9

TRANSAKCJE OSZUKAŃCZE DOKONYWANE PRZY UŻYCIU BEZGOTÓWKOWYCH INSTRUMENTÓW PŁATNICZYCH JAKO PRZYKŁAD CYBERPRZESTĘPCZOŚCI

Kamila Tomczyk

Politechnika Częstochowska
Wydział Zarządzania

Wprowadzenie

Ze względu na dynamiczny rozwój technologii informatycznych i bankowości internetowej stale rośnie znaczenie bezpiecznej transmisji i przetwarzania danych. Wraz z rozwojem techniki wymiany informacji przez Internet powstało wiele udogodnień dla klientów i użytkowników usług informatycznych. Z drugiej strony proces udostępniania informacji za pośrednictwem Internetu w postaci bankowości elektronicznej generuje wiele zagrożeń związanych z cyberprzestępczością, przechwyceniem informacji poufnych, kradzieżą danych i malwersacjami finansowymi w systemach bankowości online. Nowe rodzaje cyberprzestępczości atakują oprogramowania ransomware (oprogramowanie blokujące dostęp do komputera czy danych i wyłudzające okup) i botnety na dużą skalę kradzież danych osobowych.

Przyjęta metodologia badawcza polegała na dokonaniu analizy danych statystycznych udostępnionych przez Bank Spółdzielczy pod kątem ustalenia liczby operacji oszukańczych dokonanych kartami płatniczymi. Badania koncentrowały się głównie na okresie czasu pandemii wywołanej wirusem SARS-CoV-2 od stycznia 2019 roku do grudnia 2021 roku, kiedy bank wprowadził nowe rozwiązania dla klientów: aplikację mobilną, a pod koniec 2021 roku wdrożył usługę BLIK, która cieszy się popularnością zarówno wśród użytkowników indywidualnych, jak i instytucjonalnych.

Rozdział ma na celu wskazanie na jedno z kluczowych wyzwań, jakim jest funkcjonowanie sektora bankowego w sytuacji rosnących przypadków transakcji

oszukańczych. W pierwszej kolejności scharakteryzowano bankowość elektroniczną oraz pojęcie fraudów, a następnie przytoczono kilka przykładów ataków na systemy bankowe. Dokonano analizy transakcji oszukańczych na przykładzie Banku Spółdzielczego.

Charakterystyka bankowości elektronicznej

Bankowość elektroniczna to „forma usług świadczonych przez banki na rzecz klientów, polegająca na umożliwieniu dostępu do rachunku bankowego na odległość za pomocą urządzeń do elektronicznego przetwarzania danych, takich jak komputer, telefon, tablet, bankomat, terminal, odbiorniki telewizji cyfrowej" (Górnisiewicz, Obczyński, Pstruś 2014, s. 30). Podziałem, jakiego można dokonać w obszarze bankowości elektronicznej, jest klasyfikacja ze względu na przyjęte kanały komunikacji (dystrybucji). W bankowości elektronicznej wyróżniamy trzy podstawowe rodzaje usług (Kwaśniewski i in. 2010, s. 6):

- bankowość terminalową,
- bankowość internetową,
- bankowość telefoniczną.

