DZIAŁANIA INFORMACYJNE

mgr Jacek CHARATYNOWICZ[1]

EKONOMICZNE ASPEKTY CYBERPRZESTĘPCZOŚCI. ZAGROŻENIA ZWIĄZANE Z KONWERSJĄ I TRANSFEREM WIRTUALNYMI WALUTAMI

Słowa kluczowe: *cyberprzestępczość, wirtualne waluty, transakcje finansowe, sieć bezpieczeństwa finansowego, przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, regulacja rynku wirtualnych walut*

STRESZCZENIE

Przedmiotem niniejszego opracowania jest scharakteryzowanie systemu wirtualnych walut oraz zagrożeń wynikających z ich obrotu i konwersji. Przedstawiono, ponadto, system organów nadzoru finansowego oraz przeciwdziałania praniu pieniędzy a także finansowaniu terroryzmu. Praca ma charakter badawczo-analityczny i może stanowić przyczynek do dalszych badań.

Uwagi wstępne

Rozwój nowoczesnych technologii, cyberprzestrzeń są najszybciej rozwijającymi się przejawami i przestrzeniami aktywności człowieka. Jednak oprócz niewątpliwych szans dla rozwoju cywilizacyjnego, kulturowego i gospodarczego niosą pewne zagrożenia dla bezpieczeństwa państwa i jego obywateli.

Przestępczość występująca w cyberprzestrzeni, cyberataki, cyberterroryzm oraz elementy walki informacyjnej są nowymi zagrożeniami obserwowanymi przez policję, służby specjalne, przedsiębiorców czy uczelnie zajmujące się bezpieczeństwem w cyberprzestrzeni. Egzemplifikacją tych zjawisk są ataki DDos na systemy

[1] Jacek Charatynowicz jest doktorantem Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej,

prywatne i publiczne, przejmowanie kont pocztowych, podziemne fora internetowe (darknet). Zagrożenie stanowią również informacje przesłane drogą elektroniczną zawierające wirusy, robaki (malwery), które mogą być wykorzystane w celu uzyskania dostępu do danych czy też zablokowania możliwości takiego dostępu. To tylko niektóre z zagrożeń[2].

Różne są motywy podejmowania takich działań: od osiągniecia korzyści majątkowych, nieuczciwej konkurencji biznesowej, działań ideologicznych po zorganizowaną działalność państwową w ramach komórek służb specjalnych do zadań cybernetycznych.

Osoby zaangażowane w działania przestępcze, oprócz stworzenia pełnej anonimowości w sieci w celu ukrycia lub zalegalizowania korzyści pochodzących z cyberprzestępstw bądź uchylenia się od opodatkowania, mogą wykorzystać wirtualne waluty. System bankowy posiada instrumenty dotyczące przeprowadzenia procedury identyfikacji klienta, stosowania środków bezpieczeństwa finansowego, rejestrowania transakcji, typowania i raportowania do Generalnego Inspektora Informacji Finansowej transakcji podejrzanych czy blokowania rachunków i składania zawiadomień o podejrzeniu popełnienia przestępstwa[3]. Systemy płatności internetowych takie jak Western Union, PayPal, MoneyGram jak również inne, posiadające licencje nadzoru finansowego podmioty używają systemu analizowania ryzyka i monitorowania bezpieczeństwa transakcji. System obrotu wirtualnymi walutami nie wykształcił takich mechanizmów[4], w związku z czym jest podatny na wykorzystanie do działań przestępczych.

Celem artykułu jest scharakteryzowanie systemu wirtualnych walut oraz zagrożeń wynikających z ich obrotu i konwersji. Ponadto, będzie próbą przedstawienia systemu organów nadzoru finansowego i przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu w kontekście monitorowania transakcji wirtualnymi walutami. Nadto, zostanie podjęta próba stworzenia modeli regulacji tego zagadnienia.

---

[2] Szerzej na ten temat: J. Kosiński, *Paradygmaty cyberprzestępczości*, Wydawnictwo Difin, Warszawa 2015, s. 90 i dalsze.

[3] Szerzej na ten temat: M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Komentarz*, Wydawnictwo Lexis Nexis, Warszawa 2014.

[4] W związku z działalnością giełd wirtualnych walut obserwuje się wzrost świadomości bezpieczeństwa transakcji ich właścicieli w aspekcie prania pieniędzy, finansowania terroryzmu lub innych zagrożeń – w wewnętrznych regulacjach (regulaminach) pojawiają się zapisy dotyczące autoryzacji założenia usługi w postaci przekazania kserokopii dokumentu tożsamości, czy transakcji – wskazanie rachunku bankowego.

Wirtualna waluta

Obserwując zmiany na rynku bankowym związane z decentralizacją obrotu, szybkością transakcji oraz tworzenia alternatywnych metod transferu, powstanie wirtualnych walut wpisuje się w postępującą ewolucję pieniądza tradycyjnego[5]. Jednak o ważnym momencie w rozwoju rynku finansowego świadczy wielość publikacji na ten temat, m.in.: raporty Europejskiego Banku Centralnego *Wirtualne systemy walut* (2012) oraz *Wirtualne systemy walut – dalsza analiza* (2015), Raport Financial Action Task Force *Wirtualne waluty – kluczowe definicje i potencjalne ryzyko dla prania pieniędzy oraz finansowania terroryzmu* (2014). Innym opracowaniem jest Dokument Europejskiego Urzędu Nadzoru Bankowego z 2014 r. – *Opinia na temat wirtualnych walut*. Ponadto wirtualne waluty były przedmiotem badań naukowych w ramach projektu realizowanego wspólnie przez Uniwersytet w Opolu i Narodowy Bank Polski i opublikowane zostały pod redakcją naukową prof. Ewy Bogackiej-Kisiel pt.: *Pieniądz wirtualny i determinanty jego rozwoju w sferze ekonomii, finansów i prawa oraz jego wpływ na realną gospodarkę w latach 2010–2015.*

