Łukasz Stelmaszczyk[1]

Menedżerska Akademia Nauk Stosowanych w Warszawie

https://doi.org/10.29316/9788368103359_17

WIRTUALNY PIENIĄDZ – NOWE MOŻLIWOŚCI I ZAGROŻENIA

VIRTUAL CURRENCY – NEW OPPORTUNITIES AND THREATS

Streszczenie

Wirtualny pieniądz jest ważnym zagadnieniem we współczesnej gospodarce, powiązanym z bezpieczeństwem państwa. Rozwój nowych technologii informatycznych zmienia oblicze finansów, na poziomie gospodarstw domowych, przedsiębiorstw i struktur państwowych. W niniejszym opracowaniu uwagę skupiono na kwestiach takich, jak systemy bankowości elektronicznej, wirtualny pieniądz, nowe sposoby zdalnego przesyłania pieniędzy, jak również ich znaczenie dla nowoczesnej gospodarki. Następnie scharakteryzowano pojęcie pieniądza oraz przedstawiono wpływ powyższych na współczesną ochronę przepływu i przechowywania pieniędzy. Celem rozdziału jest przedstawienie wagi zapewnienia ochrony wirtualnego pieniądza jako kluczowego czynnika gospodarczego bezpieczeństwa państwa, dotyczącego sfery prywatnej i publicznej. Głównym problemem badawczym jest pytanie: jaka jest rola wirtualnego pieniądza w bezpieczeństwie państw i organizacji?

[1] https://orcid.org/0009-0004-4149-6820, e-mail: l.a.stelmaszczyk@wp.pl

Niniejsze opracowanie powstało w oparciu o teoretyczne metody badawcze takie, jak analiza, synteza, wnioskowanie oraz abstrahowanie. Dla pełnego zobrazowania prezentowanych kwestii wykorzystano literaturę przedmiotu.

Słowa kluczowe: cyberbezpieczeństwo, wirtualny pieniądz, bankowość internetowa, Internet, współczesne zagrożenia, bezpieczeństwo państwa

Abstract

Virtual money is a significant issue in the contemporary economy, linked to national security. The development of new information technologies is transforming finance at the level of households, enterprises, and state structures. This study focuses on issues such as electronic banking systems, virtual money, new methods of remote money transfer, and their importance for the modern economy. The concept of money is then characterized and its impact on the contemporary protection of money flow and storage is presented. The aim of this chapter is to demonstrate the importance of ensuring the protection of virtual money as a key factor in the economic security of the state, affecting both the private and public spheres. The main research problem is: what is the role of virtual money in the security of states and organizations? This study is based on theoretical research methods such as analysis, synthesis, inference, and abstraction. The literature on the subject was used to fully illustrate the issues presented.

Keywords: cybersecurity, virtual money, online banking, Internet, modern threats, state security

Wstęp

Przechodzenie do świata wirtualnego kolejnych aspektów działalności człowieka nie ominęło również pieniędzy. Środki płatnicze towarzyszyły ludzkiej cywilizacji od najdawniejszych czasów. Plemienne społeczności bazowały na handlu wymiennym, jednak, z biegiem lat pojawiły się środki płatnicze stanowiące poprzednik obecnego pieniądza. Poprzez futra zwierząt (np. sobole), muszle, metale (miedź, srebro, złoto), środki płatnicze miały zawsze kilka wspólnych cech (Dylewski, 2011, s. 11). Jedną z nich jest możliwość w miarę swobodnego przesyłania pieniądza, często na duże odległości. Złote i srebrne monety, futra niedźwiedzi i muszle cauri, można było przewozić konno, zaprzęgiem, saniami, łodzią i przenosić pieszo. Kolejną

cecha pieniądza jest jego wartość, najlepiej, jeśli dany środek płatniczy jest jak powszechnie uznawany przez wszystkie kraje, w których obowiązuje dana waluta. Bizantyjskie, arabskie, francuskie, węgierskie, hiszpańskie czy nawet brytyjskie monety były uznawane zarówno w kraju wybicia jak i na terenie innych państw o różnym stopniu rozwoju cywilizacyjnego i rozmaitym stosunku do kraju emitenta (Harrison, 2022).

Wirtualny pieniądz spełnia powyższe cechy, co jednak nie wyklucza istnienia szeregu zagrożeń od jakich wolne były tradycyjne nośniki wartości w rodzaju srebrnych groszy, złotych dukatów czy pęków skór sobolich lub kłów słonia. Stary pieniądz w wymiarze materialnym potrzebuje odpowiednich warunków do przechowywania, by zachować swoja wartość. Banknoty papierowe muszą być złożone w miejscu suchym, ciepłym i być zabezpieczone przed ogniem, czy też przed promieniami słonecznymi. Monety są bardziej odporne na wilgoć, jednak ich waga wymaga większych nakładów przy ich przewożeniu. W obecnych czasach największe nominały pięćset, dwieście, sto, pięćdziesiąt, dwadzieścia i dziesięć złotych występują na obszarze Polski w postaci papierowych banknotów. Powyższy układ sprawia, że monety obiegowe Narodowego Banku Polskiego mają niskie wartości jednostkowe, kolejno: pięć złotych, dwa złote, jeden złoty oraz wartości wynoszące od pięćdziesięciu do jednego grosza. Zważywszy na nadmienione, większość transakcji pieniężnych w postaci gotówkowej odbywa się przy użyciu banknotów papierowych (Dylewski, 2011, s. 310). W celu zabezpieczenia wirtualnego pieniądza należy odpowiednio chronić sieci informacyjne, które są podstawą dla przesyłania zapisów księgowych internetowych transakcji (Aleksandrowicz, 2016, s. 5).

Powstanie wirtualnego pieniądza

Wirtualny pieniądz pojawił się na świecie dzięki rozpowszechnieniu się komputerów osobistych PC (personal computer) na przełomie lat siedemdziesiątych i osiemdziesiątych dwudziestego wieku. W roku 1977 spółka Apple wprowadziła do masowej sprzedaży komputery stacjonarne. 12 sierpnia 1981 w Nowym Jorku w hotelu Astoria kolejna amerykańska firma IBM zaprezentowała komputer osobisty, zmieniając technologiczne oblicze milionów gospodarstw domowych. W tym samym czasie, czyli na początku lat osiemdziesiątych dwudziestego wieku, cztery banki działające

na obszarze USA wprowadziły bankowość elektroniczną poprzez instalowanie oprogramowania na komputerach domowych swych klientów. Użytkownicy bankowości elektronicznej uzyskali dostęp do swych kont bankowych, mogli sprawdzać stan konta, dokonywać przelewów i płacić w około 17 tysięcy sklepów.

