BEZPIECZEŃSTWO • TEORIA I PRAKTYKA 2018 nr 4
e-ISSN 2451-0718
ISSN 1899-6264

Dariusz Fatuła
prof. nadzw. dr hab., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Elementy kultury bezpieczeństwa a zachowania klientów instytucji finansowych

Wprowadzenie

Zachowania klientów indywidualnych instytucji finansowych są przedmiotem licznych badań[1]. Postęp technologiczny, rozwój i wprowadzanie na rynek nowych produktów oraz przemiany w zakresie społecznym, kulturowym i ekonomicznym sprawiają, że zachowania finansowe ulegają ciągłym zmianom. Najistotniejsza w ostatnich latach jest wirtualizacja czynności i produktów finansowych[2]. Istnieje jednak pewien stały element towarzyszący zmieniającym się zachowaniom – jest nim swoista kultura (przez pewną analogię do kultury organizacji), a w szczególności kultura bezpieczeństwa towarzysząca w zasadzie wszystkim elementom i etapom zachowań finansowych. Same zasady bezpieczeństwa, jako reguły towarzyszące pewnym czynnościom, mogą

[1] S. Smyczek, *Zachowania konsumentów na rynku usług bankowych*, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice 2001; D. Fatuła, *Zachowania polskich gospodarstw domowych na rynku finansowym*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2010; S. Smyczek, *Modele zachowań konsumentów na rynku usług finansowych*, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice 2007; *Finanse osobiste. Zachowania – produkty – strategie*, red. E. Bogacka-Kisiel, Wydawnictwo Naukowe PWN, Warszawa 2012; D. Maison, *Polak w świecie finansów: o psychologicznych uwarunkowaniach zachowań ekonomicznych Polaków*, Wydawnictwo Naukowe PWN, Warszawa 2012; J. Garczarczyk, M. Mocek, R. Skikiewicz, *Zachowania gospodarstw domowych na rynku usług finansowych w warunkach zmiennej koniunktury*, Wydawnictwo CeDeWu.pl, Warszawa 2014; C. Bywalec, *Gospodarstwo domowe, ekonomika, finanse, konsumpcja*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2017;

[2] K. Waliszewski, *Model doradztwa w obszarze finansów osobistych w Polsce na tle doświadczeń międzynarodowych*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2016, s.112.

być elementem takiej kultury. Wymagają jednak pewnego uzupełnienia, połączenia i spojrzenia od strony podmiotów rynkowych, tak aby nie były tylko prostymi instrukcjami do przestrzegania lub wykonania. Stanowić powinny całościowe ujęcie, wręcz rodzaj systemu wartości, którym kierują się podmioty zachowań. Tak rozumiana kultura bezpieczeństwa może wyznaczać pewne ramy zastosowań przedmiotów obrotu, wzajemnych relacji podmiotów (sprzedających i kupujących), stymulować rozwój rynku, zachęcać do innowacji[3]. Kultura bezpieczeństwa w zachowaniach finansowych ma szczególne i rosnące znaczenie ze względu na specyfikę usług finansowych ściśle związanych z najnowszym technologiami[4]. Z jednej strony wydaje się, że usługi finansowe są coraz dostępniejsze, bliższe klientowi – osiągalne wręcz „za jednym kliknięciem" w smartfonie. Z drugiej strony nawet laik zdaje sobie sprawę, że za tą pozorną łatwością i prostotą kryją się skomplikowane technologie i produkty. Wzbudza to wieloaspektowe obawy o niezrozumienie, brak umiejętności posługiwania się technologiami i urządzeniami, możliwość nadużyć, oszustw i ogólnie pojętą uczciwość konkretnego rozwiązania technicznego (np. aplikacji), instytucji (np. banku, pośrednika) czy wręcz całego systemu finansowego.

Patologie zachowań finansowych są szeroko omawiane zarówno w aspekcie technicznym, jak i ekonomicznym, psychologicznym oraz socjologicznym[5], wydaje się jednak, że brak całościowego ujęcia zagadnienia bezpieczeństwa zachowań finansowych z różnych punktów widzenia, m.in. marketingowego (w tym wizerunkowego dla instytucji finansowych). Opracowanie ma charakter koncepcyjny, a jego celem jest próba zdefiniowania kultury bezpieczeństwa oraz wskazania jej elementów i ich powiązań w szerokim aspekcie zachowań finansowych.

Identyfikacja form ryzyka, zagrożeń i obszarów bezpieczeństwa

Pojęcie kultury jest wieloznaczne i zależy od dziedziny wiedzy lub aspektu, w jakim jest używane[6]. Oprócz materialnych aspektów kultury ważnym jej elementem są zasady i reguły obowiązujące w zachowaniach społecznych. W tym też aspekcie można mówić o kulturze bezpieczeństwa[7]. Samo bezpieczeństwo zaś to pewien stan

---

[3] B. Nogalski, *Kultura organizacyjna. Duch organizacji*, Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego, Bydgoszcz 1998, s. 105; Ł. Sułkowski, *Procesy kulturowe w organizacjach*, Dom Organizatora, Toruń 2002, s. 56.

[4] K. Waliszewski, *Model doradztwa…*, *op. cit.*, s. 110.

[5] S. Smyczek, *Determinanty rozwoju patologicznych zachowań konsumentów na rynkach finansowych*, „Handel Wewnętrzny" 2016, nr 2 (361), s. 364–373; *idem*, *Badania patologii w zachowaniach konsumentów na rynku*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 460, s. 177–188; S. Smyczek, M. Grybś-Kabocik, J. Matysiewicz, A. Tetla, *Patologie w zachowaniach konsumentów na rynku*, Wydawnictwo Placet, Warszawa 2017.

[6] A.L. Kroeber, C. Kluckhon, *Culture. A Critical Review of Concepts and Definitions*, „Papers of the Peabody Museum of Archaeology and Ethnology" 1952, Vol. 47, No. 1; J. Martin, *Organizational Culture. Mapping the Terrain*, Sage, Thousand Oaks, London 2002.

[7] S. Cox, R. Flin, *Safety Culture, Philosopher's Stone or Man of AStraw*, „Work & Stress" 1998, Vol. 12, No. 3, s. 189–201; D. Cooper, *Improving Safety Culture*, John Wiley & Sons Ltd., London 1998.

odczuwany przez jednostki (czy określony przez instytucje), który oznacza brak ryzyka utraty, zniszczenia lub ingerencji w wartości bez zgody danej jednostki. Bezpieczeństwo nie musi oznaczać braku zagrożeń (taki stan rzadko istnieje), ale powinien uwzględniać świadomość zagrożeń, umiejętność przeciwdziałania im oraz ewentualną zdolność do naprawy skutków zaistnienia zdarzeń niekorzystnych dla podmiotu.

Świadomość zagrożeń jest więc kluczowa w budowaniu kultury bezpieczeństwa. Świadomość ta nie może być jednak paraliżująca i powstrzymująca od działań. Powinna być różnie budowana w zależności od tzw. postaw względem produktu. Innowatorzy, którzy są skłonni kupić produkt we wczesnej jego fazie, bez zachęt z zewnątrz i oglądania się na innych, są bardziej skłonni lekceważyć zagrożenia niż naśladowcy lub tzw. maruderzy. Równocześnie we wczesnych fazach funkcjonowania produktu nie wszystkie zagrożenia są znane, gdyż ujawniają się one dopiero w trakcie jego funkcjonowania. Tworzenie świadomości spoczywa wówczas m.in. na samych innowatorach jako użytkownikach produktu. Współczesne metody komunikacji pozwalają na szybkie dzielenie się spostrzeżeniami na temat produktów, które powinny być zauważane przez producentów i dostarczycieli usług. Ci ostatni powinni tworzyć mechanizmy pozyskiwania takich informacji w celu modyfikowania produktu czy usługi. Zadanie obserwacji danego rynku, w tym zwracanie uwagi na opinie klientów, spoczywa także na instytucjach nadzoru, takich jak Komisja Nadzoru Finansowego.