Jedną z definicji wirtualnych walut zaproponował Financial Action Task Force, zgodnie z którą, „waluty wirtualne jako cyfrowa reprezentacja wartości, mogą być przedmiotem obrotu cyfrowego i działają jako środek wymiany i/lub środek przechowywania wartości, ale nie mają statusu prawnego środka płatniczego w jakiejkolwiek jurysdykcji[6]". Europejski Bank Centralny przedstawił inną definicję: „cyfrowa reprezentacja wartości, nie wydawana przez bank centralny, instytucję kredytową lub instytucję pieniądza elektronicznego, które w pewnych okolicznościach mogą być stosowane jako alternatywa dla pieniędzy"[7].

Mimo faktu, że wirtualne waluty funkcjonują w obrocie od 2008 r. nie zostały one zdefiniowane przez polskie jednostki nadzoru finansowego, analityki finansowej – w trakcie analizy raportów regulatorów zajmujących się nadzorem nad ryn-

---

[5] Szerzej na ten temat: H. Zadroga, T. Zieliński, *Pieniądz współczesny a kryzysy finansowe*, Wydawnictwo Difin, Warszawa 2012, s. 20 i dalsze.

[6] Raport FATF, *Wirtualne waluty – kluczowe definicje i potencjalne ryzyko w zakresie prania pieniędzy oraz finansowaniu terroryzmu*, s. 4, http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [dostęp: 27.04.2016].

[7] Raport Europejskiego Banku Centralnego z 2015 r., *Wirtualne systemy walut – dalsza analiza*, s. 4, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf [dostęp: 27.04.2016].

kiem finansowym[8] nie natrafiono na publikacje dotyczące problematyki wirtualnych walut. Były one jednak przedmiotem ostrzeżeń Generalnego Inspektora Informacji Finansowej zamieszczonych w sprawozdaniu z realizacji ustawy o przeciwdziałaniu praniu brudnych pieniędzy oraz finansowaniu terroryzmu, który informował o zagrożeniach związanych z obrotem tym instrumentem. Ponadto, Generalny Inspektor Informacji Finansowej, organ właściwy w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, 14 lipca 2014 r. wydał *Komunikat w sprawie niebezpieczeństw związanych z walutami wirtualnymi,* w którym zwrócił uwagę na niepokojące zjawisko wykorzystywania obrotu wirtualnymi walutami do działań przestępczych, między innymi w procederze prania pieniędzy.

Wirtualne waluty były przedmiotem analiz przedsiębiorstw bankowych, w indywidualnej interpretacji zwrócono uwagę, że obrót wirtualnymi walutami nie jest objęty jednoznacznymi przepisami prawa polskiego – brak jest na polskim rynku regulacji oraz rekomendacji regulatorów w tym zakresie.

Cechy wirtualnych walut, które czynią je atrakcyjnymi dla uczestników obrotu to: anonimowy charakter transakcji, szybkość transakcji, międzynarodowy charakter, niskie koszty transakcyjne, bezpieczeństwo obrotu, brak ingerencji organów państwowych – brak identyfikacji stron transakcji – decentralizacja transakcji, odporność na manipulacje i kryzysy finansowe, odporność na czynniki zewnętrzne. Jednak te same cechy, które czynią je tak atrakcyjnymi mogą wpływać negatywnie na bezpieczeństwo obrotu, m.in. anonimowy charakter, decentralizacja obrotu, brak ingerencji organów państwowych.

Raport Europejskiego Banku Centralnego proponuje trzy kategorie wirtualnych walut:

1. zamknięte systemy wirtualnej waluty, które nie mają żadnego odniesienia do realnej gospodarki;
2. system wirtualnej waluty z przepływów jednokierunkowych, w którym można kupić jednostki za pomocą prawdziwej waluty po określonym kursie, ale nie mogą być wymienione z powrotem i handel z innymi użytkownikami nie jest dozwolony;
3. systemy wirtualnej waluty z przepływów dwukierunkowych, w którym jednostki mogą być kupowane i sprzedawane zgodnie z (płynnymi) kursami walut[9].

---

[8] Sprawozdania z działalności Komisji Nadzoru Finansowego, sprawozdania z realizacji przez Generalnego Inspektora informacji Finansowej ustawy z 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

[9] Raport Europejskiego Banku Centralnego, *Wirtualne systemy walut*, 2012, s. 14–15, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [dostęp: 28.04.2016].

Uczestnikami obrotu wirtualnych walut są:

- emitenci – górnicy, którzy w procesie miningu, przy wykorzystaniu jednostek obliczeniowych jednostki komputera wydobywają wirtualne waluty (bitcoin) jednak ze względu na wbudowane w mechanizm procesy antyinflacyjne ten sposób kreacji waluty traci na znaczeniu;
- indywidualni uczestnicy obrotu, którzy na własne ryzyko nabywają, w różnych celach, wirtualne waluty;
- pośrednicy instytucjonalni (tzw. giełdy obrotu wirtualną walutą);
- fundacje (które deklarują możliwość wpłat w formie wirtualnych walut);
- banki, które obsługują rachunki giełd wirtualnych walut;
- inni przedsiębiorcy.