W Europie w 1983 roku bankowość elektroniczna pojawiła się dzięki Nottingham Building Society, która we współpracy z Bank of Scotland wprowadziła usługę Homelink w Wielkiej Brytanii. W następnych latach bankowość elektroniczna pojawiła się w Finlandii i całej Skandynawii. W pierwszym okresie bankowość elektroniczna odbywała się poprzez sieć telefoniczna i telewizję handlową. Rozwój Internetu przyczynił się do zwiększenia rzesz użytkowników bankowości elektronicznej. Z początkiem lat dziewięćdziesiątych dwudziestego wieku wraz z pojawieniem się przeglądarek internetowych pozwalających na dostęp do stron internetowych. Graficzny interfejs pozwalał na czytelne odkrywanie zasobów internetowych. W tym czasie (lata dziewięćdziesiąte dwudziestego wieku) władze państwowe pozwoliły na wykorzystanie z Internetu do celów biznesowych. Pierwszy bank, który umożliwił swoim klientom (dzięki Internetowi), wirtualny dostęp do rachunku to kalifornijski bank La Jolla, a było to w 1994 roku. Pierwszy na świecie, całkowicie internetowy bank powstał w 1995 roku, w Nowym Jorku w USA. Był to Security First Network Bank. Mając na uwadze bogacenie się społeczeństwa i rozwój światowego biznesu można stwierdzić, że od końca dwudziestego wieku, do czasów współczesnych bankowość elektroniczna wpłynęła korzystnie na przepływ kapitału, transfer technologiczny, wymianę towarową i handel międzynarodowy (Krzysztoszek, 2017, s. 6).

W procesie globalizacji oprócz handlu i technologii ważny jest też przepływ ludzi. Globalne przelewy internetowe i możliwość zakupu biletu lotniczego on-line zachęcają do podróżowania. Osoba z Europy podróżując po Azji może korzystać ze swojej karty płatniczej czy karty kredytowej. Analogicznie, podróżnik z kraju azjatyckiego, jeśli korzysta z powszechnie uznawanej karty kredytowej, może płacić za restauracje, hotele, przejazdy i wejścia do muzeów. Budowa biznesu na skale globalną jest łatwiejsza za pomocą bankowości internetowej (Borcuch, 2007, s. 10). Przesyłanie pieniędzy do centrali przedsiębiorstwa z oddziałów zagranicznych pozwala zminimalizować ryzyko perturbacji w prowadzeniu biznesu. W przypadku

zawirowań politycznych, wojen, epidemii, kataklizmów naturalnych w rodzaju powodzi, czy chociażby wybuchu wulkanu, można błyskawicznie przenieść środki pieniężne z zagrożonego obszaru do innego oddziału, lub kraju macierzystego korporacji. W razie potrzeby doinwestowania przedsiębiorstwa można uzyskać pomoc od innych firm, banków zagranicznych lub od centrali korporacyjnej, z zaznaczeniem, że wszystkie te podmioty mogą być fizycznie zlokalizowane poza granicami państwa, w którym znajduje się firma potrzebująca dodatkowych środków pieniężnych. W obszarze handlu istnienie bankowości elektronicznej działającej cała dobę jest wielkim ułatwieniem zarówno dla przedsiębiorstw jak i dla pojedynczych kupców czy klientów indywidualnych.

Szybkie rozpowszechnienie wirtualnego pieniądza w Polsce

Na polskim rynku bankowym 14 października 1998 roku Powszechny Bank Gospodarczy z siedzibą w Łodzi uruchomił pierwszy wirtualny oddział dla klientów indywidualnych i małych firm. W 1999 roku Powszechny Bank Gospodarczy został przejęty przez Bank Pekao. Dzięki temu przekształceniu pojawił się internetowy rachunek Eurokonto WWW. W tym samym roku, działalność w Internecie rozpoczęły dwa inne banki: Wielkopolski Bank Kredytowy i Bank Przemysłowo-Handlowy (Bank BPH). Sławomir Lachowski piastując stanowisko wiceprezesa Powszechnego Banku Gospodarczego w Łodzi (PBG S.A.), wprowadził w 2000 roku bankowość elektroniczną do użytku, udostępniając ją dla swoich klientów. W wyniku prac zespołu Sławomira Lachowskiego powstał mBank s.a. – pierwszy polski detaliczny bank internetowy. Wspomniany bank, zainicjował swoją działalność z dniem 26 listopada 2000 roku.

Przykład sukcesu rynkowego mBanku zapoczątkował lawinowy wzrost klientów bankowości internetowej. Na początku XXI wieku z e-bankowości w Polsce korzystało około 50 tysięcy użytkowników (Ustawa z 12 września 2002 r. o elektronicznych instrumentach płatniczych, Dz.U. Nr 169, poz. 1385 ze zm.). W następnych latach klienci wirtualnej bankowości przekroczyli liczbę pół miliona, zachowując tendencję wzrostową. MBank dzięki stałemu rozwojowi oraz podążaniu za duchem czasu a przede wszystkim, inwestowani w nowoczesne technologie, stał się trzecim bankiem internetowym w Europie i piątym na świecie. Bank PKO BP S.A. od 2002

roku przejął bank Inteligo, dzięki temu bankowość internetowa zaczęła być obecna w strukturach jednego z największych banków w Polsce. W 2007 roku, firma Apple przedstawiła swój sztandarowy projekt - smartfon iPhone. To urządzenie łączyło w sobie funkcje telefonu i przenośnego komputera. W rok później, bankowość internetowa stała się dostępna przy użyciu smartfonów dla klientów banku PKO BP który, jak wzmiankowano przejął aktywa banku Inteligo. W celu technicznego połączenia telefonów komórkowych z wirtualną bankowością zastosowano system Android stworzony przez amerykańskiego globalnego potentata Google (Gawrychowski, 2016, s. 105). W obecnych czasach, każdego dnia zarówno starsze, jak i młodsze pokolenie powszechnie posługuje się telefonami komórkowymi z dostępem do Internetu. Możliwość wysyłania przelewów przez całą dobę, za pomocą telefonu dodatkowo otwiera łatwą ścieżkę dla dokonywania zakupów, płacenia za bilety komunikacji miejskiej, wizyty w restauracjach, punktach usługowych (salony fryzjerskie, solaria), bez posiadania przy sobie fizycznej gotówki. Powyższy wachlarz możliwości zachęca do aktywności turystycznej, towarzyskiej i gospodarczej. Zwiększenie mobilności społecznej jest impulsem do tworzenia coraz nowocześniejszych technologii. Wyzwaniem nie jest obecnie poziom technologii, lecz poziom rozwoju technologicznego społeczeństwa, ponieważ zwiększona mobilność wywołuje mieszanie się ludzi pochodzących z odmiennych kręgów kulturowych różniących się religią, obyczajowością, zamożnością, tradycją, stosunkiem do kobiet i rodziny, językiem i planami na przyszłość.