Reagowanie na uwagi klientów leży w interesie instytucji oferujących produkty i usługi. Przyczynia się to do poprawy wizerunku firmy (jako element *public relations*) i równocześnie wciąga klientów w działania prosumenckie. Klienci stają się wówczas także współproducentami, mogą więc poczuć się zobowiązani do przekazywania ważnych informacji, co już samo w sobie tworzy elementy kultury bezpieczeństwa. Naśladowcy, którzy kupują produkt po innowatorach, kierują się często właśnie ich opiniami. Późna większość lub maruderzy powinni być natomiast beneficjentami kultury bezpieczeństwa wpracowanej wcześniej, tak aby nie obawiać się zakupu produktu. Marketingowcy, zwracając się do grup klientów, którzy kupują produkt w późnej jego fazie obecności na rynku, powinni wskazywać na wypracowane już metody eliminowania zagrożeń lub minimalizowania ryzyka, powołując się na opnie i doświadczenia użytkowników kupujących produkt we wcześniejszych fazach. Świadomość zagrożeń po stronie instytucji finansowych i nadzorczych nie musi wymagać ich nagłaśniania. W przypadku kiedy zagrożenia są dobrze zidentyfikowane, a ryzyko niewielkie, należy raczej nagłaśniać prawidłowe wzorce działań, przykłady odpowiednich zabezpieczeń. Natomiast jeśli zagrożenia są słabo zidentyfikowane, a ryzyko duże, należy to eksponować, tak aby klienci mogli polegać także na własnej inwencji i starali się zabezpieczyć sami, bez zbytniego polegania na niedoskonałych metodach zabezpieczeń. W niektórych przypadkach sprzedawcy powinni nawet odradzać zakup produktu czy jego użytkowanie, dopóki nie zostaną wypracowane lepsze metody zabezpieczeń. Wydaje się to nielogiczne z punktu widzenia maksymalizacji zysku sprzedawcy, ale długofalowo przyniesie korzyści. Klienci, dostrzegając etyczną postawę firmy, powinni w przyszłości docenić jej działania i wybrać przed konkurentami, którzy narażali wcześniej klientów w pogoni za krótkofalowym zyskiem.

W niekorzystnych zdarzeniach, których prawdopodobieństwo zajścia można określić jako ryzyko, można zidentyfikować jedno lub wiele zagrożeń. Grupy zagrożeń określane w marketingu jako ryzyko rozpatrywane z punktu widzenia klienta można

podzielić na kilka kategorii ze względu na ich specyfikę. Najczęściej w literaturze[8] wymienia się następujące ryzyka:

- ryzyko funkcjonalne;
- ryzyko fizyczne (związane z bezpieczeństwem);
- ryzyko społeczne;
- ryzyko psychologiczne;
- ryzyko finansowe;
- ryzyko straty czasu;
- ryzyko utraconych możliwości.

Ze względu na specyfikę rynku finansowego można dodać jeszcze następujące kategorie ryzyka:

- ryzyko systemowe;
- ryzyko rynkowe;
- ryzyko stopy procentowej;
- ryzyko inflacji;
- ryzyko kredytowe;
- ryzyko walutowe;
- ryzyko utraty płynności;
- ryzyko cybernetyczne;
- ryzyko prawne.

Trzeba jednak pamiętać, że powyższe ryzyka dotyczą bezpośrednio instytucji finansowych, a klientów tylko pośrednio. Niemniej jednak mają one znaczenie w kształtowaniu kultury bezpieczeństwa także z punktu widzenia klienta detalicznego rynku finansowego. Wszystkie wyżej wymienione ryzyka można rozpatrywać (jak już wspomniano we wstępie) w aspekcie socjologicznym, psychologicznym, ekonomicznym (w szczególności marketingowym) i technicznym.

Aspekt socjologiczny dotyczy społecznego odbioru pewnych zachowań, tworzenia zachęt, presji, mitów. Aspekt psychologiczny dotyczy postrzegania własnych zachowań, zadowolenia bądź dyskomfortu z zaspokajania potrzeb, nadziei, obaw, lęków. Aspekt ekonomiczny związany jest z wymiernymi korzyściami finansowym związanymi z różnymi zachowaniami, a aspekt techniczny dotyczy rozwoju technologii i jej wpływu na zmiany zachowań. Wszystkie te aspekty zachodzą wzajemnie na siebie. Przykładowo zadowolenie własne z podejmowanych działań zależy od społecznego odbioru danych zachowań, finansowego ich rezultatu i umiejętności posługiwania się technologią. Niemniej jednak w analizie warto przyjrzeć się każdemu z aspektów z osobna, a następnie dokonać ich syntezy w szerokim ujęciu kultury bezpieczeństwa.

Analiza form ryzyka i zagrożeń

Ryzyko funkcjonalne wynika z obaw, że produkt lub dane zachowanie nie przyniesie takiego rezultatu (np. zaspokojenia potrzeby), jakiego spodziewa się klient. Inaczej mówiąc, klient obawia się, że produkt nie spełni oczekiwanych nadziei lub nie będzie

[8] L. Rudnicki, *Zachowania konsumentów na rynku*, PWE, Warszawa 2000, s. 105.

miał spodziewanych właściwości czy funkcji. Obawa taka może wynikać zarówno z obiektywnych przesłanek związanych z brakiem informacji, jak i bardziej subiektywnych czynników w rodzaju osobowości klienta i jego postawy względem elementów produktu. Obiektywna informacja o funkcjach produktu może być również subiektywnie skomplikowana dla konsumenta, który nie ma dostatecznej wiedzy na dany temat lub doświadczenia. W dziedzinie produktów i zachowań finansowych obawy takie są szczególnie silne wobec dużego skomplikowania materii. Przykładowo: klient może nie wiedzieć, czy i jak dostęp do konta bankowego w telefonie umożliwi mu płatność za zakupy. Zaspokojenie potrzeby łatwego, ale i bezpiecznego dostępu do środków finansowych umożliwiających zapłatę jest dopiero końcem pewnego „łańcuszka" działań. Niechęć do podejmowania działań pośrednich (np. instalowanie programów, aplikacji), choć prowadzących do celu, może wynikać z obaw o stratę czasu (ryzyko straty czasu) czy nieumiejętności poradzenia sobie z urządzeniami i procedurami (aspekt techniczny).

Budowanie kultury bezpieczeństwa powinno polegać w takim wypadku na takim przedstawieniu całego ciągu zadań aby klient widział ostateczny ich rezultat prowadzący do zaspokojenia danej potrzeby (łatwy i bezpieczny dostęp do środków w chwili konieczności zapłaty). Przy tym poszczególne czynności (etapy działań) powinny być przedstawione jako proste i niewymagające specjalistycznej wiedzy oraz długiego czasu wykonywania. Równocześnie jednak, co najistotniejsze w kulturze bezpieczeństwa, klient powinien rozumieć, jakie zagrożenia i środki bezpieczeństwa towarzyszą każdemu etapowi. W zależności od segmentu rynku, w jakim budowana jest kultura bezpieczeństwa, należy informacje o zagrożeniach i środkach bezpieczeństwa formułować na odpowiednim poziomie szczegółowości/ogólności. W ramach działań *public relations* instytucje finansowe powinny wspierać programy edukacji ekonomicznej i finansowej. Z badań wynika, że konsumenci stosunkowo wysoko oceniają własny poziom edukacji ekonomicznej i finansowej. E. Kieżel[9] podaje, że w opisywanych badaniach „[…] ponad 57% badanych oceniło poziom wiedzy ekonomicznej jako raczej wysoki i wysoki. Na poziomie przeciętnym wiedzą dysponuje niespełna 23% badanych, a ograniczone zasoby wiedzy posiada prawie 20% badanych". Równocześnie „badani dostrzegają potrzebę edukacji ekonomicznej (ponad 79% badanych), co świadczy także o wzrastającej świadomości ekonomicznej"[10]. Istnieje też wiele programów edukacji finansowej na różnym poziomie kształcenia dzieci i młodzieży oraz w ramach kampanii społecznych[11].