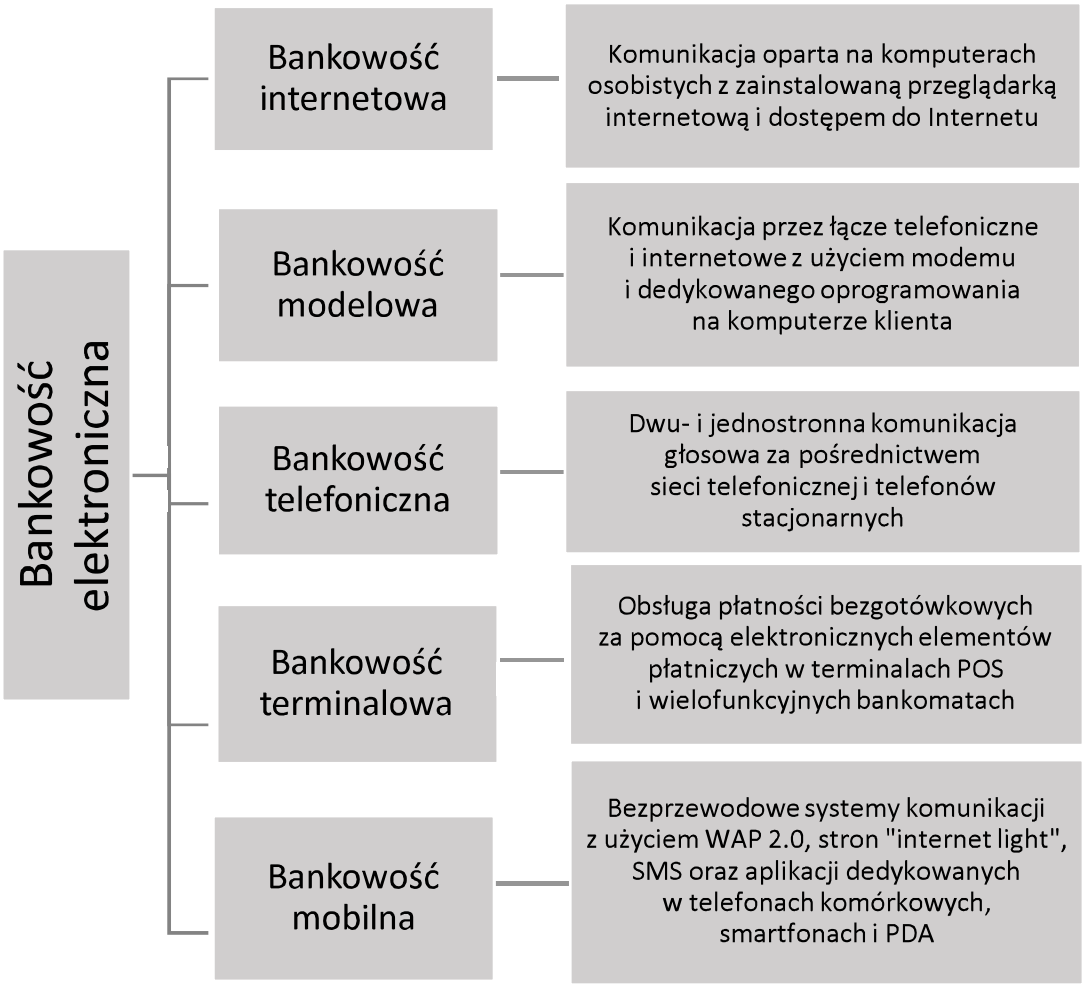
Różnorodność definicji bankowości elektronicznej w literaturze przedmiotu wynikać może z odmiennego spojrzenia na jej istotę i różnych celów, którym określone definicje mają służyć (*tabela 9.1*). Indywidualne doświadczenia autorów mogą mieć wpływ na sposób definiowania bankowości elektronicznej.

Tabela 9.1. Wybrane definicje bankowości elektronicznej

Autor definicji	Definicja bankowości elektronicznej
J.H. Górka	Całościowa koncepcja zakładająca wykorzystywanie w praktyce operacyjnej systemów informatyczno-komunikacyjnych do usprawniania i przyspieszenia realizacji zleceń klientów banków, co prowadzi do przyspieszenia obiegu pieniądza bezgotówkowego.
B. Kosiński	Wszelkie oparte na zastosowaniu elektronicznych urządzeń telekomunikacyjnych świadczenie usług bankowych na odległość, które pozwala klientowi na korzystanie z tych usług w siedzibie banku lub w miejscu zamieszkania.
G. Kotliński	Całościowa koncepcja zakładająca wykorzystywanie w praktyce operacyjnej systemów informatyczno-komunikacyjnych do usprawniania i przyspieszania realizacji zleceń klientów banków, co prowadzi do przyspieszenia obiegu pieniądza bezgotówkowego.
J. Grzywacz	Różnorodne procesy umożliwiane przez nowoczesną technologię i dotyczące tradycyjnej działalności operacyjnej banków oraz innych czynności (np. realizowania strategii marketingowej, zabezpieczania informacji), a zarazem zdalne korzystanie z usług bankowych za pomocą łączy telekomunikacyjnych oraz urządzeń informatycznych.

Źródło: Opracowanie własne na podstawie (https://9lib.org/article/…)

Podział bankowości elektronicznej w zależności od kanałów dystrybucji w sposób graficzny zaprezentowano na *rysunku 9.1*.



Rysunek 9.1. Klasyfikacja tradycyjna bankowości elektronicznej według kanałów dystrybucji i komunikacji

Źródło: (Borcuch 2016, s. 58)

Bankowość internetowa – obecnie jedna z najpopularniejszych form bankowości elektronicznej. Pozwala na dokonywanie operacji bankowych przez Internet. Bankowość internetowa jako instrument bankowości elektronicznej jest alternatywnym w stosunku do placówki oddziału bankowego kanałem dystrybucji, wykorzystującym sieć do świadczenia usług bankowych (Chmielarz 2005, s. 22).

Bankowość telefoniczna – usługi bankowe dostępne za pomocą telefonu komórkowego lub stacjonarnego. Bankowość telefoniczna jest jedną z pierwszych zautomatyzowanych usług oferowanych klientom banków (Świecka 2004, s. 18). Obecnie bankowość telefoniczna jest kojarzona jako rozmowa z konsultantem. Po stronie banku ten rodzaj komunikacji jest realizowany zazwyczaj w ramach automatycznej telefonicznej obsługi klienta (*call center*) wyposażonej w system telekomunikacyjny IVR (*Interactive Voice Response*).

Bankowość terminalowa – najstarsza i najbardziej powszechna forma bankowości elektronicznej, określana jako bankowość samoobsługowa czy też *self--banking*. Zaliczają się do niej bankomaty oraz terminale do akceptowania płatności kartami płatniczymi EFT-POS (Świecka 2012).