Zagrożenia jakie niesie z sobą wirtualny pieniądz

Społeczeństwo można łatwo kontrolować poprzez śledzenie wirtualnych transakcji bankowych. Łatwość płatności internetowych wykonywanych za pomocą telefonów komórkowych jest wielką pokusą by ograniczyć transakcje gotówkowe. Wiele banków i rządów krajowych sprzyja i dąży do ograniczenia obiegu gotówkowego na rzecz zwiększenia roli bankowości internetowej. Wywiady mogą śledzić miejsce przebywania każdej osoby wykonującej płatności za pomocą telefonu komórkowego na całym świecie. Nawet najmniejsze zakupy paliwa na stacji benzynowej czy zakup chleba w sklepie osiedlowym zostaną zarejestrowane i zapisane w historii konta internetowego.

Każde zatrzymanie dostawy prądu elektrycznego może wywołać blokadę w handlu i ograniczenia w dostępie do swych wirtualnych kont bankowych przez miliony użytkowników. Awarie serwerowni mogą zniszczyć historie transakcji giełdowych i bankowych i zaburzyć handel w Internecie. Od lat siedemdziesiątych dwudziestego wieku zaczynają się pojawiać kradzieże pieniędzy z banku przy wykorzystaniu nowoczesnej techniki. W 1973 roku w Nowym Jorku, Dime Savings Bank stracił dwa miliony dolarów w związku kradzieżą jaka został przeprowadzona przy użyciu systemu teleinformatycznego. Od tej chwili przestępcy nie musieli przeprowadzać napadów na bank wedle starego wzoru, w myśl którego przestępcy wchodzą do budynku banku i poprzez włamanie lub zastraszenie obsługi przejmują gotówkę lub papiery wartościowe. Rozwój technologii zapoczątkował przestępstwa bankowe które nie wymagały obecności kryminalistów w siedzibie instytucji finansowej. Zwiększyło się bezpieczeństwo osobiste pracowników banku, podobnie zmniejszyło się ryzyko uszczerbku dla zdrowia wśród złodziei, gdyż wcześniej ochrona banku lub wezwany oddział Policji mógł podczas walki zranić lub zabić przestępców. Jednocześnie w związku z pojawieniem się nowych sposobów na kradzież pieniędzy, środki zgromadzone na rachunkach bankowych stały się bardziej zagrożone. Władze banków w odpowiedzi na powstanie nowych zagrożeń, wprowadziły nowe procedury bezpieczeństwa informatycznego, skupiając się na uszczelnieniu systemu dostępu do kont elektronicznych.

First National Bank of Chicago stracił siedemdziesiąt milionów dolarów w 1988 roku w wyniku działania zorganizowanej grupy kryminalistów działającej w cyber przestrzeni. Narzędziem przestępstwa nie był już pistolet ani łom lub wytrych. Przestępcy posłużyli się telefonem, za którego pomocą potwierdzili przelewy bankowe z rachunków paru spółek np. przedsiębiorstw lotniczych (United Airlines) i finansowych (Merrill Lynch). Autoryzowanie przelewów odbywało się przez połączenie telefoniczne. Złodzieje znając procedury bankowe za sprawą pracowników banku podszyli się pod osoby uprawnione do telefonicznego potwierdzania przelewów. Skradzione pieniądze odnalazły się na kontach Citibanku i Chase Manhattan Banku. Pieniądze zostały odnalezione, zanim zostały przesłane do Austrii. Następnym krokiem był pełnoprawny atak hackerski przeprowadzony przez organizację kierowana przez Władimira Lewina. W 1994 roku członkowie tej kryminalnej grupy włamali się do zasobów komputerowych Citibanku skąd

ukradli dane klientów wraz z hasłami do kont. Złodzieje ukradli łącznie 3,7 miliardów dolarów w ciągu kilku tygodni. Przejęte środki pieniężne trafiły na rachunki w bankach zlokalizowane w USA, Holandii, Finlandii, Izraelu i Niemczech. Władze Citibanku zawiadomiły o kradzieży FBI (Federalna Agencja Bezpieczeństwa).

W wyniku intensywnego śledztwa udało się aresztować członków szajki, kiedy przychodzili do banków celem wypłacania pieniędzy. Po serii ataków hackerskich instytucje finansowe i duże przedsiębiorstwa wzmocniły swoja ochronę cybernetyczną, co sprawiło, że przestępcy nie skupiają się na dużych instytucjach. Kluczem do powodzenia oszustwa w przestrzeni wirtualnej jest pozyskanie danych wrażliwych. Phishing to metoda kradzieży stosowana w cyberprzestrzeni, polegająca na pozyskaniu danych klientów banków poprzez podszywanie się pod osobę godną zaufania lub organizację. Wiadomości wysyłane rzekomo przez pracowników banków lub urzędy państwowe w rodzaju Zakładu Ubezpieczeń Społecznych lub Urzędu Skarbowego stanowią poważne zagrożenie. Posiadając login i hasło do konta bankowego przestępcy są w stanie wejść na konto ofiary a dodatkowo mając dostęp do jednorazowego hasła uwierzytelnianego są w stanie dokonywać przelewów i nawet zaciągać pożyczki (Bednarczyk, 2020, s. 6). Ważnym aspektem działalności cyberprzestępców jest współpraca z pracownikami banków, dzięki którym kryminaliści mogą dokładnie wybierając cel kradzieży typując osoby majętne, posiadające znaczne kwoty pieniędzy na kontach bankowych. Dodatkowy kryterium wyboru może być wiek potencjalnej ofiary. Osoby starsze zazwyczaj mają mniej biegłe w obsłudze nowoczesnych urządzeń technicznych, stając się bardziej podatnymi na zabiegi internetowych oszustów. Tworzenie wirusów komputerowych i złośliwego oprogramowania jest kolejnym sposobem na dokonanie kradzieży w Internecie.

