Uniwersytet Ekonomiczny w Katowicach

Wydział Informatyki i Komunikacji

Kierunek: *Informatyka i ekonometria*

***Aneta Rycko***

# *Analiza bezpieczeństwa finansowego w bankowości elektronicznej*

# *Analysis of the financial security in the e-banking*

Praca magisterska
napisana w Katedrze *Informatyki*
pod kierunkiem *dr Artura Strzeleckiego*

*Pracę przyjmuję i wnioskuję o jej dopuszczenie do dalszych etapów postępowania egzaminacyjnego*

…… ……..
*(data)* *(podpis promotora pracy licencjackiej / magisterskiej)*

**KATOWICE *2016***

Katowice, dnia .....

.....Aneta Rycko.....
Imię i nazwisko

....Informatyki i komunikacji....
Wydział

...Informatyka i ekonometria....
Kierunek

**OŚWIADCZENIE**

Świadoma odpowiedzialności prawnej oświadczam, że złożona praca magisterska pt.:
*„Analiza bezpieczeństwa finansowego w bankowości elektronicznej”*
została napisana przeze mnie samodzielnie.

Równocześnie oświadczam, że praca ta nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. 1994, nr 24, poz. 83) oraz dóbr osobistych chronionych prawem.

Ponadto praca nie zawiera informacji i danych uzyskanych w sposób nielegalny i nie była wcześniej przedmiotem innych procedur związanych z uzyskaniem dyplomów lub tytułów zawodowych uczelni wyższej.

Wyrażam zgodę na przetwarzanie moich danych osobowych oraz nieodpłatne udostępnienie mojej pracy w celu oceny samodzielności jej przygotowania przez system elektronicznego porównywania tekstów oraz przechowywania jej w bazie danych tego systemu.

Oświadczam także, że wersja pracy znajdująca się na przedłożonej przez mnie płycie CD jest zgodna z wydrukiem komputerowym pracy.

.....
(podpis składającego oświadczenie)

# Spis treści

# Wstęp

Pierwsze wzmianki dotyczące banków sięgają czasów starożytnych, a istnienie obrotu pieniądza dłużnego znane jest od chwili jego powstania. Tzw. „domy bankowe" występujące w Babilonie znajdowały się najczęściej w świątyniach, co miało gwarantować bezpieczeństwo i wypłacalność. Pierwsze historyczne zetknięcie z bankowością europejską wiąże się ze skandalem, opisanym w IVw. p.n.e., w dziele „Trapesitica" przez Isokratesa. Bronił on faworyta bosforskiego króla Satyrosa, którego pieniądze zostały powierzone ateńskiemu bankierowi, będącym byłym niewolnikiem Pasion. Sprzeniewierzył on otrzymane pieniądze, przez co został oskarżony. Początkowo popłakał się, jednocześnie przyznając do winy i obiecując zwrócić złoto. Później jednak odwołał zeznania, sfałszował dokumenty i zatarł wszelkie ślady swojej winy. Na dzień dzisiejszy wiadomo, że wspomniany Pasion w chwili śmierci nie tylko uniknął wszystkich swoich długów, co więcej, dorobił się 60 talentów, dzięki którym, aktualnie uznawany byłby za multimilionera[1].

Z biegiem czasu zmieniała się forma banków, zakres ich działalności, możliwości oraz oferowanej funkcjonalności. Wciąż postępujący rozwój technologiczny przyczynia się do różnego rodzaju pozytywnych przemian, dzięki którym usługi bankowości dostosowywane są do aktualnych potrzeb jej klientów. Jak jednak wskazuje wyżej przytoczona historia, zagrożenia w bankowości występują od samego jej początku. Rozwój technologiczny wymusza niejako konieczność pokonywania nowych zabezpieczeń i zmian form ataku. Natomiast najczęstszy aktualnie aspekt zysków finansowych, pozostaje niezmiennym od lat motywów.

Celem pracy jest przybliżenie tematyki bankowości, obecnej w codziennym życiu przeciętnego człowieka, ze szczególnym uwzględnieniem zagrożeń występujących w coraz popularniejszej bankowości elektronicznej, pod postacią najczęściej wykorzystywanej bankowości internetowej, terminalowej i telefonicznej, jak również przedstawienie możliwości zapobiegania tym naruszeniom i zachowania bezpieczeństwa.

Tezą niniejszej pracy jest stwierdzenie wciąż niskiego poziomu świadomości klientów bankowości elektronicznej w zakresie występujących zagrożeń oraz zasad właściwego zachowania, przez co niezbędne jest uzmysłowienie ryzyka i ciągła edukacja w tej tematyce.

[1] Jerzy Besala, Historia banków i bankierów, [data dostępu: 9 maja 2016], <http://www.polityka.pl/tygodnikpolityka/historia/1523347,1,historia-bankow-i-bankierow.read>.

Przedmiotem pracy jest grupa 65 anonimowych ankietowanych, będących klientami tradycyjnej bankowości. Respondenci charakteryzują się zróżnicowanym wiekiem, poziomem wykształcenia, miejscem zamieszkania oraz doświadczeniem w obsłudze komputera i dostępnych im usług bankowości.

Aby możliwe było jak najlepsze zrozumienie zagrożeń, pierwszy rozdział przedstawia ogólną charakterystykę bankowości elektronicznej, z uwzględnieniem jej tradycyjnych aspektów, w oparciu o podstawowe zagadnienia wraz z ich typowymi cechami i funkcjonalnością. Przybliżono również właściwości i funkcjonalność systemów informatycznych występujących w bankowości, pamiętając o jej niezbędnych elementach: architekturze, użytkownikach i dokumentacji. W dalszej części rozdziału, opisano szczegółowo dostępne elektroniczne instrumenty płatnicze oraz kanały bankowości elektronicznej, które wykorzystywane są podczas wszelkiego rodzaju ataków.

Rozdział drugi skupia się na zagrożeniach, na jakie narażony jest przeciętny użytkownik bankowości elektronicznej. Przybliża profil cyberprzestępcy, co ułatwia określenie cech charakterystycznych zagrożeń ogólnych. W dalszej części rozdziału, wyczerpująco przedstawiono zagrożenia występujące w bankowości elektronicznej z podziałem na zagrożenia specyficzne dla: bankowości internetowej, terminalowej i telefonicznej oraz ze szczególnym uwzględnieniem danych osobowych i wartości jaką stanowią w kontekście całej bankowości.

Trzeci rozdział, w całości dotyczy przeprowadzonego badania ankietowego pt. „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością”. Zawiera prezentację i przedstawia analizę uzyskanych wyników, będących kontynuacją i potwierdzeniem zagadnień poruszanych w rozdziale poprzednim.

Czwarty rozdział porusza problematykę związaną z zapobieganiem naruszeń i zachowaniem zasad bezpieczeństwa w zakresie bankowości elektronicznej. Również metody ochrony zostały przedstawione w formie podziału na bankowość internetową, terminalową i telefoniczną, co pozwoliło na dostosowanie metod ochrony do konkretnych zagrożeń przedstawionych w poprzednich rozdziałach.

Wnioski końcowe zawarto w zakończeniu pracy.

Pracę pisano w oparciu o pozycje książkowe w języku polskim i angielskim, materiały konferencji krajowych i zagranicznych oraz materiały pozyskane z sieci Internet. W procesie realizacji ankiety internetowej wykorzystano formularz Google, przeznaczony do tworzenia i przeprowadzania ankiet, udostępniony przez Gmail.com.

# Rozdział I
# Charakterystyka bankowości elektronicznej z uwzględnieniem jej tradycyjnych aspektów

Na co dzień, spotyka się wiele sprzecznych ze sobą opinii, dotyczących początków bankowości internetowej. Najczęściej jednak, przypisuje się je Stanom Zjednoczonym, gdzie w 1994 roku kalifornijski La Jolla Bank FSB, jako pierwszy udostępnił swoim klientom możliwość przeprowadzania transakcji, dzięki wykorzystaniu sieci Internet[2]. Od tamtego wydarzenia, bankowość na świecie, a tym samym i w Polsce (od października 1998 roku, Powszechny Bank Gospodarczy w Łodzi[3]), poczyniła ogromne postępy w zakresie wykorzystania sieci i dostosowania funkcjonalności banków do potrzeb klientów indywidualnych oraz firm. Aktualnie, jak prezentuje najnowszy raport NetB@nk opublikowany przez Związek Banków Polskich, dostęp do usług bankowości internetowej w Polsce, posiada ponad 27 milionów klientów. Oznacza to, iż w ciągu roku, liczba indywidualnych klientów, którzy posiadają umowy pozwalające na dostęp do usług bankowości internetowej wzrosła o prawie 4 mln (16,77%). Wzrost odnotowała również liczba aktywnych klientów, czyli osób logujących się w systemach bankowości internetowej przynajmniej raz w miesiącu i wyniósł ponad 1,2 mln (10,07%) w ciągu roku[4]. Przedstawione dane, jednoznacznie wskazują na ciągle rosnące zainteresowanie klientów bankowością elektroniczną. Czym zatem jest owa bankowość? Jakie jej formy zostały wyróżnione oraz kim jest standardowy klient i jakie korzyści można zyskać za sprawą bankowości internetowej?

W rozdziale pierwszym podjęto próbę wyjaśnienia podstawowych zagadnień związanych z bankowością elektroniczną oraz tradycyjną. Charakterystykę bankowości uzupełniono o niezwykle istotną problematykę elektronicznych instrumentów płatniczych oraz kanałów dystrybucji bankowości elektronicznej.

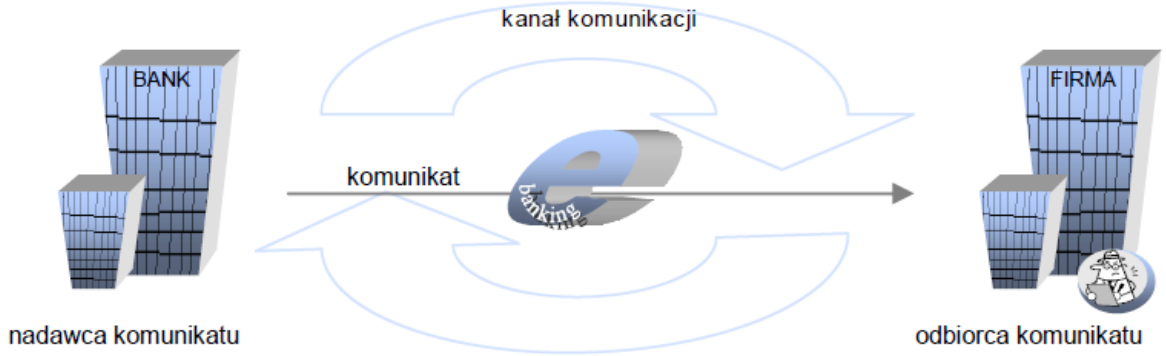
[2] Emil Ślązak, Elżbieta Guzek, *Innowacyjna bankowość internetowa*, Warszawa 2012, s. 29-30.
[3] *Ibidem*, s. 32.
[4] Związek Banków Polskich, *Raport NetB@nk: Dostęp do e-bankowości – kolejny rekord*, [data dostępu: 24 października 2015], < https://zbp.pl/dla-prasy/informacje-prasowe/raport-netb-nk-dostep-do-e-bankowosci-kolejny-rekord>.

## 1.1. Zarys bankowości w oparciu o definicję, typowe cechy oraz funkcjonalność

Podejmując próbę przedstawienia złożoności tematyki bankowości, w możliwie jak najprostszy sposób, warto na wstępie nakreślić ogólny zakres wraz z ideą bankowości elektronicznej, który sprowadza się głównie do teleinformatycznego (oprogramowanie, sprzęt, sieci) wspomagania procesów łączności pomiędzy[5]:

- klientem a bankiem,
- różnego rodzaju kontrahentami (klient, sprzedawca) za pośrednictwem banku lub instytucji parabankowych,
- bankami lub ich wewnętrznymi elementami organizacyjnymi,
- Innymi instytucjami finansowymi a bankami.

Bank, podczas świadczenia swoich usług finansowych konkretnym odbiorcom, bierze udział w procesie komunikowania się. Rysunek nr 1 przedstawia najprostszy model procesu komunikacji.




Rysunek 1. Model procesu komunikacji banku z odbiorcą usług.

*Źródło: Katarzyna Korzeń: Bankowość elektroniczna jako kanał dystrybucji usług bankowych.*

Komunikat, którym przykładowo może być oferta świadczonej przez bank usługi, powinien być dostarczony ze strony nadawcy, konkretnemu odbiorcy odpowiednim kanałem, czyli środkiem komunikowania się. Wszystkie usługi, których realizacja wykonywana jest za pośrednictwem biznesowych i technologicznych rozwiązań, przy dodatkowym wykorzystaniu różnych urządzeń wraz z wymianą informacji drogą elektroniczną, nazywane są bankowością elektroniczną[6]. Oczywistym jest, iż towarzyszy jej również w całości elektroniczna obsługa klienta, która wiąże się z wprowadzeniem interesanta do systemu bankowego w skomputeryzowanej wersji. Jednocześnie wykorzystuje się atrybut *customer-driven*,

[5] Witold Chmielarz, *Systemy elektronicznej bankowości*, Warszawa 2005, s. 13.
[6] Arkadiusz Jurkowski, *Bankowość elektroniczna, Zeszyt nr 125*, Warszawa 2001, s. 8.

co oznacza, że to sam klient inicjuje operację w systemie bankowym, w „punkcie wywołania" znajdującym się z dala od siedziby banku[7]. Fundamentalną koncepcję stanowi stworzenie systemu realizującego rozliczenia finansowe, pozwalające na obrót pieniężny bez pośrednictwa mediów papierowych, które zastąpione zostały „zespołem środków techniczno-informatycznych, magnetycznych, elektronicznych i teletransmisji"[8], zwanym pieniądzem elektronicznym.

Ze względu na teletransmisyjny charakter komunikacji elementów organizacyjnych wewnątrz banku oraz łączność z zewnętrznym środowiskiem, wszelkie dane przechowuje się i przetwarza w bazach danych systemu informatycznego, którego zadaniem jest wspomaganie działań sprzyjających poprawnemu zarządzaniu bankiem. Taki sposób komunikacji jest elementem technologii EDI (ang. Electronic Data Interchange), czyli Elektronicznej Wymiany Danych[9]. Polega na elektronicznej wymianie dokumentów, których formatowanie powinno odpowiadać obowiązującym standardom transmisji danych. Aktualnie za najpopularniejszy na świecie standard uznaje się EDIFACT (ang. Electronic Data Interchange For Administration, Commerce and Transport)[10]. Wymiana realizowana jest z wykorzystaniem komputera oraz przy możliwie najmniejszym udziale człowieka[11]. Wdrażane procesy służą przyspieszeniu i usprawnieniu obiegu pieniądza bezgotówkowego, zarówno w tradycyjnych, jak również w nowoczesnych systemach rozliczeń, rozliczeń międzybankowych, a także rozliczeń między klientem a bankiem[12].

Mimo, iż bankowość elektroniczna nie jest nowym pojęciem, wciąż trudno o jednoznaczną definicję, wyczerpującą istotę zagadnienia. Narastające z biegiem czasu komplikacje terminologiczne, wynikają przede wszystkim z nieustającej ewolucji kanałów dystrybucji usług bankowych, a także z szybkości następowania zmian społeczno-ekonomicznych, które są różnorodne i wielokierunkowe. Również zróżnicowane spojrzenie poszczególnych ekspertów, ich indywidualne doświadczenia i zdobyta z biegiem czasu wiedza, wpływają na brak jednolitej definicji bankowości elektronicznej. Wśród wielu

[7] Zygmunt Ryznar*, Multichannelling, czyli wielokanałowość*, 2003, s. 58-60.
[8] Katarzyna Korzeń, *Bankowość elektroniczna jako kanał dystrybucji usług bankowych*, Warszawa 2007, s. 8.
[9] *Ibidem*, s. 7-9.
[10] Arkadiusz Jurkowski, *Op. Cit.*, s. 9.
[11] Witold Chmielarz, *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa 1999, s. 7.
[12] Witold Chmielarz, *Op. Cit.,* s. 13-14.

funkcjonujących opisów, Michał Polasik proponuje trzy wiodące podejścia, zmierzające do zdefiniowania bankowości elektronicznej[13]:

- zestaw środków technicznych umożliwiający dostęp do usług bankowych (kanały dystrybucji),
- specyficzna usługa bankowa,
- działalność bankowa prowadzona w specyficznej formie.

Podejście skoncentrowane na *środkach technicznych*, jako kluczowe elementy traktuje: możliwość zdalnego dostępu do rachunku bankowego oraz wykorzystanie systemów informatycznych i telekomunikacyjnych. Podejmując próbę wytypowania najczęściej wykorzystywanych urządzeń wskazano: komputer (home/corporate banking, internet banking), telefon stacjonarny (call center), telefon komórkowy (mobile banking) oraz elektroniczne urządzenia do przyjmowania kart (bankomaty, elektroniczne terminale, kioski multimedialne)[14]. Jako równie ważny aspekt rozpatruje się kwestie organizacyjne jej funkcjonowania, czyli interakcje banku i klientów oraz integracje kanałów elektronicznych. Kluczową rolę odgrywa techniczna strona funkcjonowania bankowości elektronicznej, stąd też to podejście stosowane jest głównie w środowisku informatyków, specjalistów IT oraz użytkowników bankowości elektronicznej[15].

Drugie podejście przedstawia bankowość elektroniczną w kontekście *świadczonej przez bank usługi*. Zgodnie z tym punktem widzenia, bankowość elektroniczna stanowi odrębny element w ofercie konkretnej instytucji finansowej, który ma na celu wzbudzenie zainteresowania potencjalnych klientów rozbudowaną funkcjonalnością banku. Nacisk kładzie się na sposób, w jaki postrzegana jest bankowość elektroniczna oraz formalnoprawny charakter relacji występujących pomiędzy bankiem a klientem. Podejście to, najczęściej wykorzystywane jest przez pracowników banków, specjalistów do spraw marketingu oraz pracowników[16].

*Specyficzna forma działalności* skupia swą uwagę na dwóch aspektach. Pierwszym z nich jest kwestia ekonomiczna, koncentrująca się na płatnościach elektronicznych oraz dostarczaniu produktów i usług z wykorzystaniem kanałów elektronicznych. Drugim aspektem jest możliwość zdalnego dostępu. Efektywność tego podejścia pozwala na przedstawienie idei bankowości elektronicznej w zakresie funkcjonowania banku na rynku. Podejście to, stosuje

[13] Michał Polasik, *Bankowość elektroniczna, istota-stan-perspektywy*, Warszawa 2012, s. 11-12.
[14] Beata Świecka, *Bankowość elektroniczna*, Warszawa 2004, s. 8.
[15] Michał Polasik, *Op. Cit.,* s. 11-14.
[16] *Ibidem*, s. 14-16.

się głównie w instytucjach bankowych (np. NBP i Komitet Bazylejski) oraz przez teoretyków przedmiotu[17].

Każda z przedstawionych prób zdefiniowania bankowości elektronicznej oddaje część jej idei. Nie jest to jednak jej oczekiwany całokształt, co wynika z zachowania aspektów charakterystycznych dla konkretnych środowisk, które je wykorzystują. Biorąc pod uwagę złożoność zagadnienia i mnogość dostępnych definicji, Jolanta Adamiec wyodrębniła najważniejsze cechy pozwalające na scharakteryzowanie bankowości elektronicznej i tym samym, odróżnienie jej od usług oferowanych przez tradycyjną bankowość. Zestawione w połączeniu z atrybutami przedstawionymi przez Katarzynę Korzeń, będącymi znaczącym uzupełnieniem, lista cech prezentuje się następująco[18]:

- brak konieczności fizycznej obecności w banku,
- możliwość wykonania czynności bankowej o dowolnej porze,
- brak pośrednictwa personelu banku,
- automatyzacja procesów realizacji i przetwarzania zleceń oraz elektronicznego obiegu informacji,
- ograniczone możliwości pozyskania porady,
- integralna część banku (bankowości),
- stosowanie elektroniki,
- ograniczenie liczby dokumentów papierowych do niezbędnego minimum,
- wysoki poziom standaryzacji usług,
- inicjowanie operacji przez klienta,
- krótkotrwała obsługa klientów,
- obrót bezgotówkowy.

Wymienione atrybuty składają się na kwintesencję definicji bankowości elektronicznej. Ich wspólną cechą jest zapewnienie dostępu do środków przechowywanych na rachunku oraz możliwość dysponowania tymi środkami na odległość. Aby jednak możliwe było dokonywanie jakichkolwiek operacji po stronie klienta, jak również po stronie banku i jego pracowników, niezbędne są poszczególne elementy pozwalające funkcjonować każdej ze stron, łącząc ich prywatne interesy w jeden wspólny.

[17] *Ibidem*, s. 16-19.
[18] Jolanta Adamiec, *Bankowość elektroniczna*, Warszawa 2009, s. 174-175.
Katarzyna Korzeń, *Op. Cit*., s. 9.

## 1.2. Systemy informatyczne w bankowości

System informatyczny stał się fundamentalnym elementem składowym współczesnych banków. Okazał się bardzo pomocny w zakresie wspomagania zarządzania i działalności operacyjnej instytucji finansowej. Ponadto stał się czynnikiem, który bardzo często decyduje o rynkowej pozycji banku. Dzieje się tak, ze względu na wpływ systemów informatycznych na szybkość i elastyczność działania, liczbę klientów, możliwości związane z planowaniem i zarządzaniem strategicznym oraz bieżącą kontrolą realizowanych zadań. Aby jednak system był rzeczywiście przydatny, należy rozwijać go zgodnie z wymaganiami klientów, postępami konkurencji oraz wewnętrznymi potrzebami samego banku. Ważne jest także właściwe zabezpieczenie technologii, celem uniknięcia problemów natury technicznej, jak również organizacyjnej i ekonomicznej.

### 1.2.1. Właściwości i funkcjonalność systemu

Bankowe systemy informatyczne zdecydowanie wyróżniają się na tle systemów wykorzystywanych w przedsiębiorstwach produkcyjnych bądź handlowych[19]. Zygmunt Ryznar określił najistotniejsze właściwości bankowych systemów informatycznych następująco[20]:

- bardzo duży wolumen baz danych,
- duże znaczenie transakcji,
- duży wolumen i intensywność napływu transakcji (w większości wykonywanych w czasie rzeczywistym),
- samodzielność transakcji,
- rozliczanie w czasie,
- występowanie transakcji z datami przyszłymi lub przeszłymi,
- różnorodność typów transakcji,
- wielowalutowość transakcji,
- występowanie aplikacyjnych pakietów zewnętrznych,
- mnogość algorytmów obsługi produktów tej samej klasy,
- wysokie obciążenie zarówno obsługą transakcji w czasie rzeczywistym, jak i dziennym wsadowym przetwarzaniem,
- wymaga bezbłędności działania oprogramowania aplikacyjnego

[19] Dariusz Wawrzyniak, *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*, Warszawa 2002, s. 10-11.
[20] Zygmunt Ryznar, *Informatyka bankowa - próba syntezy*, Poznań 1998, s. 13-27.

oraz zabezpieczenia przed nieuprawnionym dostępem,

- znaczną zmienność rynku usług finansowych i związaną z tym konieczność ciągłej modyfikacji produktów bankowych,
- skomplikowane relacje pomiędzy wieloma typami obiektów w bazach danych,
- dużą złożoność produktów bankowych i instrumentów finansowych.

Przedstawione różnice określają specyficzną funkcjonalność banku, którą przede wszystkim system informatyczny zobowiązany jest realizować. Są to jednak czynności gwarantujące prawidłowość i efektywność prowadzonych działań projektowych, wdrożeniowych i eksploatacyjnych, które zostały obciążone dodatkowymi wymogami, określającymi relacje banku z otoczeniem pod postacią Klienta, innych banków, izby rozliczeniowej, banku centralnego czy na przykład centrum autoryzacji kart płatniczych. Te wartości, w równym stopniu wyznaczają cechy nowoczesnego bankowego systemu informatycznego[21,22]:

- **Dostępność** - Rozpatrywana w odniesieniu do użytkownika, jak również pracownika. Każdy z Klientów powinien mieć dostęp do informacyjnych zasobów systemu, które są niezbędnym elementem realizacji powierzonych mu zleceń. Natomiast pracownik powinien mieć możliwość wglądu oraz wprowadzenia wszelkich niezbędnych zmian w zakresie zgodnym z charakterem swojego stanowiska. I tak na przykład: wgląd w konta klientów, rynek międzybankowy czy dostęp do rozliczeń międzybankowych.
- **Aktualność danych w systemie** - Po każdej przeprowadzonej operacji, informacje systemowe zostają natychmiast zaktualizowane. Jest to ważny element, decydujący o zachowaniu rzetelności informacji przekazywanej Klientowi, jak również eliminujący ryzyko transakcji debetowych i pozwalający uniknąć wahań pieniężnych w obrębie tzw. „pogotowia kasowego". Tym mianem określa się minimalną sumę pieniędzy, która musi znajdować się w kasie banku, jako zabezpieczenie na nieprzewidziane wydatki[23].
- **Wiarygodność** - Jako istotna cecha szczególnie podczas przeprowadzania niestandardowych operacji. Nacisk kładzie się na zgodność nadanej i otrzymanej informacji oraz źródeł ich pochodzenia.
- **Porównywalność** - Jej celem jest zestawienie danych zebranych z konkretnych działów, oddziałów czy centrów rozliczeniowych i stworzenie ich wnikliwej analizy.

[21] Dariusz Wawrzyniak, *Op. Cit*., s. 10-13.
[22] Sylwia Wojciechowska-Filipek, *Technologia informacyjna w usługach bankowości elektronicznej*, Warszawa 2010, s. 12-16.
[23] Słownik Języka Polskiego PWN, *hasło: pogotowie kasowe*, [data dostępu: 17 listopada 2015], <http://sjp.pwn.pl/sjp/pogotowie-kasowe;2503263.html>.

Aby dostarczone treści były przydatne, wszystkie produkty bankowe wprowadza się w jednakowy sposób, według zasad obowiązujących w całym banku.

- **Niezawodność –** Dotyczy głównie dwóch aspektów: sprzętu komputerowego oraz łączności. Niezawodność techniczną uzyskuje się dzięki architekturze tolerującej błędy i pozwalającej na prace systemu, mimo uszkodzenia komponentu. Nadmiarowość podzespołów lub całych urządzeń pozwala na dokonanie drobnych napraw i wymiany konkretnych elementów w czasie ciągłej pracy systemu. Odporność systemu na awarie powinna zamykać się w 99,99% dostępności, co generuje około 50 minut niedostępności systemu w ciągu roku. Niezawodność linii telekomunikacyjnych niestety nie jest możliwa do zrealizowania w 100%, natomiast system odpowiedzialny jest za zapewnienie automatycznej aktualizacji centralnej bazy danych oraz lokalnych plików.
- **Elastyczność -** Odnosi się przede wszystkim do podążania za potrzebami własnymi i klientów oraz zgodną z nimi rozbudowę systemu. Stosuje się metody parametryzacji niewymagające zmian w źródłowym oprogramowaniu.
- **Wydajność -** Mierzona liczbą transakcji bankowych, możliwych do wykonania w jednostce czasu, jak również w szczytowych godzinach czy dniach. Ważny jest także możliwie najkrótszy czas przeznaczony na zamknięcie bieżącego dnia, przez co rozumie się na przykład obliczanie stanów końcowych na rachunkach, naliczenie odsetek, przygotowanie wszelkich raportów, wydruków oraz stworzenie kopii zapasowych.
- **Ekonomiczność -** Wykorzystywana w zestawieniu kosztów projektowania i eksploatacji systemu wraz z efektami jakie są uzyskiwane.
- **Czas reakcji systemu -** To odpowiedź systemu na pytanie zadane przez użytkownika. Aby zapewnić i utrzymać sprawną obsługę klientów, należy ograniczyć czas oczekiwania do minimum, bez względu na rozległość sieci.
- **Stabilność systemu -** Jest odzwierciedleniem odporności jaką system posiada względem zakłóceń wewnętrznych i zewnętrznych.
- **Poufność -** To cecha stosowana na kilku obszarach. Dotyczy informacji o klientach, ich danych osobowych i operacji jakich dokonują. Także pracownicy powinni mieć ograniczony dostęp do treści o Klientach, z możliwością wglądu w te informacje, które niezbędne są im do bieżącej pracy.
- **Bezpieczeństwo -** Obejmuje cztery obszary: ochronę przed utratą informacji, ochronę przed nieuprawnionym dostępem osób nieupoważnionych, ochronę przed brakiem

napięcia w sieci elektrycznej, skutkującej zaprzestaniem przetwarzania oraz ochronę przed nadużyciami osób nieuprawnionych korzystających z systemu.