Sprzedaż produktów niedopasowanych do potrzeb klienta określana jest w literaturze, angielskim określeniem „missellig" lub polskim: chybiona/zła sprzedaż[12].

---

9 E. Kieżel, *Wiedza ekonomiczna polskich konsumentów jako podstawa innowacyjnej konsumpcji*, „Handel Wewnętrzny" 2018, nr 3 (374), s. 224.

10 *Ibidem*, s. 226.

11 B. Frączek, *Zakres i formy edukacji finansowej w Polsce oraz jej skutki*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, nr 339, s. 45–57.

12 E. Wierzbicka, *Ochrona klienta ubezpieczeń w Polsce*, „Kwartalnik Nauk o Przedsiębiorstwie" 2015, nr 2, s. 71–79; M. Krasnodębska-Tomkiel, *Misselling, czyli sprzedaż nieetyczna*, „Gazeta Bankowa" 2016, nr 6, s. 30–31; A. Butor-Keler, *Misselling a ochrona konsumenta na rynku usług finansowych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, nr 326, s. 9–20; J. Cichorska, *Misselling, czyli sprzedaż niepotrzebnych instrumentów finansowych i jej skutki. Stan prawny w Pol-*

Kultura bezpieczeństwa wymaga, aby „missellig" był eliminowany zarówno jako strategia firmy, jak i tolerowanie nagannych praktyk pracowników firm finansowych niewynikających z zaleceń przełożonych. Misselling może dotyczyć wielu aspektów sprzedaży produktów finansowych, np. ich cech, warunków towarzyszących sprzedaży lub informowania klienta, a wśród najbardziej charakterystycznych wymienić można[13]:

- nieadekwatność produktu do charakteru, profilu lub potrzeb klienta (np. sprzedaż produktów długoterminowych osobom w podeszłym wieku);
- brak wyjaśnień o sposobach i czasie likwidacji instrumentu;
- brak informacji o konstrukcji instrumentu i strukturze portfela inwestycyjnego;
- brak informacji o stopniu ryzyka instrumentu;
- brak informacji o sposobie obliczania dochodu klienta.

Ważną rolę w zapobieganiu „missellingowi" powinny odegrać także instytucje nadzorcze (w Polsce KNF za pomocą rekomendacji – np. S oraz T, a także UOKiK, Rzecznik Finansowy), i prawodawcy na szczeblu krajowym (ustawa o kredycie konsumenckim z 2011 r., ustawa o działalności ubezpieczeniowej i reasekuracyjnej z 2015 r. oraz ustawa o kredycie hipotecznym[14] z 2017 r.) i europejskim (np. dyrektywy CCD w sprawie umów o kredyt konsumencki oraz MCD w zakresie kredytów hipotecznych[15]). Wspomniane akty prawne regulują sposób, w jaki instytucje finansowe powinny informować klientów o cechach produktu, jakim rygorom podlegają pośrednicy oraz jakie klauzule w umowach (niekorzystne dla klientów) są zabronione[16]. Najważniejsze kwestie dotyczą m.in. publikowania informacji o rzeczywistej rocznej stopie oprocentowania (RRSO), ograniczeniach sprzedaży wiązanej i łączonej, nakładaniu opłat wstępnych i likwidacyjnych, a także ujawniania pewnych danych dot. pośredników finansowych związanych z konfliktem interesów itp. Ważna jest kontrola przestrzegania zaleceń i prawa, nakładanie kar na instytucje niestosujące się do przepisów prawa, publikowanie ostrzeżeń przed instytucjami, które działają na granicy prawa. Przykładowo, jak pisze Cichorska[17]: „W Polsce w 2014 r. w zakresie nieuczciwych praktyk w związku z dystrybucją ubezpieczeń na życie z UFK Prezes UOKiK wydał cztery decyzje nakładające kary finansowe w łącznej wysokości 50,414 mln zł za naruszenie zbiorowych interesów konsumentów. W 2015 r. UOKiK prowadził sprawy przeciwko 17 towarzystwom ubezpieczeniowym o przerzucanie na konsumentów kosztów początkowych zawarcia ubezpieczenia".

---

sce i Wielkiej Brytanii, „Rozprawy Ubezpieczeniowe. Konsument Na Rynku Usług Finansowych / Journal of Insurance, Financial Markets and Consumer Protection" 2017, nr 2 (24), s. 18–34.

13 J. Cichorska, *op. cit.*

14 Tekst jedn. Dz.U. z 2016 r. poz. 1528; Dz.U. poz. 1844; Dz.U. poz. 819.

15 Dyrektywa Parlamentu Europejskiego i Rady 2008/48/WE z dnia 23 kwietnia 2008 r. w sprawie umów o kredycie konsumenckim oraz uchylająca dyrektywę Rady 87/102/EWG (Dz. Urz. UE L 133/66 z dnia 22 maja 2008 r.).

16 Szczegółowe omówienie regulacji prawnych w zakresie kredytu hipotecznego i pośredników finansowych można znaleźć w: K. Waliszewski, *Zmiany w pośrednictwie kredytowym w Polsce w wyniku implementacji dyrektywy hipotecznej*, „Rozprawy Ubezpieczeniowe. Konsument na Rynku Usług Finansowych / Journal of Insurance, Financial Markets and Consumer Protection" 2017, nr 2 (24), s. 3–17.

17 J. Cichorska, *op. cit.*, s. 31.

W przypadku nowoczesnych usług finansowych ryzyko funkcjonalne ma bardzo duże znaczenie w pozyskaniu nowych klientów. Z badań wynika (Badania MasterCard 2016, NBP 2017, Bank Światowy 2018), że ok. 15% Polaków powyżej 15 roku życia nie ma konta bankowego i nie posługuje się żadnymi instrumentami płatniczymi. O ile odsetek ten szybko malał jeszcze w pierwszej dekadzie XXI wieku, o tyle później jego spadek jest już niewielki. Potencjalni „nieubankowieni" klienci nie widzą żadnych korzyści w posługiwaniu się płatnościami bezgotówkowymi, a nawet dostrzegają więcej zagrożeń z tym związanych niż w tradycyjnych zachowaniach z użyciem gotówki. Brak im więc nie tylko szczegółowej wiedzy, ale także świadomości zachodzących zmian, konieczności dostosowania się do nich, czyli pewnej kultury, która kształtuje postawy i zachowania człowieka. Przekonanie, że umiejętne posługiwanie się kartami płatniczymi, bankowością internetową i mobilną jest, przy zachowaniu prostych zasad, bezpieczniejsze niż posługiwanie się gotówką, nie wynika tylko z nauczenia się tychże zasad. Muszą towarzyszyć temu tworzone przez same instytucje finansowe i nadzorcze działania o charakterze *public relations* wspierające zmianę nawyków i postaw konsumenckich.