Przejmując kontrolę nad kontem ofiary, hackerzy mogą dowolnie dysponować środkami pieniężnymi, zaciągać pożyczki i zmieniać hasła dostępowe. W przypadku kont przedsiębiorstw próba przejęcia konta może odbywać się za pomocą podawania się oszustów za wysoko postawionych przedstawicieli kontrahentów lub klientów. Zdarza się, że pracownik chcący zaradzić pojawiającemu się kłopotowi, w rzeczywistości wchodząc w rolę nieświadomego pomocnika złodziei, chcących poznać loginy i hasła firmowe by dokonać kradzieży. W przypadku osób chcących wykazywać się w pracy ponad przeciętną efektywnością, istnieje ryzyko zlekceważenia

zasad bezpieczeństwa i poufności danych na rzecz zwiększenia wydajności przedsiębiorstwa (Kubiak, Lizińska, 2025, s. 5). Chęć otrzymania awansu i podwyżki jest bardzo kuszącą perspektywą, by nie stanowiła szansy na osiągniecie powodzenia w oszustwach internetowych, co skrzętnie wykorzystują hackerzy atakując banki i przedsiębiorstwa (Szelągowska, Iwanicz-Drozdowska, Zawadzka, Jaworski, 2017, s 104).

Pełna transparentność operacji bankowych poprzez zapis każdego przelewu, wszystkich zakupów, nawet takich opiewających na niskie kwoty i dotyczące trywialnych spraw w rodzaju kupna chleba, gazety czy paliwa na stacji benzynowej czyni z bankowości wirtualnej sprawne narzędzie wywiadowcze. Rządy państw i właściciele banków mogą dokładnie prześledzić powiązania zawodowe i towarzyskie, trasę podróży, ulubione miejsca i preferencje zakupowe każdego człowieka korzystającego z bankowości wirtualnej. Sprawny profiler, śledczy czy wywiadowca analizując bilingi rachunku bankowego jest w stanie poznać wiele szczegółów z życia danej osoby. Oczywistym i obrazowym przykładem jest posłużenie się kryterium zakupu alkoholu w sklepach i lokalach gastronomicznych.

W celu osiągniecia powodzenia w akcji szpiegowskiej lub działaniu terrorystycznym ważne jest wybranie informatora lub współpracownika. Osoby często kupujące alkohol z dużą dozą prawdopodobieństwa wykazują się ponad przeciętną towarzyskością lub cierpią na chorobę alkoholową, pozostając pod wpływem nałogu. Pozyskanie takiego człowieka do własnych celów jest dużo łatwiejszym zadaniem dla wywiadu wrogiego państwa czy grupy terrorystycznej niż w przypadku człowieka zdrowego posiadającego silniejsze mechanizmy samokontroli własnego zachowania. Skrupulatne śledzenie wydatków obserwowanej osoby może przynieść wiele innych cennych wywiadowczo spostrzeżeń. Wydatki na restauracje, drogie hotele, biżuterię, spa, salony masażu, wycieczki zagraniczne mogą sugerować istnienie romansu w jakim znajduje się obserwowana postać. Jeśli dodatkowo jest to nieformalny związek, współistniejący z oficjalnym stadłem małżeńskim lub inną stałą relacją to dana informacją jest wysoko uplasowana na drabinie możliwego szantażu.

Kolejnym faktem mogącym wyniknąć z właściwej segregacji przelewów i wpłat oraz płatności jest przyjmowanie korzyści majątkowych będących przekupstwem lub wręcz dokonywanie samodzielnie kradzieży. Jeżeli wydatki nie odpowiadają osiąganym poborom w zestawieniu miesięcznym

lub rocznym, jest to ważna wskazówka dla zbadania prawdziwych źródeł środków finansowych obserwowanego człowieka. W ujęciu rocznym przy dodatkowych danych przeczących otrzymaniu podwyżki lub spadku przez obserwowaną postać lub osobę z jej najbliższego kręgu rodzinno- towarzyskiego nagłe zwiększenie wydatków powinno obudzić uzasadnione podejrzenie. Samo wzięcie kredytu i pozostawanie zadłużonym przez dłuższy czas bez wyraźnych powodów może prowadzić do uznania danego człowieka za utracjusza lubiącego rekompensować własne braki lub porażki życiem ponad własny stan majątkowy. Często dla pozyskania wpływu na ustosunkowanego człowieka będącego pracownikiem służb mundurowych, wymiaru sprawiedliwości, instytucji finansowych, firmy energetycznej czy ważnego urzędu wystarczy sama groźba ujawnienia wstydliwych szczegółów życiorysu, wykrytych poprzez sprawdzenie transakcji bankowych wykonanych w systemie informatycznych, tworzących świat wirtualnego pieniądza. Ukrywany nałóg czy choroba mogą być wykryte poprzez odczytanie przelewu skierowanego do ośrodka leczenia uzależnień lub prywatnej kliniki. Dla ludzi piastujących ważne stanowiska w prywatnych przedsiębiorstwach lub administracji rządowej ochrona własnego dobrego imienia może być cenniejsza od wierności krajowi czy lojalności korporacji (Kubik, 2024). Ujawnienie zdrady małżeńskiej lub kradzieży środków publicznych czy należących do przedsiębiorstwa załamało by karierę wielu wpływowych ludzi. Nawet jeśli nie ponieśliby konsekwencji karnych to zła sława jak otoczyłaby ich osoby w przestrzeni publicznej spowodował a by konieczność ustąpienia ze stanowiska za sprawą zakulisowych nacisków przełożonych zaniepokojonych szarganiem dobrego imienia instytucji. Obawa przed społecznym linczem w przypadku celowego przecieku hańbiących wiadomości do mediów, może stanowić decydujący czynnik stanowiący przyczynę, dla której wiele ważnych urzędów państwowych i międzynarodowych instytucji (Kunica, 2025) i przedsiębiorstw jest ciągle infiltrowana przez wrogie wywiady innych państw i grupy terrorystyczne. Jeśli przestępcy, szpiedzy obcych państw, terroryści wejdą w posiadanie danych bankowych mogą mieć dostęp do wiedzy zarezerwowanej dla służb państwowych. W celu przeciwdziałania przestępczości zorganizowanej i globalnemu terroryzmowi wszelkie przelewy środków pieniężnych powyżej kwoty piętnastu tysięcy euro są rejestrowane przez polski sektor bankowy z jednoczesnym powiadamianiu służb skarbowych i Policji oraz służb wywiadowczych (Czowalla, 2025).