Bankowość mobilna – w skrócie określana jako *m-banking*, można ją zdefiniować jako korzystanie z usług bankowych za pomocą urządzeń mobilnych, tj. smartfonów czy tabletów. Usługi bankowe dostępne na telefon komórkowy określane są mianem bankowości mobilnej (Zarańska, Zborowski 2018, s. 12).

Istota i definicje transakcji oszukańczych

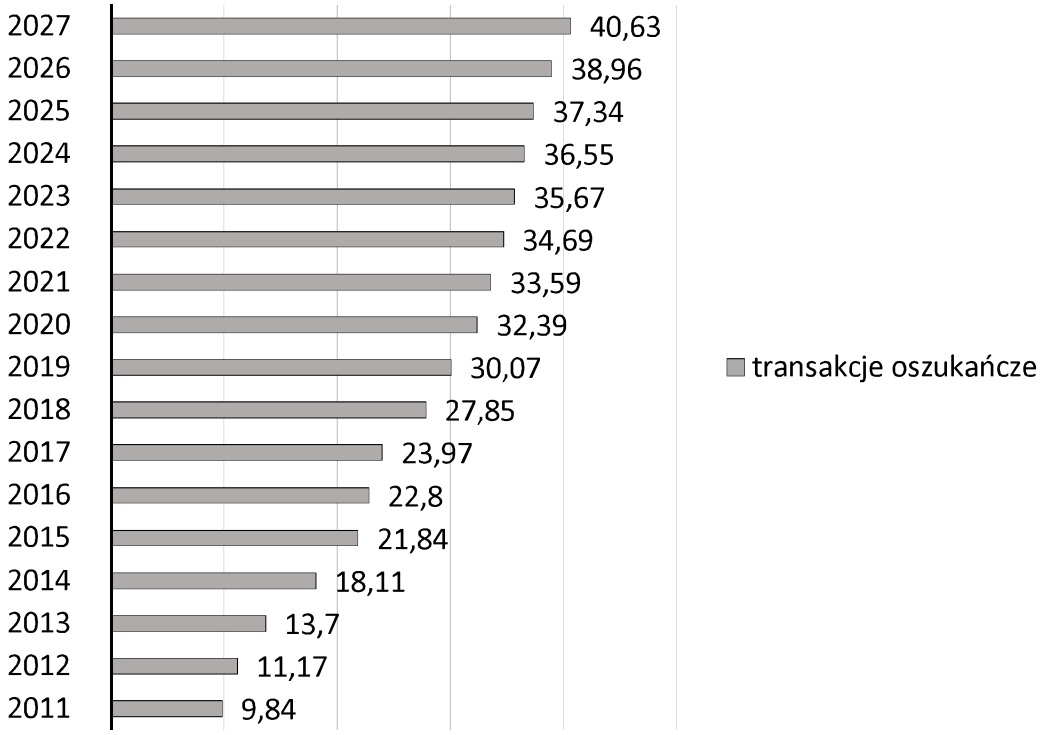
Ustawa o usługach płatniczych nie zawiera definicji legalnej pojęcia nieautoryzowanej transakcji płatniczej. Zgodnie natomiast z art. 40 ust. 1 ustawy o usługach płatniczych (u.u.p.) transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Można zatem uznać za nieautoryzowaną transakcję płatniczą w sytuacji, gdy płatnik nie wyraził na nią zgody.

Transakcja oszukańcza (transakcja nieuprawniona) – transakcja kartą płatniczą zakwestionowana przez bank, wystawcę karty to fraud. Za transakcje fraud uważa się transakcje (lub próby transakcji) kartami skradzionymi, zagubionymi (zastrzeżonymi), skopiowanymi lub otrzymanymi na podstawie fałszywych danych lub danych obcego właściciela. Transakcje oszukańcze to takie, które zostały zrealizowane w sytuacji braku zgody rzeczywistego posiadacza lub też w przypadku których poszkodowany zostaje zmanipulowany przez oszusta do wystawienia zlecenia płatniczego (manipulowanie płatnikiem – socjotechnika). Transakcje fraud to coraz częściej oszustwa przy użyciu kart skopiowanych na zasadzie skimmingu w bankomatach lub samoobsługowych automatach akceptujących karty (np. na stacji benzynowej). W przypadku transakcji fraud sprzedawca (akceptant) po zobaczeniu odpowiedniego komunikatu na wyświetlaczu terminala płatniczego powinien zatrzymać kartę (http://finansopedia.forsal.pl/…).

Prawdziwą skalę problemu nieautoryzowanych transakcji na świecie możemy zauważyć, analizując dane publikowane przez Merchant Savvy – organizację, która doradza bankom, jakich dostawców instrumentów płatniczych powinny wybrać. Skalę problemu nieautoryzowanych transakcji na świecie przedstawiono na *rysunku 9.2*.