Wirtualne waluty nie są prawnym środkiem płatniczym, nie są również instrumentem finansowym, elektronicznym instrumentem płatniczym, czy wartością dewizową. Istotną cechą tych walut jest to, że nie są emitowane przez krajowe banki, w związku z tym nie mają oparcia w realnej gospodarce państwa jak również towarach (surowce, kruszec) oraz nie są nadzorowane przez państwowy czy europejski nadzór bankowy czy finansowy. W związku z tym brak jest jednego centrum rozrachunkowego dla tych instrumentów, a to z kolei związane jest z ryzykiem transakcyjnym wynikającym z niepewności uczestników obrotu.

W nawiązaniu do problematyki obrotu wirtualnymi walutami powstają pojedyncze interpretacje prawne organów podatkowych. Przykładem może być prawna ocena służb skarbowych, która dla celów podatkowych uznaje wirtualne waluty jako prawo majątkowe. Zgodnie z interpretacją Izby Skarbowej w Warszawie z 25 lutego 2014 r., wirtualna waluta ***bitcoin*** to prawo o charakterze majątkowym – prawo podmiotowe pozostające w związku z ekonomicznym interesem uprawnionego. Jest to uprawnienie określonego podmiotu, które związane jest z jego majątkiem. Wymiana tego instrumentu na walutę krajową lub zagraniczną albo kupno za nią realnych towarów powoduje powstanie przychodu, który trzeba opodatkować. Z wyjaśnień Ministerstwa Finansów wynika, że taką transakcję należy traktować jako odpłatne zbycie praw majątkowych[10].

Trudniej jest natomiast określić jakie konsekwencje w podatku VAT ma obrót wirtualnymi walutami. Izba Skarbowa w Katowicach, w interpretacji z 21 czerwca 2013 r. (nr IBPP2/443/258/13/ICz) stwierdziła, że wymiana certyfikatów bitcoin na realną walutę nie jest zwolnioną z podatku VAT usługą pośrednictwa finansowego. Konsekwencją tego stanowiska powinno być uznanie, że jeśli roczne obroty

[10] M. Szulc, *Cyfrowe waluty podlegają realnej daninie*, http://biznes.interia.pl/podatki/news/cyfrowe-waluty-podlegaja-realnej-daninie,1945844,4211 [dostęp: 27.04.2016].

podatnika przekroczą 150 tys. złotych to będzie on zobowiązany rozliczać podatek według 23% stawki[11].

System przeciwdziałania praniu pieniędzy

System to „układ elementów mający określoną strukturę i stanowiący logicznie uporządkowaną całość"[12]. Ustawa z dnia 16 listopada 2000 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w zakresie wskazania zaangażowanych podmiotów, określenia ich zadań i wymiany informacji wprowadza system przeciwdziałania praniu pieniędzy praz finansowaniu terroryzmu[13].

System ten tworzą:
– Generalny Inspektor Informacji Finansowej (GIIF),
– instytucje obowiązane,
– jednostki współpracujące.

Do zadań GIIF należy uzyskiwanie, gromadzenie, przetwarzanie i analizowanie informacji w trybie określonym w ustawie oraz podejmowanie działań w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, a w szczególności:
- badanie przebiegu transakcji, co do których GIIF powziął uzasadnione podejrzenia;
- przeprowadzanie procedury wstrzymania transakcji lub blokady rachunku;
- rozstrzyganie w przedmiocie zwolnienia zamrożenia wartości majątkowych;
- udostępnianie i żądanie przekazania informacji o transakcjach;
- przekazywanie uprawnionym organom dokumentów uzasadniających podejrzenie popełnienia przestępstwa;
- inicjowanie i podejmowanie innych działań w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, w tym szkolenie pracowników instytucji obowiązanych w zakresie zadań nałożonych na te instytucje;
- sprawowanie kontroli przestrzegania przepisów dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu;

---

[11] Tamże.

[12] Internetowy słownik języka polskiego PWN, http://sjp.pwn.pl/sjp/system;2576909.html [dostęp: 13.11.2015].

[13] M. Capiga, *Bezpieczeństwo transakcji finansowych w Polsce*, Wydawnictwo CeDeWu sp. z o.o., Warszawa 2015, s. 182.

- współpraca z zagranicznymi instytucjami i międzynarodowymi organizacjami zajmującymi się przeciwdziałaniem praniu pieniędzy lub finansowaniu terroryzmu;
- nakładanie kar pieniężnych, o których mowa w ustawie.

Mając powyższe zadania na uwadze należy stwierdzić, że GIIF gromadzi informacje dotyczące transakcji z udziałem instytucji obowiązanych, analizuje je, w uzasadnionych przypadkach przekazuje zawiadomienia o podejrzeniu popełnienia przestępstwa do jednostek organizacyjnych prokuratury lub też przekazuje powiadomienia[14] uprawnionym organom. Do innych stosowanych procedur, istotnych z puntu widzenia przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu należy zaliczyć stosowanie procedury wstrzymania transakcji bądź blokady rachunku bankowego.

Instytucje obowiązane[15] to m.in. banki, przedsiębiorstwa ubezpieczeniowe i inwestycyjne, notariusze, kantory wymiany walut, lombardy, a także biegli rewidenci. Ponadto instytucją obowiązaną jest też przedsiębiorca, który przyjmując środki finansowe o równowartości 15.000 euro w gotówce za towar, obowiązany jest zarejestrować taką transakcję, według odpowiedniego wzoru rejestru, oraz zaraportować do GIIF.