Świat przestępczy nieustannie poszukuje nowych dróg obejścia prawa i działalności poza oficjalnymi normami. Tak zależność występuje również w przypadku systemu bankowego obracającego wirtualnymi pieniędzmi. W sytuacji, kiedy nie przestępcy nie mogą korzystać z oficjalnego systemu bankowego, pozostają im do dyspozycji alternatywne systemy obrotu pieniężnego. Przykładem takiego nieformalnego układu finansowego jest arabski system hawala, będący skupiskiem „niewidzialnych banków" (Nadolny, 2021). W powyższym systemie w jednym miejscu na świecie człowiek przekazuje gotówkę pośrednikowi, który to pośrednik za pomocą wiadomości e mail, rozmowy telefonicznej, wpisu na portalu społecznościowym lub komunikatorze internetowym zleca wypłatę środków w innym, niejednokrotnie odległym miejscu na świecie. Wypłata pieniędzy odbywa się za pomocą hasła. Nie ma potrzeby podawania imienia i nazwiska żadnej ze stron transakcji. Bez podpisywania przelewów nie można zidentyfikowania ilości przekazywanych kwot, podobnie jak nadawców i odbiorców pieniędzy. Przelew nie jest rejestrowany w żadnym systemie bankowym, nie podlega nadzorowi urzędów skarbowych, jest wolny od opodatkowania i nie podlega nadzorowi służb państwowych. Wszystkie powyższe cechy sprawiają, że z hawali korzystają organizacje przestępcze i terrorystyczne. Ten nieformalny system bankowy jest bardzo popularny w Indiach, Pakistanie i Afganistanie. W krajach, w których nie ma rozwiniętego rynku bankowego Somalia, Jemen z uwagi na niski poziom gospodarczy i długotrwałe wojny domowe i zewnętrzne hawala jest podstawą wirtualnego obiegu pieniężnego. W Ameryce Północnej i Europie ten alternatywny system został wprowadzony przez przybyszy z obszarów Azji stanowiących emigrację zarobkową i socjalną. System hawala stanowi platformę finansową z której korzystają często przestępcy i terroryści. We Wrocławiu w 2020 roku zatrzymano dwóch obywateli Iraku podejrzewanych o finansowanie bojowników Państwa Islamskiego działających na terenie Iraku i Syrii. Finansowanie odbywało się przy pomocy nieoficjalnego systemu hawala (Żaryn, 2020).

Niestosowanie się przybyszy z Afryki lub Azji (głownie Bliski Wschód, Indie, Pakistan) do standardów zachowania przyjętych w Europie lub Ameryce Północnej jest powszechnie znanym zjawiskiem. Powyższe alternatywne systemy finansowe w rodzaju hawali doskonale odzwierciedlają znaczne różnice kulturowe wśród przybyszy z globalnego południa. Osoby nie przyjmujące zwyczajów panujących w krajach rozwiniętych,

opierają się procesom integracji oraz pozostają przy własnych obyczajach często wchodząc w konflikt z miejscowymi władzami i miejscową społecznością (Warzecha, 2024).

Przyszłość wirtualnego pieniądza

Ważnym aspektem wirtualnego pieniądza jest świat gier komputerowych, które w związku z rozwojem technologii w coraz doskonalszy sposób imitują prawdziwą rzeczywistość tworząc atrakcyjne, cyfrowe, alternatywne światy równoległe. W społeczności graczy komputerowych podłączonych do całodobowej sieci internetowej waluta jest informacja, znakomicie utworzona fikcyjna postać czy budynek. Wiele osób szczególnie w społeczeństwach krajów rozwiniętych i zamożnych w USA, Europie, Japonii czy Singapurze przykłada dużą wagę do spędzania wolnego czasu w wirtualnej przestrzeni. Przepracowanie, brak więzi rodzinnych, ograniczenie relacji towarzyskich, braki wystarczającego czasu wolnego sprzyjają ucieczkom ludzi do świata wirtualnego. W społeczności graczy, twórców internetowych zamieszczających wpisy i filmy na platformach streamingowych, portalach społecznościowych i medialnych odpowiednikiem pieniądza będzie ciekawa informacja pozwalająca zwiększyć zasięgi oglądalności a tym samym zwielokrotnić zyski poprzez wzmożone zainteresowanie reklamodawców. Wiele osób jest bardzo mocno pochłoniętych przez wirtualną rzeczywistość, dlatego są gotowi na zapłatę, często wysokich kwot za dostęp do platform graczy, rozmaite benefity i rozszerzenie możliwości korzystania z wirtualnej rzeczywistości (Solarz, 2008).

W Indiach wiele gospodarstw domowych korzysta ze złota jako trwałego środka płatniczego, służącego jako zabezpieczenie rodziny poprzez oszczędności w danym metalu szlachetnym. W tradycji Indii posag kobiety wychodzącej za mąż jest wypłacany w złotych przedmiotach (np. biżuterii), ma to wpływ na duże, niesłabnące zapotrzebowanie na posiadanie fizycznego złota przez Hindusów. 8 listopada 2016 roku rząd Indii pod przewodnictwem premiera Narendra Modiego ogłosił wycofanie z obiegu banknotów o nominałach 500 i 1000 rupii, przy jednoczesnym terminie zwrotu wyżej wymienionych banknotów do końca grudnia 2016 roku. Jeśli obywatel Indii zwrócił w banku kwotę większą niż 250 000 rupii (około równowartości 15 tys. złotych w nieaktualnych banknotach wtedy grozi sankcja karna ze

strony urzędu skarbowego w postaci podatku wynoszącego 200% domiaru od hipotetycznie, niezapłaconych podatków. Banknoty, kttóre straciły ważność można było wymienić na nowe jednak w tym przypadku najwyższa kwota wymiany wynosiła 4500 rupii, po uprzednim okazaniu dowodu tożsamości. Podobną reformę walutową przeprowadziły komunistyczne władze w PRL w 1950 kradnąc oszczędności Polaków. Zakazano wtedy posiadania obcych walut, złota i platyny. Wprowadzono denominację według przelicznika 100:1 w przypadku gotówki. Depozyty bankowe, ceny i płace zdenominowano w proporcji 100:3. Wprowadzone zmiany dotknęły przede wszystkim przedsiębiorców i rolników indywidualnych.