Ryzyko fizyczne związane jest z bezpieczeństwem użytkowania. W odróżnieniu od ryzyka funkcjonalnego, w którym klienci obawiają się niespełnienia oczekiwań, tu zachodzi obawa wystąpienia jakiegoś uszczerbku, szkody fizycznej, psychologicznej czy finansowej. Największe niebezpieczeństwo dotyczy zazwyczaj utraty środków wskutek sytuacji zarówno niezawinionych bezpośrednio (np. kradzież), jak i częściowo zawinionych przez samego klienta (np. zgubienie). Sytuacje, w których ryzyko to może się ujawnić, obejmować mogą bardzo wiele sytuacji. Co prawda użytkowanie produktów finansowych nie grozi porażeniem prądem czy mechanicznym uszkodzeniem ciała, ale może się zdarzyć, że osoba zbyt ostentacyjnie prezentująca np. swoją prestiżową kartę płatniczą narazi się na akt przemocy, szczególnie w krajach, regionach lub dzielnicach miasta o dużej przestępczości. Ryzyko takiej szczególnej sytuacji nie będzie jednak większe niż w przypadku ostentacyjnego afiszowania się gotówką. Płatność bezgotówkowa jest bezpieczniejsza niż posługiwanie się anonimową gotówką. Utrata tej ostatniej – jej zgubienie lub kradzież – praktycznie nie daje szans na odzyskanie środków. Utrata w ten sam sposób fizycznych atrybutów płatności bezgotówkowych przy zachowaniu prostych reguł daje dużą szanse zachowania środków. Klient zgubionej lub skradzionej karty odpowiada za wszystkie transakcje wykonane przez osoby nieuprawnione przed zastrzeżeniem karty do 150 euro, a po zastrzeżeniu nie ponosi już żadnej odpowiedzialności za wykonane utraconą kartą transakcje. Co prawda bank może odmówić odpowiedzialności za transakcje wykonane przed zastrzeżeniem karty, ale musi udowodnić we własnym zakresie, że klient umyślnie lub wskutek rażącego niedbalstwa naruszył zasady bezpieczeństwa (np. udostępniając PIN innym osobom). W przypadku transakcji zbliżeniowych do 50 zł, gdzie nie ma potrzeby podawania PIN-u, bank praktycznie nie ma możliwości udowodnienia naruszenia zasad przez klienta (chyba że posłuży się obrazem np. z kamery przy kasie, gdzie widać, że klient sam dokonuje transakcji, którą potem reklamuje). Transakcje zbliżeniowe można zatem uznać za bezpieczniejsze, bo bank ma małą szanse na uchylenie się od odpowiedzialności za transakcje powyżej 150 euro. W przypadku transakcji potwierdzonych PIN-em znajomość PIN-u przez osobę nieuprawnioną jest silnym argumentem

dla banku, że klient naruszył zasady bezpieczeństwa, udostępniając swój PIN innym osobom. W przypadku w/w transakcji zbliżeniowych bez PIN-u ten argument odpada i klient ma pewność, że nie straci więcej niż 150 euro wskutek utraty instrumentu płatniczego.

Kultura bezpieczeństwa w odniesieniu do tego ryzyka powinna polegać na promowaniu wypracowania, a następnie przestrzegania pewnych nawyków zachowania. Po pierwsze, nie wolno udostępniać PIN-ów innym, nawet bliskim osobom. PIN może służyć tylko posiadaczowi karty. Nie wolno go zapisywać, szczególnie w jawnej formie i w miejscach dostępnych innym. Kartę płatniczą, po wykonaniu transakcji, należy chować w jedno określone miejsce, kontrolować obecność tej karty w pewnych odstępach czasu (np. po zakończeniu zakupów, po dotarciu do samochodu, po powrocie do domu), tak aby możliwie szybko wykryć kradzież lub zgubienie karty i dokonać zgłoszenia tego faktu bez zwlekania, w nadziei że karta znajdzie się w innym niż zwyczajowe miejscu. Można przedsięwziąć też inne środki ostrożności, np. ustawić limit ilościowy lub/i wartościowy wykonywanych dziennie transakcji czy ustawić powiadomienia o dokonywanych transakcjach za pomocą sms-ów na zaufany numer telefonu. W przypadku dokonywania transakcji (np. przelewów) przy użyciu bankowości internetowej należy dbać o zabezpieczenie komputera programem antywirusowym, nie logować się do stron banku za pomocą podstawionego linku (np. przesłanego w mailu), nie podawać swoich danych, a szczególnie PIN-u osobom dzwoniącym i podszywającym się za pracowników banku lub innych instytucji publicznych. Świadomość zagrożeń oraz właściwe nawyki zmniejszają ryzyko utraty środków, szczególnie w sytuacjach niezawinionych przez klienta.

Ryzyko społeczne związane jest ze społecznym postrzeganiem zakupu, użytkowania lub zachowań z tym związanych. Używanie nowoczesnych produktów, do jakich należą płatności bezgotówkowe, powinno dawać prestiż. Pozornie zła ocena społeczna jest więc mało prawdopodobna. Takie spojrzenie może być jednak mylne – w grupach preferujących konserwatywne zachowania używanie nowoczesnych produktów może być postrzegane jako „zdrada grupy" lub jako niepotrzebne narażanie się na niebezpieczeństwo, szczególnie w przypadku braku zrozumienia zagrożeń i niewspółmiernego ich wyolbrzymiania. Wówczas strach przed złą oceną grupy, w której uczestniczy potencjalny klient, może powstrzymywać przed zaakceptowaniem nowości. Może też prowadzić do ukrywania użytkowania produktu, a wskutek tego do zaniedbywania pewnych zasad bezpieczeństwa.

Subiektywnie uświadamiane **ryzyko psychologiczne** związane z odbiorem własnych działań z jednej strony może powstrzymywać przed zakupem i użytkowaniem produktu, z drugiej zaś może przyczynić się do poprawy bezpieczeństwa i eliminacji niektórych zagrożeń. Wewnętrzna niechęć czy zmniejszona akceptacja produktu przy konieczności jego użytkowania (np. wskutek przymusu narzuconego przez pracodawcę) powinna przyczyniać się do przestrzegania zasad bezpieczeństwa nawet w stopniu wyższym niż bez uświadamiana sobie ryzyka psychologicznego. Poziom ryzyka psychologicznego jest często zależny od osobowości klienta. Osobowości introwertyczne, skupione na sobie, w większym stopniu obawiają się popełnienia błędu, niewłaściwego użytkowania i wynikającej stąd straty. Działania związane z kulturą bezpieczeństwa powinny koncentrować się na właściwym „naświetlaniu" zagrożeń. Nieprawdziwe (wyimaginowane) lub przesadzone zagrożenia

powinny być obalane poprzez skierowaną docelowo edukację, przy równoczesnym potwierdzaniu i podawaniu właściwych sposobów eliminacji lub minimalizowania rzeczywistych zagrożeń.

Ryzyko finansowe dla finansowych produktów płatniczych jest ścisłe powiązane z ryzykiem funkcjonalnym i fizycznym. Brak umiejętności posługiwania się produktami finansowymi (ryzyko funkcjonalne) zwiększa możliwość narażenia się na kradzież, napaść w sensie fizycznym lub cybernetycznym (ryzyko fizyczne). Stwarza to możliwość utraty środków z konta, niewłaściwego przekierowania transakcji. Ryzyko finansowe jest jednak znacznie szersze. Klient może mieć poczucie, że ponoszone jednorazowe lub okresowe opłaty za produkt są niepotrzebnym kosztem lub są za wysokie w stosunku do korzyści, jakie generuje produkt. Wynikać to może z niedostrzegania lub umniejszania takich korzyści jak lepsza ochrona środków niż w przypadku noszonej gotówki, łatwiejszy dostęp do środków o każdej porze doby, regulacje związane z przejęciem odpowiedzialności przez bank w sytuacjach zgubienia i kradzieży kart płatniczych. Minimalizowanie ryzyka finansowego idzie w parze ze wspominanymi wcześniej działaniami w zakresie ryzyka funkcjonalnego oraz fizycznego z jednoczesnym wskazywaniem korzyści płynących z zastosowania nowoczesnych produktów i kanałów płatniczych.