Do głównych instrumentów tego systemu należy m.in. obowiązek instytucji obowiązanych raportowania do GIIF informacji o transakcjach ponadprogowych objętych przepisami Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, tj. stanowiących równowartość 15.000 euro, nawet gdy z okoliczności transakcji wynika, że są realizowane w drodze więcej niż jednej operacji, których okoliczności wskazują, że są ze sobą powiązane, a zostały podzielone na operacje o mniejszej wartości, z zamiarem uniknięcia obowiązku rejestracji[16]. Ponadto, do obowiązków instytucji obowiązanych należy, w oparciu i na podstawie analizy ryzyka środków bezpieczeństwa finansowego, typowanie transakcji podejrzanych i raportowanie ich do GIIF.

---

[14] Powiadomienia to termin dla informacji przekazywanych przez Generalnego Inspektora Informacji Finansowej na podstawie art. 33 ust. 3 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2010 r. nr 46, poz. 276 z późn. zm.) – uprawnionym organom z własnej inicjatywy. Informacje te nie należy utożsamiać z zawiadomieniem o podejrzeniu popełnienia przestępstwa.

[15] Pełną listę instytucji obowiązanych zawiera art. 2 od lit. a do t. Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

[16] Op. cit. art. 8 ust. 1 Ustawy o przeciwdziałaniu…

Do instytucji współpracujących Ustawa zalicza m.in. prokuraturę, policję, Agencję Bezpieczeństwa Wewnętrznego. Prokuratura informuje np. GIIF o wszczęciu lub zakończeniu postepowania jak również o przedstawionych zarzutach w zakresie prania pieniędzy bądź finansowania terroryzmu. Do zadań Policji czy ABW należy w szczególności prowadzenie czynności na podstawie ustaw regulujących działalność tych instytucji, np. w przypadku policji jest to grupa zadań wymienionych w Ustawie z dnia 6 kwietnia 1990 r. o Policji, lub w przypadku Agencji Bezpieczeństwa Wewnętrznego, w trybie i na zasadach określonych Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu.

Do głównych zdań tych instytucji w zakresie przeciwdziałania praniu pieniędzy lub finansowania terroryzmu należy m.in. informowanie GIIF o uzyskanych informacjach wskazujących na podejrzenia prania pieniędzy lub finansowania terroryzmu. Jednym z głównych zadań służb Policji oraz ABW jest prowadzenie czynności o charakterze operacyjno-rozpoznawczym lub dochodzeniowo-śledczym.

Warto dodać, że prokuratura, policja czy ABW może uzyskiwać informacje od GIIF dotyczące transakcji ponadprogowych czy podejrzanych, w trybie i na zasadzie Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Sieć bezpieczeństwa finansowego

W przypadku uczestników rynku finansowego, realizowanych na tym rynku transakcji, czy też gwarancji zgromadzonych aktywów zidentyfikować można mechanizm mający istotne znaczenie dla bezpieczeństwa finansowego państwa – sieć bezpieczeństwa finansowego. Tworzą ją organy posiadające uprawnienia w zakresie nadzoru, kontroli, gwarantowania środków wobec podmiotów nadzorowanych – uczestników transakcji na rynku finansowym.

Sieć tą tworzą podmioty: Narodowy Bank Polski, Komisja Nadzoru Finansowego i Bankowy Fundusz Gwarancyjny.

Narodowy Bank Polski ze względu na szczególne umocowanie prawne pełni szczególną rolę w sieci bezpieczeństwa finansowego. Podstawowym celem działalności Narodowego Banku Polskiego jest utrzymanie stabilnego poziomu cen, przy jednoczesnym wspieraniu polityki gospodarczej rządu, o ile nie ogranicza to podstawowego celu NBP. Do zadań NBP należy także:

- organizowanie rozliczeń pieniężnych;
- prowadzenie gospodarki rezerwami dewizowymi;
- prowadzenie działalności dewizowej w granicach określonych ustawami;

- prowadzenie bankowej obsługi budżetu państwa;
- regulowanie płynności banków oraz ich refinansowanie;
- kształtowanie warunków niezbędnych dla rozwoju systemu bankowego;
- działanie na rzecz stabilności krajowego systemu finansowego;
- opracowywanie statystyki pieniężnej i bankowej, bilansu płatniczego oraz międzynarodowej pozycji inwestycyjnej;
- wykonywanie innych zadań określonych ustawami[17].

„Głównym podmiotem rynku pieniężnego i polityki pieniężnej każdego państwa jest bank centralny. Jest on również bankiem emisyjnym państwa, do jego podstawowych zadań należy finansowanie i kontrola innych instytucji finansowych danego kraju. Według Międzynarodowego Funduszu Walutowego, do najważniejszych funkcji banku centralnego należy zaliczyć:
- pełnienie roli agenta kredytowego i fiskalnego rządu,
- przechowywanie rezerw banków komercyjnych,
- przechowywanie rezerw krajowych oraz złota i walut obcych, jak również administrowanie nimi,
- emitowanie znaków pieniężnych"[18].

W polskim systemie finansowym istnieje model zintegrowanego nadzoru nad rynkiem finansowym, tzn. jeden urząd nadzoruje poszczególne segmenty rynku finansowego: bankowy, kapitałowy, ubezpieczeniowy, funduszy emerytalnych, pieniądza elektronicznego[19]. Instytucją powołaną do nadzoru rynku finansowego jest Komisja Nadzoru Finansowego.

Do zadań Komisji należy w szczególności:
- podejmowanie działań służących prawidłowemu funkcjonowaniu rynku finansowego,
- podejmowanie działań mających na celu rozwój rynku finansowego i jego konkurencyjności,
- podejmowanie działań edukacyjnych i informacyjnych w zakresie funkcjonowania rynku finansowego,

---

[17] Art. 3 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz.U. z 2013 r., poz. 908, z późn. zm.).