- **Łatwość użytkowania** - Powinna być realizowana dla każdego rodzaju klienta oraz pracownika, upraszczając obsługę, a tym samym zwiększając funkcjonalność i wykorzystanie systemu.
- **Otwartość systemu** - Stała się ważna na tle globalizacji, stosowania rozwiązań w skali światowej, jak przykładowe aktywne uczestnictwo w transakcjach na światowym rynku kapitałowym, przelewy międzynarodowe czy rozliczenia międzybankowe. Istotna jest możliwość połączenia z innymi systemami, przenoszenia treści między platformami sprzętowymi oraz akceptowanie różnych protokołów sieciowych.
- **Orientacja na klienta** - To zapewnienie sprawnej obsługi, szerokiego wyboru usług, możliwość otrzymania informacji na temat Klienta z uwzględnieniem jego operacji, produktów, raportów z operacji zrealizowanych oraz przewidywanych.
- S**centralizowany charakter przetwarzania** - Zgodnie z nim, wszelkie najważniejsze treści znajdują się w obrębie jednego ośrodka. Do takich informacji zalicza się między innymi: definicje produktów oraz bazy operacyjne (zawierają informacje o rachunkach i klientach). Dostęp do tego typu danych posiadają pracownicy oddziałów, centrali oraz sami Klienci.
- **Kompleksowość i spójność rozwiązania** - Pozwala połączyć usługi bankowości komercyjnej (np. operacje zagraniczne, depozyty, kredyty, obsługa papierów wartościowych) i detalicznej (np. konta osobiste, depozyty, pożyczki dla osób fizycznych).
- **Wielowalutowość** - Uprawnia do wyboru dowolnych walut do równie dowolnych produktów i transakcji. Wszelkie operacje wykonywane są na podstawie bieżącego kursu walut.

Powyższe zestawienie szczegółowo przedstawia cechy, jakimi powinien charakteryzować się współczesny bankowy system informatyczny. Stanowi niezwykle istotną kwestię z punktu widzenia całościowego funkcjonowania, gdyż pozwala każdej z używających go stron, zwrócić uwagę na kluczowe wartości, których niedotrzymanie może być potencjalnym zagrożeniem, niosącym za sobą negatywne skutki w późniejszym czasie. Poza zakresem funkcjonalnym,

istnieje również podział na moduły wyznaczające kompleksowy system bankowy. Zygmunt Ryznar eksponuje następujące komponenty[24]:

- informacje o klientach,
- kredyty,
- rachunki,
- lokaty,
- płatności,
- obsługa dysponencko-kasowa,
- zarządzanie procedurami obsługi produktów bankowych,
- zarządzanie skarbowością oraz aktywami i pasywami,
- obsługa potrzeb informacyjnych kierownictwa,
- operacje zagraniczne,
- papiery wartościowe,
- rynek pieniężny i derywaty,
- księgowość,
- planowanie finansowe i budżetowanie,
- obsługa czeków,
- sprawozdawczość.

System transmisji/przekazu choć jest niezwykle ważnym, to nie jest jednak jedynym istotnym aspektem. Aby zapewnić jego prawidłowe funkcjonowanie wraz z uwzględnieniem wszystkich niezbędnych wartości oraz udostępnionych możliwości, niezbędne są także trzy pozostałe elementy: sprzęt *(ang. hardware)*, oprogramowanie *(ang. software)* oraz użytkownicy[25]. Dopiero te cztery cząstki tworzą współgrającą, wzajemnie uzupełniającą się całość.

### 1.2.2. Kluczowe elementy systemu: architektura, użytkownicy i dokumentacja

Dostępne na rynku systemy różnią się między sobą, ze względu na pełnione funkcje oraz posiadane moduły. Towarzyszy im także architektura, która wykorzystując podejście obiektowe do projektowania i eksploatacji systemu, ma bardzo duże znaczenie. Architektura techniczna występuje w składzie: rozłożenie sprzętu, topologia sieci, ulokowanie danych oraz

[24] Zygmunt Ryznar, *Informatyka… Op.Cit.*, s. 57.
[25] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Usługi bankowości elektronicznej dla klientów detalicznych – charakterystyka i zagrożenia*, Warszawa 2010, s. 5.

struktura oprogramowania[26]. Posiada także techniczne aspekty funkcjonalne, według których jest realizowana[27]:

- *architektura klient-serwer*
  przez co rozumiane są: technologie zarządzania danymi, system zarządzania operacyjnymi bazami danych, technologie obsługi hurtowni danych, narzędzia OLAP do eksploracji i prezentacji informacji
- *sieci finansowe*
  przykładowymi są: SWIFT, EDIFACT
- *bankowość elektroniczna*
  będąca szybko rozwijającym się obszarem bankowości, który wykorzystuje systemy informatyczno-komunikacyjne, narzędzia i konkretne kanały dystrybucji, umożliwiając swobodny dostęp do konta. Niestety dane, które przesyłane są ogólnodostępną siecią globalną silnie naruszają kwestię ich bezpieczeństwa.

Na większą uwagę zasługują równocześnie użytkownicy omawianego środowiska, gdyż czynnik ludzki odgrywa w nim najistotniejszą rolę. Dzieje się tak, ze względu na wagę informacji, które przetwarzane są w systemach bankowości oraz za sprawą ludzkiej nielojalności i omylności. Właśnie takie zestawienie współgrających ze sobą aspektów, powoduje około 80% występujących zagrożeń bezpieczeństwa bankowego systemu informatycznego[28]. Wyszczególnienie pracowników w postaci podziału na grupy jest niezmiernie ważne ze względu na prawa dostępu do systemowych zasobów, różne dla każdej z grup[29]:

- kierownictwo najwyższego szczebla
- kierownictwo średniego szczebla
- kierownictwo szczebla operacyjnego
- osoby bezpośrednio odpowiedzialne za bezpieczeństwo systemu
- administratorzy systemu
- projektanci i programiści
- użytkownicy oprogramowania aplikacyjnego

[26] Dariusz Wawrzyniak, *Op. Cit.*, s. 16.
[27] *Ibidem*, s. 16-17.
[28] *Ibidem*, s. 18.
[29] *Ibidem*, s. 18-19.

- pozostali.

Taki podział pozwala na ograniczenie dostępu do danych oraz pomaga w identyfikacji poszczególnych osób, a także przydaje się podczas tworzenia zabezpieczeń systemu. Łatwiej jest również dbać o ochronę systemu, analizując aktualną sytuację i następnie edukując poszczególne grupy pracowników pod kątem zagrożeń bezpośrednio ich dotyczących, ponadto uświadamiając siłę celowych nadużyć jak i nieświadomie popełnianych błędów i przeoczeń.

Poza architekturą systemu, całym środowiskiem oraz użytkownikami, ważnym elementem bankowości (w tym także elektronicznej) jest kwestia dokumentów, które na przestrzeni upływającego czasu, zmieniły swoją papierową formę. Na chwilę obecną, pod postacią dokumentu rozumie się zapis zbioru informacji, bez względu na nośnik, na którym ów zapis został dokonany. Jest to duża zmiana towarzysząca rozwojowi bankowości elektronicznej. Jednak pomimo tak funkcjonalnej innowacji, pojawił się problem z rozróżnialnością oryginału od kopii. Główne trudności związane są z zachowaniem integralności dokumentu, autentycznością podpisów, które pozostawiane są na dokumentach oraz koniecznością załączania dodatkowych uzupełnień do dokumentu. Stanowi to realne zagrożenie, które zobligowało do stworzenia technologii pozwalających na rzetelną identyfikację. Na swojej popularności zyskuje podpis elektroniczny[30]. Dodatkowym problemem jest forma archiwizowania dokumentów. Kwestia dokumentów w formie elektronicznej jest nieodłącznym elementem systemów informatycznych bankowości, przez co każde niedopracowanie czy niedopatrzenie stanowić może rzeczywiste zagrożenie. Ewolucje dokonujące się w zakresie dokumentacji, to nie jedyne zmiany zachodzące w bankowości wkraczającej w świat Internetu.

## 1.3. Elektroniczne instrumenty płatnicze

Aktywności związane z szeroko pojętym tematem płatności towarzyszą człowiekowi od niepamiętnych czasów. Przedstawiając dzisiejsze postrzeganie tego terminu, pracownicy Banku Finlandii zaproponowali określenie płatności obecnie występujących jako *„transakcję płatniczą oraz odpowiadający jej proces przekazywania środków przez dłużnika na rzecz wierzyciela w sposób bezpośredni lub przez pośrednika”* przy założeniu, że płatność występuje zazwyczaj w formie rekompensaty za dokonany zakup, wynajem lub użytkowanie towaru lub usługi (w postaci materialnej lub niematerialnej) bądź jako finansowy transfer środków

[30] *Ibidem*, s. 19-20.

między zainteresowanymi stronami[31]. Również pieniądze uległy elektronicznej ewolucji. Płatności elektroniczne, nazywane także e-płatnościami czy usługą płatniczą to wszelkie operacje finansowe dokonywane na odległość, za pośrednictwem Internetu oraz przy użyciu różnego rodzaju urządzeń elektronicznych, takich jak przykładowe: telefony komórkowe, tablety czy komputery[32]. Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 13 listopada 2007 roku w sprawie usług płatniczych w ramach rynku wewnętrznego (ang. Payment Services Directive - PSD) bardziej szczegółowo określa zagadnienie usługi płatniczej, podkreślając konkretne działania gospodarcze w zakresie tematu[33]:

- Umieszczenie gotówki na rachunku płatniczym oraz jej wypłacanie wraz ze wszelakimi działaniami potrzebnymi do należytego prowadzenia rachunku
- Dokonywanie transakcji płatniczych, również transferu środków na rachunek płatniczy (u tego samego lub innego dostawcy usług płatniczych) z wykorzystaniem:
    - Usług polecenia zapłaty (jednorazowych lub cyklicznych),
    - Przelewów bankowych,
    - Transakcji płatniczych z wykorzystaniem instrumentów płatniczych,
    - Transakcji płatniczych mających pokrycie w linii kredytowej.

Poza wskazanymi działaniami, wymienia się także czynności wydania lub nabycia instrumentów płatniczych, świadczenia usług przekazów pieniężnych oraz transakcji za pośrednictwem operatorów systemów teleinformatycznych. Wyszczególnione płatności realizowane są przy pomocy dynamicznie rozwijających się instrumentów płatniczych[34]. Posiadają dostęp do środków pieniężnych, a ich przeznaczeniem jest umożliwienie dokonania operacji przy jednoczesnym użyciu elektronicznych nośników[35]. Nie sposób pominąć fakt, iż powstanie i wciąż rosnąca popularność płatności elektronicznych, ściśle związana jest z rozwojem Internetu, a w szczególności sektoru skupionego na e-handlu, czyli dokonywaniu zakupów przez Internet.

[31] Michał Polasik, Krzysztof Maciejewski, *Innowacyjne usługi płatnicze w Polsce i na świecie*, Materiały i studia, Zeszyt nr 241, Warszawa 2009, s. 15.
[32] Bartłomiej Chinowski, *Elektroniczne metody płatności. Istota, rozwój, prognoza*, Warszawa 2013, s. 5.
[33] Michał Polasik, Krzysztof Maciejewski, *Op. Cit*., s. 15-16.
[34] *Ibidem*
[35] Beata Świecka, *Op. Cit.*, s. 43-44.

Dodatkowy wpływ mają następujące cechy:

- **wygoda** (zadania, jakie Klient musi wykonać zostały ograniczone do niezbędnego minimum, to dostawca usług płatniczych zapewnia właściwą wymianę danych i informacji między stronami transakcji),
- **bezpieczeństwo** (w interesie dostawcy usług jest zapewnienie bezpieczeństwa klienta i jego transakcji, zdarza się, iż dostawca dodatkowo daje gwarancję bezpieczeństwa),
- **szybkość** (realizacja transakcji niemal natychmiast widoczna jest na rachunku, dzięki czemu Klient posiada ciągle aktualną informację na temat swoich finansów),
- **pewność** (przykładowo, podczas dokonywania przelewów klient ma za zadanie sprawdzić i potwierdzić polecenie przelewu, uzupełnione przez dostawcę usług, przez co ryzyko pomyłki przy wpisywaniu danych zostaje zminimalizowane)[36].

Dzięki nim, klienci darzą bankowość elektroniczną coraz to większym zaufaniem, z czego korzyści czerpią obie strony – i klient i bank. Za elektroniczne instrumenty płatnicze uznaje się karty płatnicze oraz pieniądze elektroniczne.

### 1.3.1. Karty płatnicze

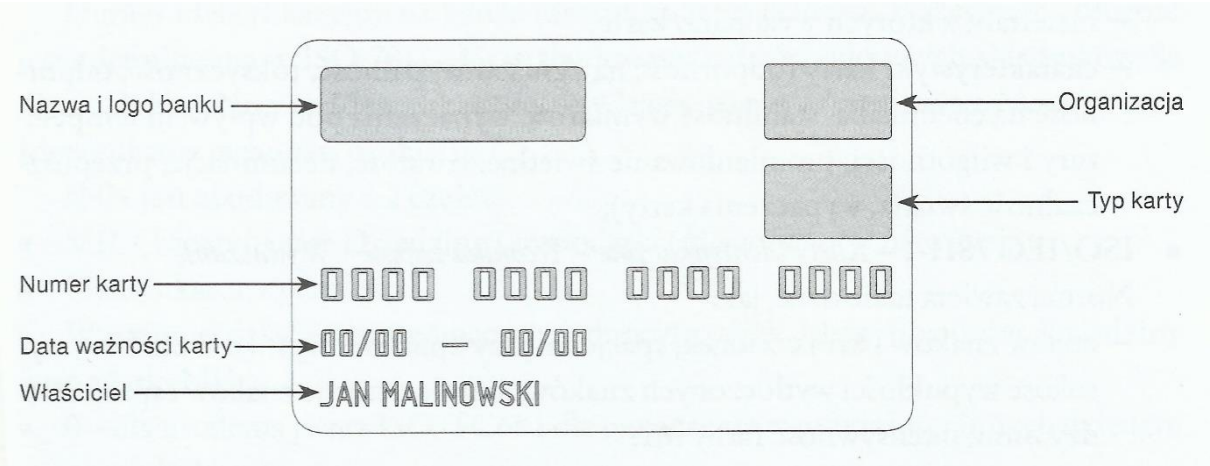
Niegdyś dostępne wyłącznie dla „bogatych wybrańców", a obecnie jako najstarszy i jednocześnie najbardziej rozpowszechniony instrument pieniądza elektronicznego. Ustawa prawa bankowego określa kartę płatniczą jako *„kartę identyfikującą wydawcę i upoważnionego posiadacza, uprawniającą do wypłaty gotówki lub dokonywania zapłaty, a w przypadku karty wydanej przez bank lub instytucję ustawowo upoważnioną do udzielania kredytu – także do dokonywania wypłaty gotówki lub zapłaty z wykorzystaniem kredytu"*[37]. Jest to zatem, środek płatności będący ekwiwalentem gotówki, funkcjonujący we wskazanych przez odpowiedni bank punktach oraz podlegający ściśle określonym normom.

#### *1.3.1.1. Opis karty*

Oczywistym jest, że wygląd kart zmieniał się na przestrzeni upływającego czasu. Wszystkie współczesne karty płatnicze podlegają ujednoliconej formie. Muszą mieć kształt prostokąta, być wykonanymi z plastiku i posiadać konkretne elementy. Wszelkie obowiązujące wzorce zostały określone przez ISO (ang. International Organization for Standarization). Zgodnie z międzynarodową standaryzacją z 1985 roku i aktem ISO 7810, rozmiar kart płatniczych powinien wynosić: wysokość: 53,98mm, szerokość: 85,6mm oraz grubość:

[36] Bartłomiej Choinowski, *Op. Cit.*, s. 5-6.
[37] Ustawa Prawo Bankowe, DzU 1997r. nr 140, poz. 939.

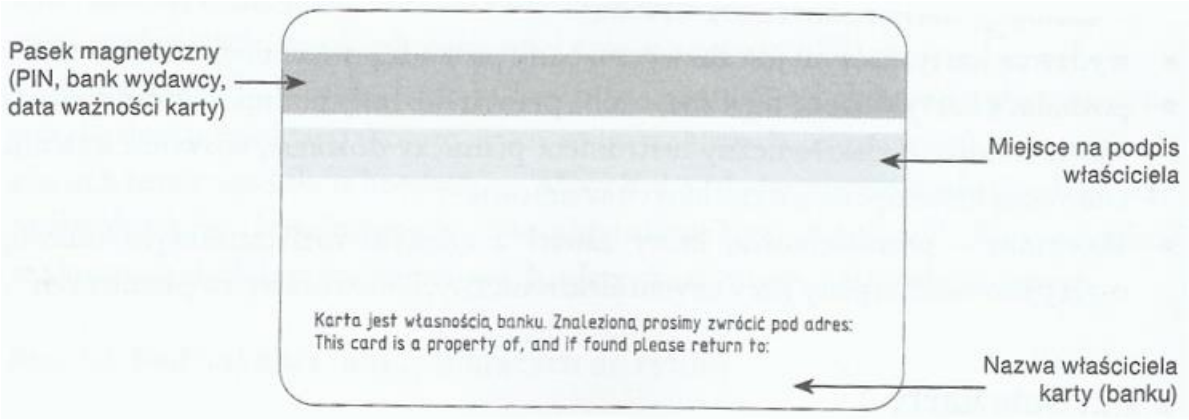
0,76mm. Każda karta płatnicza posiada awers i rewers[38]. Poniżej przedstawiono obie strony wraz z elementami, które standardowo się na niej znajdują.




Rysunek 2. Awers karty płatniczej

*Źródło: Sylwia Wojciechowska-Filipek: Technologia informacyjna w usługach bankowości elektronicznej.*

Na rysunku 2 przedstawiono awers, czyli przednią część karty płatniczej. Elementy, które się na niej znajdują to: cechy systemów (logo, hologram organizacji), logo banku, numer karty, imię i nazwisko właściciela karty, okres ważności karty (do ostatniego miesiąca, w którym upływa jej ważność). Opcjonalnie występuje na nim również zdjęcie właściciela (okaziciela) karty oraz mikroprocesor. Dodatkowo, jeśli karta może być używana wyłącznie w środowisku elektronicznym, posiadać będzie napis „*Electronic use only*”[39].




Rysunek 3. Rewers karty płatniczej

*Źródło: Sylwia Wojciechowska-Filipek: Technologia informacyjna w usługach bankowości elektronicznej.*

[38] *Definicja i budowa karty płatniczej*, [data dostępu: 20.11.2015], <http://www.kartyplatnicze.info/definicja.php>

[39] Sylwia Wojciechowska-Filipek, *Op.Cit.*, s. 27.

Z kolei rewers karty płatniczej (Rysunek nr 3), zawiera standardowo następujące elementy: pasek magnetyczny z naniesionymi danymi, pasek do podpisu, informacje od wystawcy (czyją własnością jest karta oraz co robić w przypadku zgubienia)[40]. Poszczególne normy ISO bardzo wnikliwie opisują konkretne elementy. Wyróżnia się takie kategorie opisu jak[41]:

- karty identyfikacyjne – charakterystyka fizyczna (ISO/IEC 7810),
- karty identyfikacyjne – technika zapisu (ISO/IEC 7811-1),
- karty identyfikacyjne – technika zapisu – pasek magnetyczny (ISO/IEC 7811-2),
- karty identyfikacyjne – technika zapisu – rozmieszczenie znaków wytłaczanych na kartach ID-1 (ISO/IEC 7811-3),
- karty identyfikacyjne – technika zapisu – rozmieszczenie ścieżek tylko do odczytu. Ścieżki 1 i 2 (ISO/IEC 7811-4,-5),
- karty identyfikacyjne – identyfikacja wydawców. System numeracji. (ISO/IEC 7812-1)

Z technologicznego punktu widzenia, każda karta traktowana jest jako karta identyfikacyjna.

#### *1.3.1.2. Karty funkcjonujące na rynku polskim*

Warto wspomnieć, iż karty płatnicze choć tak popularne, nie są jedynymi dostępnymi aktualnie na rynku kartami. Prócz nich występują także karty: identyfikacyjne, wstępnie opłacone oraz bankomatowe[42]. W ten sposób określono ich funkcje użytkowe.

**Karta identyfikacyjna** występująca także pod nazwą „karta dostępowa" służy przede wszystkim do utożsamiania osób, najczęściej tych, które składają dyspozycje w banku. Wyróżnia się trzy ich rodzaje. Pierwszy z nich, niejako zastępuje dowód osobisty klienta i służy jego uwiarygodnieniu przy okienku bankowym. Drugi rodzaj, to tak zwane karty gwarancyjne do czeków, które zabezpieczają przed zgubieniem lub kradzieżą. Trzeci rodzaj ma na celu identyfikacje pracowników konkretnej firmy podczas udostępniania im pomieszczeń, dostępu do programów komputerowych (również pełne wersje oprogramowań) czy automatyzacji poszczególnych operacji (również o charakterze finansowym)[43].

**Karta wstępnie opłacona**, zwana też przedpłaconą lub wstępnie ładowaną. Jej funkcjonowanie opiera się o uprzednie wykupienie karty o konkretnej, z góry ustalonej wartości, a następnie dokonywanie transakcji za jej pomocą w bankomatach lub w punktach

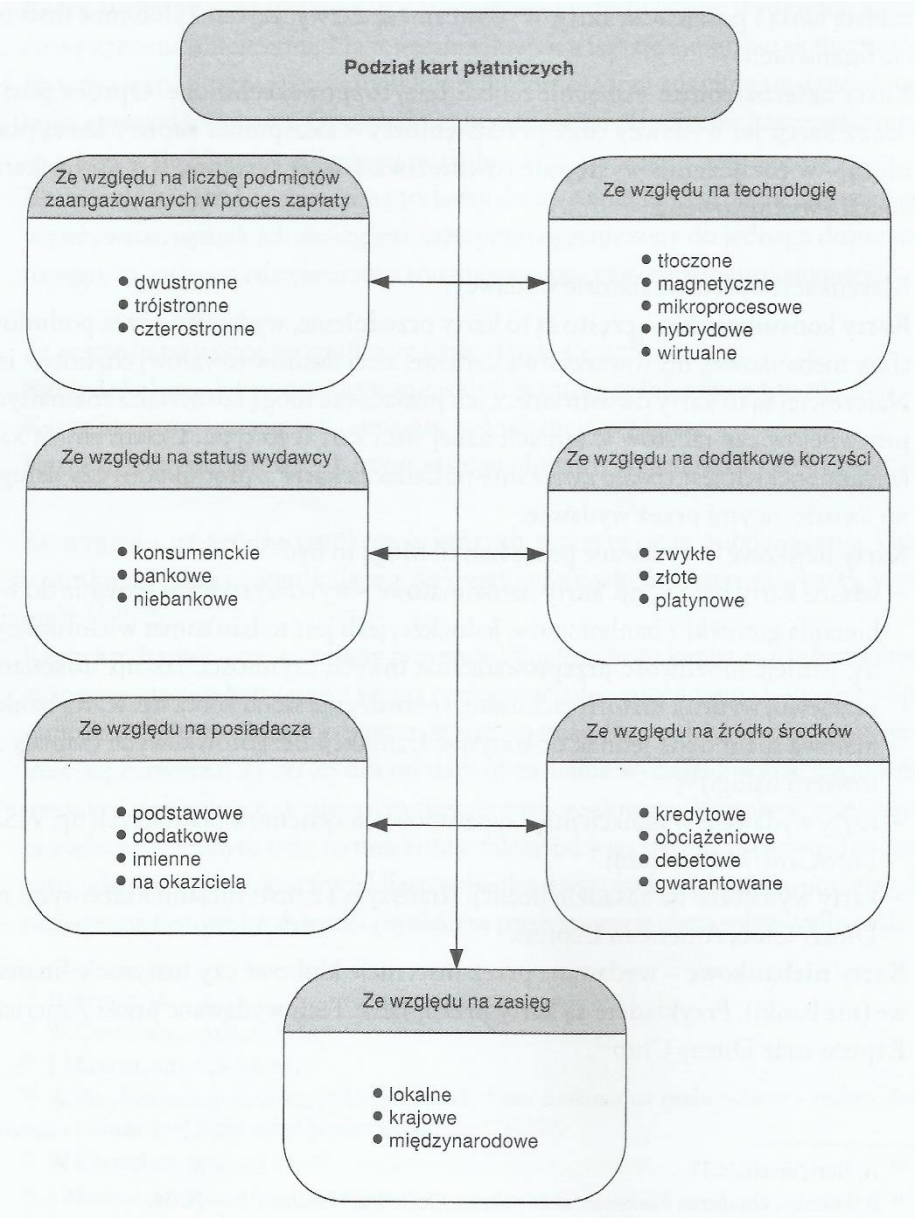
[40] *Ibidem*, s. 28.
[41] *Ibidem*, s. 28-29.
[42] Witold Chmielarz, *Systemy elektronicznej bankowości*, *Op. Cit.*, s. 111.
[43] *Ibidem*, s. 111.

np. handlowych, które są do tego przystosowane (punkt musi być wyposażony w elektroniczny terminal). Jest to wygodna forma dla sprzedawców, którzy nie muszą obawiać się przyjęcia karty nieważnej lub bez pokrycia finansowego (kwota dostępna na karcie zostaje przepisana do pamięci terminala) jak również dla banku, który nie musi dokonywać autoryzacji ani obawiać się o przekroczenie salda na rachunku. Do najpopularniejszych systemów kart przedpłacowych należą: Visa Cash (Visa), Mondex (MasterCard) oraz Proton (American Express)[44].

**Karta bankomatowa** *(ang. ATM card, cash card)* służy realizacji wszelkich operacji w bankomatach (głównie wypłata/wpłata gotówki). Jej funkcje są zróżnicowane w zależności od banku, który ją wydał, a tym samym bankomatów, w jakich można jej użyć[45],

**Karta płatnicza** – według Beaty Świeckiej jest formą bezgotówkowego pieniądza, instrumentem bezgotówkowym rozliczeń pieniężnych. Służy do płacenia za usługi i towary w punktach, które je akceptują tzn. w restauracjach, sklepach, stacjach benzynowych, hotelach, lotniskach itp[46]. Karty płatnicze stanowią szerokie zagadnienie, a ich podziału można dokonać na podstawie przeróżnych kryteriów klasyfikacyjnych. Rysunek 4 przedstawia najpopularniejszą aktualnie klasyfikację.

