tabela nr 26

Rodzaj wykorzystanych usług, produktów finansowych	legalna działalność podmiotów gospodarczych
Ogólny opis ryzyka	wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Firma X działająca na rynku samochodów używanych finansuje terroryzm z przychodów uzyskanych z tytułu sprzedanych pojazdów. 2. Finansowanie działalności organizacji terrorystycznej z dochodów osiągniętych przez firmę zajmującą się leasingiem i obrotem nieruchomościami. 3. Celowe łączenie środków uzyskanych od sponsorów organizacji terrorystycznej z legalnymi przychodami podmiotu gospodarczego zajmującego się handlem międzynarodowym w celu utrudnienia identyfikacji procederu finansowania terroryzmu.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Założenie spółki prawa handlowego czy też rozpoczęcie działalności jako osoba fizyczna prowadząca działalność gospodarczą jest w pewnymi zakresie

	ograniczona przepisami prawa, wymagającymi ich rejestracji i spełnienia pewnych warunków (np. w przypadku spółek kapitałowych i spółki komandytowo-akcyjnej posiadaniem kapitału zakładowego w określonej wysokości). Istnieją możliwości ukrycia danych beneficjenta rzeczywistego posłużeniem się słupami lub przedsiębiorstwami symulującymi. Wniesienie kapitału założycielskiego lub też kupno/nabycie już istniejącego podmiotu może być dokonane za pośrednictwem transakcji finansowej o międzynarodowym charakterze lub tez przy udziale osób/podmiotów zagranicznych. Tylko część podmiotów gospodarczych należy do IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2
Uzasadnienie dla poziomu zagrożenia	Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu jest jednym z podstawowych sposobów finansowania działalności terrorystycznej. Legalnie funkcjonujące firmy działają na rzecz organizacji terrorystycznych, a część bądź całość zysków tych firm jest przekazywana na działalność związaną z terroryzmem. Firmy te zazwyczaj są ulokowane w branżach związanych z handlem nieruchomościami, handlem elektroniką, używanymi samochodami, metalami szlachetnymi, tekstyliami, eksportem i importem żywności oraz gastronomią. Legalnie działające firmy mogą zostać wykorzystane zarówno do bezpośredniego pozyskiwania funduszy wspierających działania terrorystyczne, jak i jako pasy transmisyjne do przekazywania środków związanych z finansowaniem takiej działalności. Często legalne środki podmiotu gospodarczego mieszane są ze środkami uzyskanymi ze źródeł finansujących terroryzm i przekazywane dalej, by utrudnić identyfikację środków jako wspierających terroryzm. Częstokroć legalnie działające firmy zajmujące się przepływem środków związanych z finansowaniem terroryzmu są prowadzone przez członków jednej grupy etnicznej, co wpływa na trudności w rozpoznaniu tego procederu. Jest to sposób stosunkowo łatwy i szeroko dostępny, jego zastosowanie niewiele kosztuje i może być postrzegany przez sprawców raczej jako w miarę atrakcyjny. Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu z reguły nie wzbudza podejrzeń. Wysoki wolumen obrotów przedmiotowych firm pozwala ukryć wykorzystanie tych firm do przekazywania pieniędzy na cele działalności terrorystycznej. Zwłaszcza gdy nie są to jednorazowo sumy zbyt wysokie. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystuje się sfałszowaną dokumentację transakcji. Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o rachunkowości i umiejętności logistycznych. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu stwarza w Polsce średnie zagrożenie.