[18] W. Dębski, *Rynek finansowy i jego mechanizmy. Podstawy teorii i praktyki*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 61.

[19] M. Zdyb, J. Stelmasiak, K. Sikora, *Podstawowe płaszczyzny zagrożeń bezpieczeństwa wewnętrznego. Aspekty materialnoprawne*, Wydawnictwo Lex Wolters Kluwer business, s. 76.

- udział w przygotowywaniu projektów aktów prawnych w zakresie nadzoru nad rynkiem finansowym,
- stwarzanie możliwości polubownego i pojednawczego rozstrzygania sporów między uczestnikami rynku finansowego, w szczególności sporów wynikających ze stosunków umownych między podmiotami podlegającymi nadzorowi Komisji a odbiorcami usług świadczonych przez te podmioty,
- wykonywanie innych zadań określonych ustawami[20].

Innym elementem wzmacniającym bezpieczeństwo finansowe obrotu bankowego jest działalność Bankowego Funduszu Gwarancyjnego. Ustawa o Bankowym Funduszu Gwarancyjnym reguluje m.in. tworzenie, organizację, zadania, źródła finansowania i nadzór nad Bankowym Funduszem Gwarancyjnym. Wśród podmiotów, których depozyty wchodzą w zakres działania i ochrony Bankowego Funduszu są banki i spółdzielcze kasy oszczędnościowo-kredytowe oraz wierzytelności wynikające z czynności bankowych, czy też należnych z tytułu przeprowadzonych przez kasę rozliczeń finansowych. „Bankowy Fundusz zapewnia deponentom, w przypadku strat, wypłatę środków ulokowanych w banku lub spółdzielczej kasie objętych gwarancją ich zwrotu. Gwarantowane są środki pieniężne zgromadzone przez tego samego deponenta, na które wystawiono dowody imienne w walucie polskiej oraz w walutach obcych, bez względu na liczbę umów zawartych w tym banku bądź kasie SKOK”[21].

Bankowy Fundusz Gwarancyjny jest istotnym elementem bezpieczeństwa finansowego państwa z uwagi na zapewnienie gwarancji środków finansowych zdeponowanych w banku oraz spółdzielczych kasach oszczędnościowo- kredytowych, z tytułu powstałych w tych wierzytelności czy rozliczeń.

Warto wspomnieć o przepisach Ustawy z dnia 2 kwietnia 1994 r. o niektórych zabezpieczeniach finansowych, która reguluje zasady ustanawiania i wykonywania zabezpieczeń na środkach pieniężnych, wierzytelnościach kredytowych, lub instrumentach finansowych (zabezpieczenia finansowe) wierzytelności pieniężnych lub wierzytelności, których świadczenie polega na dostarczeniu instrumentów finansowych (wierzytelności finansowe), w tym wierzytelności przyszłych, zależnych od terminu lub warunku albo okresowych, a także zasady zaspokajania się z tych

[20] Art. 4 ustawy z dnia 21 lipca 2005 r. o nadzorze nad rynkiem finansowym (Dz.U. 2015, poz. 1357).

[21] Z. Krzyżkiewicz, W. L. Jaworski, M. Puławski, R. Walkiewicz, *Leksykon Bankowo-Giełdowy*, Wydawnictwo Poltex, Warszawa 2006, s. 59.

zabezpieczeń[22]. Jednak przedmiotowy mechanizm funkcjonuje w obrębie banków centralnych, instytucji finansowych, centr rozrachunkowych – nie stosuje się do nieuregulowanych form transakcyjnych np. z udziałem wirtualnych walut.

W kontekście wirtualnych walut Komisja Nadzoru Finansowego nie posiada istotnych prerogatyw. Jej działalność skupia się na podmiotach przez nią nadzorowanych[23], w związku z tym zarówno indywidualni uczestnicy, jak również przedsiębiorcy prowadzący działalność gospodarczą w zakresie obrotu lub konwersją wirtualnej waluty nie są objęci tym nadzorem. Jedynie banki, realizujące transakcje giełd wymiany wirtualnej waluty podlegają nadzorowi KNF. Nie odnalazłem jednak żadnych publikacji, ostrzeżeń czy też rekomendacji KNF dla przedsiębiorstw bankowych w obszarze wirtualnych walut. Podobnie zresztą jak Narodowy Bank Polski, który posiada kompetencje na rynku pieniężnym, bankowym oraz w systemie spółdzielczych kas oszczędnościowo-kredytowych. Ze względu na brak przepisów prawnych nie może ingerować w zdecentralizowany system wirtualnych walut.

Bankowy Fundusz Gwarancyjny realizuje zadania w zakresie gwarantowania zgromadzonych aktywów w bankach i spółdzielczych kasach oszczędnościowo- kredytowych. Nie zabezpiecza aktywów giełd wirtualnych walut.

Zagrożenia oraz czynniki ryzyka

Zagrożenia związane z cyberprzestrzenią uwarunkowane są tempem rozwoju technologicznego. W ujęciu strategicznym są przedmiotem analiz Unii Europejskiej i Rzeczpospolitej. Strategia Bezpieczeństwa UE z 2003 r. wśród globalnych wyzwań i głównych zagrożeń dla UE, oprócz m.in. terroryzmu, proliferacji broni masowego rażenia czy przestępczości zorganizowanej wymienia również cyberbezpieczeństwo. Deklarując jednocześnie, że konieczne są dalsze prace w celu przeanalizowania możliwości przyjęcia kompleksowego podejścia unijnego, podniesienia poziomu świadomości i zacieśnienia współpracy międzynarodowej.