[44] *Ibidem*, s. 111.
[45] *Ibidem*, s. 111.
[46] Beata Świecka, *Op. Cit.*, s. 49-50.




Rysunek 4. Podział kart płatniczych

*Źródło: Sylwia Wojciechowska-Filipek: Technologia informacyjna w usługach bankowości elektronicznej.*

W proces realizacji płatności mogą być zaangażowane różne podmioty, które ze względu na zróżnicowane znaczenie kart i ich zastosowań w systemie, nie zawsze akceptują każdą z nich. Wśród podmiotów biorących udział w procesie zapłaty kartą wyróżnia się[47]:

- **wydawców karty** w postaci banków lub niebankowych podmiotów, najczęściej prowadzących rachunek klienta, odpowiadają również za przyjęcie zgłoszeń posiadacza o zniszczeniu bądź utracie karty, a także podjęcia aktywnego działania w tym temacie

[47] Beata Świecka, *Op.Cit.,* s. 44-47.

- **posiadaczy karty** będącymi osobami fizycznymi, prawnymi lub jednostkami organizacyjnymi nieposiadającymi osobowości prawnej, które w swoim imieniu i na swoją rzecz, dokonują operacji na podstawie umowy o elektroniczny instrument płatniczy. Obciążenie konta posiadacza obejmują jednocześnie operacje przeprowadzone przez inne podmioty, którym udostępniono kartę bądź kod identyfikacyjny. Takie obciążenie obowiązuje do momentu zgłoszenia zaginięcia karty, chyba, że udowodnione zostanie nieodpowiednie przechowywanie karty lub zła ochrona PIN-u.
- **agentów rozliczeniowych i akceptantów** w postaci banków, przedsiębiorstw, innych podmiotów (także niebankowych), którzy posiadają umowę o przyjmowanie zapłat przy użyciu elektronicznych instrumentów płatniczych oraz z poręczeniem banku na realizację zobowiązań z tytułu operacji wykonywanych z użyciem kart płatniczych
- **systemy kart płatniczych**, czyli organizacje wystawców kart płatniczych, które uczestniczą w realizacji transakcji przy użyciu kart płatniczych. Aktualnie istniejące na świecie systemy kart płatniczych to[48]:
    - Diners Club International
    - American Express
    - JBC International
    - Visa International
    - Europay/MasterCard

W związku z tym, powstał podział kart ze względu na liczbę podmiotów zaangażowanych w proces zapłaty kartą płatniczą. **Karty dwustronne** akceptowane są jedynie przez ich wydawcę, którymi najczęściej są: domy towarowe, biura podróży, linie lotnicze czy ogólnie pojęte przedsiębiorstwa handlowe. Emitent karty jest jednocześnie jej akceptantem, a karta ma ograniczony zasięg i użyteczność. **Karty trójstronne** bazują na współpracy i porozumieniu wydawcy karty, akceptantów płatności oraz posiadacza karty. Niezbędne jest zdefiniowanie praw i obowiązków każdego z podmiotów oraz określenie relacji między każdym z nich. Płatność tym rodzajem karty możliwa jest w punktach je akceptujących, posiadających odpowiedni system rozliczeń, a jej wydanie jest zazwyczaj odpłatne. **Karta czterostronna** to obecnie najbardziej rozpowszechniony typ. Jej podmiotami są: posiadacz karty, emitent, przedsiębiorstwo akceptujące oraz właściciel systemu. Dzięki takiej formie, system korzysta reklamując siebie oraz organizację poprzez logo, co potencjalnie wpływa

[48] Andrzej Bury, *Karty płatnicze w Polsce*, Warszawa 2002, s. 43-51.

na wzrost kręgu posiadaczy. Dodatkowo kwestie rozliczeniowe w większości realizowane są przez centrum rozliczeniowe, przez co wydawca zajmuje się już tylko obowiązkami wynikającymi z obsługi posiadacza karty[49].

Kolejny typ jest oparty o status wydawcy. Głównym celem **kart konsumenckich** jest pobudzenie poczucia więzi i związania posiadacza karty z usługami czy produktami świadczonymi przez emitenta sfery niebankowej (np. sieci domów towarowych lub hoteli). Przeważnie są to karty dwustronne, oferujące przywileje i rabaty w danej sieci[50]. **Karty bankowe**, jak nazwa słusznie wskazuje, wydawane są przez banki. Zalicza się do nich karty, które wydaje się w ramach międzynarodowych systemów płatniczych typu VISA czy EuroCard/MasterCard, karty działające na zasadzie licencji z instytucjami klubowymi np. Diners Club lub American Express, a także własne karty banku, wykorzystywanych do zarządzania zgromadzoną gotówką na rachunku, we własnym zakresie[51]. **Karty niebankowe** z kolei, wydawane są przez instytucje klubowe lub finansowe, nie będące bankami, najczęściej jednak, są to wielkie korporacje międzynarodowe, a wydanie takiej karty obciążone jest wysokim kosztem.

Karty zdefiniowane ze względu na posiadacza opisane są następująco: **podstawowe**, które otrzymuje się będąc posiadaczem odpowiedniego rachunku bankowego, **dodatkowe** - przeznaczone dla osób wskazanych przez posiadacza rachunku oraz karty **imienne**, za które uznaje się wszystkie wydane na świecie karty trój i czterostronne, gdzie na rewersie znajduje się pasek do podpisu oraz pasek magnetyczny lub mikroprocesor z danymi identyfikującymi. Karta **na okaziciela** cieszy się dużą popularnością. Ich zasięg jest dość mocno ograniczony np. do jednego domu towarowego i są to karty dwustronne oraz przedpłatne[52].

Kolejną dość wąską kategorię wyznacza zakres geograficzny. Wyróżnia się tu karty **lokalne** – o zasięgu miejskim, stanowym lub regionalnym, **krajowe** – ważne tylko w kraju, gdzie wydano kartę oraz **międzynarodowe**, o zasięgu globalnym, czyli ważne na całym świecie[53].

[49] *Definicja i budowa karty płatniczej*, [data dostępu: 22.11.2015], <http://www.kartyplatnicze.info/typologia.php>.
[50] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 34.
[51] Andrzej Bury, *Op. Cit.*, s. 17.
[52] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 35.
[53] Witold Chmielarz, *Op. Cit.*, s. 112.

Następny podział uwzględnia sposób obciążenia klienta, definiując źródło środków. **Karta kredytowa** pozwala na dokonywanie płatności w zakresie limitu kredytowego przyznanego przez bank, dzięki czemu posiadacz może posługiwać się kartą, jednocześnie nie posiadając własnych środków. Wysokość kredytu, termin oraz minimalna wysokość spłaty ustalane są przez bank. Najczęstszy termin spłaty zmyka się w przedziale od 21 do 25 dni od otrzymania wyciągu za ubiegły okres rozliczeniowy. Po uiszczeniu minimalnej kwoty, możliwe jest zaciągnięcie kolejnego kredytu. Karta wydawana jest stałym klientom, o wysokich dochodach, nienagannej historii kredytowej oraz wyrażającym chęci do spłaty zadłużenia. Jest to oferta korzystna przede wszystkim dla banku, gdyż oprocentowanie kredytu jest dużo wyższe niż przeciętnie zaciągniętego. Choć istnieje również ryzyko, iż ze względu na niezabezpieczony charakter kredytu, Klient go nie spłaci[54]. **Karta obciążeniowa** jest bardzo zbliżona w swym funkcjonowaniu do karty kredytowej. Różnica polega na konieczności spłaty całości zadłużenia (również raz na miesiąc), aby móc zaciągnąć kolejny kredyt. Jest to karta najczęściej powiązana z rachunkiem oszczędnościowo-rozliczeniowym, wydawana również stałym klientom. **Karty debetowe** natomiast, powiązane są z rachunkiem osobistym właściciela, a limit pieniężny określa saldo rachunku. To dogodny typ, zarówno dla banku jak i klienta. Ich wydanie nie zależy od zdolności kredytowej posiadacza, dzięki czemu dostępna jest dla większości chętnych klientów[55]. **Karty gwarantowane** są odpowiednikiem karty kredytowej z tą różnicą, iż kredyt zabezpieczony jest oprocentowanym depozytem[56].

Kolejny podział związany jest z przywilejami, jakie zyskuje posiadacz karty, a warunkuje je poziom zamożności oraz status i znaczenie Klienta. W związku z tym, **karty zwykłe**, zwane również masowymi, dostępne są dla każdego klienta, który nie jest obciążony żadnymi negatywnymi cechami finansowymi. **Karty złote** otrzymują zamożni, wysoko sytuowani klienci, dzięki czemu zyskują prestiż oraz dodatkowy pakiet zniżek wszelkiego rodzaju. Przeznaczeniem **kart platynowych** są klienci o najwyższych dochodach, korzystający ze specjalnej obsługi private banking. Ci klienci zyskują nieograniczone limity wydatków oraz bardzo szeroki pakiet pozapłatniczych usług. Wydanie tego typu kart ograniczone jest do minimum, przez co zdarza się, że obejmują one zaledwie kilkudziesięciu klientów danego banku[57].

[54] Sylwia Wojciechowska-Filipek, *Op.Cit.*, s. 35-36.
[55] *Ibidem*, s. 36.
[56] *Ibidem*, s. 36.
[57] *Definicja i budowa karty płatniczej*, [data dostępu: 22.11.2015], <http://www.kartyplatnicze.info/typologia.php>.

Ostatnim wyróżnionym kryterium i niewątpliwie najbardziej znaczącym w kwestiach bezpieczeństwa, są karty podzielone ze względu na technologię. **Karty tłoczone (embosowane)** posiadają wytłoczone informacje: dane identyfikacyjne, datę ważności oraz numer konta. Do ich akceptacji nie potrzeba specjalistycznego sprzętu, a podpisanie rachunku po przeprowadzonej transakcji stanowi podstawę do obciążenia konta. Ze względu na rażącą łatwość skopiowania danych, ten rodzaj został stopniowo wycofywany od 1995 roku i aktualnie nie występuje w Polsce[58]. **Karty magnetyczne (płaskie)** posiadają nadrukowane dane, a głównym nośnikiem informacji jest pasek magnetyczny. Posiadacz identyfikowany jest za pomocą porównania wprowadzonego PIN-u z danymi zawartymi na pasku magnetycznym. Proces płatności automatycznie dokonuje autoryzacji, sprawdzenia pokrycia finansowego oraz zmniejszenia dostępnych na koncie środków. Zagrożeniem dla tego typu karty jest kradzież, zakupy na odległość przy wykorzystaniu cudzej karty oraz skopiowanie paska magnetycznego[59]. **Karty mikroprocesorowe (inteligentne)** posiadają wbudowany układ scalony wyposażony w pamięć i procesor, co usprawnia zapisanie o wiele większej ilości danych w porównaniu z innymi kartami. Zwiększona została również ochrona, dzięki specjalnemu algorytmowi sprawdzającemu kod PIN, lepszej autoryzacji i możliwości budowy dodatkowych mechanizmów zabezpieczających[60]. **Karty hybrydowe** wykorzystują pasek magnetyczny oraz mikroprocesor. Natomiast wykorzystywane są w państwach o niedostatecznej infrastrukturze do powszechnego przyjmowania i akceptowania kart z mikroprocesorem[61]. Ostatnim omawianym rodzajem są **karty wirtualne (ang. Virtual credit cards)**. Znalazły swoje zastosowanie w miejscach, gdzie nie wymaga się fizycznej obecności karty, tzn. przy transakcjach dokonywanych przez Internet, telefon lub za pośrednictwem poczty. Niestety karta ta, nie posiada żadnych dodatkowych zabezpieczeń. Warto również wspomnieć, że w użyciu funkcjonują karty stykowe oraz coraz popularniejsze karty zbliżeniowe. Każda z wymienionych kart jest kartą płatniczą, będącą jednym z dwóch funkcjonujących elektronicznych instrumentów płatniczych.

[58] *Ibidem*
[59] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 37.
[60] *Definicja i budowa karty płatniczej*, [data dostępu: 22.11.2015], <http://www.kartyplatnicze.info/typologia.php>.
[61] *Ibidem*.

### 1.3.2. Pieniądz elektroniczny

Drugim funkcjonującym elektronicznym instrumentem płatniczym jest pieniądz elektroniczny. Cytując ustawę prawa bankowego[62], pieniądz elektroniczny jest to „wartość pieniężna stanowiąca elektroniczny odpowiednik znaków pieniężnych, która spełnia łącznie następujące warunki:

- jest przechowywana na elektronicznych nośnikach informacji,
- jest podawana do dyspozycji na podstawie umowy w zamian za środki pieniężne o nominalnej wartości nie mniejszej niż ta wartość,
- jest przyjmowana jako środek płatniczy przez przedsiębiorców innych niż wydający ją do dyspozycji,
- na żądanie jest wymieniona przez wydawcę na środki pieniężne."

Jest to zatem jednostka monetarna na okaziciela, będąca środkiem płatniczym typu prepaid, czyli wstępnie opłacana lub wstępnie ładowana, zapisywana na nośnikach należących do użytkownika. Środek ten, nie wymaga bezpośredniego połączenia z kontem bankowym podczas dokonywania transakcji[63]. Dzięki temu zachowana zostaje tak ważna w dzisiejszych czasach anonimowość. Jej stopień silnie związany jest z systemem, jaki zastosowano. Funkcjonuje system otwarty i zamknięty. System otwarty wyklucza kontakt z pośrednikiem, e-pieniądz przemieszcza się między różnymi podmiotami, nie tracąc na swej wartości i nie zużywając się jak pieniądz gotówkowy. System zamknięty natomiast, opiera się na relacji z pośrednikiem, gdyż każda jednostka pieniężna jest jednorazowa i niezbędne jest jej odnowienie po każdej przeprowadzonej transakcji[64]. Podobnie jak w przypadku kart płatniczych, tak i pieniądz elektroniczny podlegać powinien ogólnym zasadom, choć opisane zostały w teorii, to warto się nad nimi zastanowić, a prezentują się następująco[65]:

**Bezpieczeństwo**, mówiące o konieczności występowania pieniądza w charakterze jednorazowym oraz obowiązującym, wysokim stopniu bezpieczeństwa zastosowanym w protokole obsługującym transakcje.

[62] Ustawa z dnia 29 sierpnia 1997r. Prawo bankowe, DzU 2002r. nr 72, poz. 665.
[63] Beata Świecka, *Op. Cit.*, s. 55.
[64] Dorota Korenik, *Innowacyjne usługi banku*, Warszawa 2006, s.250-251.
[65] Witold Chmielarz, *Systemy elektronicznej bankowości*, Op. Cit., s. 139.

**Anonimowość**, której celem jest brak możliwości wyśledzenia powiązań między sprzedawcą, a kupującym i przeprowadzonej przez nich transakcji, a w efekcie gwarancja zachowania pełnej prywatności użytkowników.

**Niezależność od postaci fizycznej**, co pozwala na przesyłanie z wykorzystaniem dowolnej sieci oraz możliwość przechowywania na dowolnym urządzeniu.

**Nieograniczona ważność**, dzięki której gromadzenie gotówki nie byłoby uzależnione od ram czasowych.

**Płatność poza siecią (off-line)**, gdzie poza koniecznością autoryzacji, możliwa jest płatność bez dostępu do sieci.

**Możliwość przekazywania bez pośredników (peer-to-peer)**, pozwalająca na bezpośrednie przekazywanie pieniędzy między użytkownikami.

**Podzielność**, dzięki której możliwe jest przesyłanie dowolnych kwot pieniężnych, a następnie ich połączenie w większe kwoty.

**Powszechna akceptowalność**, nieograniczona terytorialnie, wartością walut, dostępnymi formami płatności, ani w żaden inny sposób.

**Łatwość użycia**, która dostępna powinna być zarówno dla sprzedających, jak i klientów, co przynosiłoby korzyści dla obu stron.

**Niezależność polityczna**, dzięki której wartość pieniądza cyfrowego powinna opierać się na rozwoju i efektach pracy mechanizmów rynkowych.

Mimo, iż są to postulowane zasady, analizując całokształt współcześnie występującej formy pieniądza elektronicznego, dostrzegalne są silne zależności z wyżej wymienionymi cechami. Wyróżnia się dwa typy e-pieniądza: bazujący na kartach oraz funkcjonujący w oparciu o Internet[66].

**Pieniądz elektroniczny bazujący na kartach** występuje także pod nazwą elektronicznej portmonetki lub elektronicznego portfela. Jego ideą jest dokonanie bezgotówkowej transakcji, której zgodnie z ustawą o elektronicznych instrumentach płatniczych, kwota zgromadzona na karcie nie może przekraczać 150 euro. Płatność dokonywana jest za towary bądź usługi. Jest to karta przedpłacowa, za którą klient musiał

[66] Beata Świecka, *Op. Cit.*, s. 56.

wcześniej zapłacić[67]. Mylnie postrzega się pojęcie elektronicznej portmonetki za tożsamą z kartą płatniczą. W tabeli poniżej przedstawiono podstawowe różnice między tymi dwoma środkami płatniczymi.

| **Kryterium porównawcze** | **Karta płatnicza** | **Elektroniczna portmonetka** |
|---|---|---|
| *Forma płatności* | Transfer środków pomiędzy dwoma rachunkami bankowymi | Transfer środków znajdujących się bezpośrednio w pamięci karty, bez angażowania rachunków bankowych podczas przeprowadzania transakcji |
| *Przeznaczenie* | Realizacja transakcji dotyczących wyższych kwot | Realizacja transakcji dotyczących niższych kwot |
| *Dostęp do środków* | Wartość środków uzależniona od stanu konta bankowego (dot. kart debetowych) lub od limitów przyznanych przez bank (dot. kart kredytowych i obciążeniowych) | Wartość środków nie przekraczająca 250 euro |
| *Możliwość uzyskania kredytu* | W zależności od karty: pozwala na zaciągnięcie kredytu | Brak |
| *Dokonywanie i rozliczanie transakcji* | Najczęściej wymagana jest autoryzacja online; Zostaje obciążony rachunek bankowy | Transakcja dokonywana w trybie offline; Bez rejestracji na rachunku bankowym |
| *Różnica czasowa pomiędzy momentami dokonania transakcji a momentem zapłaty* | W momencie przeprowadzania transakcji zostaje obciążony rachunek posiadacza | Posiadacz karty z góry płaci za jej określoną wartość nabywczą |

Tabela 1. Wykaz podstawowych różnic pomiędzy kartą płatniczą a elektroniczną portmonetką.

*Źródło: Opracowanie własne na podstawie: Rafał Janowicz, Pieniądz elektroniczny w wybranych krajach – charakterystyka, główne funkcje i zastosowanie.*

Zgodnie z przeznaczeniem, wyróżnia się dwa rodzaje kart gotówkowych: jednorazowe, które posiadają stałą wartość, a po jej wykorzystaniu karta nie nadaje się do ponownego użytku oraz karty wielokrotnego użytku, które cechuje możliwość ponownego naładowania, za pomocą specjalistycznych urządzeń, sieci i aplikacji. Możliwa jest również bieżąca kontrola dostępnych na karcie środków. Systemy elektronicznego pieniądza wykorzystuje

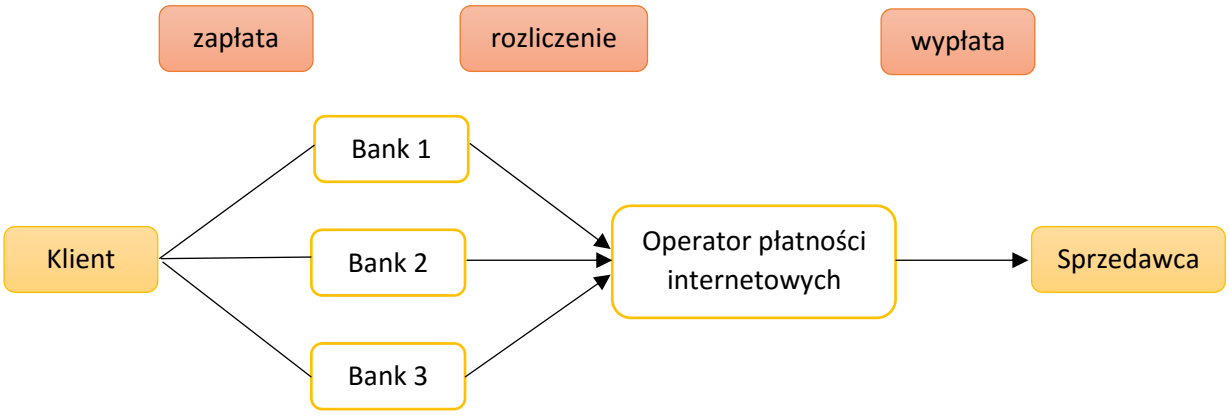
[67] Sylwia Wojciechowska-Filipek, *Op.Cit.*, s. 48-49.

się w Ameryce Północnej, Europie i Azji, choć różnią się funkcjonalnością i opłatami za użytkowanie[68]. Karta ta wydaje się być bezpieczną formą płatności, ponieważ podczas zgubienia bądź kradzieży, utracie podlegają wyłącznie środki ulokowane na karcie, a przez brak połączenia karty z kontem bankowym, nie ma żadnego zagrożenia pozostałych środków pieniężnych.

**Pieniądz elektroniczny funkcjonujący w oparciu o Internet**, zwany także pieniądzem sieciowym lub pieniądzem internetowym. Forma bazująca na specjalnym oprogramowaniu, które zainstalowane na prywatnym komputerze klienta, generuje pieniądze elektroniczne, nie posiadające materialnej postaci. Są to zapisywane na dysku piliki, chronione przed kopiowaniem, posiadające swój unikalny numer seryjny i posiadający zabezpieczenie w postaci podpisu cyfrowego. Aby ich użycie było możliwe, konkretne pliki przesyłane są do banku celem ich autoryzacji, a następnie odsyłane do tzw. elektronicznego portfela. Po dokonaniu zapłaty stają się nieważne. Posiada także zabezpieczenie przed próbą ponownej zapłaty tym samym banknotem - *double spending*[69].

### 1.3.3. Elektroniczne formy płatności

Płatności elektroniczne są niezwykle efektywną formą płatności. Przede wszystkim pozwalają na zaoszczędzenie pieniędzy i czasu, a jednocześnie sprawdzają się w realizacji, a nawet uproszczeniu codziennych płatności, dzięki czemu wciąż zyskują na popularności. Różnorodność transakcji przeprowadzanych na rynku, wymusza powstawanie, a następnie rozwój systemów płatności, które je obsługują. Poniższa ilustracja przedstawia podstawowy proces przebiegu płatności internetowej.




Rysunek 5. Schemat działania płatności internetowych.
*Źródło: Opracowanie własne na podstawie:*
*Bartłomiej Choinowski, Elektroniczne metody płatności. Istota, rozwój, prognoza.*

[68] Beata Świecka, *Op. Cit.*, s. 56-57.
[69] Sylwia Wojciechowska-Filipek, *Op.Cit.*, s. 51-52.

Rysunek 5 obrazuje trzy podstawowe kroki[70]. W pierwszym z nich, klient podejmuje decyzję o nabyciu towaru bądź usługi i decyduje się na podjęcie płatności, wybierając przykładowy przelew, co skutkuje przeniesieniem na stronę internetową swojego banku. Po zalogowaniu, przygotowany jest już wypełniony wniosek przelewu, który wymaga akceptacji i autoryzacji. W drugim kroku klient powraca na stronę internetową sprzedawcy, który w tym samym czasie powinien otrzymać informację o dokonanej płatności. W ostatnim kroku sprzedawca otrzymuje przelew bezpośrednio z banku lub za pośrednictwem dostawcy płatności. Przedstawiony proces nie jest jedynym, jaki dokonuje się podczas realizacji płatności elektronicznych. Możliwa jest zmiana sposobu regulacji zobowiązań np. poprzez podpięcie karty kredytowej, e-portfela bądź innych, w zależności od oferty jaką proponuje konkretny bank. Płatności internetowe dzieli się na 4 rodzaje, wyróżnione na podstawie wartości pojedynczej transakcji[71]:

- **Milipłatności** (ang. milipaymats) – to płatności mieszczące się w granicach od kilku do kilkunastu groszy. Wykorzystywane są najczęściej celem pokrycia zobowiązania w systemach *pay-per-view*, np. za przeczytany artykuł. Ze względu na możliwie najniższe koszty, wymagania dotyczące ochrony milipłatności są równie niskie.
- **Mikropłatności** (ang. micropayments) – płatności od 1zł do 80zł. Najczęściej wykorzystywane są podczas regulowania opłat za oprogramowanie pobierane z Internetu. Wymagają nieco większych zabezpieczeń.
- **Minipłatności** (ang. minipaymets) - płatności od 80zł do 800zł. Jest to najczęściej większość zakupów przeprowadzanych przez sieć. Wymagane jest zapewnienie pełnego bezpieczeństwa.
- **Makropłatności** (ang. macropaymets) – płatności powyżej 800zł. W ramach tak wysokich kwot mieszczą się zakupy komputerów, sprzętu RTV czy sprzętu AGD. Bardzo ważna jest kwestia bezpieczeństwa w tak dużych przedziałach kwotowych.