Z danych wynika, że od 2011 roku wartość nieautoryzowanych transakcji wzrosła trzykrotnie z 10 do 30 miliardów dolarów. Suma transakcji nieautoryzowanych w 2027 roku może przekroczyć ponad 40 miliardów dolarów, co jest przerażające.

Dane europejskiej komisji wskazują, iż 56% respondentów miało do czynienia z oszustwem internetowym w ciągu dwóch ostatnich lat. Polska znajduje się poniżej średniej Unii Europejskiej – doświadczenia z fraudami potwierdziło 46% badanych. Przodują Dania i Irlandia, gdzie odpowiednio 69% i 68% pytanych spotkało z się z takim oszustwem.



Rysunek 9.2. Nieautoryzowane transakcje – prognoza do roku 2027 [USD]

Źródło: Opracowanie na podstawie danych publikowanych przez Merchant Savvy (za: Prawnik .One 2021)

Transakcje oszukańcze, metody cyberprzestępców:

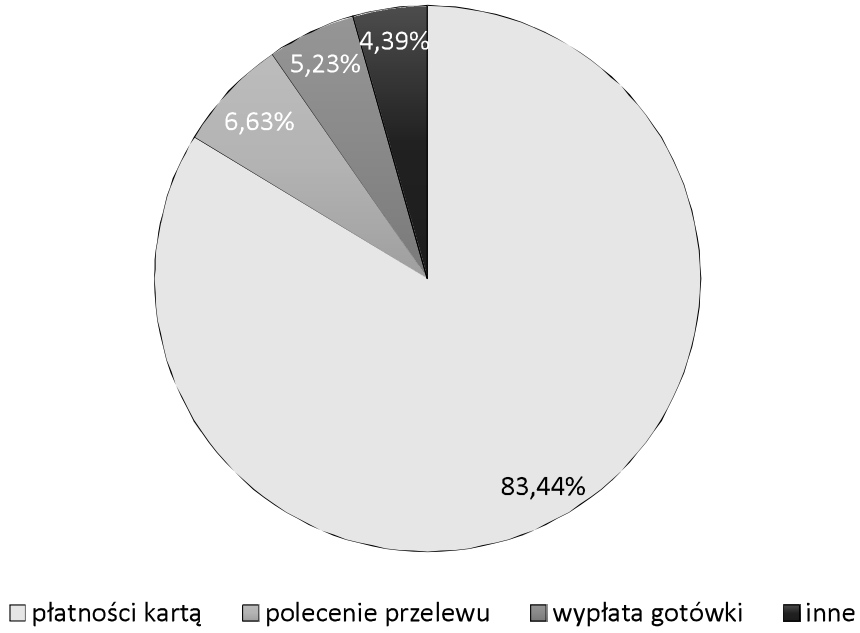
- ***Phishing*** to jedna z najpopularniejszych metod oszustwa sieci. Polega na wysyłaniu fałszywej korespondencji w postaci e-maili lub SMS-ów, w której znajduje się link kierujący do sfałszowanej strony banku (Vayansky, Kumar 2018, s. 15).
- ***Vishing*** to rozmowy telefoniczne i podszywanie się pod inny podmiot (oszuści najczęściej podają się za: pracowników banku, konsultantów inwestycyjnych, pracowników UKNF, BIK, sanepidu, funkcjonariuszy policji, lekarzy, pracowników misji ONZ). To telefoniczne wyłudzenie informacji osobistych/ finansowych[14].
- ***Spoofing*** to oszustwo polega na podszywaniu się pod inne urządzenia lub innego użytkownika. Hakerzy zmieniają numer telefonu, IP, z których się kontaktują. Zawsze są dobrze przygotowani, aby uśpić czujność odbiorcy[15].

Transakcje oszukańcze, oszustwa internetowe stają się powoli codziennością – już co drugi Polak spotkał się z próbą wyłudzenia. Analiza światowych i europejskich danych o fraudach pozwala wnioskować, że skala nadużyć będzie się zwiększać. Z danych przedstawionych na *rysunku 9.2* wynika, iż prognozy nie są

[14] Więcej informacji na temat metody *vishing* (https://www.hhs.gov/…).
[15] Więcej informacji na temat metody *spoofiing* (https://www.gov.pl/…).

optymistyczne i zapowiadają systematyczny wzrost liczby fraudów bankowych. Pandemia COVID-19 spowodowała przyspieszenie wdrażania nowych technologii szczególnie w bankach spółdzielczych. Część naszego życia przeniosła się do świata wirtualnego, a to przyczynia się do tego, że rodzajów oszustw stosowanych przez cyberprzestępców jest coraz więcej. Edukacja użytkowników przestrzeni online jest najlepszym sposobem na ograniczenie liczby fraudów. Istotna jest znajomość zasad bezpiecznego poruszania się w sieci oraz wiedza na temat tego, jak cyberprzestępcy próbują oszukiwać i okradać.

W 2020 roku odnotowano ponad 322 tys. przypadków transakcji oszukańczych na łączną kwotę 264,7 mln zł[16].