Zagrożenie denominacją i niepewność co do polityki monetarnej rządu skłania wielu ludzi do szukania alternatywnych sposobów oszczędzania. Moim zdaniem w następnych latach i dziesięcioleciach złoto, opierając się na wcześniej przytoczonym przykładzie Indii będzie w dalszym ciągu jednym z ważniejszych zamienników pieniądza, również tego wirtualnego. Mając w pamięci denominacje i wymianę banknotów przez banki centralne można mieć uzasadnione obawy o dostępność pieniędzy ulokowanych na kontach internetowych. Podczas światowego kryzysu gospodarczego w 2008 roku wielu klientów banków nie mogło wypłacić pieniędzy z bankomatu lub w oddziale banku ani dokonać przelewu wirtualnego, choć mieli zgromadzone środki na swych wirtualnych rachunkach. Takie ograniczenie dotknęło między innymi klientów banku Icesave (Wypijewska, Kuk, 2008). Wprawdzie obywatele Islandii otrzymali pieniądze od rządu w Reykjaviku, lecz już zagraniczni klienci upadłego, islandzkiego banku pochodzący głównie z Wielkiej Brytanii i Holandii nie mogli liczyć na podobną pomoc. Wedle orzeczenia trybunału Europejskiego Stowarzyszenia Wolnego Handlu (EFTA) rząd islandzki mógł wypłacić pieniądze jedynie własnym obywatelom jacy ucierpieli w wyniku upadku islandzkich banków. Banki stały się niewypłacalne i ogłosiły bankructwo, które przyczyniło się do nacjonalizacji wielu instytucji finansowych. Upadły trzy największe banki Kaupthing, Landsbanki i Glitnir. Wielu ludzi traciło oszczędności przez denominację, zwiększyło się bezrobocie.

Kryzys finansowy był jedną z przyczyn braku zaufania do pieniądza i przeniesienie uwagi inwestorów na nieruchomości. W latach 2015-2027 ceny nieruchomości na Islandii wzrosły o ponad 30%. Wprowadzono bardziej restrykcyjne zasady przyznawania pożyczek, gdyż wielu klientów

banku nie było w stanie spłacić swych zobowiązań kredytowych. Te wydarzenia podważyły zaufanie do banków i do długotrwałej wartości pieniądza, również tego wirtualnego. Uważam, że w przyszłości klienci dalej będą skłonni zakupić nieruchomość jako lokatę kapitału pamiętając o kryzysach finansowych jakie uniemożliwiały podjęcie pieniędzy z wirtualnych kont. W obecnej dobie rozwoju technologii, zwiększenia mobilności i przepływów kapitału można zakupić ziemię, domy lub mieszkania w odległych krajach takich jak Hiszpania (Hass, 2024) .

Kryptowaluty pojawiły się w obiegu w niedawnym czasie, lecz wywarły znaczący wpływ na światowy rynek finansowy, stając się jednym z najlepiej rozpoznawalnych wirtualnych wartości pieniężnych. 3 stycznia 2009 roku powstał blok Genesis zapoczątkowując powstanie kryptowaluty Bitcoin. Kryzys finansowy z 2008 roku objawiający się między innymi upadkiem banków, inflacja i denominacją oraz utratą dostępu do pieniędzy ulokowanych na wirtualnych kontach spowodował powstanie powszechnego zapotrzebowania na nową walutę, dostępną na całym świecie, a przy tym odporną na zawirowania polityczne i gospodarcze (Piotrowska, 2018). Za twórcę całego projektu uważa się anonimowa postać Satoshi Nakamoto, która równie dobrze może być całym zespołem ukrywającym swoje tożsamości pod zbiorczym pseudonimem. W celu pozyskania Bitcoina czyli inaczej wirtualnej monety należy dokonać na komputerze skomplikowanych obliczeń matematycznych, aby potwierdzić transakcję. Następnie transakcja jest oznaczana na liście dotychczasowych obrotów kryptowalutą nazywaną łańcuchem bloków (blockchain). Pierwszy zakup przy pomocy Bitcoina został przeprowadzony 22 maja 2010 roku. W tamtych czasach jeden Bitcoin kosztował około 20 dolaróww, obecnie jeden Bitcoin ma wartość 380 tysięcy złotych (Misztal, 2023). Bitcoin z racji braku nadzoru ze strony banków centralnych i urzędów może być wykorzystywany do płatności w świecie przestępczym. Wszelkie nielegalne towary w rodzaju narkotyków, broni, ukradzionych dzieł sztuki mogą być kupowane za pośrednictwem kryptowalut. Ponadto opłacanie dokonanych przestępstw lub aktów terrorystycznych, również może być dokonywane dzięki kryptowalutom. W tym przypadku unikanie podatków jest tylko jednym z wykroczeń przeciwko prawu. Kradzieże, sabotaż, zamachy terrorystyczne zabójstwa, przemyt to tylko jedne z wielu przestępstw jakie mogą być zlecane i opłacane przez Bitcoina lub inne podobne, alternatywne środki płatnicze (Opitek, Butor-Keller, Kanclerz,

2022). Nawet polska prokuratura zgadza się przyjąć poręczenie majątkowe w Bitcoinach (Rycerski, 2025).

Sposoby na ograniczenie strat w przypadku zatrzymania dostępu do wirtualnego pieniądza

W przypadku braku dostępu do wirtualnego pieniądza może dojść do wielu przestępstw i zaburzeń w funkcjonowaniu społeczeństw. W chwili braku dostępu do wirtualnych przelewów może dość do próby oszustw i spekulacji obliczonych na osiągnięcie znacznych zysków poprzez pośrednictwo w wymianie towarowej (np. poprzez listy zastawne w oparciu o trwałe wartości w rodzaju paliw, drewna, żywności, ziemi, złota itp.).