---

[22] Art. 1 ustawy z dnia 2 kwietnia 1994 r. o niektórych zabezpieczeniach finansowych (Dz.U. 2004, nr 91, poz. 871).

[23] Pewnym wyjątkiem są tu podmioty, co do których istnieje podejrzenie prowadzenia, bez zezwolenia, działalności polegającej na gromadzeniu środków pieniężnych innych osób fizycznych, osób prawnych lub jednostek organizacyjnych niemających osobowości prawnej, w celu udzielania kredytów, pożyczek pieniężnych lub obciążania ryzykiem tych środków w inny sposób. Szerzej art. 171 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. 1997, nr 140, poz. 939 z późn. zm).

Zgodnie ze Strategią Bezpieczeństwa Narodowego z 2014 r., jednym z głównych celów strategicznych w dziedzinie bezpieczeństwa jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni. Istotnym dokumentem w tej materii jest również Doktryna Cyberbezpieczeństwa RP z 2015 r., która identyfikuje i wskazuje na koncepcje działań preparacyjnych i operacyjnych w dziedzinie cyberbezpieczeństwa.

Wspomniana Doktryna Cyberbezpieczeństwa wskazuje na dwa rodzaje zagrożeń:

1. wewnętrzne, a wśród nich:
   - cyberprzestępczość, cyberprzemoc, cyberprotesty czy cyberdemonstracje o charakterze destrukcyjnym, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego;
   - dotyczące zagrożeń infrastruktury krytycznej państwa, sterowanej za pomocą systemów informatycznych – ataki na systemy komunikacji, zapewniające jego sprawne funkcjonowanie;
   - dotyczące sektora prywatnego – kradzież danych, naruszenie integralności danych, naruszenie poufności prowadzonych działań czy dostępności usług;
   - dotyczące osób prywatnych – kradzieże danych, kradzieże tożsamości, i przejmowanie kontroli nad prywatnymi komputerami.
2. zewnętrzne;

– cyberkryzysy i cyberkonflikty z udziałem podmiotów państwowych i niepaństwowych, w tym także groźba cyberwojny;
– cyberszpiegostwo związane z prowadzeniem przez służby obcych państw i podmioty pozapaństwowe, w tym organizacje terrorystyczne, działań wykorzystujących specjalistyczne narzędzia i mających na celu uzyskanie dostępu do danych newralgicznych z punktu widzenia struktur państwa;
– organizacje ekstremistyczne, terrorystyczne oraz zorganizowane, transnarodowe grupy przestępcze, których ataki w cyberprzestrzeni mogą mieć podłoże ideologiczne, polityczne, religijne, biznesowe i kryminalne[24].

Innym dokumentem opisującym aspekty prawne bezpieczeństwa w cyberprzestrzeni jest Konwencja Rady Europy o Cyberprzestępczości, sporządzona w Budapeszcie 23 listopada 2001 r. Instrumenty oraz instytucje zawarte w tym akcie mają istotne znaczenie dla pragmatyki zwalczania cyberprzestępczości. Konwencja identyfikuje zachowania w cyberprzestrzeni, które ze względu na z szkodliwość spo-

[24] Opracowano na podstawie dokumentu *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 r.*, s. 10–13.

łeczną w prawie karnym stron tej umowy uznaje za przestępstwa, w tym: nielegalny dostęp do całości lub części systemu informatycznego, nielegalne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych, naruszenie integralności danych i systemu komputerowego, przestępstwa komputerowe, oszustwa komputerowe oraz naruszenia praw autorskich i praw pokrewnych.

Istnieje również aspekt finansowy cyberprzestępczości. Osoby uzyskujące korzyści ekonomiczne z przestępczości występującej w cyberprzestrzeni coraz częściej wykorzystują mechanizmy wirtualnych walut do prania pieniędzy, ukrywania majątku czy uchylania się od opodatkowania. Generalny Inspektor Informacji Finansowej, komunikatem z 10 lipca 2014 r., zwrócił uwagę na niepokojące zjawisko wykorzystywania obrotu wirtualnymi walutami do działań przestępczych. Ponadto, GIIF w swoich sprawozdaniach z realizacji Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wskazywał na transakcje wirtualnymi walutami wykorzystywanymi w procesie prania pieniędzy na rynku e-hazardu.

Do największych zagrożeń wynikających z obrotu wirtualnymi walutami należy wymienić:

1. W polskim systemie prawnym brak jest regulacji opisujących zjawisko wirtualnych walut w kontekście transakcyjnym, nadzorczym, czy gwarancji aktywów. Przedmiotowa okoliczność może powodować, iż osoby fizyczne, przedsiębiorcy z uwagi na brak jednoznacznych rekomendacji dla tego rynku nie będą korzystać z tych instrumentów.
2. Obrót wirtualnymi walutami nie jest objęty nadzorem instytucji państwowych – Komisji Nadzoru Finansowego i Narodowego Banu Polskiego w związku z czym istnieją wątpliwości co do bezpieczeństwa realizowanych konwersji wirtualnych walut, gwarancji przekazywanych wartości majątkowych.
3. Transakcje i konwersja wirtualnymi walutami nie są objęte gwarancjami Bankowego Funduszu Gwarancyjnego, w związku z czym nie ma pewności bezpieczeństwa realizowanych transakcji i zgromadzonych aktywów.
4. Obrót wirtualnymi walutami nie jest realizowany przez instytucje systemu przeciwdziałania praniu pieniędzy bądź finansowania terroryzmu – instytucje obowiązane i jednostki współpracujące. Instytucje obowiązane nie rejestrują tych transakcji, nie analizują pod kątem zagrożeń, w związku z czym wykazują podatność do wykorzystaniem tego instrumentu do prania pieniędzy, finansowania terroryzmu, czy też ukrywania majątku.
5. Wirtualne waluty nie mają pokrycia w realnej ekonomii – surowcach, kruszcu, czy innych walutach. Nad emisją, podażą i popytem nie czuwa bank centralny,

z związku czym ten instrument podatny jest na ryzyka związane z manipulacjami wartości.