Rysunek 9.3. Transakcje oszukańcze dokonywane przy użyciu bezgotówkowych instrumentów płatniczych w 2020 roku

Źródło: (https://www.nbp.pl/…)

Największą grupę oszukańczych bezgotówkowych transakcji płatniczych w 2020 roku stanowiły płatności kartą, co niewątpliwie jest powiązane z rozwojem rynku e-commerce i szeroko rozumianego handlu elektronicznego. Dla posiadaczy kart płatniczych i kredytowych można sformułować kilka kluczowych zasad bezpieczeństwa:

- Nie klikać w linki otrzymane w SMS-ach oraz komunikatorach społecznościowych.
- Nie podawać żadnych danych osobowych ani nie klikać w BLIK-a otrzymanego od znajomego.

[16] Więcej informacji na temat transakcji oszukańczych (https://www.knf.gov.pl/…).

- Zmienić (zmniejszyć) limity na karcie, w aplikacji mobilnej, bankowości internetowej.
- Ważne, by dokładnie czytać powiadomienia autoryzacyjne w aplikacji mobilnej, SMS-y.
- Zawsze dokładnie sprawdzać, co autoryzujemy, na jaką kwotę i na jaki numer.
- Kierować się zasadą ograniczonego zaufania. Sprawdzać dwa razy rodzaj operacji, upewnić się, czy przypadkiem nie nastąpiło dodanie do konta zaufanego, numer telefonu.

Możliwości, jakie daje współczesny Internet, ułatwiają życie. Pozwalają bez ograniczeń korzystać z bankowości elektronicznej, jednak nie powinny przysłonić zagrożeń.

Prawidłowe zachowanie w cyberprzestrzeni, korzystanie z aplikacji antywirusowych, zapoznawanie się komunikatami bezpieczeństwa instytucji, takich jak policja czy banki, prowadzi do zmniejszenia nadużyć i zwiększa bezpieczeństwo.

Procedury uwierzytelnienia i autoryzacji

Pojęcie autoryzacji (jego właściwe rozumienie) może wywoływać pewne wątpliwości interpretacyjne. Wynika to z faktu, że – podobnie jak w przypadku całej regulacji dotyczącej dokonywania płatności kartą płatniczą – zastosowana siatka pojęciowa czerpie z dwóch różnych źródeł, tj. obrotu biznesowego oraz prawnego. Często jest ono używane w oderwaniu od znaczenia nadanego jej przez u.u.p. (art. 40 i nast.), a jego zastosowanie bywa mylące i wewnętrznie niespójne[17].

Uwierzytelnienie zostało zdefiniowane na gruncie dyrektywy PSD2 (ang. *Payment Services Directive*) – to Dyrektywa Parlamentu Europejskiego i Rady UE z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego. Głównym celem dyrektywy było zwiększenie bezpieczeństwa uczestników rynku finansowego, konsumentów, czyli beneficjentów indywidualnych korzystających z oferty banków. Uwierzytelnienie to – zgodnie z ustawową definicją – „procedura umożliwiająca dostawcy usług płatniczych weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika" (art. 2 pkt 33b u.u.p.). Uwierzytelnienie to

[17] Potwierdzeniem przywołanego problemu jest dostrzeżone w doktrynie mylenie pojęcia autoryzacji z uwierzytelnieniem (do czego doszło nawet na etapie procesu tłumaczenia dyrektywy na język polski). Szerzej: (Grabowski 2012, komentarz do art. 2, nb 31). W wersji angielskiej dyrektywy PSD, w art. 4 pkt 19, użyto pojęcia „*authentication*", podczas gdy art. 54 dyrektywy PSD (którego implementacją jest art. 40 i nast. u.u.p.) posługuje się już pojęciem „*authorisation*". W polskiej wersji tego aktu w obu sytuacjach użyto terminu „autoryzacja". Pomijając samą nieścisłość językową, jakiej dopuszczono się na etapie tłumaczenia dyrektywy, należy podkreślić, że powyższe, w sposób oczywisty, stoi w sprzeczności z jedną z podstawowych zasad prawidłowej legislacji, jaką jest zasada, że każdy termin użyty w danym akcie prawnym może mieć przypisane tylko jedno znaczenie. Co ciekawe, wydaje się, że błąd ten został dostrzeżony, gdyż dyrektywa PSD2 (następca obecnej regulacji), również posługująca się pojęciem „*authentication*", została już przetłumaczona z użyciem poprawnych terminów.

zespół czynności, które służą potwierdzeniu tożsamości płatnika. Dyrektywa PSD2 została stworzona m.in. po to, aby klienci mogli przeprowadzać transakcje bez obawy o utratę swoich środków. Dyrektywa PSD2 wprowadziła pojęcie silnego uwierzytelnienia klientów. To najbardziej odczuwalna dla konsumentów zmiana, polegająca na podwójnej weryfikacji tożsamości konsumenta, która wydłuża proces logowania się do bankowości internetowej. W praktyce oznacza to zastosowanie co najmniej dwóch elementów, które należą do kategorii:

- wiedza – coś, co wie wyłącznie użytkownik (ciągi znaków używane jako ustalone hasło, np. numer PIN);
- posiadanie – coś, co posiada wyłącznie użytkownik (używane w połączeniu z hasłami jednorazowymi przekazywanymi za pośrednictwem telefonu lub aplikacji mobilnej, np. karta płatnicza lub token);
- cechy klienta – coś, co jest charakterystyczne wyłącznie dla użytkownika (np. biometria, przepływ krwi, odcisk palca).