Przeciwdziałanie spekulacji i oszustwom artykułów pierwszej potrzeby (żywność, leki, paliwo) może odbywać się poprzez korzystanie z rządowych rezerw materiałowych i zastosowanie zakupów kredytowych w odniesieniu do hurtowni, sklepów wielkopowierzchniowych i stacji paliw. W chwili, kiedy nie można dokonywać płatności kartami kredytowymi i dokonywać przelewów internetowych artykuły pierwszej potrzeby powinny być zapewniane przez koordynowaną akcję rządową przy pomocy Wojska Polskiego, Policji i Wojsk Obrony Terytorialnej. Mając na uwadze napięcia społeczne, ryzyko wystąpienia paniki i wzmożenie przestępczości należy wprowadzić zwiększone środki bezpieczeństwa w postaci ochrony sklepów (zwłaszcza wielkopowierzchniowych), banków i punktów wydawania żywności i leków. Największa firma paliwowa w Polsce to Orlen S.A., jest zarządzana przez polski rząd, co jest szczególnie ważne w sytuacjach kryzysowych. Państwo poprzez swoje agendy (NBP, Bank PKO) powinno ułatwić pozyskiwanie gotówki przez obywateli w przypadku awarii systemów bankowości internetowej.

Na wypadek ataku hackerskiego w wyniku, którego klienci banków tracą swoje oszczędności, powinien zadziałać mechanizm Bankowego Funduszu Gwarancyjnego zabezpieczającego depozyty bankowe. Równie istotne są mechanizmy wyśledzenia ukradzionych pieniędzy jakie zostały wysłane z kont klientów do innych banków, często znajdujących się za granicą. Jeśli pieniądze zostały przelane przez hackerów do banków umiejscowionych w krajach, które honorują praworządność i są otwarte na współpracę z organami ścigania (policją, prokuraturą) i władzami banku, który stał się celem

kradzieży. Jeśli działania śledcze zostaną przeprowadzone szybko i sprawnie oraz spotkają się z pomocą zagranicznych banków i wymiaru sprawiedliwości krajów, gdzie złodzieje przelali zagrabione pieniądze jest duża nadzieja na odzyskanie strat. Szybkie działanie sądów sprawia, że środki pieniężne co do których zachodzi uzasadnione podejrzenie, iż pochodzą z przestępstwa zostaną zablokowane. Następnym krokiem jest przeprowadzenie śledztwa w wyniku, którego zostaje wydany wyrok nakładający na bank, do którego trafiły ukradzione pieniądze obowiązek dokonania przelewu zwrotnego. Ważne jest szczegółowe doprecyzowanie z jakiego banku hackerzy ukradli pieniądze by środki zostały przelane na właściwe konta, jeśli mamy do czynienia z wieloma bankami jakie stanowiły stacje pośrednie w zatarciu śladów przestępstwa. Oprócz szybkości działania kluczem do odzyskania pieniędzy skradzionych przez atak hackerski jest umiejętność pracowników banku, którzy są biegli w poruszaniu się w wirtualnym świecie. Mamy tu do czynienia z dwiema stronami konfliktu: hackerami dokonującymi kradzieży oraz informatykami zatrudnionymi przez banki i policję.

Podsumowanie

Wirtualny pieniądz niesie ze sobą zarówno nowe możliwości i zagrożenia. Oprócz łatwości dokonywania zakupów, prowadzenia przedsiębiorstw i podróżowania wirtualny pieniądz wpisuje się w nowoczesny świat przesiąknięty nowymi technologiami. Kontekst społeczny łączy się tutaj z rozwojem technologii. Telefony komórkowe są powszechnie użytkowane przez wszystkie grupy społeczne, a złożoność nowoczesnych telefonów pozwala dokonywać zakupów i przelewów przez całą dobę.

Ataki hackerskie na pieniądze zgromadzone na wirtualnych kontach istnieją od chwili powstania wirtualnej bankowości. W odpowiedzi na zagrożenie przestępstwami internetowymi banki zaczęły wzmacniać zabezpieczenia swych systemów internetowych. Mając na uwadze bezpieczeństwo depozytów bankowych, klienci indywidualni zostali wyposażeni w dodatkowe progi dostępowe, obejmujące zarówno hasła dostępowe jak i dodatkowe hasła wysyłane za pomocą wiadomości SMS. Polska jest w awangardzie wirtualnej bankowości, gdyż zarówno polskie banki jak ich klienci, działaj sprawnie w przestrzeniach Internetu. Pomimo zagrożeń jakie są stale obecnie w przestrzeni internetowej, bankowość wirtualna ciągle się rozwija,

zyskując nowych klientów. Od chwili powstania wirtualnej bankowości zwiększają się zastępy jej użytkowników.

Należy zaznaczyć, że istnieją też alternatywne instrumenty finansowe działające w wirtualnym świecie. Bitcoin i inne kryptowaluty stały się odpowiedzią na potrzebę anonimowości w wirtualnych finansach bez nadzoru państwa i ingerencji władz banków. Pomimo ryzyka niespodziewanej zmiany wartości i oszustw istnieje społeczność mająca zaufanie do kryptowalut. Dokonywanie nielegalnych zakupów i użytkowanie danych instrumentów finansowych przez świat przestępczy to ciemna strona kryptowalut. Alternatywna bankowość w postaci systemu Hawala często służy finansowaniu terroryzmu i unikaniu opodatkowania. Dany system Hawala, podobnie jak kryptowaluty nie podlega nadzorowi urzędów państwowych i banków. Pomimo rozwoju wirtualnego pieniądza, wiele osób na całym świecie wybiera tradycyjne formy oszczędzania. Niesłabnąca popularność złota sprawia, że stare sposoby zachowania swego majątku nie tracą na znaczeniu, pomimo gwałtownego rozwoju cywilizacyjnego. W celu ochrony wirtualnego pieniądza banki wprowadzają szereg zabezpieczeń informatycznych, aby uniemożliwić lub zminimalizować próby kradzieży środków pieniężnych poprzez ataki hackerów.

Władze państwowe są zobowiązane w jak największym stopniu chronić swoich obywateli przed cyberprzestępczością. W razie kryzysu bankowości elektronicznej i ograniczonego dostępu do wirtualnych pieniędzy w wyniku awarii technologicznej, zorganizowanej akcji hackerskiej władze państwowe muszą być gotowe do zapewnienia ładu społecznego i ciągłości zaopatrzenia ludności w artykuły pierwszej potrzeby jak leki, paliwo i żywność oraz szybkiego dostępu do gotówki. Szybkie działania podjęte po ataku hackerskim pozwalają na odzyskanie skradzionych pieniędzy z wirtualnych kont bankowych.