Tabela nr 27

Rodzaj wykorzystanych usług, produktów finansowych	przedsiębiorstwa symulujące
Ogólny opis ryzyka	wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej do finansowania terroryzmu

Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	1. Zakup spółek, które wcześniej prowadziły działalność gospodarczą, w celu wykorzystania ich do utrudnienia identyfikacji transferu wartości majątkowych mających za cel finansowanie terroryzmu. 2. Prowadzenie na rzecz spółki z o.o. należącej do cudzoziemca usług z zakresu księgowości i administracji przez polski podmiot gospodarczy specjalizujący się w obsłudze przedsiębiorstw. Wykorzystanie omawianej spółki z o. o. do finansowania terroryzmu. 3. Sprawcy tworzą skomplikowane i długie łańcuchy powiązań organizacyjno-własnościowych pomiędzy podmiotami gospodarczymi, stowarzyszeniami, organizacjami charytatywnymi, trustami (przy zaangażowaniu podmiotów zarejestrowanych w różnych jurysdykcjach, w tym w rajach podatkowych) w celu utrudnienia identyfikacji rzeczywistych właścicieli podmiotów wykorzystywanych do finansowania terroryzmu. 4. Transferowanie wartości majątkowych za pośrednictwem ww. podmiotów pod fikcyjnymi tytułami (np. kupna/sprzedaży towarów/usług, udziałów/akcji, udzielenia/spłaty pożyczek) w celu sfinansowania potrzeb terrorystów.
Poziom podatności	2
Uzasadnienie dla poziomu podatności	Założenie spółki prawa handlowego czy też rozpoczęcie działalności jako osoba fizyczna prowadząca działalność gospodarczą jest w pewnym zakresie ograniczona przepisami prawa, wymagającymi ich rejestracji i spełnienia pewnych warunków (np. w przypadku spółek kapitałowych i spółki komandytowo-akcyjnej posiadaniem kapitału zakładowego w określonej wysokości). Istnieją możliwości ukrycia danych beneficjenta rzeczywistego posłużeniem się słupami lub przedsiębiorstwami symulującymi. Wniesienie kapitału założycielskiego lub też kupno/nabycie już istniejącego podmiotu może być dokonane za pośrednictwem transakcji finansowej o międzynarodowym charakterze lub tez przy udziale osób/podmiotów zagranicznych. Tylko część podmiotów gospodarczych należy do IO. Organy administracji publicznej posiadają wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwość gromadzenia i analizowania informacji. Istnieje duże prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy zostanie wykryty, a następnie w wyniku dochodzenia/śledztwa nastąpi oskarżenie i skazanie sprawców. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	2

Uzasadnienie dla poziomu zagrożenia	Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej jest jednym z podstawowych sposobów dla przesyłu środków związanych z finansowaniem działalności terrorystycznej. Legalnie założone, ale nie funkcjonujące w praktyce działalności gospodarczej firmy, posługują się kilkoma rachunkami, które funkcjonują tylko jako pasy transmisyjne dla przesyłu środków finansowych na rzecz organizacji terrorystycznych. Dokonywane na rzecz firmy wpłaty gotówkowe bądź przelewy mają służyć zaciemnieniu pochodzenia środków, które są przekazywane dalej, często na rachunki innych podmiotów ulokowanych już w rejonach wrażliwych z punktu widzenia zwalczania terroryzmu. Częstokroć te pozornie tylko działające firmy zajmujące się przepływem środków związanych z finansowaniem terroryzmu są prowadzone przez członków jednej grupy etnicznej, co wpływa na trudności w rozpoznaniu tego procederu. Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej dla przesyłu środków związanych z finansowaniem działalności terrorystycznej jest sposobem stosunkowo łatwym i szeroko dostępnym, a jego zastosowanie niewiele kosztuje i może być postrzegany przez sprawców raczej jako w miarę atrakcyjne. Wykorzystanie funkcjonujących podmiotów gospodarczych do finansowania terroryzmu z reguły nie wzbudza podejrzeń, choć zagrożeniem jest czasem widoczna niestandardowość tych firm w podejściu biznesowym. W celu ukrycia beneficjenta rzeczywistego częstokroć wykorzystuje się sfałszowaną dokumentację transakcji. Zastosowanie tego *modus operandi* wymaga jednak zaplanowania, wiedzy o rachunkowości i umiejętności logistycznych. GIIF otrzymywał nieliczne informacje o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej. WNIOSEK: Wykorzystanie spółek nieprowadzących w praktyce działalności gospodarczej do finansowania terroryzmu stwarza w Polsce średnie zagrożenie.