6. Transakcje wirtualnymi walutami związane są również z ryzykami kursowymi. Przy czym należy zaznaczyć, że wartość wirtualnej waluty jest uzależniona od aktualnej podaży i popytu tej waluty, nie jest odzwierciedleniem wartości gospodarki danego kraju, kondycji finansowej emitenta, pochodną innego bazowego instrumentu finansowego. W związku z tym brak jest kryteriów, zgodnie z którymi można analizować zmienność wartości tej waluty. Ekonomista amerykański N. Roubini zwraca uwagę, że transakcje z udziałem wirtualnej waluty typu bitcoin mogą być wykorzystywane jako piramida finansowa[25].

Wnioski

Zagrożenia występujące w cyberprzestrzeni dotykają strategicznych zagadnień bezpieczeństwa indywidualnego obywateli, korporacyjnego, państwowego czy też ponadpaństwowego (organizacji międzynarodowych). Głównymi aktorami cyberprzestępstw (cyberzagrożeń) są indywidualni przestępcy, zorganizowane grupy przestępcze, grupy o charakterze ekstremistycznym i terrorystycznym. W tym kontekście możemy również wyróżnić specyfikę działania państwa w zakresie wojny informacyjnej, cybernetycznej.

Istotny jest również aspekt finansowy cyberprzestrzeni, który oprócz niewątpliwych dobrodziejstw dla indywidualnych użytkowników, klientów korporacyjnych czy też państw, podatny jest na zagrożenia. Aspekt finansowy możemy opisywać w płaszczyźnie:

1. transakcji bankowych realizowanych z udziałem rachunków bankowych, w tym transakcji elektronicznych oraz z udziałem elektronicznych instrumentów płatniczych;
2. transakcji finansowych realizowanych z udziałem autoryzowanych podmiotów takich jak PayPal, MoneyGram, Western Union – oferujących transakcje typu money transfer, przy czym przedsiębiorstwa zagraniczne posiadają zezwolenie – licencję nadzoru finansowego kraju rejestracji działalności gospodarczej;
3. podmiotów prowadzących system autoryzacji i rozliczeń na podstawie decyzji prezesa Narodowego Banku Polskiego oraz świadczące usługi płatnicze w cha-

[25] Puls Biznesu, Bitcoin to piramida finansowa, http://www.pb.pl/3592126,35620,bitcoin-to-piramida-finansowa [dostęp: 26.04.2016].

rakterze krajowej instytucji płatniczej na podstawie decyzji Komisji Nadzoru Finansowego – wpisanej do rejestru usług płatniczych;
4. wirtualnych walut – transakcje tym instrumentem mają charakter zdecentralizowany, nie są ewidencjonowane, rejestrowane przez instytucje bankowe, ich wartość w czasie nie jest oparta o czynniki ekonomiczne czy gospodarcze.

Narodowy Bank Polski nie uczestniczy w procesie emisji i kontroli podaży tego instrumentu jak również nie uczestniczy w procesie autoryzowania podmiotów biorących udział w ich obrocie. Komisja Nadzoru Finansowego nie posiada uprawnień w zakresie nadzoru nad rynkiem obrotu wirtualnych walut, zaś Generalny Inspektor Informacji Finansowej nie monitoruje podmiotów uczestniczących w transakcji wirtualnymi walutami w zakresie podejrzenia prania pieniędzy bądź finansowania terroryzmu.

W kontekście tych twierdzeń obrót wirtualną walutą oraz podmioty realizujące transakcje tym instrumentem narażone są w szczególny sposób na ryzyko prania pieniędzy, finansowania terroryzmu, ukrywania majątku, uchylania się od opodatkowania. W związku z tym istnieje konieczność uregulowania tego obrotu, przy czym należy rozważyć kilka rozwiązań w tym zakresie:
1. Regulacji wirtualnej waluty w kontekście objęcia nadzorem Komisji Nadzoru Finansowego podmiotów uczestniczących w obrocie i konwersji, określenie wysokości kapitału spółek, formy prawnej – istotnym elementem jest okoliczność, że członkowie zarządu i rad nadzorczych spółek handlowych podlegają rygorowi art. 18 Ustawy z dnia 15 września 2000 r. Kodeks Spółek Handlowych tj. niekaralności za wybrane przestępstwa gospodarcze.
2. Uregulowanie wirtualnych walut przez nadanie im statusu pieniądza, pieniądza elektronicznego bądź instrumentu finansowego jest zabiegiem trudnym do przeprowadzenia pod kątem prawnym, ekonomicznym i technologicznym. W niemieckim systemie prawnym wirtualna waluta (bitcoin) jest uznawana za środek płatniczy – obrót nadzorowany jest przez Urząd Nadzoru Finansowego[26] – jest to jedyny kraj Unii Europejskiej, który zdecydował się na taki kierunek regulacji. W pozostałych krajach UE[27] instrument ten jest poza regulacją.

[26] Bitcoin oficjalnym środkiem płatniczym w Niemczech, http://biznes.interia.pl/waluty/news/bitcoiny-oficjalnie-srodkiem-platniczym-w-niemczech,1944051,1023 [dostęp: 27.04.2016].