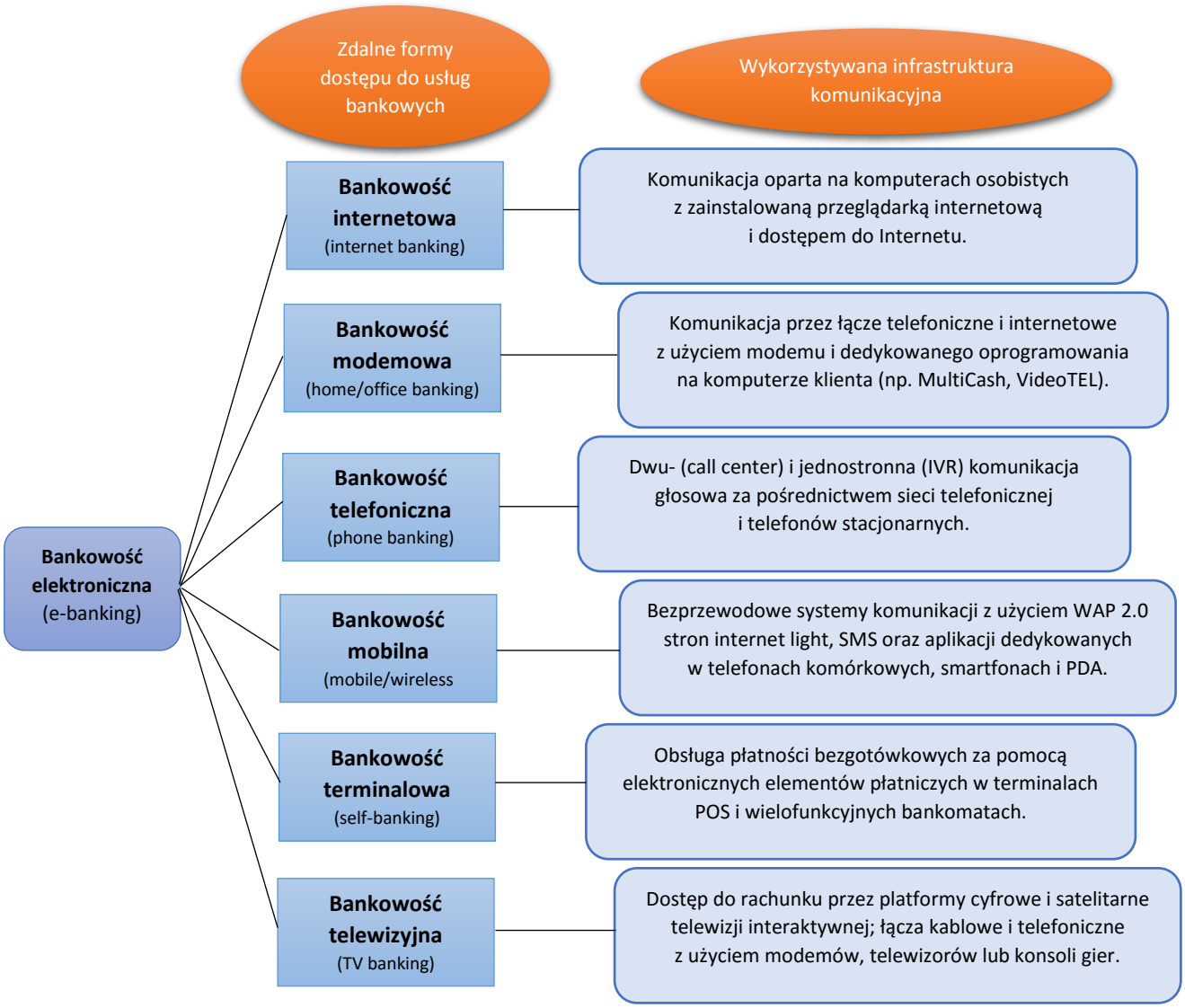
System milipłatności najczęściej jest pomijany i traktowany jako część mikropłatności. Wyróżnia się także płatności z uwzględnieniem czasu ich dokonania: płatność w czasie rzeczywistym (ang. pay now), płatność z góry, tzw. przedpłata (ang. prepaid) oraz płatność odroczona (ang. pay later)[72]. Przedstawione systemy są podstawowymi metodami płatności. W związku z ciągle rosnącym zapotrzebowaniem na przeprowadzanie transakcji

[70] Bartłomiej Choinowski, *Op. Cit.*, s. 8-9.
[71] Janina Banasikowska, *Rodzaje płatności i systemy płatności na rynku elektronicznym*, s. 181-187.
[72] Beata Świecka, *Op. Cit.*, s. 83.

bez ograniczeń czasowych i terytorialnych, dostępne są również rozwiązania oryginalne, dostosowane do możliwości Internetu w połączeniu z technologią.

## 1.4. Kanały bankowości elektronicznej

Aby zwiększyć efektywność zarządzania środkami pieniężnymi z wykorzystaniem najnowszych technologii informatycznych oraz komunikacyjnych, ukształtowały się przeróżne podziały, zależne od oferowanych przez bank usług oraz podpisanych przez Klientów umów. Zasadniczym kryterium kwalifikacji są kanały dystrybucji[73]. Podlegają ciągłej rozbudowie, są stale w użyciu, a każda z gałęzi cały czas narażona jest na działania niepożądane, dostosowane do swojej specyfiki.




Rysunek 6. Tradycyjna klasyfikacja usług bankowości elektronicznej z uwzględnieniem głównych kanałów dystrybucji i ich infrastruktury komunikacyjnej.
Źródło: Opracowanie własne na podstawie: Witold Chmielarz, *Systemy elektronicznej bankowości*.

[73] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 22-24.

Powyższy rysunek przedstawia główne kanały dystrybucji wraz z infrastrukturą komunikacyjną, z której korzystają. Ich głównym celem jest umożliwienie użytkownikowi wykorzystania przynajmniej podstawowej oferty usług udostępnianych przez banki. Na chwilę obecną, większość z tych kanałów pozwala na skorzystanie z o wiele większych funkcjonalności, niż tylko te, pierwotnie uznane za bazowe. Wynika to z wyzwań, jakie współczesna technologia stawia bankowości, również tej elektronicznej. Oferowana różnorodność kanałów dystrybucji, rozbudowana o dodatkowe funkcjonalności decyduje o prestiżu banku i wskazuje na stopień dbałości o swoich klientów.

### 1.4.1. Bankowość modemowa

Bankowość modemowa jest określeniem dwóch rozwiązań: home banking oraz office banking. Różnice pomiędzy nimi skupiają się głównie wokół grup docelowych, którym są dedykowane[74]. **Home banking**, zwany także bankowością domową, skierowany jest do klientów indywidualnych, którzy korzystają z systemu bankowości elektronicznej w zaciszu swojego mieszkania, za pośrednictwem komputera domowego, łącza telefonicznego i specjalistycznego oprogramowania. Dokonanie operacji finansowych może się odbywać zarówno w trybie rzeczywistym (on-line), jak również off-line, gdzie złożenie zlecenia, z jego realizacją dzieli odstęp czasu. Możliwe jest wykorzystanie syntezatorów mowy lub mikrofonów, które przyczyniają się do identyfikacji oraz łatwiejszej łączności z bankiem[75]. **Office banking**, nazywany także bankowością firmową lub korporacyjną, służy do obsługi klientów zbiorowych, na przykład pod postacią firm lub przedsiębiorstw. System zajmuje się uzyskaniem podstawowych informacji typu: kursy walut czy oprocentowanie kredytów i depozytów, które następnie wykorzystywane są do zarządzania przedsiębiorstwem oraz korzystaniem z ogólnodostępnych usług bankowych. Zarówno system bankowości domowej, jak i bankowości firmowej, oparte są na tzw. bankowości modemowej, co oznacza, że działają wykorzystując modem oraz specjalne oprogramowanie po stronie klienta. System korzysta z linii telefonicznych, rzadziej stałych łączy lub z telefonu ekranowego, spełniającego rolę pośrednika transmisji[76]. Usługa ta pozwala na dokonywanie tradycyjnych operacji bankowych z własnego pomieszczenia biura lub domu, choć ze względu na wysokie koszty, detaliczny klient częściej wybiera bankowość internetową.

[74] Iwona Smykla, *Analiza form zastosowania bankowości elektronicznej dla obsługi przedsiębiorstw*, s. 21.
[75] Beata Świecka, *Op. Cit.*, s. 22.
[76] Iwona Smykla, *Op. Cit.*, s. 21.

### 1.4.2. Bankowość internetowa

Bankowością internetową określa się formę świadczenia usług, z wykorzystaniem ogólnodostępnej sieci Internet, standardowego oprogramowania, jakim jest przeciętna przeglądarka lub oprogramowania służącego łączności z bankiem (home/corporate banking) [77]. Z tego też powodu, w literaturze można znaleźć podziały, zgodnie z którymi bankowość domowa i korporacyjna, figurują jako elementy bankowości internetowej. Obecnie wyróżnia się trzy modele funkcjonowania usług przez Internet[78]:

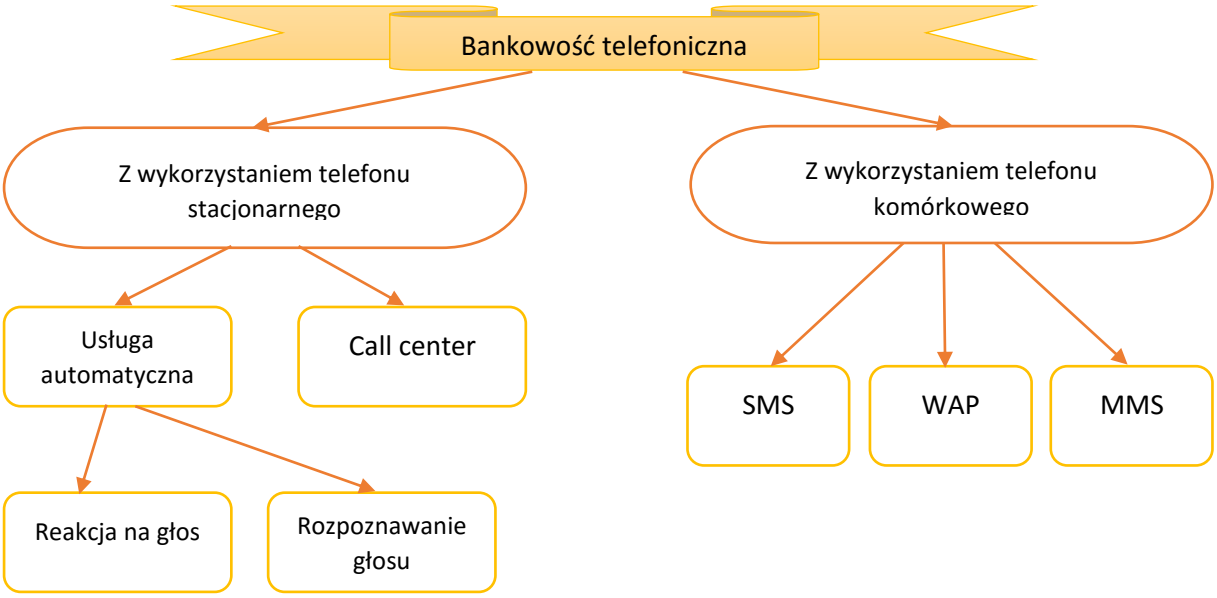
- *model wielokanałowy (ang. Bricks & Cliks)* – to model banku, który oferuje wszystkie lub najważniejsze kanały dystrybucji, traktując Internet jako źródło alternatywne. Posiada również tradycyjne kanały dystrybucji w postaci oddziałów bankowych.
- *model banku wirtualnego (ang. Cliks only)* – to model banku, którego podstawą jakichkolwiek działań, a nawet istnienia jest Internet. Wszelkie operacje finansowe dokonywane są za pomocą elektronicznych metod.
- *model banku supermarketu finansowego* – to bardzo specyficzny model, zdecydowanie odmienny od dwóch poprzednich. Bank występuje w roli doradcy i pośrednika finansowego w sieci. Celem jest oferowanie usług innych banków, biur maklerskich oraz ubezpieczycieli, co wiąże się z szerokim wykorzystaniem outsourcingu finansowego, często pod własną marką.

Za jej główne cechy, z punktu widzenia klienta uznano[79]: brak ograniczeń terytorialnych, oszczędność czasu, kontrolę finansów, brak ograniczeń czasowych, niskie koszty transakcji, łatwość skorzystania z ofert innego banku. Ze strony banku, są to[80]: niskie stałe koszty, niski koszt obsłużenia klienta, tania aktualizacja informacji, możliwość większych zysków, większe możliwości marketingowe.

### 1.4.3. Bankowość telefoniczna

Jedną z pierwszych zautomatyzowanych usług bankowości jest bankowość telefoniczna. Jest to usługa, która do obustronnej komunikacji klienta z bankiem wykorzystuje telefon. Ze względu na rodzaj stosowanego telefonu, wyróżnia się dwa typy: bankowość telefoniczną (ang. phone banking) oraz bankowość mobilną (ang. mobile banking).

[77] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 24.
[78] Michał Polasik, *Bankowość elektroniczna…, Op. Cit.*, s. 29-32.
[79] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 69-70.
[80] *Ibidem*, s. 70.




*Rysunek 7. Klasyfikacja bankowości telefonicznej.*
*Źródło: Opracowanie własne na podstawie: Iwona Smykla,*
*Analiza form zastosowania bankowości elektronicznej dla obsługi przedsiębiorstw.*

Rysunek 7 przedstawia jednoznaczną klasyfikację bankowości elektronicznej i jej poszczególnych elementów składowych. **Phone banking** to najstarsza forma zdalnej komunikacji klienta z bankiem, która zamyka się w dwóch rozwiązaniach: call center oraz usłudze automatycznej. Call center to nic innego, jak telefoniczny serwis banku, wykorzystujący dwustronną komunikację głosową. Obsługiwany przez operatora banku, który dokonuje identyfikacji klienta poprzez podanie hasła lub zadanie szeregu pytań. Operacje, których można dokonać tą metodą są bardzo zróżnicowane i zależą od ofert konkretnych banków. Najczęściej jednak, możliwe jest zrealizowanie przelewu, sprawdzenie salda i historii zleceń, założenie lokaty, obsługa karty kredytowej oraz uzyskanie informacji o ofertach banku[81]. Usługa automatyczna, krócej określana jako IVR (ang. Interactive Voice Response) to bankowy serwis, wykorzystujący jednostronną komunikację głosową. Zadaniem automatycznego operatora jest pomoc klientowi w przejściu przez kolejne etapy rozmowy. Klient steruje rozmową używając klawiatury telefonu, dzięki niej dokonując wyboru odpowiedzi na otrzymane komunikaty głosowe. Usługa ta wspierana jest przez dwie technologie. System reagujący na głos (ang. voice response) działa w bezpośrednim połączeniu z systemem komputerowym banku. Rozpoznaje wysokość dźwięków wydawanych przez klawisze telefonu i na tej podstawie wykonywane są konkretne operacje bankowe. W związku z czym, niezbędna jest aktywność użytkownika. System rozpoznawania głosu

[81] Witold Chmielarz, *Op. Cit.*, s. 19.

(ang. voice recognition) poddaje analizie polecenia wydane głosem, na ich podstawie realizuje zleconą operację i za pomocą syntezatora mowy generuje odpowiedź zwrotną. Jakość tej metody uzależniona jest od zastosowanego oprogramowania służącego tworzeniu i rozpoznawaniu mowy. Technologia IVR pozwala na sprawdzenie salda rachunku, otwarcie lub zamknięcie rachunku terminowej lokaty oszczędnościowej oraz realizację przelewu[82]. Jak widać, jest dość mocno ograniczony w zakresie swojego działania, tym bardziej, że nie przewiduje sytuacji, a tym bardziej realizacji operacji precedensowych, których obsługa w przypadku call center zostanie zlecona do wykonania. IVR nie obejmuje w swoim działaniu aktywności, które nie zostały wcześniej odpowiednio zdefiniowane w bankowym automatycznym serwisie telefonicznym.

**Mobile banking** opiera się na telefonach komórkowych lub innych przenośnych urządzeniach. Bardzo szybko zyskuje uznanie, podążając tuż za popularnością bankowości internetowej. Jej główną zaletą jest połączenie funkcjonalności telefonu i komputera, przez co pozwala między innymi na: identyfikację użytkownika, przekazanie różnego rodzaju informacji (np. głos, impulsy tonowe, dane), wprowadzenie i edycję danych na ekranie a także przetwarzanie danych[83]. Bankowość mobilna składa się z 3 elementów: SMS, WAP i MMS. *SMS Banking (ang. Short Messaging Service Banking)* wykorzystuje krótkie wiadomości tekstowe w dwóch formach: usługi push oraz usługi pull.

| Usługa typu push | Usługa typu pull |
|---|---|
| Zrealizowanie przelewu | Uzyskanie informacji o saldzie rachunku |
| Odrzucenie przelewu | Wykonanie przelewu (na wcześniej zdefiniowane rachunki odbiorców) |
| Zmiana salda | Uzyskanie informacji o predefiniowanym rachunku klienta |
| Wystąpienie debetu | Otrzymanie wykazu ostatnio przeprowadzanych operacji |

Tabela 2. Zestawienie usług typu push i pull

*Źródło: Opracowanie własne na podstawie: Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, Usługi bankowości elektronicznej dla klientów detalicznych – charakterystyka i zagrożenia.*

Powyższa tabela przedstawia możliwości konkretnych usług. Usługi typu push odpowiadają za automatyczne generowanie i wysyłanie krótkich wiadomości, informując klienta o zdarzeniach, które miały miejsce w obrębie jego rachunku. Usługi typu pull, umożliwiają klientowi

[82] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 39-40.
[83] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 56.

wykonanie określonych operacji, za pomocą wysłania krótkiej wiadomości tekstowej[84]. *Protokół WAP (ang. Wireless Application Protocol)* stworzony, aby umożliwić stały dostęp do Internetu posiadaczom urządzeń bezprzewodowych. Umożliwia dostęp do stron internetowych bankowości, z uwzględnieniem ograniczeń technicznych oraz łącza danych[85]. Ostatnim typem jest *MMS (ang. Multimedia Messaging Service)*, będący bardziej rozbudowanym odpowiednikiem wiadomości SMS. Jego główne cechy to: mniejsze ograniczenia dotyczące ilości znaków, a także pełna multimedialność, co pozwala na dołączenie dźwięków, animacji czy filmów do wiadomości. Najczęściej stosowane przy rozpowszechnianiu materiałów marketingowych, reklam, infoserwisów z kursami walut, wiadomościami z giełd czy prognozami gospodarczymi. Poza opisanymi formami usług, o wiele rzadziej wyróżnia się: PDA (ang. Personal Data Assistant) oraz SIM Aplication Toolkit (STK)[86]

### 1.4.4. Bankowość terminalowa

Najstarsza, a za razem najczęściej wykorzystywana forma bankowości elektronicznej to bankowość terminalowa, nazywana również bankowością samoobsługową[87]. Umożliwia zarządzanie własnym rachunkiem, bez pośrednictwa pracownika banku, ale z wykorzystaniem następujących urządzeń bankowych[88]:

- bankomaty
- elektroniczne terminale do akceptacji kart
- kioski multimedialne

Powszechnie znane i używane **bankomaty** są to urządzenia, które pozwalają posiadaczom kart płatniczych, na dokonywanie bankowych operacji gotówkowych oraz bezgotówkowych. Głównie wykorzystywany do wypłaty pieniędzy, choć możliwe jest także wpłacanie pieniędzy na rachunki w dowolnie wybranym banku, przelew środków między rachunkami, otwarcie, edycja lub likwidacja stałych zleceń, otwieranie i zamykanie lokat, sprawdzanie stanu konta, a nawet doładowania telefonów[89]. Wśród podstawowych elementów z jakich składa się przeciętny bankomat wymienia się: personalny komputer z klasycznym systemem operacyjnym, czytnik paska magnetycznego, urządzenie do wpłacenia pieniędzy ze skarbca

[84] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 41.
[85] *Wireless Application Protocol*, [data dostępu: 5 grudnia 2015r], <https://pl.wikipedia.org/wiki/Wireless_Application_Protocol>.
[86] Katarzyna Korzeń, *Op. Cit.*, s. 34-35.
[87] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 16.
[88] Iwona Smykla, *Op. Cit.*, s. 25.
[89] Beata Świecka, *Op. Cit.*, s. 24.

wbudowanego w bankomat, drukarkę dzienną operacji i drukarkę wyciągów. Wprowadzone oprogramowanie mikrokomputera odczytuje dane z karty bankowej, sprawdza ich poprawność oraz realizuje polecenia w zależności od trybu pracy jakiemu podlega[90]. Mogą pracować w systemie off-line, co oznacza, że nie są bezpośrednio połączone z bankiem, więc autoryzacja opiera się o limity wypłat z bankomatu. Poprzez brak połączenia z centralą bazy danych, bankomat nie wie ile pieniędzy znajduje się na koncie klienta. Tryb pracy on-line, pozwala na natychmiastowe przekazanie informacji o dyspozycjach do banku i tym samym, bezzwłoczne obciążenie konta klienta. Miejsca usytuowania bankomatów dzieli się na 3 lokalizacje: *wewnętrzne* – wewnątrz pomieszczeń, na przykład w bankach, *przyścienne* – posiadające monitor z panelem operacyjnym na zewnątrz budynku, a część pozostałą w banku oraz *zewnętrzne*, gdzie znajdują się poza bankiem jako urządzenie wolnostojące[91].

**Elektroniczne terminale do akceptacji kart**, czyli tzw. Terminale POS (ang. Point of Sale Terminal) posiadają czytnik danych z paska magnetycznego i mikroprocesora, dzięki czemu możliwe jest dokonanie transakcji w punkcie akceptującym karty. Działają w oparciu o standardowe łącza telekomunikacyjne lub przenośne łącza GSM[92].

Ostatnim urządzeniem wspierającym bankowość terminalową są **kioski multimedialne**, podłączone do sieci Internet i bazujące na wideokonferencji. Beata Świecka podkreśla dwie funkcje użytkowe kiosków multimedialnych: *jako punkty informacyjne (ang. Point of Information),* dostarczające danych na temat czasu pracy i kompetencji w sferze administracyjnej oraz *jako punkty sprzedaży (ang. Point of Sales)* wykorzystywane przede wszystkim w bankowości, celem finalizacji podstawowych operacji bankowych[93].

[90] Katarzyna Korzeń, *Op. Cit.*, s. 18.
[91] Beata Świecka, *Op. Cit.*, s. 26.
[92] *Ibidem*, s. 27-30.
[93] *Ibidem*, s.30.

### 1.4.5. Bankowość telewizyjna

Ostatnim kanałem dystrybucji jest bankowość telewizyjna, która udostępnia elementy bankowości elektronicznej m.in. za sprawą telegazety, telewizji cyfrowej, satelitarnej czy kablowej. Istnieją niejako dwa kanały dystrybucji usług bankowych pod tą postacią[94]:

- **Kanał satelitarny**, porównywalny z telegazetą. Użytkownik zgłasza chęć uzyskania konkretnych informacji poprzez wybranie odpowiedniej opcji w bezpłatnej aplikacji. Jej informacyjny charakter przejawia się w możliwościach jakie oferuje np.: dostęp do informacji w zakresie danych o koncie, ostatnich operacjach czy wolnych środkach.
- **Kanał modemowy**, do którego niezbędne jest uzyskanie aktywacji modemu zainstalowanego w dekoderze cyfrowym i wykonanie połączenia z modemem docelowym. W odróżnieniu od kanału satelitarnego umożliwia wykonanie przelewów, założenie lokat czy złożenia zamówienia na kartę płatnicza. Jest to także o wiele bardziej wymagające rozwiązanie, gdyż trzeba brać pod uwagę koszty związane z użytkowaniem linii telefonicznej oraz ewentualnych opłat dla dostawcy usług internetowych.

W literaturze można znaleźć wiele zalet tej formy bankowości, wśród których wyróżnia się niskie koszty dla konsumentów, ogólną dostępność odbiorników cyfrowych w gospodarstwach domowych użytkowników, możliwość jednoczesnej dystrybucji innych usług oraz system *user friendly* (tzn. bardzo łatwy w obsłudze, dla użytkownika końcowego)[95]. Są to znaczące cechy, lecz przy zestawieniu ich z brakiem infrastruktury teleinformatycznej pozwalającej na przesył dużych ilości danych, nastawienie tego medium głównie na pasywny odbiór i konsumpcję rozrywki, a także ogromnym rozwojem innych, mimo wszystko, bardziej dostępnych kanałów bankowości, skutecznie ograniczyły popularność i rozwój bankowości telewizyjnej.

W powyższym rozdziale przybliżono istotę bankowości elektronicznej, szczegółowo uzupełniając jej obraz o wybrane instrumenty płatnicze, formy płatności oraz dostępne kanały dystrybucji i inne części składowe. Dokładność konkretnych opisów sporządzona została celowo, aby przedstawiając dostępne narzędzia i schemat działania uświadomić, iż każdy z przedstawionych elementów łączący użytkownika z jego kontem bankowym, narażony jest na niebezpieczeństwo.

---

[94] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 62-63.
[95] *Ibidem*, s. 63.

# Rozdział II
# Wybrane zagrożenia bankowości elektronicznej

W świecie wciąż postępującego rozwoju technologicznego, gdzie niemal każdy posiada dostęp do Internetu, świat rzeczywisty częściowo lub w całości (w zależności od dziedziny życia) przenosi się do świata wirtualnego. Podobnie przestępstwa popełniane w świecie rzeczywistym, znalazły swoje odzwierciedlenie w sieci. Zjawisko to określa się mianem: „przestępstwa komputerowego", „przestępstwa związanego z wykorzystaniem komputera", „przestępstwa internetowego", „cyberprzestępstwa", „przestępstwa związanego z technologią cyfrową". Terminologia zawarta w Konwencji Rady Europy o cyberprzestępczości, jako termin właściwy wskazuje „cyberprzestępstwo". Przyjęło się użycie nazwy „przestępstwo komputerowe", co wynika ze zbieżności występujących w językach innych państw, jak na przykład: „*computer criminality*" czy „*Computerkriminalität*"[96]. Jak widać, wybór adekwatnego terminu rodzi wiele problemów, nie inaczej jest w przypadku jasnego, jednorodnego zdefiniowania tego zjawiska.

Przestępczość komputerową początkowo rozumiano na dwa sposoby: po pierwsze - jako określoną grupę czynów, które polegały na naruszeniu jakiegokolwiek dobra prawnego chronionego prawem karnym przy pomocy komputera, po drugie, jako przestępstwa popełnione przez osoby posiadające wysokie umiejętności i wiedzę z zakresu elektroniki lub informatyki[97]. K.J. Jakubski precyzyjniej zdefiniował przestępstwo komputerowe, traktując je jako „zjawisko kryminologiczne, obejmujące wszelkie zachowania przestępcze związane z funkcjonowaniem elektronicznego przetwarzania danych, godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz w całym systemie połączeń komputerowych, a także w sam sprzęt komputerowy oraz prawo do programu komputerowego"[98]. Aby zapewnić możliwie najwyższy poziom bezpieczeństwa teleinformatycznego, ciągle dokonuje się nowelizacji polskiego prawa karnego materialnego oraz procedur karnych, które w dużym stopniu odpowiadają standardom wyznaczonym przez ustawodawstwo unijne i Konwencję o cyberprzestępczości. Podejmowane inicjatywy i ciągle trwające prace naukowo-badawcze stanowią problem dla użytkowników sieci informatycznych, głównie ze względu na złożoność i czasochłonność wielu proponowanych

[96] Anna Zalesińska, *Technologia informacyjna dla prawników*, Wrocław 2011, s. 79.
[97] Maciej Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 10.
[98] K.J.Jakubski, *Przestępczość komputerowa – podział i definicja*, „Przegląd Kryminalistyki", nr 2/7, 1997, s.31.

procesów oraz występujące luki zabezpieczeń[99]. W związku z tym, Międzynarodowa Organizacja Policji Kryminalnych „Interpol" dzieli przestępczość w zakresie technologii komputerowych na sześć obszarów[100]:

a) naruszanie praw dostępu do zasobów,
b) przechwytywanie danych; kradzież czasu, czyli korzystanie z systemu poza uprawnionymi godzinami; modyfikację zasobów przy pomocy bomby logicznej, konia trojańskiego, wirusa i robaka komputerowego,
c) oszustwa przy użyciu komputera (w szczególności oszustwa bankowe; fałszowanie urządzeń wejścia lub wyjścia, np. kart magnetycznych lub mikroprocesorowych; oszustwa poprzez podanie fałszywych danych identyfikacyjnych; oszustwa w systemach telekomunikacyjnych),
d) powielanie programów,
e) sabotaż zarówno sprzętu jak i oprogramowania,
f) przechowywanie zabronionych prawem zbiorów:
    a. przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (nielegalny dostęp, nielegalne przechwytywanie danych, naruszenie integralności danych lub systemu, niewłaściwe użycie urządzeń),
    b. przestępstwa komputerowe (fałszerstwo, oszustwo komputerowe),
    c. przestępstwa ze względu na charakter zawartych informacji,
    d. przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Powyższe zestawienie prezentuje ogólny podział cyberprzestępczości. Każdy z wymienionych jest zaledwie wprowadzeniem do zagrożeń, jakie kryją się pod jego ramową postacią.