Celem stosowania się do tych wymogów przez wydawców instrumentów płatniczych oraz podmioty świadczące usługę acquiringu jest podwyższenie poziomu bezpieczeństwa w transakcjach elektronicznych (NBP 2022).

Dokonując rozróżnienia pomiędzy uwierzytelnieniem i autoryzacją transakcji płatniczych, należy zwrócić uwagę na istotę dwóch pojęć. W doktrynie wskazuje się, że uwierzytelnienie „polega na zweryfikowaniu tożsamości płatnika lub ważności stosowania instrumentu płatniczego" (Wyżykowski 2019, s. 107). Takie podejście pozwala na odróżnienie uwierzytelnienia od autoryzacji transakcji, która polega na wyrażeniu przez płatnika zgody na wykonanie transakcji płatniczej. Pojęcie autoryzacji, chociaż nie jest tożsame z oświadczeniem woli płatnika, jest przeciwne do pojęcia uwierzytelnienia, które będzie jedynie zdarzeniem faktycznym podobnym do okazania dokumentu tożsamości dokonywanym przy osobistym wstawieniu stron. Nie każde oświadczenie woli płatnika będzie autoryzacją, np. istnieją przypadki, w których oświadczenie nie odpowiada wymogom ustanowionym w umowie pomiędzy płatnikiem a dostawcą usług płatniczych.

Do nieautoryzowanej transakcji płatniczej dochodzi wówczas, gdy bez wiedzy rzeczywistego właściciela karty płatnika dokonywana jest transakcja płatnicza na jego rachunek. Zgodnie z nowym brzmieniem art. 46 ust. 1 u.u.p. w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika niezwłocznie, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwraca płatnikowi kwotę nieautoryzowanej transakcji płatniczej. W przypadku gdy płatnik korzysta z rachunku płatniczego, dostawca płatnika (bank) przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Zmiana ta w ocenie Rzecznika Finansowego ma ogromne znaczenie dla instytucji finansowych i ich procedur postępowania w przypadku wystąpienia nieautoryzowanej transakcji płatniczej. Zdaniem Rzecznika Finansowego, zgodnie

z obecnym stanem prawnym, w przypadku wystąpienia nieautoryzowanej transakcji można mówić o kilku podstawowych zasadach:

- obowiązku bezwarunkowego zwrotu środków klientowi (z przepisu art. 46 ust. 1 u.u.p. po nowelizacji wynika przede wszystkim, że ustawodawca krajowy, w ślad za ustawodawcą unijnym, wprowadził obowiązek bezwarunkowego zwrotu kwoty nieautoryzowanej transakcji płatnikowi przez dostawcę);
- obowiązku zwrotu kwoty nieautoryzowanej transakcji w terminie D+1 (ustawodawca unijny postanowił wprowadzić zatem bardzo krótki termin dla dostawcy na zwrot kwoty nieautoryzowanej transakcji płatniczej, dokonanie zwrotu najpóźniej następnego dnia po zgłoszeniu lub wykryciu takiej transakcji);
- odpowiedzialności płatnika za nieautoryzowaną transakcję dopiero po zwrocie środków (następuje ustalenie zasad ewentualnej współodpowiedzialności płatnika za nieautoryzowaną transakcję płatniczą, w ocenie Rzecznika Finansowego powinna ona następować w toku postępowania sądowego) (Rzecznik Finansowy 2019, s. 5-7).