[27] Op. cit. Raport Europejskiego Banku Centralnego (2015) s. 34–37.

3. Można również zaproponować system mieszany – składający się z regulacji instrumentu wirtualnej waluty oraz podmiotów (przedsiębiorstw) biorących udział w obrocie tym aktywem.
4. Propozycją w tym zakresie może być również wprowadzenie zmian w Ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu polegających na rozszerzeniu katalogu instytucji obowiązanych o podmioty prowadzące działalność w zakresie giełd wirtualnych walut. Ten kierunek regulacji gwarantuje objecie podmiotów uczestniczących w obrocie wirtualnymi walutami systemem przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmowi.
5. Należy umożliwić, przez adekwatne regulacje prawne, służbom podległym ministrowi spraw wewnętrznych i administracji, służbom skarbowym oraz służbom specjalnym uzyskiwanie informacji od podmiotów prowadzących giełdę obrotu wirtualna walutą w zakresie stron transakcji, wartości oraz innych towarzyszących transakcji (adresy e-mail, IP, telefonu).
6. Zmiany w ustawie o Bankowym Funduszu Gwarancyjnym, celem wprowadzenia giełd wirtualnych walut do katalogu podmiotów, których część aktywów jest gwarantowana przed upadłością takiej giełdy.
7. Przedmiotowe działania należy podjąć pozyskując analizy instytucji finansowych, regulatorów, uczestników obrotu, a także doświadczenia zagraniczne. Podjęcie zbyt głębokich zmian może spowodować przeregulowania systemu wirtualnych walut – może to niekorzystnie wpłynąć na ilość zatrudnienia, wpływy podatkowe czy składki ubezpieczeniowe.

Bibliografia

1. Capiga M., *Bezpieczeństwo transakcji finansowych w Polsce*, Wydawnictwo CeDeWu Warszawa 2015.
2. Dębski W., *Rynek finansowy i jego mechanizmy. Podstawy teorii i praktyki*, Wydawnictwo Naukowe PWN, Warszawa 2007.
3. Hara M., Kierzynka R., Kołodziejski P., *Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Komentarz*, Wydawnictwo Lexis Nexis, Warszawa 2014.
4. Krzyżkiewicz Z., Jaworski W.L., Puławski M., Walkiewicz R., *Leksykon Bankowo-Giełdowy*, Wydawnictwo Poltex, Warszawa 2006.
5. Kosiński J., *Paradygmaty cyberprzestępczości*, Wydawnictwo Difin, Warszawa 2015.
6. Zadroga H., Zieliński T., *Pieniądz współczesny a kryzysy finansowe*, Wydawnictwo Warszawa 2012.
7. Zdyb M., Stelmasiak J., Sikora K., *Podstawowe płaszczyzny zagrożeń bezpieczeństwa wewnętrznego*, Wydawnictwo Wolters Kluwer business, Warszawa 2014.

Akty prawne

1. Ustawa z 2 kwietnia 1994 roku o niektórych zabezpieczeniach finansowych (Dz.U. 2004, nr 91, poz. 871).
2. Ustawa z 14 grudnia 1994 r. o Bankowym Funduszu Gwarancyjnym (Dz.U. 2014, poz. 1866 z późn. zm.).
3. Ustawa z 29 sierpnia 1997 r. Prawo bankowe (Dz.U. 1997, nr 140, poz. 939 z późn. zm).
4. Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz.U. z 2013 r. poz. 908 z późn. zm.).
5. Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (Dz.U. z 2000, nr 94, poz. 1037 z późn. zm).
6. Ustawa z 16 listopada 2000 r o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2010 r., nr 46, poz. 276 z późn. zm.).
7. Ustawa z dnia 21 lipca 2005 r. o nadzorze nad rynkiem finansowym (Dz.U. 2015, poz. 1357).
8. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie 23 listopada 2001 r.

Źródła internetowe

1. Raport Europejskiego Banku Centralnego *Wirtualne systemy walut* (2012).
2. Raport Financial Action Task Force *Wirtualne waluty – kluczowe definicje i potencjalne ryzyko dla prania pieniędzy oraz finansowania terroryzmu* (2014).
3. Raport Europejskiego Urzędu Nadzoru Bankowego – *Opinia na temat wirtualnych walut (2014)*.
4. S*trategia Bezpieczeństwa Narodowego* z 2014 roku.
5. Raport Europejskiego Banku Centralnego *Wirtualne systemy walut – dalsza analiza* (2015).
6. Doktryna Cyberbezpieczeństwa RP z 2015 roku.
7. Internetowy słownik języka polskiego PWN. http://sjp.pwn.pl/sjp/system;2576909.html
8. Szulc M. *Cyfrowe waluty podlegają realnej daninie*, http://biznes.interia.pl/podatki/news/cyfrowe-waluty-podlegaja-realnej-daninie,1945844,4211
9. Bitcoin oficjalnym środkiem płatniczym w Niemczech, http://biznes.interia.pl/waluty/news/bitcoiny-oficjalnie-srodkiem-platniczym-w-niemczech,1944051,1023

Keywords: *cybercrime, virtual currency, financial transaction, financial safety net, combating money laundering and financing of terrorism, market regulation of virtual currency*

SUMMARY

In this article the author takes up the subcject of functioning virtual currecies, entities participating in turnovers of this financial instrument. He indicates a state authority system holding the issuance and supervision of money supply and demand, supervision of financial market or counteracting money laundering, terrorism financing and analyzing their tasks in the context of threats related to virtual currency transactions. Furthermore, he undertakes the attempt of creating a model of regulation this phenomenon in Poland.