14. Obszar – świadczenia socjalne

Tabela nr 28

Rodzaj wykorzystanych usług, produktów finansowych	renty, zasiłki i emerytury
Ogólny opis ryzyka	wykorzystywanie świadczeń socjalnych przez zagranicznych bojowników terrorystycznych
Scenariusz wystąpienia ryzyka (tj. możliwy przykład wystąpienia ryzyka)	Wykorzystanie świadczeń socjalnych (otrzymanych legalnie lub wyłudzonych) do opłacenia podróży i pobytu zagranicznych bojowników terrorystycznych w strefie konfliktu.
Poziom podatności	3
Uzasadnienie dla poziomu podatności	Otrzymanie tego typu świadczeń wymaga spełnienia pewnych warunków, określonych przepisami prawa. Trudne jest ukrycie danych identyfikacyjnych beneficjentów. Istnieje możliwość realizacji transakcji o charakterze międzynarodowym (tj. przekazywanie rent, emerytur, zasiłków na rzecz osób uprawnionych, posiadających rachunki poza granicami kraju). Organy przyznające renty/ emerytury/ zasiłki są jednostkami współpracującymi. Jednak ich poziom świadomości obowiązków w zakresie PPP/PFT może nie być wystarczający. Organy administracji publicznej posiadają podstawową wiedzę nt. ryzyka PP/FT w tym zakresie. GIIF ma ograniczone możliwości gromadzenia i analizowania informacji przyznania emerytur/zasiłków/rent. Istnieje prawdopodobieństwo, że przypadek FT w zakresie analizowanych scenariuszy nie zostanie wykryty. Krajowa i międzynarodowa współpraca organów administracji publicznej jest na relatywnie dobrym poziomie. Istniejące przepisy prawne odpowiadają w dużej części zakresowi analizowanego ryzyka.
Poziom zagrożenia	1

Uzasadnienie dla poziomu zagrożenia	Wykorzystywanie świadczeń socjalnych przez zagranicznych bojowników terrorystycznych w Polsce (np. do opłacenia podróży i pobytu zagranicznych bojowników w strefie konfliktu) jest dosyć trudnym do zastosowania sposobem finansowania działalności o charakterze terrorystycznym. Wysokość świadczeń dla cudzoziemca w Polsce na pokrycie we własnym zakresie kosztów pobytu na terytorium RP wynosi najwięcej 750 zł/os na miesiąc przy założeniu, że jest to pojedyncza osoba, natomiast na członka czteroosobowej rodziny przypada już tylko 375 zł na miesiąc.[32] W ośrodkach dla imigrantów świadczenia pieniężne są wielokrotnie niższe. Jak z powyższego wynika świadczenia socjalne w Polsce, ze względu na swoją wysokość, są raczej trudne do wykorzystania w celu finansowania terroryzmu. Wielokrotnie wyższe świadczenia socjalne dla uchodźców czy imigrantów oferują bogatsze kraje Europy Zachodniej. Ww. metoda finansowania terroryzmu w postaci opłacenia podróży i pobytu zagranicznych bojowników w strefie konfliktu jest w warunkach polskich nie do zastosowania, a przez identyfikację przez organ udzielający świadczenia i kontrolę wykorzystania świadczenia również ryzykowna dla sprawców. Brak jest informacji o możliwości wykorzystania tej metody do finansowania działalności terrorystycznej w Polsce. WNIOSEK: Wykorzystanie świadczeń socjalnych przez zagranicznych bojowników terrorystycznych w Polsce do finansowania terroryzmu stwarza w Polsce niskie zagrożenie.

[32] Źródło - https://udsc.gov.pl/uchodzcy-2/pomoc-socjalna/system-pomocy-socjalnej/rodzaje-przyznawanej-pomocy/, dostęp 21.06.2019 r.