Rozdział drugi, w całości poświęcony został niebezpieczeństwom występującym w sieci. Przybliża sylwetkę przeciętnego cyberprzestępcy, wskazując jego uniwersalne cechy i kierujące nim motywy. Następnie przybliża ogólną charakterystykę występujących zagrożeń. Pozostała część rozdziału poświęcona została przedstawieniu kluczowej wartości danych osobowych w kontekście zagrożeń wynikających z socjotechniki oraz bardziej szczegółowo omówionym, najpowszechniejszym zagrożeniom, z jakimi zmaga się przeciętny klient

[99] Anna Zalesińska, *Op. Cit.*, s. 80.
[100] *Ibidem*, s. 81.

bankowości elektronicznej, w odniesieniu do bankowości terminalowej, internetowej oraz telefonicznej.

## 2.1. Profil cyberprzestępcy

Biorąc pod uwagę treść definicji cyberprzestępstwa, może się wydawać, iż do dokonania przestępstwa komputerowego wystarczy komputer i sieć. Należy jednak pamiętać, że mimo ciągłych badań i postępów z dziedziny sztucznej inteligencji, aktualny stan rozwoju techniki nie pozwala na samoczynną działalność kryminalną komputerów. Każde przestępstwo w sieci, ściśle związane jest z działalnością przynajmniej jednego człowieka, który odpowiedzialny jest za pomysł, opracowanie i wprowadzenie w życie niezgodnego z prawem planu. Aby możliwe było odnalezienie cyberprzestępcy, stosuje się całe mnóstwo różnorodnych metod, próbując zrozumieć cele i motywy jego działania. Tworzone są profile cyberprzestępców (ang. *criminal profiling*), będące nauką, a jednocześnie sztuką, polegającą na opisaniu fizycznych, intelektualnych oraz emocjonalnych charakterystyk przestępców, na podstawie informacji, które zebrano na miejscu przestępstwa. Jest to psychologiczna ocena, składająca się ze zbioru określonych cech. Bardzo prawdopodobny jest fakt, iż są one wspólne dla osób, które popełniają ściśle określony rodzaj przestępstw. Jego celem jest zawężenie pola podejrzeń, stworzenie odniesienia do powiązanych przestępstw oraz dostarczenie cennych wskazówek postępowania, osobom je prowadzącym. Taki profil tworzony jest tuż przed ustaleniem tożsamości sprawcy[101]. Dzięki niemu, możliwe stało się stworzenie profilu typowego cyberprzestępcy, bogatego w ogólne cechy, które często w większości pasują do sprawców wszystkich typów. Wśród nich wymienia się[102]:

- przynajmniej minimalna sprawność techniczna,
- lekceważenie prawa i poczucie, że przebywa się ponad nim lub poza jego zasięgiem,
- aktywna wyobraźnia,
- chęć podporządkowania sobie innych i (lub) skłonność do podejmowania ryzyka,
- silne, zróżnicowane motywacje.

Ludzie z reguły używają narzędzi, którymi potrafią się posługiwać w sposób swobodny i komfortowy, szczególnie w sytuacji podejmowania ryzyka. Znajomość podstawowych zadań

[101] Debra Littlejohn Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004, s.109-113.
[102] *Ibidem*, s. 120-121.

i funkcjonalności jest niezbędna, a w razie jakichkolwiek wątpliwości zawsze pomocny okazuje się Internet.

Często zdarza się, że osoby, w szczególności przestępcy, widzą samych siebie w ciemnych barwach, a łamane przez siebie prawo usprawiedliwiają krótkim stwierdzeniem, że w całości lub częściowo prawo jest złe. W związku z tym, najłatwiej przychodzi im jego nieprzestrzeganie. Czynią to ze świadomością i pogardą, jednocześnie uznając za uczciwe łamanie praw, z którymi sami się nie zgadzają. Internet to także miejsce spełnienia wielu ludzkich fantazji. Dzięki temu możliwe staje się tworzenie fikcyjnych tożsamości, które utrudniają identyfikację rzeczywistych osób. Również nierzadkie marzenia o zawładnięciu całym światem i sprawowaniu kontroli przyczyniają się do podejmowania niezgodnych z prawem czynów. Każde przestępstwo, mniej lub bardziej przemyślane, wymaga czasu, energii i niemniej ważnego elementu jakim jest motywacja. To ona najczęściej stanowi pewnego rodzaju impuls, będący czynnikiem decydującym o powodzeniu całego przedsięwzięcia. Powszechnie wymienia się następujące powody[103]:

- dla zabawy,
- dla zysku,
- ze złości, zemsty i z innych powodów emocjonalnych,
- z motywów politycznych,
- pod wpływem pożądania seksualnego,
- z powodu poważnej choroby psychicznej.

Jak widać, powody są przeróżne. Ze względu na cel działania oraz rodzaj i poziom posiadanej wiedzy teoretycznej, a także umiejętności praktycznych, wyróżnia się kilka typów cyberprzestępców. Poniżej przedstawiono je pod kątem dwóch istotnych kategorii [104]:

- **Przestępcy, dla których Internet jest narzędziem służącym do popełniania przestępstw:**
  - *Przestępcy w „białych kołnierzykach”*

    Nie przypadkowo nazwa kojarzy się z urzędniczym strojem pod postacią białej koszuli. Bardzo często nie jest ona tak nieskazitelna, jak wymagałaby tego pełniona przez nich funkcja, niewątpliwie jednak, wiąże się z zaufaniem publicznym. Znanych jest wiele przestępstw, których się dopuszczają i wymienia się wśród nich:

[103] *Ibidem*, s. 122-128.
[104] *Ibidem*, s. 128-137.

- Zmianę treści rekordów w firmowych komputerach, efektem czego jest wypłata nienależnego wynagrodzenia, usunięcie negatywnych ocen bądź wpisanie dodatkowych kosztów,
- Złamanie zasad U.S. Securities and Exchange Commision (SEC) poprzez zyskanie dostępu, wykorzystanie wewnętrznych informacji, a następnie zakup akcji lub ubezpieczeń,
- Manipulowanie kontami elektronicznymi w celu przywłaszczenia sobie pieniędzy klienta lub firmy,
- Modyfikacja firmowych ksiąg lub informacji finansowych, których celem jest przekazanie fałszywych danych kredytodawcom, inwestorom itp.

Przestępcy tego typu wzbudzają podejrzenia głównie ze względu na niewyjaśnione źródła dochodu, dokonywanie wielu transakcji gotówką, posiadanie wielu kont bankowych w różnych bankach, miastach lub nawet krajach.

- *Oszuści komputerowi*

Są to osoby, które dzięki internetowym narzędziom typu: e-mail, strony WWW lub przykładowe pokoje czatowe, intensywnie poszukują swoich ofiar. Na listach Federalnej Komisji ds. Handlu, wśród najczęstszych oszustw sieciowych (według Online Buyer's Guide) można znaleźć:

- Aukcje internetowe – uczestnicy nie otrzymują zamówionych towarów pomimo, iż wcześniej wysłali pieniądze,
- Wyłudzanie pieniędzy na usługi – klienci opłacają dostęp do konkretnych usług, których nie otrzymują w późniejszym czasie bądź zostają namówieni do kupna usług, których nie potrzebują,
- Oszustwa dotyczące kart kredytowych – głównym celem jest zebranie danych dotyczących karty kredytowej, aby w późniejszym czasie móc dokonywać zakupów za ich pomocą,
- Cramming sieciowy – polegający na udostępnieniu usług na okres próbny i natychmiastowe obciążenie rachunków telefonicznych lub kart kredytowych tuż po zakończeniu okresu próbnego,
- Marketing wielopoziomowy (MLM – Multilevel Marketing) i piramidy finansowe – polegają na nakłanianiu ofiar na pokaźne kwoty pod określonym pretekstem.

- *Hakerzy, krakerzy i włamywacze sieciowi*

  Społeczność hakerska cechuje się licznymi podziałami, wyszczególnionymi ze względu na różne kategorie. Zgodnie z podziałem stworzonym przez Billa Landreth'a, wymienia się następujące typy[105]: nowicjusz, analityk, turysta, wandal oraz złodziej. Analizując mentalność hakera, podział jest bardziej ogólny, lecz zyskuje na swojej wyrazistości. Głównie wyróżnia się „czarne kapelusze" i „białe kapelusze", choć pojawiają się również „szare kapelusze". Czarne kapelusze (ang. *black hat*) stanowi grupa hakerów, których działalność prowadzona jest poza granicami prawa bądź ściśle z nimi graniczy. W nielegalny sposób wykorzystują luki i błędy, czerpiąc z nich własne korzyści lub publikują je pod postacią gotowych do użytku programów (tzw. exploitów), przeznaczonych dla użytkowników mniej zaawansowanych. Grupa białych kapeluszy (ang. *white hat*) stanowi ich całkowite przeciwieństwo. Ich działalność prowadzona jest zgodnie z prawem, a wszelkie napotkane luki lub błędy są opisywane, a następnie zgłaszane do właścicieli aplikacji. Aktywność białych kapeluszy sprawdza się również w zakresie testowania systemów pod kątem poprawienia ich zabezpieczeń[106]. Szare kapelusze (ang. *grey hat*) to mniej liczna grupa, będąca połączeniem działań wykonywanych przez czarne i białe kapelusze. Działają w granicach prawa, a także poza nią[107].

Drugą z kategorii jest grupa przestępców, dla których sieć jest jedynie narzędziem dodatkowym i służy głównie do wyszukiwania ofiar, przechowywania danych lub kontaktu ze wspólnikami za pomocą e-maili lub usług czatowych. Profil przestępcy jest istotnym elementem, dającym możliwość przewidzenia jego zachowań bądź potencjalnych zagrożeń. Dzięki temu możliwa jest wcześniejsza analiza i dokonanie odpowiednich zabezpieczeń albo przynajmniej uwrażliwienie użytkowników i wyostrzenie ich uwagi na pewne zachowania oraz ograniczenie zaufania.

## 2.2. Ogólna charakterystyka zagrożeń

Zagadnienie bezpieczeństwa bankowości elektronicznej bardzo często przedstawia się w ogólnym ujęciu, tym samym spłycając wielkość problemu i zamykając ją w obrębie najpopularniejszych trudności związanych z hasłem dostępu bądź podpisem cyfrowym. Tymczasem kwestia ta, obejmuje niemalże wszystkie aspekty bezpieczeństwa

[105] Józef Bednarek, *Cyberświat: możliwości i zagrożenia*, Warszawa 2009, s.357.

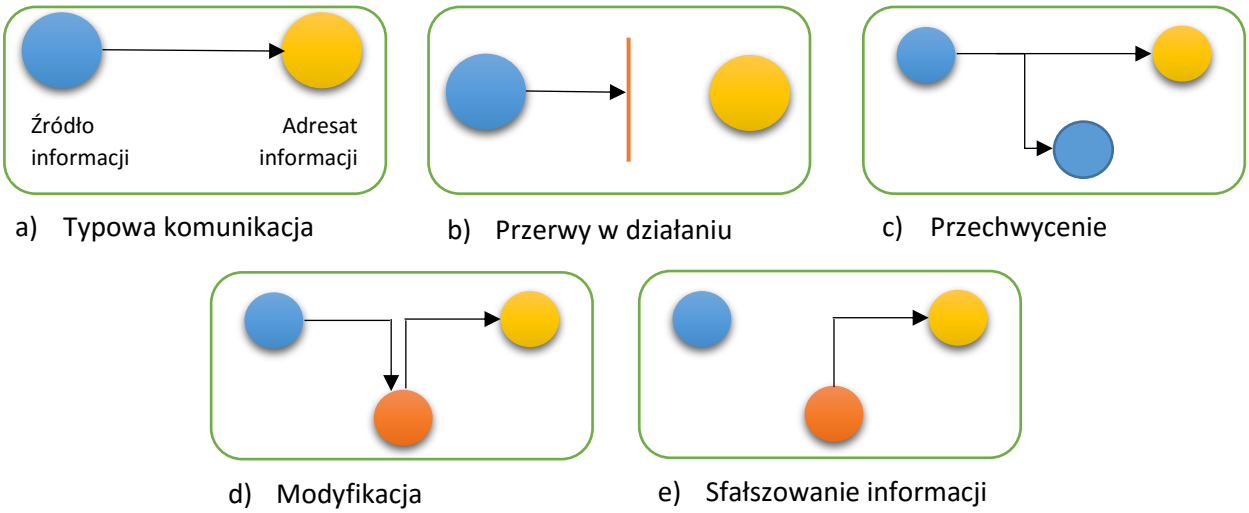
[106]

[107] Cyberwojna, [dostęp:17.03.2016], <http://securelist.pl/analysis/26,analiza_mentalnosci_hakera.html>

teleinformatycznego, przez co staje się niezwykle złożonym zagadnieniem. W znaczeniu informatycznym, bezpieczeństwo traktuje się jako pewien stan, charakteryzowany określonym poziomem najważniejszych atrybutów[108] [109]:

- **Poufność** (ang. *confidentiality*): dostęp do danych przechowywanych i przetwarzanych w systemie posiadają tylko uprawnione do niego osoby, podmioty lub procesy,
- **Integralność** (ang. *integrity*): składają się na nią dwa podrzędne elementy: integralność danych oraz integralność systemu, są gwarancją na niezmienność danych i informacji przesyłanych w czasie transmisji elektronicznej,
- **Autentyczność** (ang. *authenticity*): dzięki której sprawdza się zgodność podmiotu z tym, za jakiego się podaje,
- **Niezaprzeczalność** (ang. *accountability*): będąca potwierdzeniem nadania lub odbioru komunikatu drogą elektroniczną,
- **Dostępność** (ang. *availability*): pozwalająca na stały dostęp do systemu bankowości elektronicznej poprzez autoryzowany dostęp,
- **Niezawodność** (ang. *reliability*): gwarantująca działanie systemu w oczekiwany sposób.

Biorąc pod uwagę wymienione atrybuty bezpieczeństwa, można na ich podstawie określić potencjalne zagrożenia bankowości elektronicznej, uwzględniając cztery typy ataków na system informatyczny[110].




Rysunek 8. Podział ataków na bezpieczeństwo systemów informatycznych
*Źródło: Opracowanie własne na podstawie: William Stallings, Systemy operacyjne – Struktura i zasady budowy*

[108] Andrzej Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006, 2007, s. 35.
[109] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 75.
[110] William Stallings, *Systemy operacyjne – Struktura i zasady budowy*, Warszawa 2006, s. 756-758.

Podczas typowego przepływu danych (ilustracja „a"), informacje przekazywane są ze źródła do adresata. Cztery pozostałe ilustracje obrazują ogóle kategorie ataków. Ilustracja „b" przedstawia przerwy w działaniu. Odnosi się ona do braku możliwości skorzystania z systemu, braku dostępności systemu lub zniszczenia danego zasobu systemu. Jest to atak przeciwdziałający właściwości dostępności. Przykład: zniszczenie dysku twardego, odcięcie łącza komunikacyjnego. Na ilustracji „c" widnieje sytuacja przechwycenia będąca atakiem na poufność danych, gdzie dane lub informacje trafiają do osób, programów lub komputerów do tego nieupoważnionych. Przykład: nielegalne kopiowanie oprogramowania lub plików, podpięcie się pod łącze celem uzyskania danych. Modyfikacja (ilustracja „d") stanowiąca trzeci rodzaj ataku skupia się na ingerencji w integralność danych. Podmiot zyskuje nielegalny dostęp do systemu i dodatkowo ma możliwość dokonywania zmian w jego zasobach. Przykład: modyfikacja zawartości komunikatów przesyłanych w sieci. Ostatnia ilustracja „e" przedstawia sytuację fałszowania informacji. Jest to atak na system autoryzacji, gdzie nieautoryzowany podmiot, umieszcza w systemie sfałszowane obiekty. Przykład: wstawianie rekordów do pliku. Nie sposób pominąć kwestii klasyfikacji zagrożeń dokonywanych na podstawie przeróżnych kryteriów. Najczęściej występującymi w literaturze są[111]:

- **Bierne i czynne**

  Zwane również pasywnymi i aktywnymi. Zagrożenia bierne występują w sytuacji nieuprawnionego ujawnienia informacji, lecz bez narażenia i wpływu na system informatyczny. Przykładem mogą być: podsłuch oraz analiza ruchu w sieci. Zagrożenia czynne, aktywnie oddziałują na system. Spowodowane są najczęściej przez pracowników banku w formie stosowanych nadużyć lub zwykłych przeoczeń[112].

- **Wewnętrzne i zewnętrzne**

  Zagrożenia wewnętrzne wynikają z działań legalnych użytkowników systemu lub sieci. Głównymi czynnikami odpowiedzialnymi za ich powstawanie są: brak polityki bezpieczeństwa, nadmierne przywileje pracowników, brak dokumentowania zdarzeń, brak planów ciągłości działania oraz brak lub zbyt późna reakcja na nieprawidłowości. W następstwie dochodzi do popełniania błędów, przeoczeń oraz celowych nadużyć. Zagrożenia zewnętrzne występują za sprawą intruzów, którzy dążą do uzyskania biernego lub czynnego dostępu do zasobów systemu[113].

[111] Dariusz Wawrzyniak, Op. Cit., s. 40.
[112] *Ibidem*, s. 40.
[113] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 76.

- **Przypadkowe i celowe**

  Zagrożenia przypadkowe opierają się o błędy i przeoczenia powodowane przez użytkowników oraz awarie sprzętu i błędy w oprogramowaniu, nie wykryte podczas testów. Celowe zagrożenia powodowane są umyślnie przez użytkowników systemu[114].
- **Sprzętowe i programowe**

  Zagrożenia sprzętowe wynikają z nieprawidłowości w funkcjonowaniu sprzętu komputerowego. Natomiast programowe – z błędnego działania oprogramowania.

Wymienione grupy w żaden sposób się nie wykluczają, co więcej, ściśle współpracują z wcześniej przedstawionymi typami ataków. System bankowości elektronicznej stanowi indywidualny przypadek systemu informatycznego, gdzie serwer (bank) i klient (użytkownik systemu) posiadają nieco odmienne obowiązki i zadania, których celem jest zapewnienie bezpieczeństwa całemu procesowi przetwarzania danych[115]. W związku z tym, dodatkowo wyodrębnia się trzy grupy zagrożeń[116]:

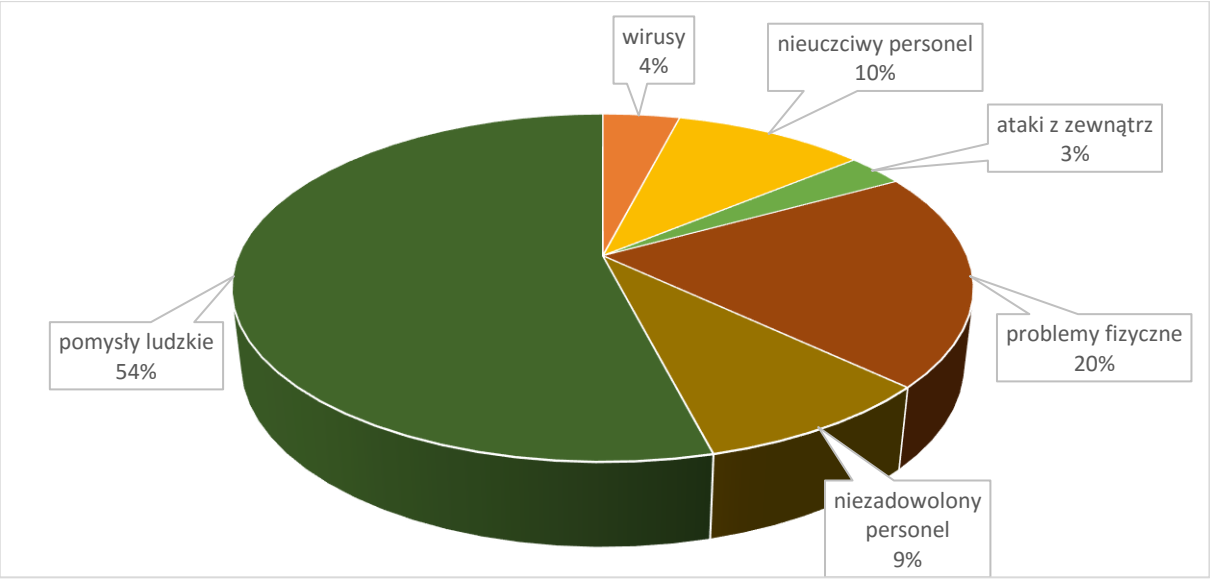
- *wspólne dla serwera i klienta*, związane z podsłuchiwaniem lub modyfikacją danych przesyłanych sieciami,
- *serwera*, związane z atakami na zasoby serwera,
- *klienta*, związane z procedurami logowania się do systemu oraz pracy z oprogramowaniem klienta.

Na każdą z tych grup składają się pewne zachowania i sytuacje, stanowiące różnorodne zagrożenia, zależne od źródła swojego pochodzenia. Określenie tych zbiorowości pomaga przeciwdziałać konkretnym, powielającym się negatywnym postępowaniom.

## 2.1. Przestępstwa w bankowości elektronicznej w Polsce

Rozwój technologii przyniósł wiele korzyści w różnych dziedzinach życia codziennego. Przede wszystkim przyczynił się do rozwoju wszelkich zagrożeń, również tych występujących w sieci. A. Gospodarowicz sporządził zestawienie, które wykorzystując przeprowadzone badania wskazują udział poszczególnych jednostek oraz elementów w sytuacjach naruszających bezpieczeństwo systemu.

[114] Dariusz Wawrzyniak, Op. Cit., s. 40.
[115] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 77.
[116] Andrzej Gospodarowicz, *Bankowość elektroniczna*, Warszawa 2005, s. 74.




Rysunek 9 Zagrożenia bezpieczeństwa systemów informatycznych w bankowości
*Źródło: opracowanie własne na podstawie: Andrzej Gospodarowicz, Bankowość elektroniczna.*

Poruszając temat zagrożenia bezpieczeństwa w bankowości elektronicznej, przeciętny użytkownik przede wszystkim pomyśli o wirusach (4%), atakach z zewnątrz (3%) bądź problemach fizycznych (20%), które ze względu na fakt, iż rzeczywiście stanowią zagrożenie, zostaną bardziej szczegółowo omówione w kontekście najpopularniejszych kanałów dystrybucji bankowości elektronicznej. Należy jednak pamiętać, iż wymienione elementy są jedynie pewną częścią zagrożeń i zazwyczaj są zaledwie narzędziem, wykorzystywanym przez nieuczciwy lub niezadowolony personel bądź użytkowników, w oparciu o ich pomysły. Człowiek wraz z czynami, których się podejmuje, stanowi największe zagrożenie dla otoczenia.

### 2.1.1. Dane osobowe w systemach informatycznych

Nieustanny rozwój technologii, od lat znacząco przyczynia się do polepszenia codziennego funkcjonowania przeciętnego człowieka. Przeróżne technologie obecne są w każdym zakątku, a coraz nowsze możliwości wiążą się z koniecznością wykorzystania bardziej zaawansowanych technik przetwarzania informacji. W czasach, gdzie ciężko stworzyć coś nowego, a temat wszechobecnie występujących zagrożeń nie jest obcy społeczeństwu, należałoby zastanowić się nad wartością informacji i danych osobowych. Jest to zagadnienie traktowane przez większość ludzi z tzw. „przymrużeniem oka", choć w rzeczywistości, informacja zyskała wartość materialną, dzięki czemu stała się pewnego rodzaju towarem, rozpatrywanym w kontekście dóbr materialnych wystawianych na rynek. Coraz częściej zdarzają się sytuacje kupna/sprzedaży informacji czy konkretnych danych, a nawet całych baz danych osób publicznych i prywatnych. Dzieje się tak ze względu na fakt, iż dane osobowe są jednym z niewielu już elementów, opisujących indywidualne cechy człowieka, dzięki czemu

możliwa jest jego identyfikacja. Wyróżnia się zwykłe i wrażliwe dane osobowe. Za identyfikację konkretnej osoby fizycznej odpowiadają zwykłe dane, do których zalicza się np. imię, nazwisko i numer PESEL oraz informacje, których pozyskanie wymaga więcej zaangażowania, typu: wykształcenie czy adres zamieszkania. Mianem danych osobowych wrażliwych, określa się natomiast zamknięty katalog obejmujący „pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia oraz dane dotyczące skazań, kar i innych orzeczeń sądowych”[117]. Określenie tożsamości w świecie wirtualnym, przede wszystkim odbywa się na podstawie loginu, którym określa się ciąg znaków i hasła[118]. Dodatkowo są to: adres IP, „ksywa” oraz adres poczty elektronicznej. Użycie takich informacji pozwala na rozpoznanie uprawnień oraz przypisanie działań dokonanych w sieci komputerowej lub komputerowym systemie wielodostępowym, jak również dopuszcza możliwość zarządzania i edycji danych, udostępnionych podczas jakiejkolwiek rejestracji[119].

Gwałtowny wzrost wartości danych osobowych oraz podobnych informacji spowodował, że jednym z największych aktualnie zagrożeń jest kradzież tożsamości, określana także mianem fałszerstwa tożsamości. Zjawisko to można opisać jako świadome transferowanie, posiadanie bądź używanie informacji służących do identyfikacji innej osoby, bez upoważnienia, celem popełnienia czynu zabronionego przez prawo[120]. Jest to proces składający się z dwóch etapów: przywłaszczenia danych, a następnie ich wykorzystania[121]. Jako motywacje takiego czynu uznaje się: włamanie dla żartu, zaspokojenie ciekawości, dla sławy i chwały, w efekcie politycznych lub ideologicznych upodobań, w ramach odwetu lub wandalizmu. Często motywy ataków są trudne do ustalenia ze względu na nakładanie się poszczególnych motywów oraz powody osobiste przestępcy. Najczęstszą jednak motywację stanowi chęć zyskania korzyści finansowych[122]. Wśród dokonywanych ataków wyróżnia się

[117] Piotr Waglowski, *Ochrona dóbr osobistych i danych osobowych*, Warszawa 2009, s.7-8.
[118] William Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych – Koncepcje i metody bezpiecznej komunikacji*, Gliwice 2012, s. 93.
[119] Generalny Inspektor Ochrony Danych Osobowych, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, Warszawa 2009, s.11-16.
[120] Maciej Siwicki, Kradzież tożsamości – pojęcie i charakterystyka zjawiska. Część 1., [dostęp: 10 kwietnia 2016], < http://www.edukacjaprawnicza.pl/artykuly/artykul/a/pokaz/c/artykul/art/kradziez-tozsamosci-pojecie-i-charakterystyka-zjawiska-czesc-i.html>.
[121] Marian Merritt, Kradzież tożsamości: podstawowe informacje, [dostęp: 10 kwietnia 2016], <http://pl.norton.com/identity-theft-primer/article>.
[122] Alex Lukatsky, *Wykrywanie włamań i aktywna ochrona danych*, Gliwice 2005, s. 74-78.

atak zmasowany oraz atak kierunkowy[123]. Atakiem zmasowanym określa się zgromadzenie informacji, takich jak np.: dane personalne, numery kart płatniczych wraz z datami ich ważności, dzięki którym możliwe jest dokonanie elektronicznych transakcji finansowych. Takie działanie nie wymaga stosowania bardziej zaawansowanych technik, gdyż skierowane jest w przypadkowo wybraną grupę osób. Z kolei atak kierunkowy, wymierzony jest w stronę konkretnej osoby. Zebranie informacji na jej temat, z wszelkich dostępnych źródeł, może wiązać się z jej podsłuchem lub obserwacją. Włamanie do systemu będącego własnością ofiary, sygnalizuje chęć zyskania konkretnych danych, którymi mogą być: dane personalne, baza kontaktów, dane pozwalające dokonać transakcji finansowych, zawarcie umów kupna-sprzedaży lub wzięcie udziału w wydarzeniach serwisów aukcyjnych lub portali.