Ryzyko straty czasu charakterystyczne jest dla etapu wyboru produktu i uczenia się jego funkcji oraz sposobu użytkowania. Rolą nowoczesnych produktów finansowych, które zapewniają dostęp elektroniczny do szerokiej gamy usług, jest właśnie minimalizowanie czasu potrzebnego na kontakt z instytucją finansową. Dostrzeżenie takich możliwości samo w sobie będzie minimalizacją wspomnianego ryzyka. Umiejętność przedstawienia sposobu, w jaki produkty finansowe oszczędzają czas ich użytkownika, może być trudne w stosunku do klientów, dla których czas nie jest istotna wartością. Wykluczenie cyfrowe i finansowe dotyka głównie osoby, które nie wykorzystują intensywnie czasu w aktywności zawodowej lub spędzaniu wolnego czasu. Kluczowym może być przedstawienie ryzyka straty czasu jako odwróconego ryzyka społecznego. Presja na dotrzymanie kroku przemianom w zachowanych społecznych, naśladowanie rodziny, otoczenia lub liderów może wyeliminować ryzyko straty czasu w adaptowaniu nowych produktów do własnych zachowań i wyrabianiu sobie nowych nawyków.

Ryzyko utraconych możliwości wynika ze świadomości tego, że wybierając jeden produkt, rezygnujemy z innych. Posługiwanie się bezgotówkowymi formami płatności i ogólniej – elektronicznymi instrumentami płatniczymi daje dostęp do bardziej rozbudowanej oferty, która często zawiera w sobie inne elementy. Umiejętne uświadomienie tego powinno zredukować omawiane ryzyko, bez narażenia się na niebezpieczeństwo wybrania nieodpowiedniego produktu.

Inne ryzyka dotyczące bezpośrednio instytucji finansowych, a tylko pośrednio klientów są dla klientów indywidualnych w zasadzie niemożliwe do zredukowania. Ważną kwestią jest raczej ich rozumienie w kontekście podejmowania decyzji zakupowych. Ryzyka systemowe, rynkowe, stopy procentowej i inflacji, obejmujące możliwości zakłóceń na rynkach finansowych, dotknąć może wszystkich obszarów funkcjonowania rynku. Najskuteczniejszym działaniem ograniczającym te ryzyka jest dywersyfikacja instytucjonalna (wybór kilku instytucji, z których korzysta równocześnie klient), dywersyfikacja produktowa (w zakresie ryzyka inwestycyjnego,

płynności) oraz śledzenie wydarzeń wpływających na stabilność ekonomiczną w wymiarze lokalnym i globalnym, analiza trendów rynkowych, branżowych.

Ryzyko kredytowe, utraty płynności i walutowe po stronie klienta indywidualnego obejmuje nadmierne zadłużenie się, utratę możliwości spłaty rat kredytowych wskutek spadku lub przesunięcia w czasie dochodów oraz wzrostu wartości waluty kredytu innej niż dochody kredytobiorcy. Ryzyka te są ograniczane systemowo przez instytucje nadzoru poprzez rekomendacje (np. S,T, wydane przez Komitet Nadzoru Finansowego – KNF) oraz akty prawne (ustawy o kredycie konsumenckim i hipotecznym). Klient powinien mieć natomiast świadomość i wiedzę na temat funkcjonowania poszczególnych produktów, jak również umiejętność wyboru najkorzystniejszego wariantu z punktu widzenia własnych korzyści i ograniczeń. Przykładowo – przy nieco większej zdolności kredytowej zawsze korzystniejszy dla klienta jest kredyt o malejącej sumie rat kapitałowej i odsetkowej od kredytu o stałej spłacie. W tym pierwszym przypadku koszt kredytu jest zawsze niższy mimo wyższej spłat na początku, co wymaga właśnie nieco wyższej zdolności kredytowej. Inna korzyścią jest zmniejszenie spłat w kolejnych okresach kiedy sytuacja finansowa klienta może ulec zmianie. Banki podsuwają jednak klientom z reguły wariant stałej raty kapitałowej i odsetkowej ze względu na własną korzyść – wyższe wpływy w całym okresie spłaty kredytu.

Ryzyko cybernetyczne związane jest z rosnącym udziałem zbierania i przetwarzania danych finansowych przez systemy komputerowe oraz przesyłanie ich w sieciach lokalnych i globalnych. Ryzyko to może dotyczyć zarówno instytucji finansowych, jak i poszczególnych klientów. Dla tych ostatnich ryzyko to mieści się w ramach ryzyka funkcjonalnego i fizycznego opisanego wcześniej. Instytucje finansowe zmniejszają to ryzyko poprzez korzystanie z usług profesjonalnego personelu informatycznego oraz firm zewnętrznych. O skali tego zagrożenia oraz możliwości ubezpieczenia się od ryzyka cybernetycznego na polskim rynku szerzej pisze Grzegorz Strupczewski[18].

Ryzyko prawne w większej mierze dotyczy funkcjonowania instytucji finansowych. Zmiany prawne mogą dotknąć także klientów indywidualnych, ale najczęściej instytucje finansowe są zobowiązane lub z własnej inicjatywy informują klientów o dotykających ich zmianach. Rozwiązania prawne sprzyjają ochronie konsumentów, działa też Rzecznik Finansowy konsumentów oraz UOKiK, do których można zwrócić się po poradę lub interwencję w konkretnych sprawach.

Synteza elementów kultury bezpieczeństwa w reakcji na ryzyka

Klient instytucji finansowych w praktyce nie dzieli ryzyka na poszczególne kategorie i ich zazwyczaj nie odróżnia. Ważne jest dla niego całościowe poczucie bezpieczeństwa bez wnikania, jakie elementy na to wpływają. Postrzeganie bezpieczeństwa

[18] G. Strupczewski, *Zagrożenia cybernetyczne instytucji finansowych*, „Rozprawy Ubezpieczeniowe. Konsument Na Rynku Usług Finansowych / Journal of Insurance, Financial Markets and Consumer Protection" 2017, no. 2 (24), s. 65–83.

przez klienta odbywa się raczej przez sytuacje, w jakich może się znaleźć, użytkując dany produkt, porównywanych z korzyściami możliwymi do uzyskania. Klient zazwyczaj wyobraża sobie pewne korzyści, które chciałby uzyskać. Jedną z najważniejszych korzyści używania nowoczesnych form komunikacji jest łatwiejszy dostęp do środków i możliwość zarządzania nimi (np. przelewy, zakup produktów) bez konieczności fizycznego kontaktu z instytucją finansową. Wielu klientów nie widzi potrzeby rezygnacji z dotychczasowych przyzwyczajeń płatniczych, gdyż są zadowoleni i przekonani o ich bezpiecznym używaniu. Nowe sposoby wymagają zmiany przyzwyczajeń, nauczenia się pewnych zasad i ich przestrzegania. Tworzenie kultury bezpieczeństwa wymaga więc współdziałania klientów, instytucji, nadzoru finansowego i państwa w zakresie tworzenia prawa dostosowanego do nowych uwarunkowań. Kultura bezpieczeństwa powinna być także wpisana w działania marketingowe instytucji i współtworzyć elementy społecznej odpowiedzialności biznesu.