Analiza transakcji oszukańczych w Banku Spółdzielczym

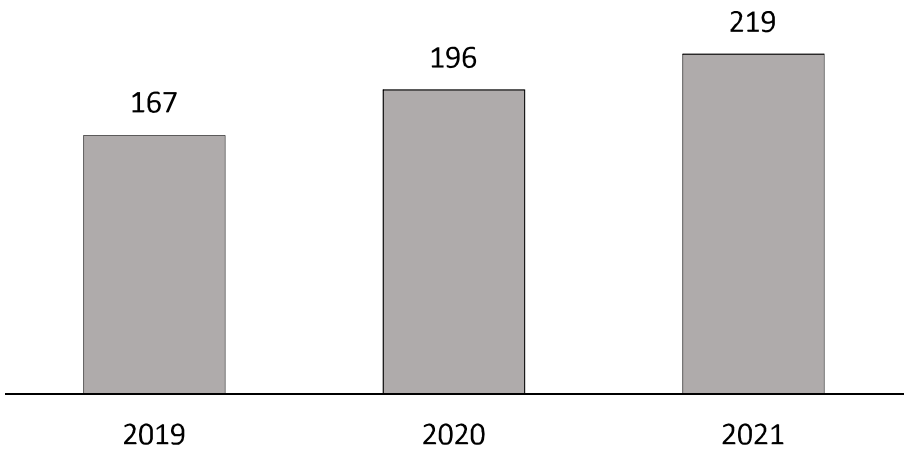
Polem badawczym niniejszego rozdziału jest analiza w bankowości spółdzielczej transakcji oszukańczych dokonywanych przy użyciu bezgotówkowych instrumentów płatniczych jako przejaw cyberprzestępczości. Badania zostały przeprowadzone w jednym z banków spółdzielczych działających na terenie województwa łódzkiego; ze względu na bezpieczeństwo autorka nie może podać pełnej nazwy Banku Spółdzielczego ani jego lokalizacji.

Przeanalizowane zostały dane statystyczne dotyczące transakcji oszukańczych udostępnione przez Bank Spółdzielczy. Do analizy wybrano okres czasu pandemii COVID-19 od stycznia 2019 roku do grudnia 2021 roku. Do wyboru okresu przyczyniło się wiele czynników. Jednym z nich było to, iż w 2019 roku analizowany bank wprowadził aplikację mobilną i pod koniec roku wdrożył usługę BLIK. Okres pandemii w bankach spółdzielczych był przyspieszeniem we wdrażaniu nowych technologii, konieczne stało się bezzwłoczne podejmowanie decyzji, szybkie tworzenie np. aplikacji, które borykały się z problemami; jednym słowem – wdrożono i udoskonalono te aplikacje, dziś są bardzo dopasowane do potrzeb klienta. W okresie pandemii klient musiał zmienić swoje podejście do bankowości elektronicznej czy mobilnej. Współczesna bankowość spółdzielcza jest osadzona w tradycji, ugruntowana na rynku lokalnym. Stojąca u progu coraz większych wyzwań w celu dostosowania do potrzeb młodego pokolenia klientów.

Analiza danych statystycznych została przeprowadzona od stycznia 2019 roku do grudnia 2021 roku. Liczbę transakcji oszukańczych przedstawiono na *rysunku 9.4*.

Według danych statystycznych udostępnionych przez Bank Spółdzielczy liczba operacji oszukańczych dokonanych kartami płatniczymi wykazuje tendencję wzrostową. Wykorzystanie nowych technologii w sektorze usług finansowych dało ogromny impuls do rozwoju. Wraz z rosnącym uzależnieniem od

elektronicznych i cyfrowych narzędzi do przeprowadzenia transakcji płatniczych dokonywanych bezgotówkowo występuje poważne zagrożenie bezpieczeństwa i niezawodności operacji finansowych, a wraz z rosnąca tendencją rozpowszechnienia dostępu online liczba oszustw w tych płatnościach wzrasta (Soni, Soni 2013, s. 22).



Rysunek 9.4. Transakcje oszukańcze w Banku Spółdzielczym

Źródło: Opracowanie własne na podstawie udostępnionych danych statystycznych przez Bank Spółdzielczy

Cyberbezpieczeństwo to bezpieczeństwo technologii informatycznych. Dla większości z nas to ogół praktyk i zasad postępowania w celu ochrony komputerów, telefonów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem, w tym przed kradzieżami i wyłudzeniami środków z rachunku bankowego. Niewątpliwie nowoczesne rozwiązania oferowane przez banki ułatwiają życie. Pozwalają na dostęp do własnych środków w dowolnym czasie i miejscu. Umożliwiają szybki transfer gotówki, bezpieczne zakupy w sieci, ale również łatwy dostęp do różnych platform, np. Ministerstwa Zdrowia czy PUE ZUS. Wszystkim tym dobrodziejstwom towarzyszy wzrost zainteresowania przestępców. Wykorzystują oni zarówno nowe elektroniczne formy ataku, jak i klasyczne oszustwa w celu przechwycenia środków klientów banków. Dlatego Zespół Cyberbezpieczeństwa w Komisji Nadzoru Finansowego (CSIRT KNF) ostrzega przed oszustami[18].

Podsumowanie

Zagadnieniem badawczym w niniejszym rozdziale była analiza transakcji oszukańczych dokonywanych bezgotówkowych transakcji płatniczych jako przejaw cyberprzestępczości w czasie pandemii.

[18] Więcej informacji na temat ostrzegania przez CSIRT KNF (KNF 2021).

Bank Spółdzielczy poddany analizie wpisuje się w tendencje zmian sektora banku spółdzielczego, dąży do wykorzystania potencjału technologicznego, wdrażając różne kanały dostępu. Z badań statystycznych udostępnionych przez bank wynika, że transakcje oszukańcze mają tendencję wzrostową, co przedstawiono na *rysunku 9.4*.