Rozwój telefonii komórkowej oraz Internetu przyczynił się do powstania tzw. „społeczeństwa informacyjnego", którego cele, w opinii Urzędu Komitetu Integracji Europejskiej to wykorzystanie Internetu jako środka informacji publicznej oraz komunikacji obywatelskiej, powszechny dostęp do informacji oraz rozwój edukacji[124]. Wzajemne relacje opierają się o znacznie ułatwiony, swobodny dostęp do informacji, przekazywanie i dzielenie się dostępną wiedzą oraz obszerną komunikację, bez względu na odległość. Zwiększyła się szybkość zdobycia, przesyłania oraz analizy określonych danych[125]. Z biegiem czasu Internet stał się głównym źródłem łatwej do pozyskania wiedzy. Również jej szczegółowość bywa zaskakująca. Podczas, gdy świat realny bardzo intensywnie przeplata się ze światem wirtualnym, niezwykle częstym zjawiskiem jest dobrowolne udostępnianie swoich danych oraz informacji z życia prywatnego na portalach społecznościowych, forach i innych miejscach w sieci. Użytkownicy najczęściej nie są świadomi, jak wielkie szkody mogą zostać im wyrządzone na podstawie tak łatwo uzyskanych przez osoby niepowołane informacji.

Nagromadzenie cennych treści w sieci, postępująca globalizacja oraz ciągle wzrastająca wartość danych osobistych i informacji, skutecznie przyczyniły się do powstania nowych zagrożeń. Bardzo powszechną, a jednocześnie niezwykle wyrafinowaną formą naruszenia bezpieczeństwa jest socjotechnika, wykorzystywana w celach ocenianych jako moralnie pozytywne bądź negatywne dla społeczeństwa. Zwana również „inżynierią społeczną"

[123] *Ochrona informatyczna danych – „Phishing" i kradzież tożsamości*, [dostęp: 10 kwietnia 2016], <http://www.policja.pl/pol/kgp/bsk/dokumenty/cyberprzestepczosc/58792,Ochrona-informatyczna-danych-phishing-i-kradziez-tozsamosci.html>.
[124] Grzegorz Bliźniuk, Jerzy S. Nowak, *Społeczeństwo informacyjne*, Katowice 2005, s. 29.
[125] Piotr Sienkiewicz, Jerzy S. Nowak, *Społeczeństwo informacyjne – Krok naprzód, dwa kroki wstecz*, Katowice 2008, s. 1-2.

lub „inżynierią socjalną", w odniesieniu do wykorzystania człowieka jako najsłabszego elementu w relacji człowiek-system[126]. Nazywana także „cybernetyką społeczną" lub „socjocybernetyką", jeśli zdarzenie opiera się o proces manipulacji całym społeczeństwem[127]. Najczęstszym celem socjotechnika jest staranne wydobycie najcenniejszych dla niego danych i wykorzystanie ich dla własnych korzyści w niedalekiej przyszłości. Poza wykorzystaniem dostępnych narzędzi technicznych, w swoich działaniach wykorzystuje także zagadnienia związane z takimi dziedzinami naukowymi jak: psychologia społeczna, socjologia kultury, socjologia i psychologia matematyczna, ekonomia polityczna oraz nauki polityczne[128]. Są to trudne do wykrycia i obrony ataki, ponieważ bazują głównie na rozpraszaniu i odwracaniu uwagi poprzez wzmożoną gadatliwość lub kłamstwo, a także fakt, iż ofiara często nie jest świadoma ataku[129].

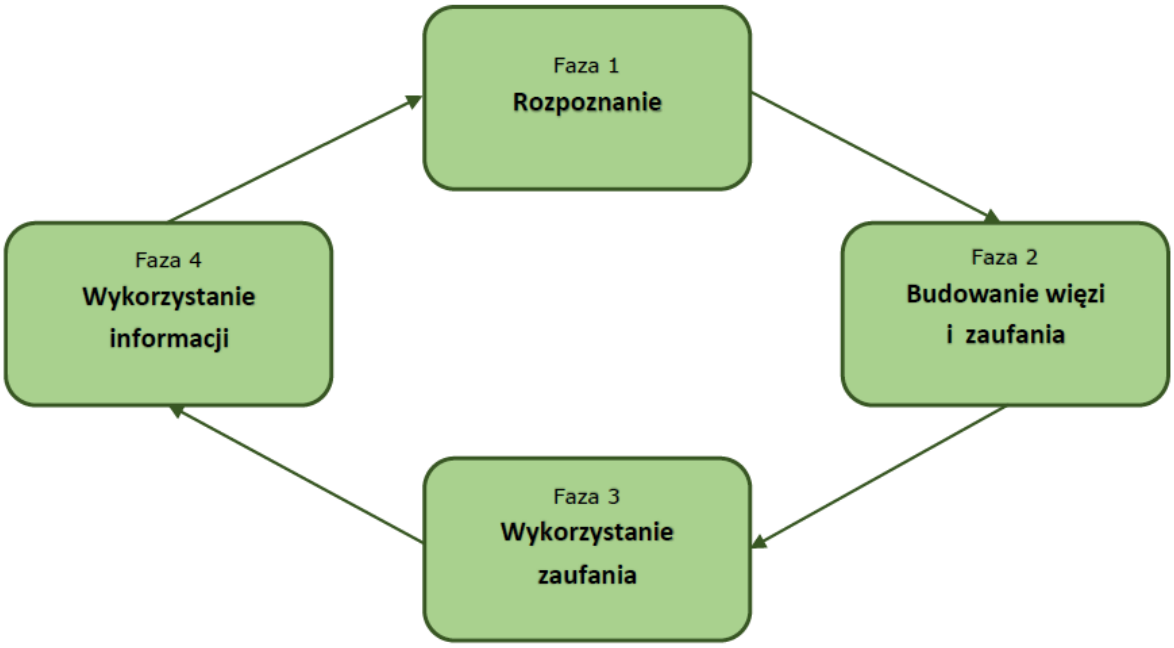
W ogólnym ujęciu, socjotechnikę można przedstawić jako pewną formę stosowania perswazji, wywierania wpływu na ludzi i wzbudzania zaufania, dzięki czemu, oszukuje się w sposób, który pozwala wierzyć ofierze, że socjotechnik jest osobą o sugerowanej przez siebie tożsamości, która uprzednio została stworzona na potrzeby konkretnej manipulacji[130]. Niewątpliwie manipulator musi posiadać umiejętność wnikliwej analizy zachowań i psychiki ludzkiej, dodatkowo posiadając przynajmniej dobre zdolności aktorskie. Są to ważne cechy ze względu na konieczność wzbudzenia zaufania ofiary i zapewnienie sobie szans na powodzenie ataku[131]. Do postępowania ofiary zgodnie z zamysłem manipulatora przyczyniają się także błędy oceny rzeczywistości. Głównymi uchybieniami są[132]:

- **ograniczony horyzont**, czyli oparcie całej posiadanej wiedzy na temat przedmiotu, osoby, sytuacji lub cechy wyłącznie na jednej informacji, fakcie lub cesze. Socjotechnik dopowiada sobie resztę niezbędnych informacji, którym ofiara ulega. Taka sytuacja wynika z podążania „na skróty", które oparte jest o założenia perspektywy poznawczej społecznej psychologii, mówiącej o skłonności ludzi do wybierania w pierwszej kolejności najprostszych rozwiązań, a dopiero później tych najbardziej im odpowiadających[133].

[126] Wikipedia, *Inżynieria społeczna*, [dostęp: 14 kwietnia 2016], <https://pl.wikipedia.org/wiki/In%C5%BCynieria_spo%C5%82eczna_(informatyka)>.
[127] Józef Kossecki, *Cybernetyka kultury*, Warszawa 1974, s. 5.
[128] Józef Kossecki, *Cybernetyka społeczna*, Warszawa 1981, s. 6.
[129] Tomasz Trejderowski, *Socjotechnika, podstawy manipulacji w praktyce*, Warszawa 2009, s. 15.
[130] Kevin Mitnick, William Simon, *Sztuka podstępu*, Gliwice 2003, s. 4.
[131] Tomasz Trejderowski, *Op.Cit.,* s. 61-63.
[132] *Ibidem*, s. 16-17.
[133] Robert Cialdini, *Wywieranie wpływu na ludzi. Teoria i praktyka*, Gdańsk 2000, s. 18-20.

- **przenoszenie cech** jest połączeniem dwóch faktów ze sobą, tylko ze względu na ich wspólne występowanie. Wymieniane cechy to[134]:
    - sympatia – oddziaływanie na odczucia innej osoby poprzez podświadome przenoszenie cech pozytywnych z jednej jednostki na drugą, jej towarzyszącą,
    - autorytet – przeniesienie cech osoby cenionej, cieszącej się zaufaniem i szacunkiem, na osobę jej towarzyszącą,
    - wzajemność – podświadome odwołanie się do powinności dokonania rewanżu konkretnego zachowania w stosunku do innej osoby.
- **zmiana punktu widzenia**, silnie wiąże się z wyższym wartościowaniem zdania innych osób od swojego. Ofiara akceptuje zaistniałe sytuacje lub fakty, ponieważ boi się reakcji otoczenia na zachowanie inne niż to, którego się od niej oczekuje[135].

Dzięki analizom występujących przypadków, możliwe stało się wyodrębnienie cyklu postępowania przeciętnego socjotechnika. Model socjotechniczny, w jasny sposób określa sztywne ramy przebiegu cyklu manipulacji.




Rysunek 10. Przebieg cyklu socjotechnicznego.
*Źródło: Opracowanie własne na podstwaie: Kevin Mitnick, Sztuka podstępu.*

Przedstawiony cykl składa się z czterech następujących po sobie faz. Faza pierwsza – **rozpoznanie** – głównie skupia się na rozpoznaniu celu ataku i zgromadzeniu konkretnych

[134] Tomasz Trejderowski, *Op.Cit.,* s. 17-18.
[135] *Ibidem*, s. 19.

danych[136]. Wymaga ścisłej analizy, jakie informacje są potrzebne i w jaki sposób można je pozyskać, a następnie niezbędne jest zaplanowanie i przygotowanie ataku. W poszukiwaniu informacji korzysta się z wielu różnych, ogólnie dostępnych źródeł. Jako podstawowe, od którego rozpoczyna się jakiekolwiek poszukiwania, uchodzi strona internetowa osób prywatnych i firm. Witryny firmowe najczęściej udostępniają informacje na temat swojej historii, zakresu działalności, dostępnych ofert, lokalizacji aktualnych wydarzeń w firmie oraz danych kontaktowych pracowników czy biografii i osiągnięć kierownictwa najwyższego szczebla[137]. Prywatne strony natomiast, do których zalicza się także portale społecznościowe i fora, są bogatym źródłem intymnych informacji Internautów, którzy chętnie chwalą się informacjami o swoich dzieciach, członkach rodziny, znajomych, współpracownikach, domach, miejscu zatrudnienia, zajmowanym stanowisku pracy, a nawet aktualnym miejscu pobytu. Nie zdają sobie sprawy, że wszystkie te informacje są niezwykle przydatne podczas planowania ataku socjotechnicznego.

Manipulator korzysta również z takich narzędzi jak wyszukiwarki internetowe, pamiętając o tym, że dane i informacje umieszone w sieci, nie giną bezpowrotnie nawet po ich wykasowaniu przez użytkownika. Warto również mieć na uwadze wszelakie przedmioty wyrzucane bez uprzedniego zniszczenia. Bardzo dużo informacji można zdobyć dzięki notatkom, listom, płytom CD, nośnikom pamięci, całym fakturom a nawet dokumentom i czekom. Społeczeństwo w dalszym ciągu nie pamięta, jak ważne jest niszczenie takich przedmiotów.

Faza druga – **budowanie więzi i zaufania** – wykorzystuje wcześniej zebrane dane oraz model komunikacji, aby za pomocą różnych, dostępnych socjotechnikowi środków, przekazać szczegółowo sformułowaną informację do odbiorcy[138]. Podjęte zachowania mają na celu stworzenie nowej tożsamości i wykreowanie fikcyjnego scenariusza, którego następstwem będzie wydobycie potrzebnych informacji lub w późniejszych etapach poskutkuje podświadomym skłonieniem ofiary do podjęcia przewidzianych działań. Wchodzenie w rolę jest swego rodzaju elastycznym przejściem z fazy II cyklu (nawiązanie kontaktu, zdobycie zaufania, weryfikacja posiadanych informacji i uzyskanie dokładniejszych) w fazę III. Według Amerykańskiej National Security Agency, **wywołanie** obejmuje delikatne pozyskanie informacji podczas pozornie normalnej, niewinnej rozmowy[139]. Jej celem jest wypracowanie

[136] Andrzej Guzik, *Zagrożenia socjotechniczne, a bezpieczeństwo informacji*, 2007, s. 1.
[137] Christopher Hadnagy, *Socjotechnika – sztuka zdobywania władzy nad umysłami*, Gliwice 2011, s. 48-54.
[138] Kevin Mitnick, *Op. Cit.*, s. 368.
[139] Christopher Hadnagy, *Op.cit.*, s. 87.

za pomocą zyskanego zaufania, konkretnej reakcji. Jest to bardzo skuteczny sposób, ponieważ przeciętny użytkownik przynajmniej stara się być uprzejmym, szczególnie jeśli rozmówca jest obcą osobą. Podobne zachowanie wywołuje okazywane zainteresowanie innych osób. Również pochwały bardzo często skutkują wylewnością rozmówcy oraz fakt, iż bez konkretnego powodu bądź jakichkolwiek podejrzeń, ludzie nie mają w zwyczaju z założenia kłamać[140]. Wyróżnia się wiele metod wywołania, odwołujących się przede wszystkim do ludzkich emocji, zachowań, reakcji oraz przyzwyczajeń. Aby wywołanie miało szanse się powieść, bardzo ważne jest, aby manipulator naturalnie się zachowywał, poszerzył swoją wiedzę oraz powstrzymał się od zachłanności, żeby ofiara nie nabrała żadnych podejrzeń. Większość ludzi potrafi wyczuć nienaturalne zachowanie, nieszczerość, przesadną ciekawość oraz brak wiedzy w danym temacie. Jakiekolwiek zniechęcenie rozmówcy może zaprzepaścić cały wysiłek socjotechnika. Ostatnią fazą jest **wykorzystanie zebranych informacji**. To właśnie w tym momencie, użytkownicy najczęściej dowiadują się, że stali się ofiarami przestępstwa, gdy są zmuszeni zmierzyć się z jego przykrymi efektami.

W dalszej części opisane zostały najczęstsze ataki bezpośrednio związane z naruszeniem bezpieczeństwa danych osobowych.

### Phishing (spoofing)

Nazwa tego przestępstwa nie została wybrana przypadkowo. Jest połączeniem słowa „fishing" (tj. rybołówstwo) ze słowem „phreaking" (tj. oszukiwanie systemów telekomunikacyjnych)[141]. Odnosi się do chęci zdobycia (złowienia) poufnej informacji osobistej pod postacią haseł lub np. szczegółów kart kredytowych wraz z innymi niezbędnymi danymi, za pomocą efektywnej przynęty. Atak polega na udawaniu osoby godnej zaufania, koniecznie potrzebującej konkretnej informacji, tym samym wprowadzając użytkownika w błąd[142]. W celu wyłudzenia informacji, atrakcyjnie i przede wszystkim wiarygodnie wyglądające wiadomości, rozsyła się poprzez sfałszowaną stronę WWW, pocztę elektroniczną lub komunikator internetowy[143]. Określając to przestępstwo w sposób dosłowny, należałoby stwierdzić, iż jest to ominięcie zabezpieczeń umysłu człowieka, a nie jak zazwyczaj – osłon

[140] *Ibidem*, s. 78-79.
[141] Maciej Gajewski, *Phishing – łowienie naiwnych*, [dostęp: 19 kwietnia 2016], <http://www.chip.pl/artykuly/trendy/2009/11/phishing-lowienie-naiwnych>.
[142] Arkadiusz Skowron, *Phishing, czyli jak się łowi hasła w Internecie*, Wrocław 2006, s. 4.
[143] Norton, *Słownik bezpieczeństwa internetowego*, [dostęp: 19 kwietnia 2016], <http://pl.norton.com/security-glossary/article#p>.

systemowych. Cały proces odbywa się w dwóch krokach. Stworzenia strony internetowej, fałszywej, będącej wierną kopią oryginału np. strona logowania do serwisu bankowości internetowej. A następnie przyciągnięcia jak największej ilości ofiar, skłonnych udostępnić swoje indywidualne dane i informacje[144]. Głównym czynnikiem, który oddziałuje na potencjalne ofiary jest wywołanie poczucia natychmiastowej reakcji np. poprzez prośbę o zalogowanie się na konto, celem potwierdzenia tożsamości lub podczas chęci wzięcia udziału w konkursie – niezbędne jest udostępnienie danych.

**Pharming**

Jest to o wiele trudniejsza do wykrycia odmiana phishingu. Wykorzystuje się stronę tworzoną i fałszowaną, zgodnie z potrzebami atakującego. Jej głównym celem jest przejęcie danych, bezpośrednio udostępnionych przez użytkownika. Znacznym utrudnieniem, odróżniającym tę formę od phishingu jest dodatkowe zastosowanie serwera DNS[145]. Charakterystycznym jest także fakt przekierowania Internauty na fałszywą stronę, nawet po wpisaniu prawidłowego adresu URL[146]. Przestępstwo pharmingu przeprowadzane jest na podstwie jednego z dwóch znanych ataków. Pierwszy - na globalny serwer DNS, którego zainfekowanie pozwala na skojarzenie prawdziwego adresu URL z serwerem, na którym znajduje się fałszywa strona wykradająca poufne dane. Drugi, który za pomocą trojanów, skupia się na ingerencji w system użytkownika i modyfikacji jego plików lokalnych, odpowiadających za wstępne tłumaczenie nazw URL na wcześniej sfałszowany adres IP, z umyślnym pominięciem globalnego serwera DNS, który zajmuje się tłumaczeniem nazw domen na adresy IP[147]. Wyróżnia się dwa rodzaje takich serwerów: serwery rejestratorów domen i operatorów hostingu, zajmujące się przechowywaniem informacji dotyczących konfiguracji domen, a także serwery, które należą do operatorów udostępniających łącza do Internetu (ISP – Internet Service Provider – firma, która zapewnia podłączenie do Internetu), nie zajmują się konfiguracją domen, ale pośredniczą między siecią serwerów DNS, a komputerem[148].

[144] Arkadiusz Skowron, *Op. Cit.*, s. 14.
[145] *Ibidem*, s. 4.
[146] Pharming, [dostęp: 19 kwietnia 2016], <https://pl.wikipedia.org/wiki/Pharming>.
[147] Słownik pojęć internetowo-reklamowych, *serwer DNS*, [dostęp: 19 kwietnia 2016], <https://slownik.intensys.pl/definicja/36/serwer-dns/>.
[148] *Ibidem*.

**SMiShing (SMS phishing)**

Jest to kolejne zagrożenie socjotechniczne, będące odmianą wcześniej omawianego phishingu. Główne założenia to rozsyłanie wiadomości tekstowych (SMS-ów), których zadaniem jest nakłonienie potencjalnej ofiary do podjęcia z góry założonego przez sprawcę zachowania. Najczęściej spotykanym w Polsce przykładem SMiShingu są wiadomości wysyłane do losowo wytypowanych numerów, z informacją o wygranej i konieczności odesłania SMS'a zwrotnego na podany numer.

**Oszustwa rekrutacyjne**

Na równie naiwnym działaniu opierają się wszelkie oszustwa rekrutacyjne. Ich podstawę stanowi Internet, prasa oraz spam. Najlepszym przykładem, są oferty pracy, otrzymywane z fałszywych adresów mailowych. Często adresy te, pochodzą z darmowych serwisów mail'owych, co natychmiast powinno wzbudzić pewne podejrzenia. Internauta odpowiadający na taką ofertę przesyła swoje CV, które jest bogatym źródłem szczegółowych danych. Nierzadko zdarzają się sytuacje, w których oprawca prosi o uzupełnienie o kolejne informacje typu: numer konta bankowego lub kopia dowodu tożsamości[149]. Tak zdobyte dane wystarczą do założenia kont na ebay, stworzenia fałszywych sklepów internetowych na nazwisko ofiary lub rachunków bankowych, na które przelewane są pieniądze pochodzące z przestępstw. W ten sposób, ofiary stają się tzw. słupami np. w procederze prania pieniędzy[150].

**Spam**

Ważnym elementem, z którym styczność miał każdy Internauta jest bardzo uciążliwy w swojej formie spam. Zostały przeprowadzone badania oparte o ruch sieciowy, zgodnie z którymi, aż 73% maili kwalifikuje się jako spam[151]. Wysyłany masowo, do wielu odbiorców i o identycznej treści. „*Elektroniczna wiadomość jest spamem jeżeli:*

1. *Treść i kontekst są niezależne od tożsamości odbiorcy, ponieważ ta sama treść może być skierowana do wielu innych potencjalnych odbiorców.*

[149] *Oszustwa rekrutacyjne*, [dostęp: 19 kwietnia 2016], <http://www.oszustwsieci.pl/oszustwa_rekrutacyjne.php>.
[150] Mateusz Górnisiewicz, Radosław Obczyński, Mariusz Pstuś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną*, Warszawa 2014, s. 19-20.
[151] Mariusz Mikoś, *SPAM – metody walki i obrony*, CBKE e-biuletyn 1/2005, s.1.

2. *Jej odbiorca nie wyraził uprzedniej, możliwej do weryfikacji zamierzonej, wyraźnej i zawsze odwoływalnej zgody na otrzymanie tej wiadomości.*
3. *Treść wiadomości daje odbiorcy podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść korzyści nieproporcjonalne w stosunku do korzyści odbiorcy wynikających z jej odebrania*"[152].

Wyróżnia się wiele rodzajów spamu np. hoax, reklamy, nigeryjski szwindel, joe-job, których szczegółowe omawianie w kontekście zagrożeń bankowości elektronicznej nie jest konieczne. Spam prócz tego, że stanowi sporą część niechcianych wiadomości elektronicznych, niepotrzebnie zapełniających miejsce na skrzynce pocztowej, najczęściej jednak, bywa także narzędziem do rozsyłania różnego rodzaju złośliwego oprogramowania, jak również pluskiew internetowych. Niezbyt znane wśród przeciętnych użytkowników sieci, będące obrazem o rozmiarach jednego piksela. Niemal niezauważalny dla zwykłego Internauty. Pluskwa przesłana przez serwer do przeglądarki internetowej, ma za zadanie kompletować informacje dotyczące identyfikatora strony, która tę pluskwę zawiera, adresu IP komputera, który ja pobrał, a także datę z godziną i typem przeglądarki. Pluskwy łączą się także z plikami cookies, co umożliwia zebranie większej ilości informacji, jak np. odwiedzanych stron[153]. Podobnym działaniem charakteryzują się wszelkiego rodzaju programy szpiegujące (ang. *spyware*) obserwujące poczynania użytkownika. Umożliwiają przechwytywanie zrzutów ekranu, rejestrację informacji z zakresu spędzania czasu wolnego w sieci, zapisują znaki wprowadzane z klawiatury, a nawet potrafią uzyskać numery kart kredytowych i haseł. Spam wykorzystywany podczas procesu manipulacji bardzo często odwołuje się do emocji i uczuć odbiorcy[154]. Celowa prowokacja, jak w większości podobnych przypadków, ma na celu wywołanie założonego przez oprawcę działania, co w efekcie ma przynieść bogaty zasób danych i informacji lub konkretny zysk finansowy.

Bardzo często niedoceniane dane osobowe, potrafią wyrządzić wiele szkód w świecie wirtualnym, jak i w codziennym, realnym życiu. Skutki przejęcia danych osobowych potrafią namieszać w zakresie reputacji ofiary, jej prestiżu oraz dobrego imienia. Przede wszystkim jednak zagrożony jest sektor finansowy ofiary. Posiadając niezbędne dane, przestępca ma możliwość zaciągnięcia kredytów, pożyczek, dokonania zakupów, jak również swobodnego zarządzania oszczędnościami lub nawet dorobkiem życiowym ofiary. W dzisiejszych czasach,

[152] *Ibidem*, s. 1.
[153] Wallace Wang, *Op. Cit.*, s. 228-229.
[154] *Ibidem*, s. 235-236.

chęć wzbogacenia się jak najniższym kosztem jest tak wysoka, że zaawansowane metody socjotechniczne stanowią największe, lecz nie jedyne zagrożenie dla klientów banków. Na wysokie niebezpieczeństwo narażone są także czynności i przedmioty codziennego użytku, związane z różnymi kanałami dystrybucji usług bankowości elektronicznej.

### 2.1.2. Bankowość terminalowa

Przestępstwa związane z bankowością terminalową można rozważać pod kątem ścisłego powiązania z bankomatem oraz kartą płatniczą, chociaż wiadomo, iż oba te elementy wzajemnie się uzupełniają.

Jednym z najczęstszych sposobów okradania klientów podczas korzystania z bankomatu jest **skimming bankomatowy**. Przestępstwo polegające się na skopiowaniu treści takich jak: wydawca karty, jej numer oraz data ważności zawarte na pasku magnetycznym karty, bez wiedzy jej posiadacza. Numer karty wraz z kodem PIN podlegają szyfrowaniu za pomocą algorytmu DES lub 3DES. Ich weryfikacja polega na sprawdzeniu przez wydawcę karty zgodności wprowadzonego między innymi kodu PIN z kodem zawartym w bazie danych. Następnie udostępniany jest numer rachunku bankowego odpowiedniego dla danej karty i sprawdzona zostaje ilość środków dostępnych na koncie. Jeśli wszystko się zgadza, transakcja zostaje zrealizowana[155]. Aby możliwe było skopiowanie danych, przestępca wprowadza do bankomatu swoją kartę, na której znajduje się szkodliwe oprogramowanie. Najpopularniejszym w ostatnim czasie jest Trojan.Skimer.18. Dzięki niemu, zainfekowany bankomat omija zabezpieczenie weryfikacji kodu, przez co złodziej zyskuje kontrolę nad bankomatem. Wymieniony wirus posiada różnorodne zastosowania. Potrafi wyleczyć zainfekowany bankomat, wyświetlić statystyki dotyczące skradzionych danych, restartować urządzenie, zmieniać tryb jego pracy, skasować plik logu oraz dokonać aktualizacji złośliwej biblioteki bądź całego kodu. Wszystko możliwe jest za pomocą aplikacji znajdującej się w pamięci karty użytej przez przestępcę. Mimo tak różnorodnych możliwości oprogramowania, najczęściej użyty jest do uruchomienia nienależnej wypłaty z bankomatu[156].

Zapisywaniem danych z paska magnetycznego cechuje się również podstawianie **fałszywych bankomatów**. Jest to bardzo wymagający sposób, lecz niezwykle skuteczny. Przez pewien okres czasu funkcjonalność tych bankomatów nie wzbudza podejrzeń, gdyż należycie

[155] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 19-20.
[156] Jerzy Gąsiorowski, Piotr Podsiedlik, *Przestępstwa w bankowości elektronicznej w Polsce – próba oceny z perspektywy prawno-kryminalistycznej*, Dąbrowa Górnicza 2015, s. 55-57.

obsługują klientów, wypłacając im pieniądze. Jednak w tym samym czasie zapisują PIN i rejestrują informacje z paska magnetycznego karty[157]. Znane są również przypadki fałszywych bankomatów, które nie wypłacają wskazanych kwot, dodatkowo uniemożliwiając odbiór karty. Dzięki czemu przestępca zyskuje kartę wraz z kodem PIN do niej[158].