Ilustracje tworzenia kultury bezpieczeństwa zarówno po stronie instytucji, jak i klienta można pokazać na procesie pozyskiwania nowego klienta, który wcześniej nie używał nowoczesnych produktów finansowych danej instytucji. Nowy produkt wirtualizujący zachowania klientów jest zazwyczaj wynikiem postępu technologicznego. Pozyskanie klienta odbywa się najczęściej poprzez interakcje tradycyjnego marketingu i oddziaływań społecznych. Potencjalny klient, obserwując swoje otoczenie, zauważa innowatorów, którzy najwcześniej adaptują do swoich zachowań nowe produkty. Proces ten występuje na wszystkich rynkach w mniejszym lub większym stopniu, ale w zakresie skomplikowanych produktów ma szczególne znaczenie. Tak zwana marketingowo większość (szczególnie późna) jest nieufna, nie rozumie funkcjonowania produktu lub nie widzi korzyści z jego zastosowania. Dużą barierą psychologiczną jest wówczas wspomniane wcześniej ryzyko straty czasu. Ludzie nie chcą poświęcić czasu na zapoznanie się z produktem, na jego zrozumienie i nauczenie się zasad bezpieczeństwa. Wśród innowatorów bariera ta jest mniejsza, co często wiąże się z większą skłonnością do ryzyka, otwartością na nowe idee (i wynikające stąd produkty i usługi), lepszym wykształceniem lub profesjonalnymi umiejętnościami. Zgodnie z klasycznymi zaleceniami marketingu na tym etapie najważniejsza jest informacja skierowana do wybranego grona potencjalnych użytkowników. Niewielka liczba użytkowników może dawać możliwość przetestowania wprowadzanego produktu i jego cech. W przypadku drogich produktów każdy użytkownik (lub określona grupa) może mieć na początku swojego „anioła stróża", który będzie monitorował skutki korzystania z produktu i ewentualne zagrożenia. W wielu przypadkach jest to możliwe ze względu na wirtualny charakter produktów funkcjonujących w sieci internetowej. Ważne jest wówczas zapewnienie klienta, że jego wrażliwe dane nie będą wykorzystane bez jego zgody lub, co gorsza, przeciwko niemu. Wymaga to stworzenia odpowiednich procedur. Korzyścią dla klienta jest wówczas poczucie bycia wyróżnionym jako ktoś, kim instytucja specjalnie się interesuje. Przykładowo: doradcy klientów posiadających prestiżowe karty płatnicze mogą zadzwonić do nich w celu osobistego potwierdzenia, w przypadku pojawienia w systemie podejrzanej, nietypowej lub o dużej wartości transakcji, wykonanej np. poza miejscem zamieszkania klienta, a w szczególności za granicą. W przypadku klienta „masowego" takie działania przejmują obecnie „inteligentne" systemy informatyczne, które uczą się typowych zachowań klientów i reagują na nietypowe.

Budowanie kultury bezpieczeństwa musi rozpocząć się już od pierwszego kontaktu z klientem. Klienci mają zazwyczaj świadomość pewnego przesłodzenia przekazów reklamowych, są one ponadto bezosobowe, skierowane co prawda do wszystkich lub określonej grupy, ale niekoniecznie osobiście do danego klienta. Personalny kontakt (np. w celu podpisania umowy) z pracownikiem instytucji finansowej (np. banku), skierowany jest natomiast do konkretnej osoby – pozostawia w pamięci klienta zazwyczaj pierwsze wrażenie, które może rzutować na jego późniejszą postawę bądź ocenę instytucji. Długie, niezrozumiałe umowy, pisane fachowym i niedostępnym dla laika językiem, a w szczególności przypisy drobnym drukiem, nawet mimo domniemanej zgody i pozorowanego zrozumienia mogą pozostawić u klienta złe wrażenie i podejrzenie chęci oszukania, co rodzi często nieufność i przekorę w przestrzeganiu procedur bezpieczeństwa opracowanych przez instytucje. Zbyt obszerne opisy zniechęcają do czytania i zwrócenia uwagi na to, co najistotniejsze z punktu widzenia bezpieczeństwa klienta. Takie najważniejsze informacje powinny być wydzielone w oddzielnym przekazie (jako dodatkowe, wybrane/ważne informacje) lub dobrze wyróżnione w ogólnym szerszym przekazie docierającym do klienta.

Najważniejszym elementom, stanowiącym o bezpieczeństwie klienta dokonującego transakcji za pomocą elektronicznych instrumentów płatniczych, poświęcono dalszą część artykułu.

Należy zachować bezwzględną konieczność nieudostępniania komukolwiek kodów, PIN-ów, haseł i innych danych koniecznych do logowania bądź potwierdzania wykonywanych operacji w urządzeniach elektronicznych. Informacje takie nie mogą być zapisywane i przechowywane, szczególnie w formie jawnej, niezakodowanej lub nieprzekształconej. Jeśli użytkownik chce zapisać takie informacje, powinien je zakodować – przekształcić w taką formę, aby jej odtworzenie było możliwe tylko dla niego na podstawie nieoczywistej prywatnej wiedzy, wynikającej np. z doświadczeń, wspomnień itp. Nawet tak przekształcone informacje nie mogą być zapisywane w bezpośrednim sąsiedztwie czy otoczeniu związanym z wykonywaniem transakcji. Należy pamiętać, że nikt, a w szczególności pracownicy instytucji finansowych (pod których najczęściej podszywają się oszuści) nie może żądać ujawnienia takich danych, nie można ich również przesyłać za pomocą maili, sms-ów i innych powszechnych form komunikacji niezwiązanych z wykonywaniem transakcji. O ile to możliwe, należy unikać logowania, wpisywania haseł i dokonywania operacji finansowych na publicznych urządzeniach, do których mają dostęp inni anonimowi użytkownicy. Mogą one być pod obserwacją kamer lub nielegalnie założonych nakładek, które potrafią odtworzyć sekwencje wpisywanych znaków po odejściu użytkownika od urządzenia. Najbezpieczniej jest więc dokonywać transakcji na prywatnych urządzeniach udostępnianych co najwyżej zaufanym osobom. Urządzenia takie powinny być chronione legalnym i aktualizowanym programem antywirusowym. W przypadku wykonywania transakcji w bankomatach, wpłatomatach i innych urządzeniach w miejscach publicznych należy zachować ostrożność, zwracając szczególną uwagę, czy ktoś niepowołany nie obserwuje lub nie nagrywa z bliskiej odległości wykonywanych czynności. Podejrzenie wzbudzić powinien też zmieniony wygląd urządzeń i ich nietypowe działanie. Należy wówczas zaniechać transakcji i zawiadomić bank lub policję o podejrzeniu oszustwa za pomocą takiego urządzenia.

W punktach usługowych karty płatnicze nie powinny być oddawane obsłudze w celu wykonania transakcji poza zasięgiem wzroku właściciela karty. Obecnie większość terminali płatniczych używanych w różnych miejscach jest bezprzewodowa, co umożliwia dostarczenie ich do rąk właściciela karty, a nie noszenie karty do terminala. Dzięki mikroprocesorom, w które wyposażone jest już większość kart płatniczych, ryzyko zeskanowania paska magnetycznego i wykonania dzięki temu transakcji bez wiedzy właściciela karty jest już wysoce ograniczone. Mogłoby się jednak zdarzyć, że nieuczciwy sprzedawca za pomocą wyniesionej karty dokona, zamiast jednej, kilku transakcji zbliżeniowych niewymagających potwierdzenia PIN-em.

Dobrym zabezpieczeniem i kontrolą dokonywania wydatków za pomocą kart płatniczych jest opcja dostępna w większości banków, polegająca na przesyłaniu sms-a na zdefiniowany numer telefonu po każdej transakcji (lub po transakcji powyżej określonej kwoty). Jest to dobre zabezpieczenie zwłaszcza w podróży, kiedy właściciel karty może być szczególnie narażony na ryzyko kradzieży i wolniejszą reakcję ze względu na nieznajomość okolic, barierę językową itp.

W przypadku płatności kartą poza granicami własnego kraju ryzyko finansowe polegać może na niekorzystnych kursach walutowych do przeliczenia transakcji z waluty, w której dokonywana jest płatność, na walutę, w której prowadzone jest konto. Minimalizacja takiego ryzyka może polegać na założeniu konta w walucie docelowej (np. euro), w której ktoś będzie płacił poza granicami kraju, na wydaniu karty tzw. wielowalutowej, która podpięta jest do kliku kont w różnych walutach i „sama" rozpoznaje, z którego konta należy pobrać środki. Obecnie terminale płatnicze oferują płatność w walucie kraju, z którego pochodzi karta płatnicza. Jest to tzw. dynamiczna konwersja walut (ang. DCC – Dynamic Currency Convertion). W przypadku karty podpiętej tylko do krajowej waluty najkorzystniej jest wybierać opcje płatności w walucie danego kraju, w którym dokonujemy transakcji, a nie w złotówkach. Należy więc unikać DCC, gdyż przewalutowanie odbywa się wówczas po kursie instytucji sprzedającej usługę lub towar bądź lokalnego banku, który właściwie nigdy nie jest lepszy dla klienta od przewalutowania przez Visa/Mastercard lub krajowy bank. Bankowi, który wydał kartę, bardziej zależy na zaufaniu klienta i jego lojalności niż bankowi zagranicznemu lub przypadkowej instytucji zagranicznej, która pośredniczy w pojedynczym, z punktu widzenia danego klienta, zakupie.