Literatura

1. Aleksandrowicz, T. (2016). *Podstawy walki informacyjnej*. Warszawa: CeDeWu.

2. Harrison, M. (2022). *Niemcy zapłaciły ostatnią ratę odszkodowań za I wojnę światową po 92 latach.* Pobrano z: https://www.bankier.pl/wiadomosc/Niemcy-zaplacily-ostatnia-rate-odszkodowan-za-I-wojne-swiatowa-po-92-latach-8386364.html (dostęp: 20.03.2026).
3. Bednarczyk, P. (2020). Bankowość Internetowa w Polsce. *Zeszyty Naukowe Wydziału Ekonomii i Finansów Uniwersytetu Technologiczno-Humanistycznego im. Kazimierza Pułaskiego w Radomiu Studia Ekonomiczne, Prawne i Administracyjne.* Rocznik *2020* (Zeszyt 2), 6-20.
4. Borcuch, A. (2007). *Pieniądz elektroniczny – Pieniądz przyszłości - analiza ekonomiczno-prawna*. Warszawa: CeDeWu.
5. Kunica, M. (2025). *Korupcja w Parlamencie Europejskim. Osiem osób oskarżonych.* Pobrano z: https://businessinsider.com.pl/wiadomosci/korupcja-w-parlamencie-europejskim-huawei-pod-lupa-sledczych/5hyywp2 (dostęp: 20.03.2026).
6. Czowalla, A. (2025). *Od tej kwoty bank powiadomi skarbówkę. Sumują przelewy.* Pobrano z: https://biznes.interia.pl/finanse/news-od-tej-kwoty-bank-powiadomi-skarbowke-sumuja-przelewy,nId,7910612 (dostęp: 20.03.2026).
7. Dylewski, A. (2011). *Historia Pieniądza na Ziemiach Polskich*. Warszawa: Carta Blanca.
8. Gawrychowski, M. (2026). *Banki w sieci*. Pobrano z: https://mowiawieki.pl/templates/site_pic/files/Pewne_jak_w_banku_Historia_zabezpieczen_bankowych_odcinek_8(sierpien_2016).pdf (dostęp: 20.03.2026).
9. Hass, W. (2024). *Coraz chętniej kupujemy domy w Hiszpanii. Padł rekord udziału Polaków w hiszpańskim rynku nieruchomości*. Pobrano z: https://strefainwestorow.pl/artykuly/nieruchomosci/20240904/polacy-hiszpanski-rynek-nieruchomosci-2q24 (dostęp: 20.03.2026).
10. Krzysztoszek, M. (2017). *Bankowość elektroniczna w teorii i praktyce.* Pobrano z: https://www.knf.gov.pl/knf/pl/komponenty/img/Bankow%C5%9B%C4%87%20elektroniczna%20w%20teorii%20i%20praktyce_60154.%20Materia%C5%82y%20dla%20%C5%9Brodowiska%20szkolnego_60154.pdf (dostęp: 20.03.2026).
11. Kubiak, J., Lizińska, J. (2025). *Finanse Przedsiębiorstw*. Warszawa: CeDeWu.

12. Kubik, W. (2024). *Tomasz Szmydt nie planował ucieczki? Sensacyjne doniesienia z Białorusi*. Pobrano z: https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9508675,tomasz-szmydt-nie-planowal-ucieczki-sensacyjne-doniesienia-z-bialorus.html (dostęp: 20.03.2026).
13. Misztal, J. (2023). *14 lat minęło jak jeden dzień. Bitcoin świętuje urodziny*. Pobrano z: https://www.bankier.pl/wiadomosc/Bitcoin-ma-14-lat-8466320.html.
14. Nadolny, D. (2021). *Akt oskarżenia za finansowanie działalności tzw. „państwa islamskiego"*. Pobrano z: https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-za-finansowanie-dzialalnosci-tzw-panstwa-islamskiego (dostęp: 20.03.2026).
15. Opitek, P., Butor-Keller, A., Kanclerz, K. (2022). *Terroryzm, studia, analizy, prewencja.* Pobrano z: https://www.abw.gov.pl/ftp/foto/Wydawnictwo/terroryzm/nr4/8_-_artykul8_-_artykul_-_P__Opitek_i_inni.pdf(dostęp: 20.03.2026).
16. Piotrowska, A. I. (2018). *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*. Warszawa: CeDuWu.
17. Rycerski, A. (2025). *Sprawa Red is Bad i poręczenie majątkowe w formie bitcoina. Czy to dopuszczalne?*. Pobrano z: https://www.rp.pl/opinie-prawne/art41841381-adrian-rycerski-poreczenie-w-formie-bitcoina-prokuratura-moze-miec-problem (dostęp: 20.03.2026).
18. Solarz, M. (2008). *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2004-2007*. Pobrano z: https://stat.gov.pl/banki-i-bazy-danych (dostęp: 20.03.2026).
19. Szelągowska, A., Iwanicz-Drozdowska, M., Zawadzka, Z., Jaworski, W. L. (2017). *Bankowość. Instytucje, operacje, zarządzanie*. Warszawa: Poltext.
20. Ustawa z 12 września 2002 r. o elektronicznych instrumentach płatniczych, Dz.U. nr 169, poz. 1385 ze zm.
21. Warzecha, Ł. (2024). *Europoseł PO sprawdził przestępczość wśród imigrantów. I wyraził zaskoczenie*. Pobrano z: https://www.salon24.pl/newsroom/1369095,europosel-po-sprawdzil-przestepczosc-wsrod-imigrantow-i-wyrazil-ogromne-zaskoczenie (dostęp: 20.03.2026).
22. Wypijewska, M., Kuk, M. (2008). *Islandia kolejną ofiarą kryzysu*. Pobrano z: https://www.rp.pl/banki/art16001161-islandia-kolejna-ofiara-kryzysu (dostęp: 20.03.2026).

23. Żaryn, S. (2020). *Zatrzymani przez ABW obywatele Iraku oskarżeni o finansowanie ISIS.* Pobrano z: https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/zatrzymani-przez-abw-obywatele-iraku-oskarzeni-o-finansowanie-isis (dostęp: 20.03.2026).