Zdarzają się również bardziej fizyczne formy oddziaływania na bankomat. Jedną z nich jest metoda **„wenezuelskiego śrubokręta"**, do której używa się śrubokręta i kleju, blokując zasobnik. Niemożliwe staje się odebranie banknotów, które zatrzymane zostają przez elementy np. z taśmą lub klejem montowanym w środku bankomatu. Po odejściu klienta, zamontowane nasadki zostają zdjęte wraz z banknotami[159]. Przedstawiając bardziej fizyczne formy oddziaływania na bankomat, należy również pamiętać o najbardziej prymitywnych formach kradzieży jaką jest wyłamanie bankomatu z podłoża i przywłaszczenie jego zawartości oraz wysadzenie bankomatu za pomocą wtłoczonego do środka gazu i spowodowaniem zapłonu[160].

Znana jest również metoda **„Libijskiego oczka"**, będąca szczególnym rodzajem działania. Metoda polega na zablokowaniu otworu na kartę zwykłą folią plastikową i oczekiwaniu na ofiarę, która wypłaca wskazaną kwotę pieniędzy, lecz poprzez ówcześnie zablokowany otwór, nie potrafi odzyskać karty. Przestępca ofiaruje swoją pomoc, wpisując kod PIN podany przez klienta. Po kilku nieudanych próbach, karta nie zostaje odzyskana, a klient odchodzi. Przestępca w ten sposób zyskuje PIN wraz z kartą[161].

Większość oszustw terminalowych związana jest jednak bezpośrednio z kartą płatniczą. Popularność transakcji przeprowadzanych za pomocą kart płatniczych ciągle cieszy się tendencją rosnącą, co wpływa na coraz to nowsze funkcje i zastosowania wymyślane i oferowane przez banki. Wraz z ich rosnącą popularnością, wzrasta także zainteresowanie niedoskonałościami coraz to nowszych rozwiązań i wykorzystaniem ich dla zyskania własnych korzyści. Spowodowane straty, nie są już tylko odczuwalne dla klienta, traci na tym również bank oraz rozwój rynku kart płatniczych. Przestępstwa związane z kartą płatniczą kwalifikowane są w oparciu o różne przepisy polskiego prawa karnego, lecz nie sposób

[157] Policja podlaska, *Oszustwa bankomatowe*, [data dostępu: 3 kwietnia 2016], <http://www.podlaska.policja.gov.pl/pod/dzialania-policji/przestepczosc-gospodar/struktura-wydzialu/zespol-ii/oszustwa-bankomatowe/28417,Oszustwa-bankomatowe.html>
[158] Małgorzata Niedźwiedzka-Małecka, *Przestępstwa związane z wykorzystaniem kart płatniczych*, „Studia Iuridica" XXXIX 2001, s. 175.
[159] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op.cit.*, s. 58.
[160] *Ibidem*, s. 56-58.
[161] *Ibidem*, s. 59.

jednoznacznie je zdefiniować[162]. Dokładne zestawienie tego rodzaju przestępstw proponuje J. Forysek, dzieląc je na trzy następujące grupy[163]:

- **Czynności przygotowawcze:**
  i. spisanie cudzego numeru karty płatniczej,
  ii. skopiowanie zawartości paska magnetycznego lub mikroprocesora (skimming),
  iii. przewożenie, przechowywanie, przenoszenie lub przesyłanie kart płatniczych osób trzecich,
  iv. przechowywanie numerów kart płatniczych przez Internet lub łącza telekomunikacyjne,
  v. wyłudzenie karty płatniczej na podstawie wniosku z fałszowanymi danymi.

- **Czynności poprzedzające i ułatwiające nielegalne przesunięcia majątkowe:**
  i. posiadanie karty zastrzeżonej przez emitenta,
  ii. posługiwanie się cudzym numerem karty płatniczej przy zamówieniach pocztowych lub przez Internet,
  iii. przerobienie lub podrobienie karty płatniczej,
  iv. kradzież kart płatniczych,
  v. włamanie się do systemów informatycznych i telekomunikacyjnych,
  vi. transakcje z bankomatami,
  vii. zmuszenie groźbą lub przemocą do wydania karty płatniczej wraz z numerem PIN.

- **Transakcje kartowe powodujące nielegalne przesunięcia majątkowe:**
  i. posługiwanie się skradzionymi lub zgubionymi kartami płatniczymi,
  ii. posługiwanie się przerobionymi lub podrobionymi kartami płatniczymi,
  iii. posługiwanie się kartami niedoręczonymi,
  iv. wykorzystanie karty zgłoszonej jako utracona,
  v. wyłudzanie towarów lub usług przez legalnego posiadacza karty,
  vi. wystawienie fałszywych dowodów zawarcia transakcji.

[162] *Ibidem*, s. 79-80.
[163] Jerzy Kosiński, *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych,* Szczytno 2003, s. 73-74.

Jest to jeden z wielu dostępnych podziałów przestępstw, przedstawiony ze względu na jego szczegółowość i istotność występujących elementów. Chociaż mówi się, iż ze względu na szybkość modyfikacji działań przestępczych, klasyfikacja powinna być oparta o dwa kryteria: przestępstwa, gdzie karta jest jego przedmiotem bądź narzędziem[164]. W I półroczu 2014 roku, zostały opublikowane dane przez NBP, zgodnie z którymi, liczba oszukańczych operacji dokonanych za pomocą karty płatniczej wyniosła 36,5 tyś, natomiast agenci rozliczeniowi przekazują informację o liczbie 15,9 tyś oszukańczych transakcji. Struktura tych operacji przedstawia się następująco[165]:

- Karty skradzione – 26,9%
- Karty niedoręczone – 0,2%
- Karty zgubione – 6,7%
- Karty uzyskane na podstawie fałszywych danych – 5,6%
- Karty sfałszowane – 25,1%
- Inne (np. transakcje internetowe) – 35,5%

Dokonując analizy przedstawionych danych, grupa „inne", do której zaliczane są różnorodne formy przestępstw (również tych internetowych) występuje najczęściej. Drugą kategorią są karty skradzione, a trzecią – sfałszowane. Zaprezentowane zestawienie po raz kolejny pokazuje, iż stworzenie jednoznacznego, a zarazem wyczerpującego temat katalogu zagrożeń jest niemal nie możliwe**.**

**Kradzież karty płatniczej** jest wejściem w posiadanie karty będącej własnością innej osoby, w sposób nielegalny. Często zdarza się, że kod PIN zapisany jest na którejś ze stron karty, ułatwiając tym samym dokonanie przestępstwa. Najczęstszym aktualnie sposobem kradzieży jest tzw. kradzież kieszonkowa, choć zdarzają się także przywłaszczenia, kradzież z włamaniem oraz rozbój. Sprawca podszywa się pod właściciela karty, a następnie dokonuje różnorodnych transakcji, bez konieczności zmiany danych. Podobne zastosowanie spotyka karty zgubione[166].

[164] *Ibidem*, s.74.
[165] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op.cit.*, s. 88.
[166] Krzysztof Mikołajczyk, *Przestępstwa związane z wykorzystaniem bankowości elektronicznej*, [data dostępu: 4 kwietnia 2016], <http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-1/1008,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-10-6-2014.html>

**Wyłudzenie karty płatniczej** odbywa się poprzez złożenie wniosku o wydanie karty, posługując się sfałszowanymi dokumentami. Stwierdzają tożsamość oraz wysokie zarobki. Celem jest spełnienie wymogów banku i uzyskanie oryginalnej karty, a następnie dokonanie transakcji, za które przestępca nie zamierza płacić[167]. W Polsce praktykuje się wysyłanie kart płatniczych zwykłym listem, dzięki usługom Poczty Polskiej. Kod PIN dosyłany jest tą samą drogą w późniejszym czasie lub posiadacz sam definiuje PIN dokonując aktywacji karty za pośrednictwem strony internetowej banku lub przy pierwszej transakcji z wykorzystaniem bankomatu.

Przestępstwo zwane **„posłużeniem się kartą niedoręczoną”**, wiąże się z przechwyceniem karty, zanim dotrze do prawowitego właściciela i dokonaniu transakcji lub wypłaty gotówki z bankomatu. Jest to naruszenie prawa, które cechuje późna wykrywalność, głównie ze względu na nieświadomość prawowitego właściciela karty dotyczącej jej przejęcia[168].

Równie niebezpieczne są przestępstwa związane z **utratą karty zbliżeniowej**. Zagrożenie wynika z funkcjonalności tych kart, których użycie polega na odpowiednim zbliżeniu karty płatniczej do terminala bez konieczności potwierdzenia transakcji do określonej kwoty, najczęściej jest to wysokość 50zł. Utrata takiej karty daje możliwość dokonywania płatności do kwoty określonej limitem, jak również może być użyta przy płatnościach w Internecie[169]. Warto również podkreślić rodzący się nowy typ zagrożenia, jakim jest zeskanowanie karty zbliżeniowej. Do realizacji tej czynności wystarczy użycie specjalnego czytnika lub oprogramowania, które można zainstalować w coraz popularniejszych smartfonach obsługujących technologię NFC. Dzięki temu, przestępca wchodzi w posiadanie numeru karty oraz daty jej ważności, a w niektórych wersjach skanowane jest również imię i nazwisko właściciela karty[170].

Następną metodą jest **skimming karty płatniczej**. Jak spora grupa innych metod, wiąże się on z bezprawnym skopiowaniem treści zawartych na pasku magnetycznym w trakcie wypłacania gotówki z bankomatu. Tę metodę wyróżnia realizacja, która dokonuje się podczas wkładania karty do urządzenia. Konieczne jest odpowiednie przygotowanie bankomatu. Sprawcy montują odpowiednie urządzenie wyposażone w czytnik kart bankomatu, skaner oraz pamięć pozwalające na odczytanie i zapamiętanie danych paska magnetycznego,

[167] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op.cit.*, s. 84-85.
[168] *Ibidem*, s. 127.
[169] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 23.
[170] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 131-133.

miniaturowe kamery oraz nakładki na klawiaturę mające na celu uzyskanie kodu PIN. Jest to tym bardziej niebezpieczna metoda, gdyż narzędzia do jej realizacji dostępne są bez większych problemów na rynku[171].

Bezpośrednio ze skimmingiem związane jest **fałszerstwo kart**. Zdobyte dane zostają naniesione na karty podrobione lub stworzone od nowa na tzw. białym plastiku. Przestępstwa przerobienia karty płatniczej najczęściej polegają na[172]:

- zmianie tłoczenia numerów,
- zmianie daty ważności karty,
- zaprasowaniu starego numeru i wybiciu nowego,
- wycinaniu i doklejaniu odpowiednich elementów karty (stosuje się żywice oraz odpowiednie kleje szybkoschnące),
- zmianach w pasku przeznaczonym na podpis posiadacza karty, polegających na zrywaniu bądź zaklejaniu nowymi paskami.

Zdarzają się jednak sytuacje, w których przerobienie karty okazuje się zupełnie nieopłacalne. W takich okolicznościach, przestępcy podejmują decyzję o stworzeniu sfałszowanej karty zupełnie od początku. Wymaga to uzyskania odpowiedniego sprzętu, wykorzystania konkretnych technologii oraz zdobycia informacji do wykorzystania. Celem tych starań jest stworzenie karty najbardziej zbliżonej do autentycznej. Graficzne elementy drukowane są techniką komputerową, sitodrukiem lub barwną kserokopią. Na taką kopię nakładany jest pasek magnetyczny lub jego imitacja. Następnie tłoczy się konieczne litery i cyfry, które malowane są srebrną farbą. Hologramy tworzy się przy użyciu specjalnych farb, na folii odblaskowej. Zdaniem B. Hołysta, aktualnie zidentyfikowano 21 sposobów służących sfałszowaniu kart bankomatowych[173]. Należy pamiętać, iż technika wciąż się rozwija, pomysłowość przestępców również.

Wszystkie wymienione zagrożenia są jedynie tymi najważniejszymi, najbardziej niebezpiecznymi i najczęściej występującymi. Nie jest to jednak wyczerpująca lista niebezpieczeństw jakie dotyczą bankomatów, kart płatniczych oraz szeroko pojętej bankowości terminalowej.

---

[171] Piotr Podsiedlik, Tomasz Czylok, *Przestępczość w bankowości elektronicznej – Skimming karty bankomatowej*, Katowice 2010, s. 15-21.
[172] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 101-104.
[173] *Ibidem*, s. 104-106.

### 2.1.3. Bankowość internetowa

Transakcje internetowe funkcjonują przede wszystkim w oparciu o proces ich autoryzacji. Wiąże się to z weryfikacją danych bądź kodów autoryzacyjnych wprowadzanych do systemu bankowości internetowej, dostępnej głównie na prywatnych urządzeniach osobistych klienta. Dzięki temu, identyfikacja tożsamości użytkownika nie jest potrzebna, a główny element bezpieczeństwa stanowią hasła dostępu oraz narzędzia służące do ich generowania. W związku z tym, zagrożenia na jakie narażony jest klient bankowości internetowej można podzielić na dwie grupy: bezpośrednie i zdalne[174]. Poniżej przedstawiono najczęściej występujące zagrożenia, których głównym celem jest chęć łatwego wzbogacenia się, działając na szkodę innych.

**Metoda „man-in-the-middle"**

Atak stanowiący odmianę wcześniej przedstawionego phishingu. Bazuje głównie na dobrej znajomości technik internetowych sprawcy oraz braku ostrożności klienta. Sprawca przejmuje kontrolę nad domowym routerem ofiary, a następnie zmienia ustawienia serwerów DNS. Dzięki temu, użytkownicy lokalnej sieci zaczynają używać serwerów DNS kontrolowanych przez przestępców. Ich działanie nie różni się niczym nadzwyczajnym od działalności poprzednich serwerów użytkowników, z jednym wyjątkiem. Użytkownik chcący skorzystać ze strony swojego banku, zostaje przekierowany na serwer pośredniczący, który imituję bankową witrynę. Klient wprowadzający dane niezbędne do autoryzacji, łączy się z bankiem pozostając pod kontrolą przestępców, którzy w tym momencie posiadają już dostęp do konta ofiary, a nawet są zdolni modyfikować przesyłane dane i informacje. Aby sprawa była bardziej skomplikowana, atakujący przekierowują połączenie na inny, wcześniej przejęty router, nie łącząc się bezpośrednio z przestępczego serwera. Routery przejmowane są poprzez złamanie hasła zabezpieczającego dostęp do panelu[175].

**Metoda „man-in-the-browser"**

Atak skupiony jest głównie na przeglądarce i jest niebezpieczny dla klienta, jak również dla instytucji. Złośliwy kod modyfikuje dane wprowadzane w formularzach, podczas

[174] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 29-32.
[175] *Kolejna kampania ataków na routery klienckie*, [data dostępu: 9 kwietnia 2016r], <http://www.cert.pl/news/tag/man-in-the-middle>

użytkowania systemu bankowości internetowej. Najczęściej zapisuje się na dysku twardym klienta, będąc sparametryzowanym pod kątem konkretnego systemu bankowego[176].

**Carding**

Jest przestępstwem mało znanym w Polsce, ale na chwilę obecną, bardzo powszechnym np. w Niemczech. Polega na nielegalnym wykorzystaniu numerów karty płatniczej. Dodatkowo potrzebna jest data ważności karty oraz kod CVV2/CVC2 (ang. *Card Verification Value/Card Verification Code*), znajdującego się na pasku z tyłu karty, służący do weryfikacji transakcji zdalnych, jednocześnie będący potwierdzeniem, iż płatnik jest w rzeczywistym posiadaniu karty[177]. Istotnym jest fakt, iż to przewinienie opiera się o numer karty płatniczej, a nie dane dotyczące jej posiadacza. Przestępstwo ściśle związane jest z postępem handlu online i dokonywane jest głównie podczas zamówień pocztowych, telefonicznych lub za pomocą sieci komputerowej. Znane są 4 główne metody pozyskiwania cudzych numerów kart[178]:

- **Metoda „mechaniczna" lub elektroniczna**, gdzie wykorzystuje się techniki komputerowe, programy szpiegowskie typy spyware, konie trojańskie, wirusy oraz pharming,
- **Metoda wyłudzenia danych** (ang. *scam*), sprawcy posługują się celowymi działaniami, dzięki którym, wyłudzenie danych dokonane jest bezpośrednio od ofiary,
- **Metoda „podejrzenia" danych**, gdzie głównym działaniem jest obserwacja ofiary,
- **Metoda zakupu danych od nieuczciwych osób**, które posiadają dostęp do baz danych banków lub instytucji zajmujących się przetwarzaniem danych.

Znana jest także metoda tzw. **trash diving**, którą określa się zwyczajne przeszukiwanie kosza na śmieci, gdzie można znaleźć między innymi paragony z numerami kart ze sklepów i jednostek, w których dokonano płatności kartą. Cały proceder wygląda następująco:

1. Oszust kradnie informacje o kartach płatniczych i przesyła je swojemu koledze (tzw. carderowi) informacją o towarach do zakupienia i osobach, do których ma je wysłać.

2. Carder przygotowuje spis sklepów, które cechują się niezbyt zaawansowanymi zabezpieczeniami i zamawia konkretne towary, wykorzystując skradzione numery kart

[176] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 36.
[177] *Ibidem*, s. 21-22.
[178] Roland Szymkiewicz, *Czym jest carding?*, [data dostępu: 9 kwietnia 2016], <http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298323,Czym-jest-carding.html>

w ramach płatności. Jako odbiorcy towarów wskazany zostaje jeden lub kilku następnych pośredników.

3. Rolą pośredników jest odebranie towaru osobiście bądź w punktach odbioru paczek oraz przekazanie ich oszustowi. Oszust zakupiony towar zostawia dla własnych korzyści lub sprzedaje np. na aukcjach internetowych, dzieląc się jednocześnie zyskami z carderem.

W przestępstwo cardingu zamieszana jest zazwyczaj grupa od kilku do kilkunastu osób: zleceniodawców, pośredników i informatorów. Rzadko się zdarza, by zajmowały się tym pojedyncze osoby. Poza osobą okradzioną, ofiarami bardzo często są również pośrednicy, werbowani za pomocą drobnych ogłoszeń lub spamu. Zyskują kilkadziesiąt złotych dodatkowego dochodu, lecz bardzo często nie są świadomi, iż pełnią rolę pasera na zlecenie cyberprzestępców[179].

**Sniffing**

Polega na przechwytywaniu informacji przesyłanych w lokalnych sieciach oraz sieciach WiFi. W tym celu wykorzystuje się programy komputerowe, tzw. *sniffery*. Ich zadaniem jest odbieranie i analizowanie danych z sieci. Programy wykorzystywane do podsłuchu w sieci są oprogramowaniem szpiegującym, tzw. spyware. Najczęściej zajmują się przejmowaniem informacji oraz monitorowaniem ruchu w sieci, lecz nie wpływają na zmianę ich treści. Zalicza się do nich[180]:

- **Password sniffer**, który przechowuje początkową sekwencję danych każdej sesji, zawierającej identyfikatory i hasła użytkowników danej sieci.
- **Keyloggers** (rejestrator klawiatury), umożliwia odczytanie hasła i innych danych, które użytkownik zmuszony jest wprowadzić korzystając z usług bankowości elektronicznej. Rejestruje wszystkie wpisy dokonanie przez użytkownika z użyciem klawiatury.
- **Browser hijacker**, pozwala na przejęcie strony internetowej i zmianę jej ustawień, dzięki czemu możliwe jest np. przekierowanie użytkownika na zupełnie inną stronę.

W większości przypadków, programy spyware potrzebują pomocy człowieka, aby móc zainfekować komputer. Wykorzystuje się do tego luki w oprogramowaniu bądź wprowadza się

[179] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 178-182.
[180] Marek Siwicki, *Op. Cit.*, s. 122.

użytkownika w błąd. Uzyskane dane osobowe najczęściej używane są do podszycia się pod ofiarę i podjęcia działań na jej szkodę[181].

**Tampering**

Przestępstwo ściśle związane z bankowością internetową. Polega na przechwyceniu i zmianie danych lub informacji przez osoby postronne. W efekcie takiego działania, odbiorca otrzymuje informację o fałszywej treści, czego najprawdopodobniej może być nieświadomym. W najlepszym wypadku, skutkiem będzie jedynie nieporozumienie. W najgorszym – straty finansowe może ponieść i klient i bank, gdy przykładowo, zmienione informacje będą dotyczyć numeru rachunku bankowego, na który powinna zostać przelana kwota pieniędzy[182].

**Atak słownikowy**

Jest to atak polegający na próbie zalogowania się do systemu bez znajomości hasła dostępu. W jego miejsce podstawiane są kolejne słowa, które znajdują się w pliku będącym słownikiem. Plik ten, może posiadać nawet do kilku tysięcy słów, co bezpośrednio wiąże się z jego skutecznością – im więcej słów, tym większe szanse powodzenia[183].

**Bezpośrednia kradzież haseł i narzędzi**

Jest to bardzo częste zjawisko, którego potencjał z reguły nie jest doceniany. W natłoku codziennych spraw i obowiązków, społeczeństwo stara się możliwie jak najbardziej uprościć sobie życie. Wychodząc naprzeciw tej potrzebie, została stworzona i powszechnie udostępniona możliwość zapisywania loginów i haseł na wszelkiego rodzaju urządzeniach, „zapamiętanych" w przeglądarkach lub aplikacjach. Niewątpliwie jest to przydatna funkcjonalność, gdyż pozwala zaoszczędzić czas i sprawia, że dostęp do rachunku bankowego nie wymaga żadnego większego wysiłku. Możliwe jest także zachowanie tych danych w formie jawnej, pod postacią pliku .txt lub krótkich notatek. Są to sposoby bardzo wygodne dla użytkowników, a jeszcze bardziej dla przestępców. Dzięki temu, zwykła kradzież przykładowych tokenów, tabletów czy telefonów komórkowych, które wykorzystuje się do autoryzacji dostępu do rachunku i przeprowadzania transmisji internetowych, pozwala

[181] Mateusz Górnisiewicz, Radosław Obczyński, Mariusz Pstuś, *Op. Cit.* , s. 35-36.
[182] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 187.
[183] Związek Banków Polskich, Bankowość internetowa. Atak słownikowy, [data dostępu: 10 kwietnia 2016], <https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=10>.

złodziejowi na pełną dowolność w użyciu zapisanych danych i rozdysponowaniu kwotą dostępną na koncie[184].

### Zdalna kradzież haseł i kodów jednorazowych

Kradzież zdalna jest nieco bardziej utrudnioną dla przestępcy formą wejścia w posiadanie danych dostępowych użytkownika. Niezbędne do autoryzacji informacje zapisane na dysku wykradane są przez użycie specjalnego oprogramowania lub dzięki wykorzystaniu luk (ang. *vulnerability*) w systemie zabezpieczeń komputera osobistego. Wiąże się to najczęściej ze skopiowaniem treści zawartych na dysku urządzenia lub rejestracji sekwencji znaków, kolejno wpisywanych z klawiatury[185]. Jest to przewinienie, którego czynności sprawcze opierają się o nielegalny dostęp do systemów informatycznych, nielegalną ingerencję w system oraz nielegalną ingerencję w dane[186]. Szkodliwe oprogramowanie, znane także pod nazwą malware (ang. *malicious software*) wprowadzane jest do systemu poprzez różne aplikacje, strony internetowe, pliki, zewnętrzne nośniki danych, skrzynkę mailową i wiele innych sposobów. Jego funkcjonowanie możliwe jest niezależnie (robaki i zombie), bez konieczności posiadania dodatkowego oprogramowania, działa i poddaje się szeregowaniu i uruchamianiu przez system operacyjny. Może funkcjonować również zależnie (w przypadku bomb logicznych, koni trojańskich i wirusów) od aplikacji lub innych programów systemowych, pełniących rolę „żywiciela”[187]. Co równie ważne, maleware może być replikowalny (wirusy, robaki i zombie), co oznacza, że programy lub jego fragmenty, potrafią uaktywnić się w dowolnym czasie, w tym samym lub innym systemie. Oprogramowanie niereplikowalne (bomby logiczne, konie trojańskie) uruchamia się jednocześnie z wywołaniem danego programu[188]. Poniższa tabela przybliża obraz poszczególnych elementów.

| Zagrożenie | Opis |
|---|---|
| *Wirus*<br>*(ang. virus)* | Fragment kodu, infekuje program lub cały system. Jego zadaniem jest zarażanie i poszukiwanie kolejnej ofiary. Nielegalne zmiany przeprowadza w programie nosiciela lub innym, dowolnym miejscu na dysku[189] |
| *Robak*<br>*(ang. worm)* | Potrafi wprowadzić inne szkodliwe oprogramowanie (np. konia trojańskiego), zachowywać się jak wirus oraz rozpowszechniać się poprzez połączenia |

[184] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 33.
[185] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 184.
[186] *Ibidem*, s. 143.
[187] William Stallings, *Kryptografia…, Op. Cit.,* s. 355-356.
[188] William Stallings, *Systemy… Op. Cit.,* s.781-782.
[189] Marek Wrona, *Niebezpieczeństwo komputerowe*, Warszawa 2000, s. 55-60.

| | |
|---|---|
| | sieciowe (np. poprzez pocztę elektroniczną). Wysyła kopię samego siebie do innego systemu lub loguje się zdalnie w innym systemie i tworzy kopię samego siebie[190]. |
| *Zombie, bot* | Aktywacja zombie na zainfekowanym komputerze, pozwala z jego poziomu na rozsyłanie spamu i ataki na inne komputery[191]. |
| *Koń trojański* | Program rozsyłany przez innych użytkowników. Nie potrafi rozprzestrzeniać się we własnym zakresie. Ukrywa się pod postacią innych narzędzi. Może wyświetlać niechciane komunikaty, usunąć dane, kraść informacje, skonfigurować zdalny dostęp do systemu oraz wprowadzić inne niebezpieczne programy[192]. |
| *Bomba logiczna* | Jest to fragment niechcianego kodu, wbudowany w dany program. Aktywuje się w odpowiednio określonym czasie, terminie lub po dokonaniu konkretnych czynności. Skutkiem jego „eksplozji" mogą być: skasowanie lub modyfikacja plików, włączenie lub ponowne uruchomienie komputera lub zablokowanie pracy użytkownika[193]. |
| *Pobieracz (ang. downloader)* | Program pobiera i instaluje szkodliwe oprogramowanie w systemie użytkownika. Najczęściej rozsyłany za pomocą poczty elektronicznej[194]. |
| *Kod przenośny (ang. mobile code)* | Programy zapisane między platformami, w językach przenośnych, o identycznej semantyce, jak np. VBScript i JavaScript. Najczęściej wysyłany pocztą elektroniczną, transportuje inne zagrożenia (wirusy, robaki, trojany)[195]. |

*Tabela 3. Wybrane zagrożenia danych, informacji i plików autoryzacyjnych zawartych w systemie.*
Źródło: Opracowanie własne na podstawie: William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, William Stallings, Systemy operacyjne – struktura i zasady budowy, Wallace Wang, Tajemnice internetu, hackingu i bezpieczeństwa, Marek Wrona, Niebezpieczeństwo komputerowe.

W ostatnim czasie bardzo popularny stał się tzw. **„wirus bankowy",** funkcjonujący także pod nazwą VBKlip. Jest to rodzaj złośliwego oprogramowania, wykorzystujący codzienne przyzwyczajenia użytkowników bankowości internetowej. W momencie kopiowania przez użytkownika 26 cyfrowego numeru konta do schowka systemu Windows, numer zostaje podmieniony na inny. W efekcie, zamierzony przelew zasila konto cyberprzestępcy[196].