Innym ważnym zagadnieniem z perspektywy klientów jest kwestia komunikacji zbliżeniowej terminali płatniczych z kartami lub telefonami za pomocą technologii NFC. Wokół tego tematu narosło wiele mitów. Wiele osób sądzi, że posiadanie karty z funkcją zbliżeniową naraża ją na ściągnięcie środków z karty w tłoku (autobusie, tramwaju) bez wiedzy właściciela. W rzeczywistości takie działanie wymagałoby zbliżenia „złodziejskiego terminala" na odległość mniejszą niż 2–3 cm i manipulowanie urządzeniem (przy większych odległościach – 3–10 cm wymagałoby to już co najmniej kilkunastocentymetrowej anteny, która nie mogłaby ujść uwadze i która utrudniałaby manipulowanie urządzeniem). Karta trzymana w portfelu, torebce czy inaczej poprawnie zabezpieczona właściwie nie ma możliwości dostania się w zasięg takiego nieautoryzowanego urządzenia bez zwrócenia uwagi właściciela. Po drugie, urządzenie takie musiałoby być właśnie autoryzowane przez firmę pośredniczącą i zarejestrowane na określoną osobę lub firmę. Zakładając jednak nawet, że oszust jest w stanie stworzyć swoimi sposobami skomplikowane urządzenie, musiałby

przekazywać pieniądze na konkretne konto, które w systemach większości krajów nie może być anonimowe. Zgłoszenie przynajmniej jednej takiej transakcji dość szybko wpłynęłoby na zablokowanie takiego konta i dochodzenie, kto je wykorzystuje. Po trzecie, coraz częściej zbliżeniowe karty płatnicze stają się wirtualne i są generowane jako oprogramowanie telefonu. Można wówczas po wykonaniu transakcji wyłączyć w telefonie funkcje NFC, co całkowicie wyklucza transakcje zbliżeniowe.

Informacja o w/w i innych zagrożeniach oraz o możliwościach ich uniknięcia powinna być częścią polityki marketingowej instytucji finansowych. Powinny one używać łatwego języka i aparatu pojęciowego, słuchać opinii klientów nt. poprawy sposobów działania i wprowadzania ewentualnych modyfikacji. Równocześnie instytucje te powinny z własnej inicjatywy, a nie tylko pod wpływem wymuszenia w sytuacjach kryzysowych, poruszać drażliwe dla klientów zagadnienia. Omijanie czy zatajanie informacji, które pomogą klientowi zachowywać się zgodnie z własnym interesem, choćby miało to wpływ na zmniejszenie zysku banków, rodzi atmosferę nieufności i przyczynia się do postrzegania instytucji finansowych jako „wyzyskiwaczy i oszustów". Rodzi się wówczas potrzeba oszukania „oszusta", co może obrócić się zarówno przeciwko klientowi, jak i instytucji finansowej oraz spowodować że skorzystają na tym prawdziwi oszuści.

Stosunkowo nowym zjawiskiem finansowym, które pociąga za sobą wiele opisanych wcześniej form ryzyka, są wirtualne waluty. Najbardziej znaną z nich jest Bitcoin. Waluty te generowane są na podstawie wyszukanego algorytmu informatycznego. Nie podlegają nadzorowi żadnego z państw. Nie mają więc oparcia w realnych gospodarkach. Co prawda powstają w wyniku określonej pracy intelektualnej, ale ich łączna wartość znacznie przewyższa wartość podobnej zaawansowanej pracy na tradycyjnym rynku. Notowania wirtualnych walut są bardzo niestabilne. Zyskują one lub tracą w stosunku do tradycyjnych walut po kilkadziesiąt procent w ciągu kilku lub nawet jednego dnia. Są też wykorzystywane na opłacenie nielegalnych transakcji. Wady te wskazują. że zaangażowanie się w transakcje takimi walutami jest bardzo ryzykowne. Nie powinny tego robić osoby, dla których środki przeznaczane na kryptowaluty są niezbędne do codziennego życia. Rozpowszechnienie się tego typu walut stoi pod znakiem zapytania. Wśród zalet kryptowalut najważniejsza wydaje się być technologia, na której się opierają: tzw. rozproszony rejestr polega na rozpraszaniu informacji o dokonywanych transakcjach i stanie posiadania poszczególnych podmiotów. Kopie rejestrów, zabezpieczone kryptograficznie, przechowywane są w różnych węzłach sieci i żadna pojedyncza osoba lub instytucja nie ma nad nimi kontroli. Zdarzenia transakcyjne są więc nie do podrobienia, a informacja, kto dokonał transakcji, dzięki kodowaniu nie jest publiczne znana. Cechy te mogą być w przyszłości wykorzystywane m.in. do zabezpieczenia tradycyjnych transakcji finansowych opartych na tradycyjnych walutach emitowanych przez państwa. Pojawiają się próby połączenia walut tradycyjnych z nowymi lub istniejącymi już walutami wirtualnymi, nad którymi pewną kontrolę sprawować może państwo lub wiarygodne organizacje. Dla osób posiadających nadwyżki finansowe, których strata nie będzie miała istotnego wpływu na poziom życia i komfort psychiczny, inwestycja w kryptowaluty może być intersującym doświadczeniem, skłaniającym do obserwacji nowych trendów w dziedzinie technologii i finansów.

Zarządzanie procedurami bezpieczeństwa w instytucjach finansowych

Obserwacje wydarzeń związanych z sytuacjami kryzysowymi wskazują, że najsłabszym ogniwem w systemie najczęściej są ludzie – niestety, słabe, skomplikowane i nieprzejrzyste mogą być także procedury mające na celu ograniczenie możliwości popełnienia nieświadomych lub celowych błędów przez ludzi. Najogólniej mówiąc, procedury powinny być proste i czytelne, ale równocześnie na tyle dokładne, aby nie pozostawiały miejsca na swobodną interpretacje prowadzącą do wypaczeń lub obejścia elementów zapewniających prawidłowe funkcjonowanie danego systemu. Niezwykle ważne jest także aktualizowanie procedur i zasad pod szybko zmieniające się produkty i technologie.

Nowe badania dotyczące tzw. teorii racjonalnej nieuwagi (ang. *rational inattention*) wskazują, że konsumenci nie uwzględniają w swoich decyzjach wszystkich ważnych informacji i zmian, bo koszt tego byłby wyższy niż straty z tytułu ich nieuwzględnienia[19]. Teoria ta ma zastosowanie do badania reakcji na zmianę parametrów finansowych (np. stóp procentowych), ale można ją zastosować do ignorowania niektórych procedur bezpieczeństwa. Użytkownikom wydaje się, że nie ma potrzeby zwracania uwagi na nowe niebezpieczeństwa i sposoby ochrony przed nimi. Aktualizacje procedur bezpieczeństwa powinny być więc automatyczne i w pewnym sensie narzucane klientom. Dobrą zasadą jest tu podejście tzw. *opt-out*, polegające na tym, że przyjęcie określonego działania nie wymaga żadnej reakcji klienta/decydenta. Jeśli ten chciałby jednak odrzucić sugerowane zachowanie (np. instalację uaktualnienia), musi podjąć pewne aktywne działania. Ekonomia behawioralna wskazuje, że większość ludzi unika podejmowania dodatkowych działań i ma większą skłonność do przyjmowania sugerowanego rozwiązania, jeśli nie wymaga to od nich żadnego wysiłku czy dodatkowych działań. Równocześnie należy zabezpieczyć klientów przed podszywaniem się oszustów pod prawdziwą instytucję, tak aby nie byli oni narażeni na pokusę akceptacji podsuniętego fałszywego oprogramowania, przesyłania danych lub środków podejrzanym instytucjom. Oprogramowanie musi być tak skonstruowane, aby jego aktualizacja możliwa była tylko dla właściwej instytucji (posiadającej np. kody zabezpieczeń przed nieautoryzowaną aktualizacją). Klienci powinni z kolej mieć świadomość, że nie wolno wchodzić na strony instytucji finansowych z przesłanych w mailach lub inaczej dostarczonych linków. Powinni zwracać uwagę na tzw. „kłódkę" bezpiecznego połączenia i nie logować się na publicznie dostępnych urządzeniach.