Sektor finansowy jest celem wyrafinowanych działań przestępczych, głównie z powodu wartości aktywów, jakimi się w nim zarządza. Wyścig o pierwszeństwo w wygodnej sprzedaży online staje się dla przestępców okazją do wyłudzeń. To powoduje, że banki i inne instytucje finansowe stają przed dylematem wyboru między wygodą dla klientów a utrzymaniem jej bezpieczeństwa w taki sposób, aby owa wygoda nie stwarzała okoliczności dogodnych dla przestępców.

Sektor bankowy jest liderem cyberbezpieczeństwa, zatem klienci mogą czuć się bezpiecznie, korzystając z bankowości elektronicznej. Należy pamiętać, aby dbać o bezpieczeństwo urządzeń i ciągle poszerzać wiedzę o cyberbezpieczeństwie. Bardzo dużo zależy od wiedzy i postaw klientów banków. FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP to specjalny adres do zgłaszania przypadków nadużyć.

Podjęta problematyka stanowi wstęp do badań mających na celu identyfikowanie czynników ryzyka, określenie, czy te ryzyka są generowane głównie przez techniczne niedoskonałości systemów informatycznych, czy przez umyślne ignorowanie przez klientów zasad bezpiecznego korzystania z bankowości elektronicznej pod kątem skłonności do korzystania z nowych, innowacyjnych usług bankowych.

Literatura

Borcuch A. (2016), *The Sharing Economy: Understanding and Challenges*, „International Journal of Humanities & Social Science Studies (IJHSSS)", 2(5).

Chmielarz W. (2005), *Systemy elektronicznej bankowości*, Difin, Warszawa.

Górnisiewicz M., Obczyński R., Pstruś M. (2014), *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną. Poradnik klienta usług finansowych*, Komisja Nadzoru Finansowego, Warszawa.

Grabowski M. (2012), *Ustawa o usługach płatniczych. Komentarz*, Legalis, Warszawa.

http://finansopedia.forsal.pl/wiki/Fraud (dostęp: 21.08.2022).

https://9lib.org/article/poj%C4%99cie-i-elementy-bankowo%C5%9Bci-elektronicznej.zwv1rx9v (dostęp: 21.08.2022).

https://www.gov.pl/web/cyfryzacja/spoofing-i-phishing--grozne-narzedzia-w-rekach-cyberprzestepcow (dostęp: 05.08.2022).

https://www.hhs.gov/sites/default/files/vishing-attacks-on-the-hph-sector-analyst-note.pdf (dostęp: 05.08.2022).

https://www.knf.gov.pl/komunikacja/wnioski_formularze (dostęp: 21.08.2022).

https://www.nbp.pl/systemplatniczy/informacja-o-transakcjach-oszukanczych-2020q3 (dostęp: 21.08.2022).

KNF (2021), *Oszuści na portalach aukcyjnych OLX – jak nie dać się okraść?*, https://www.knf.gov.pl/dla_rynku/CSIRT_KNF?articleId=73548&p_id=18 (dostęp: 08.08.2022).

Kwaśniewski P., Leżoń K., Szwajkowska G., Woźniczka F. (2010), *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Urząd Komisji Nadzoru Finansowego, Warszawa.

NBP (2022), *Informacja o transakcjach oszukańczych dokonywanych przy użyciu bezgotówkowych instrumentów płatniczych w I kwartale 2022*, Narodowy Bank Polski, Warszawa.

Prawnik.One (2021), *Kradzieże z kont bankowych – skala fraudów na świecie*, https://prawnik.one/2021/04/22/kradzieze-z-kont-bankowych-skala-fraudow-na-swiecie/ (dostęp: 05.08.2022).

Rzecznik Finansowy (2019), *Nieautoryzowane transakcje płatnicze – analiza Rzecznika Finansowego 2019*, https://rf.gov.pl (dostęp: 05.08.2022).

Soni R.R., Soni N. (2013), *An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks*, „Research Journal of Management Sciences", 2(7), July, http://www.isca.in/IJMS/Archive/v2/i7/4.ISCA-RJMS-2013-062.pdf (dostęp: 21.08.2022).

Świecka B. (2004), *Bankowość elektroniczna*, CeDeWu, Warszawa.

Świecka B. (2012), *Bankowość elektroniczna*, wyd. 2, CeDeWu, Warszawa.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. 2011 nr 199 poz. 1175, z późn. zm.).

Vayansky I., Kumar S. (2018), *Phishing Challengesand Solutions*, „Computer Fraud & Security", 2018(1), DOI:10.1016/S1361-3723(18)30007-1.

Wyżykowski B. (2019), *Odpowiedzialność za nieautoryzowane transakcje płatnicze wybrane zagadnienia wynikające z implementacji PSD2*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny (iKAR)", 8(8).

Zarańska K., Zborowski M. (2018), *Charakterystyka bankowości elektronicznej*, [w:] Gospodarowicz A. (red.), *Bankowość elektroniczna. Istota i innowacje*, C.H. Beck, Warszawa.