W przypadku zaistnienia sytuacji kryzysowej klienci powinni być szybko i rzetelnie poinformowani o przyczynach i skutkach ograniczeń, tak aby uniemożliwić paniczne reakcje, wynikające z braku informacji lub rozprzestrzeniających się szybko plotek. Informacja powinna zawierać przede wszystkim przewidywany czas ograniczeń (np. braku dostępu do konta) oraz sposób radzenia sobie z niedogodnościami.

---

[19] P. Bacchetta, E. van Wincoop, *Rational Inattention: A Solution To The Forward Discount Puzzle*, "Working Paper" 2005, 11633 National Bureau of Economic Research; http://www.Nber.Org/Papers/W11633 [dostęp: 9.09.2018].

Statystyki oszustw w Polsce wskazują, że jesteśmy jednym z bezpieczniejszych rynków na świecie. „W II półroczu 2017 r. oszukańcze operacje kartowe stanowiły 0,002% liczby i 0,005% wartości wszystkich transakcji dokonanych kartami płatniczymi wydanymi przez raportujące do NBP banki (w poprzednim półroczu zanotowano odpowiednio 0,003% i 0,004%)”[20]. Dane te obejmują transakcje oszukańcze w kraju i za granicą kartami wydanymi w Polsce, nie obejmują jednak transakcji oszukańczych dokonanych w Polsce kartami wydanymi w innych krajach. Nieco inne wartości prezentują agenci rozliczeniowi, którzy podają dane dot. transakcji oszukańczych dokonanych tylko w Polsce, niezależnie od miejsca wydania karty. „Transakcje oszukańcze wg danych przekazywanych przez agentów rozliczeniowych stanowiły 0,001% ogólnej liczby i 0,008% wartości transakcji kartami płatniczymi, obsługiwanych przez agentów rozliczeniowych (w poprzednim półroczu było to 0,001% ogólnej liczby i 0,01% wartości transakcji)”[21]. W obu przypadkach odsetki te wskazują, że transakcje oszukańcze stanowią bardzo niewielki promil rynku (kilka setnych promila). Dane NBP są warte większej uwagi z punktu widzenia polskiego klienta rynku finansowego, gdyż dotyczą instrumentów płatniczych wydanych w Polsce. W liczbach bezwzględnych liczba transakcji oszukańczych (wg NBP) w całym 2017 r. wynosiła ok. 120 tys. sztuk, a ich wartość ok. 30 mln zł, co wskazuje, że przeciętna transakcja oszukańcza miała wartość ok 250 zł. Dane te wskazują, że przy zachowaniu podstawowych wymogów bezpieczeństwa prawdopodobieństwo stania się ofiarą oszustwa jest znikome, a transakcje te są raczej o małej wartości, niezagrażającej stabilności finansowej przeciętnego konsumenta.

Podsumowanie

Szybki rozwój rynku finansowego w Polsce na początku lat 90. XX wieku, przy równoczesnym braku szczegółowych uregulowań prawnych i doświadczenia w zakresie dobrych praktyk oraz edukacji ekonomicznej klientów spowodował powstanie wielu zagrożeń o charakterze mikro- i makroekonomicznym. Na przestrzeni prawie 30 lat zaowocowało to kilkoma dużymi aferami finansowymi (np. krach na Giełdzie Papierów Wartościowych w Warszawie w 1994 r. powiązany z niefortunną prywatyzacją Banku Śląskiego, upadek kilku banków, w tym spółdzielczych i SKOK-ów, afera AmberGold, GetBack). Mimo początkowego stosunkowo chaotycznego rozwoju rynku powstawały kolejne regulacje prawne porządkujące rynek i zwiększające bezpieczeństwo uczestnictwa w systemie zarówno dla instytucji jak i klientów. Na szczęście żadna z afer nie zachwiała w sposób istotny całością polskiego systemu finansowego. W tej dziedzinie Polska stosunkowo dobrze przeszła zawirowania światowego kryzysu finansowego, który rozpoczął się w 2007 r. Obecnie nie widać większych całościowych zagrożeń dla rynku finansowego, a polski system giełdowy, ubezpieczeniowy i bankowy nie odbiega od standardów europejskich. Jak wskazują dane NBP, ryzyko padnięcia ofiarą przestępstw związanych z płatnościami

[20] *Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2017 r.*, Departament systemu Płatniczego NBP, Warszawa, maj 2018, s. 107.

[21] *Ibidem*, s. 109.

bezgotówkowymi jest w Polsce niewielkie. Ofiarami takich przestępstw stają się w większości przypadków osoby nieprzestrzegające podstawowych reguł bezpieczeństwa. Istnieje oczywiście szansa stania się ofiarą przestępstwa mimo przestrzegania wszystkich reguł, ale straty z tego tytułu, jak opisano powyżej, są dla klienta instytucji finansowych niewielkie.

Przedstawiona koncepcja i elementy kultury bezpieczeństwa powinny być wdrażane przez instytucje nadzorcze i finansowe oraz rozumiane, i przestrzegane przez klientów. Pozwoli to zmniejszyć poszczególne ryzyka i sprawić, że wzrośnie poczucie bezpieczeństwa wśród uczestników szeroko rozumianego rynku finansowego.

Elementy kultury bezpieczeństwa a zachowania klientów instytucji finansowych
Streszczenie

Artykuł omawia ryzyka i zagrożenia towarzyszące zachowaniom klientów instytucji finansowych. Szczególne miejsce poświęcono nowym technologiom wykorzystywanym w instrumentach płatniczych. Wskazano, jak różnicować działania instytucji finansowych zapewniające bezpieczeństwo w zależności od postaw klientów i cyklu życia produktu. Podano ogólne zasady zarządzania procedurami bezpieczeństwa w instytucjach finansowych. Na końcu przedstawiono wybrane statystyki dotyczące oszustw z wykorzystaniem kart płatniczych.

Słowa kluczowe: zachowania finansowe, zarządzanie finansami osobistymi, ryzyko finansowe

Elements of security culture, and the behaviour patterns of financial institutions clients
Abstract

The paper looks at the risks and threats that accompany the behaviour of clients of financial institutions. It puts emphasis on the variety of modern technologies used for payment and indicates how to differentiate the activities of financial institutions that provide security, depending on the attitudes of the clients, and the life cycle of a given product. The paper also discusses the general principles of managing security procedures in financial institutions and concludes with an overview of selected statistics on fraud committed with the use of payment cards.

Key words: financial behaviour, personal finance management, financial risk

Элементы культуры безопасности и поведение клиентов финансовых учреждений
Резюме

В статье рассматриваются риски и угрозы, характерные поведению клиентов финансовых учреждений. Особое внимание уделено новым технологиям, используемых в платежных инструментах. Указано, как диверсифицировать деятельность финансовых институтов, обеспечивающих безопасность, в зависимости от действий клиентов и цикла существования продукта. Приведены общие принципы управления

процедурами безопасности в финансовых учреждениях. В заключении представлены некоторые статистические данные касающиеся мошенничества с использованием платежных карт.
Ключевые слова: финансовое поведение, управление персональными финансами, финансовые риски