Nie ulega wątpliwości, iż najczęstszym sposobem na zainfekowanie systemu operacyjnego jest rozsyłanie niechcianych wiadomości pocztą elektroniczną, zwanych

[190] William Stallings, *Systemy… Op. Cit.,* s.784.
[191] William Stallings, *Kryptografia…, Op. cit.*, s. 359.
[192] Wallace Wang, *Tajemnice Internetu, hackingu i bezpieczeństwa*, Gliwice 2005, s. 93-102.
[193] William Stallings, *Kryptografia…, Op. cit.*, s. 359.
[194] *Ibidem*, s. 355.
[195] *Ibidem*, s. 359.
[196] NASK, *Wirus podmieniający numery kont bankowych wciąż groźny*, [data dostępu: 11 kwietnia 2016], <https://www.nask.pl/wydarzeniaID/id/919>.

spamem. Aktywacja szkodliwego oprogramowania najczęściej skutkuje: nieupoważnionym kasowaniem danych, rozsyłaniem spamu, dokonywaniem ataków na inne hosty w sieci, kradzieżą danych (jak np. hasła, numery kart płatniczych, dane osobowe), uniemożliwieniem dalszej pracy oraz przejęciem przez osobę nieupoważnioną kontroli nad osobistym komputerem. Złośliwe programy stanowią zagrożenie nie tylko dla bankowości internetowej, są równie niebezpieczne dla pozostałych kanałów dystrybucji. W konsekwencji podjętych przez przestępcę działań, użytkownik narażony jest na ingerencję w integralność danych, poufność treści, usług, które mogą ulec sparaliżowaniu oraz wszelkie procesy związane z uwierzytelnianiem.

### 2.1.4. Bankowość telefoniczna

Bankowość telefoniczna, jest stosunkowo młodym kanałem dystrybucji bankowości elektronicznej i charakteryzuje się głównie dwoma zagrożeniami, wynikającymi z funkcjonalności dostępnych aktualnie telefonów. Należy jednak pamiętać, że ze względu na swoje rozmiary, są to urządzenia dużo bardziej podatne na kradzieże niż np. komputery czy tablety, a przejęcie danych przechowywanych na smartfonach, także może wyrządzić wiele bolesnych szkód.

**Vishing**

Nazwa tego przestępstwa powstała z połączenia słów zawartych w wyrażeniu voice phishing, co oznacza phishing głosowy. Jest to przestępstwo, którego podstawą działania jest phishig (również polega na nielegalnym pozyskaniu danych), lecz w nieco odmiennej postaci. Przestępca najczęściej podszywa się pod osoby lub instytucje godne zaufania. W pierwszej kolejności sprawca dzwoni do klienta banku (klient najczęściej słyszy nagrany głos lektora), informując go o problemach z autoryzacją transakcji, blokadą karty, problemem dostępu do rachunku lub podobnych sytuacjach. Jednocześnie prosi klienta o natychmiastowy kontakt z bankiem, zostawiając numer telefonu, który nie jest rzeczywistym numerem banku, lecz przestępcy. Nieświadomy klient oddzwania i zostaje poproszony o potwierdzenie danych typu: numer rachunku, login, hasło, numer karty kredytowej, kod PIN itp. Przestępca oszukując ofiarę, zyskuje wszelkie niezbędne informacje. Inną, zbliżoną metodą działania w ramach vishingu jest rozsyłanie informacji do klientów, rzekomo pochodzących z banku bądź innych publicznych instytucji, mówiących o konieczności aktualizacji danych osobowych klienta.

Aby zdobyć większe zaufanie i nie wzbudzać podejrzeń, wiadomości te, uzupełniane są o numery telefonów lub adresy mailowe. W odpowiedzi ofiara również spotyka się z automatyczną odpowiedzią i koniecznością podania danych osobowych, „niezbędnych" do weryfikacji użytkownika[197]. Dzięki temu, niczego nieświadomy klient podaje swoje dane. Zdarzają się również programy, które korzystając z listy wcześniej pozyskanych numerów, same telefonują do klientów banku i jak w poprzednich przypadkach, przekonują ofiarę o konieczności udostępnienia swoich danych. Schemat działania jest bardzo prosty: Klient zgłasza się pod podany numer, w odpowiedzi słyszy powitanie np. „Witamy w banku X" i prośbę o podanie numeru konta, hasła itp. celem identyfikacji klienta banku[198]. W ten prosty sposób klient staje się ofiarą vishingu. Jak w przypadku zwykłego phishingu, przestępca bazuje na uśpieniu czujności ofiary i wydobyciu danych, wykorzystując do tego jedynie numer telefonu i prośbę o kontakt.

**Złośliwe oprogramowanie**

Funkcjonalność tzw. inteligentnych telefonów komórkowych (smartfonów) opiera się o przeglądarkę internetową bądź zainstalowane aplikacje, co sprawia, że bankowość telefoniczna pozwala na wykonywanie niemal tych samych czynności, które możliwe są do przeprowadzenia w bankowości internetowej. W związku z tym, złośliwe oprogramowania, pod postacią wirusów, robaków, koni trojańskich czy oprogramowania szpiegującego, również zagrażają bezpieczeństwu bankowości telefonicznej. Użytkownik jest tym bardziej narażony na utratę swoich treści, ingerencję w dane czy inne nieprzyjemności, gdyż smartfony dużo rzadziej zabezpieczane są programami antywirusowymi, niż np. komputery osobiste. To lekceważenie jest niezrozumiałe, ponieważ tak jak za pomocą bankowości internetowej, tak również za pomocą telefonu można korzystać z bankowości elektronicznej, a zagrożenia wynikające z infekcji telefonów mają taki sam charakter jak te, które przytrafiają się w bankowości internetowej[199].

Powyższy rozdział znacząco przybliżył zjawisko zagrożeń występujących w bankowości elektronicznej. Każde przestępstwo z nią związane, ściśle łączy się

[197] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 43-44.
[198] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 209-210.
[199] *Ibidem*, s. 212-213.

z wykorzystaniem danych osobowych klientów, jedynie ich pozyskanie jest zróżnicowane, ze względu na użyte narzędzie przestępstwa oraz kanał dystrybucji, którego dotyczy. Metody kradzieży mienia oraz tożsamości są bardzo zróżnicowane, a ich wachlarz rozpościera się pomiędzy najprostszymi, a najbardziej zaawansowanymi metodami, pamiętając, że postępująca technologia wciąż daje szerokie możliwości rozwoju. Przestępstwa i wykroczenia skupiające się wokół bankowości elektronicznej są bardzo popularne, ze względu na wysokie korzyści majątkowe, które zachęcają sprawców do podejmowania ryzyka ataku. Kusząca okazuje się również naiwność, lekceważenie zabezpieczeń oraz niewiedza klientów, ułatwiające przejęcie pieniędzy przez osoby niepowołane. Wszystkie opisane przestępstwa są jedynie tymi, które występują najczęściej, przynosząc największe szkody ofierze. Nie jest to wyczerpująca lista czynów zabronionych, na jakie narażeni są klienci bankowości. Natomiast wszystkie z nich podlegają karom, lecz jak wskazują wszelkie statystyki dotyczące przestępstw w bankowości elektronicznej, konsekwencje nie odstraszają sprawców, a wykrywalność ich czynów także bywa różna.

# Rozdział III
# „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością” - analiza wyników ankiety

## 3.1. Cel ankiety

Przeprowadzone badanie miało na celu sprawdzenie i określenie poziomu świadomości przeciętnych klientów bankowości elektronicznej, w szeroko pojętym zakresie zachowania podstawowych zasad bezpieczeństwa, dotyczących zarządzania pieniędzmi umieszczonymi na prywatnym koncie bankowym. Pod uwagę wzięto przede wszystkim posiadaną przez klientów wiedzę z zakresu ochrony danych osobowych oraz aktualnie występujących zagrożeń. Przeprowadzoną analizę oparto o wybrane kanały dystrybucji bankowości elektronicznej.

## 3.2. Adresaci ankiety

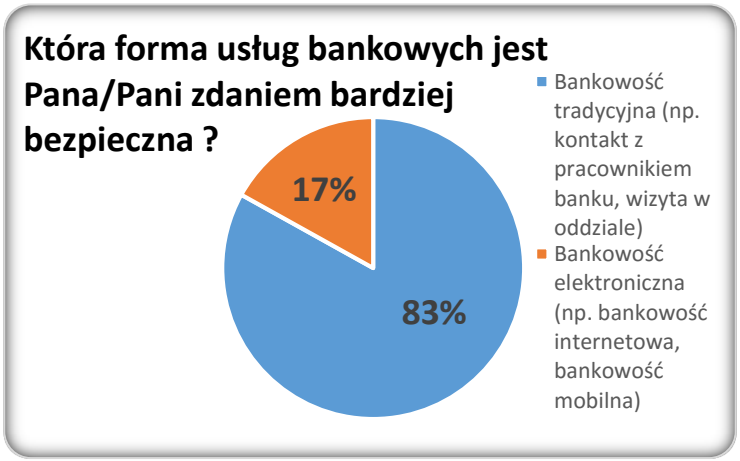
W pełni anonimowa ankieta skierowana została do osób korzystających z konta bankowego za pomocą bankowości elektronicznej. W badaniu udział wzięło 65 respondentów, wśród których 45% (29 ankietowanych) to kobiety, a 55% (36 osób) to mężczyźni. Odpowiedzi najczęściej udzielały osoby w przedziale wiekowym pomiędzy 16 a 25 lat (75% respondentów – 49 osób), a najrzadziej w wieku powyżej 65 lat (3% - 2 osoby). Średnio usytuowała się grupa osób w wieku między 26 a 45 lat (15% - 10 osób) i tuż za nią grupa respondentów w wieku 46-65 stanowiący 6% wszystkich odpowiadających (4 osoby). Już wyniki wstępnej część badania, potwierdziły przekonanie, ogólnie znane w społeczeństwie, iż największe zainteresowanie bankowością elektroniczną przejawiają osoby poniżej 45 roku życia, ze szczególnym naciskiem na użytkowników Internetu, którzy nie osiągnęli 30 roku życia. Są to najczęściej osoby dobrze bądź bardzo dobrze zaznajomione z tematyką obsługi komputera i wykorzystania Internetu w życiu codziennym, co przez naturalne czynniki i różnice pokoleniowe, jest o wiele rzadszym zjawiskiem u osób powyżej 50 roku życia, których przywiązanie do technologii nie jest zbyt wysokie. Zdecydowana większość respondentów (89%) to mieszkańcy miast, posiadający wyższe (40% - 26 ankietowanych) lub niepełne wyższe (34% - 22 osoby) wykształcenie. Pozostali ankietowani posiadają średnie, zawodowe lub podstawowe wykształcenie. Różnorodność respondentów pod kątem wieku, miejsca zamieszkania oraz osiągniętego poziomu edukacji, jak również szczegółowość pytań zawartych w kwestionariuszu pozwalają na odwzorowanie rzeczywistych przyzwyczajeń użytkowników.

## 3.3. Opis ankiety

Badanie rozpoczęło się z dniem 15 listopada 2015r, a zakończyło 25 listopada 2015r. Ankieta dostępna była wyłącznie w elektronicznej formie i wykorzystywała narzędzie tworzenia formularzy, udostępnionego za pośrednictwem zasobów Google. Umożliwia dowolne tworzenie pytań, a także ich edycję czy całościowe dostosowanie do potrzeb ankietera. Udzielone odpowiedzi gromadzone są w bardzo przystępnej formie arkusza kalkulacyjnego Microsoft Excel. Narzędzie to pozwala także na prezentację ogólnych wyników ankietowanym tuż po zakończeniu badania, które trwa między 10 a 15 minut, zachowując jednocześnie całkowitą anonimowość respondentów. Pytania zawarte w kwestionariuszu występowały w otwartej jak również zamkniętej formie, a każdemu z nich przypisano funkcję, która wymuszała konieczność udzielenia odpowiedzi.

## 3.4. Prezentacja i analiza uzyskanych wyników ankiety

Polacy coraz chętniej korzystają z możliwości oferowanych przez bankowość elektroniczną. Jej popularność stale wzrasta, choć jak dotąd nie udało jej się wyprzeć bankowości tradycyjnej. Codziennemu funkcjonowaniu każdego człowieka towarzyszą przekonania, które pielęgnowane od lat, nabierają na swojej sile. Analizując pierwsze skojarzenia, bankowość tradycyjna kojarzy się przede wszystkim z dobrą obsługą Klienta, łatwym i przystępnym dostępem do wybranej placówki, jak również znajomym środowiskiem. Bankowość elektroniczna natomiast, kojarzy się głównie z nieporównywalną szybkością obsługi, łatwym dostępem do transakcji bankowych oraz szeroko pojętą nowoczesnością[200]. Z tego względu, każda próba przekonania użytkowników do zmiany swoich poglądów, a tym samym przyzwyczajeń i zachowań, najprawdopodobniej spotka się z uporczywymi przeciwnościami. Wśród ankietowanych aż 83% osób (54 respondentów) zdaje się być przekonanych o wyższym poziomie bezpieczeństwa bankowości tradycyjnej. Tylko 17%

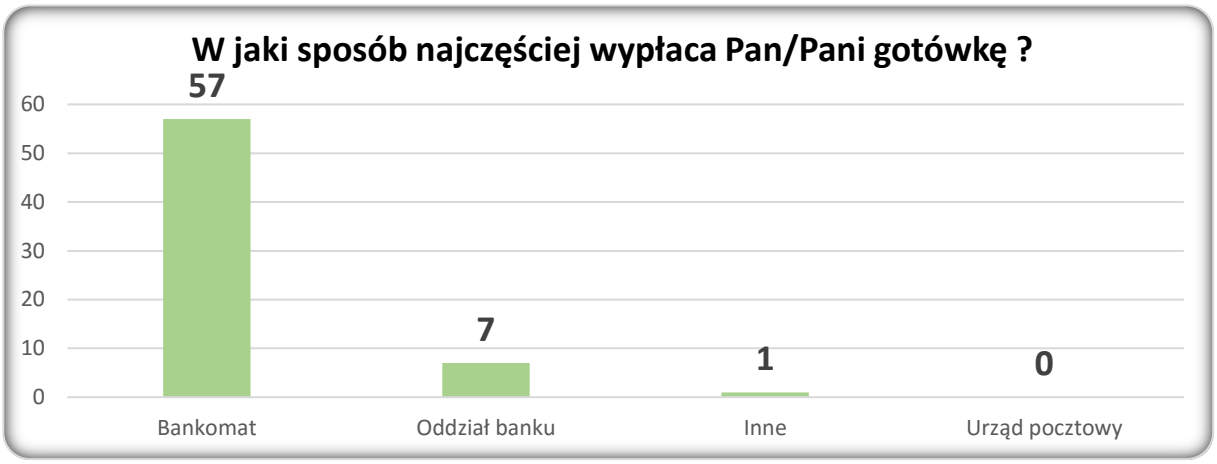



Rysunek 11. Która forma usług bankowych jest Pana/Pani zdaniem bardziej bezpieczna ?

*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

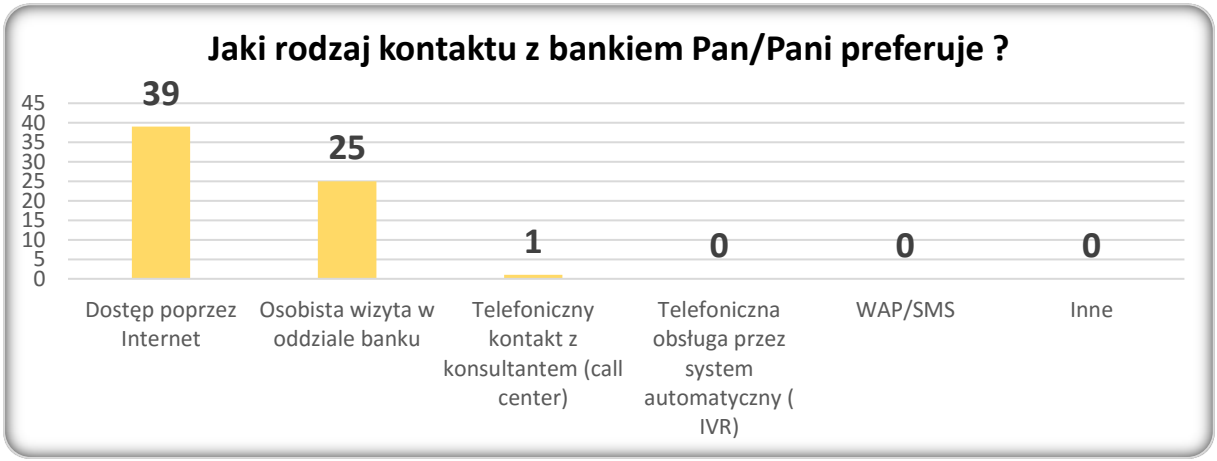
[200] Andrzej Poszewiecki, Przemysław Kulawczuk, *Bankowość tradycyjna a internetowa*, [data dostępu: 14 kwietnia 2016], <http://www.gazeta-msp.pl/?id=pokaz_artykul&indeks_artykulu=422&id_autor=139>.

(11 osób) opowiedziało się po stronie bankowości elektronicznej. Natomiast takie podejście nie uzyskało odzwierciedlenia w deklarowanych preferencjach kontaktu z bankiem.




Rysunek 12. W jaki sposób najczęściej wypłaca Pan/Pani gotówkę?
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

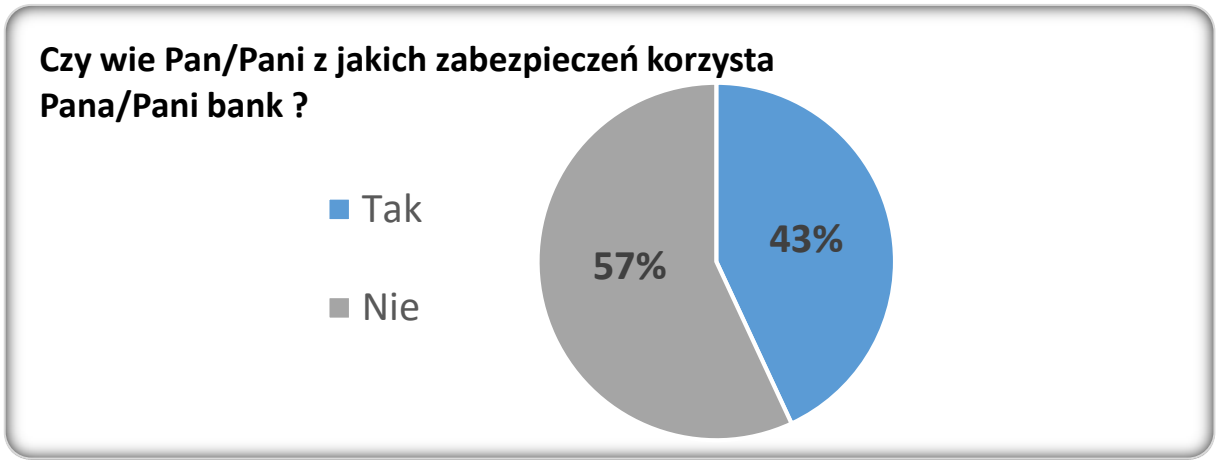
Jest to interesujące zjawisko, ponieważ mimo silnego przekonania o wyższości tradycyjnych usług bankowości pod kątem bezpieczeństwa, zdecydowana większość, bo aż 88% (57 respondentów) Klientów wypłaca gotówkę za pomocą bankomatu, reszta stanowiąca 12% (8 osób) odwiedza placówkę banku lub korzysta w inny sposób. Również preferencje dotyczące poszczególnego kontaktu z bankiem, przemawiają raczej za bankowością elektroniczną, choć w tym przypadku poza wypłatą czy wpłatą gotówki, brana jest pod uwagę również przykładowa chęć zaczerpnięcia informacji o promocjach lub dokonywanie innych operacji bankowych.




Rysunek 13. Jaki rodzaj kontaktu z bankiem Pan/Pani preferuje?
*Źródło: Opracowanie własne na podstawie ankiety pt.*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

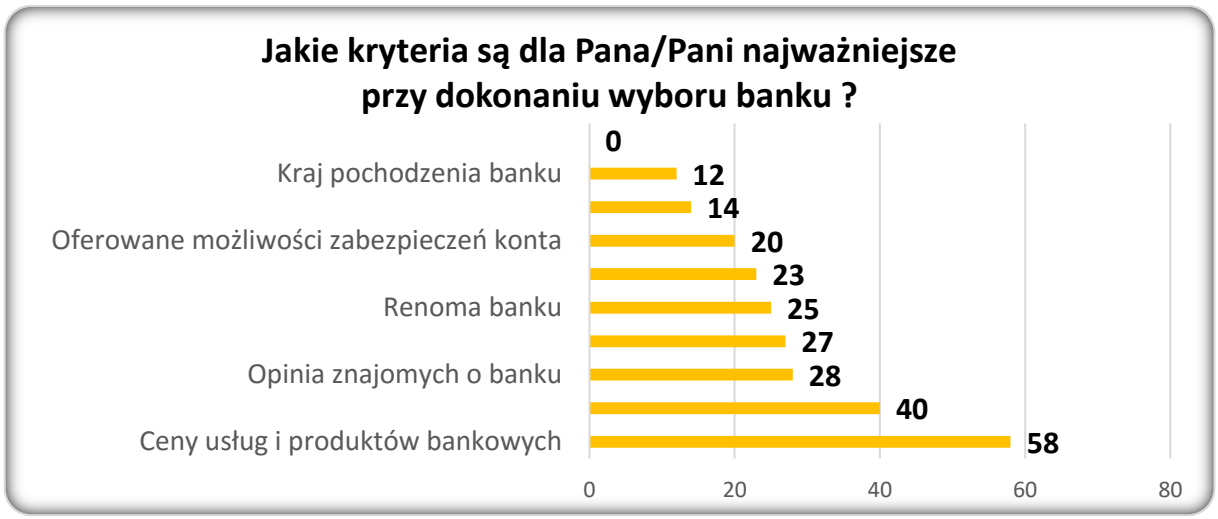
60% respondentów to zwolennicy wykorzystania dostępu do bankowości poprzez Internet, osobistą wizytę w banku praktykuje 38% Klientów. Poruszając kwestię postrzegania

bezpieczeństwa w tradycyjnej i elektronicznej formie bankowości, nie sposób pominąć pytania o zabezpieczenia.




Rysunek 15. Czy wie Pan/Pani z jakich zabezpieczeń korzysta Pana/Pani bank?
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Aż 57% (37 osób) nie wie, z jakich zabezpieczeń korzysta bank prowadzący ich własne pieniądze. Tylko 43% (28 osób) orientuje się w tym zakresie. Jest to bardzo niski wynik, biorąc pod uwagę osobisty interes każdego z użytkowników w posiadaniu wiedzy na ten temat. Czym zatem kieruje się przeciętny Kowalski, przy dokonaniu wyboru banku dla siebie, podczas przeglądania różnorodnych ofert, które aktualnie zalewają rynek?

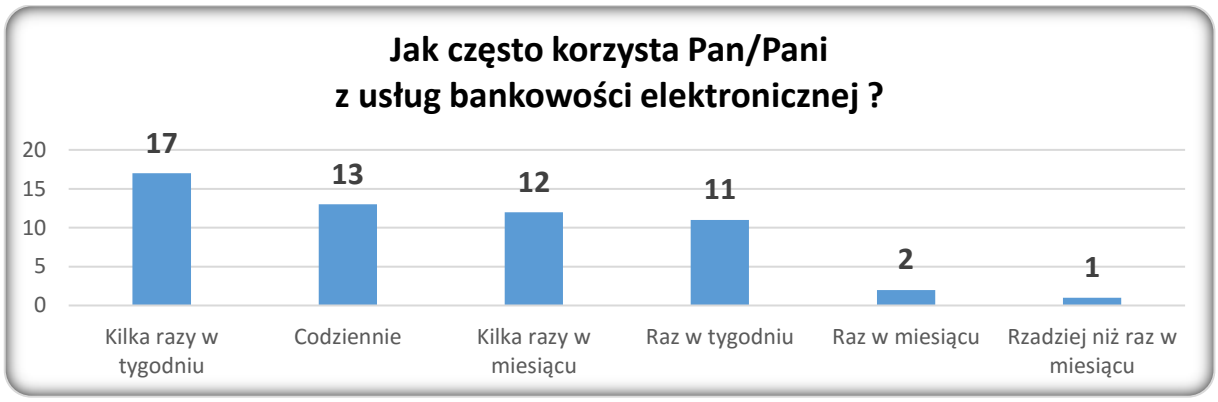



Rysunek 14. Jakie kryteria są dla Pana/Pani najważniejsze przy dokonywaniu wyboru banku?
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Decydującymi czynnikami są ceny usług i produktów bankowych oraz jakość obsługi Klienta. Niewiele mniej ważnymi, aczkolwiek już niekoniecznie decyzyjnymi elementami są: opinia znajomych o banku, zarówno ta pozytywna jak i negatywna, wysokie oprocentowanie lokat, renoma banku, położenie poszczególnych oddziałów oraz jak już wcześniej podkreślono,

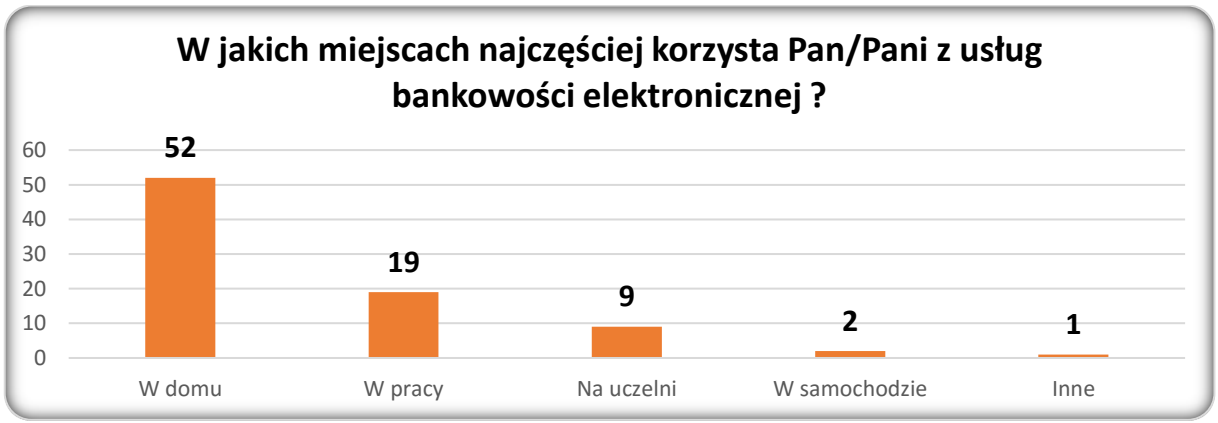
niepokojąco niski poziom zainteresowania oferowanymi możliwości zabezpieczeń własnego konta. Dla naszych ankietowanych najmniej istotnymi okazały się innowacyjne usługi oraz kraj pochodzenia banku.

Tak powszechnie znana i ciesząca się dużą popularnością bankowość elektroniczna to nic innego, jak wszelkie formy zdalnego zarządzania pieniędzmi, które stanowiąc dużą wygodę, ciągle zyskują uznanie wśród obecnych jak i nowych użytkowników. 86% ankietowanych (56 osób) korzysta z bankowości elektronicznej.



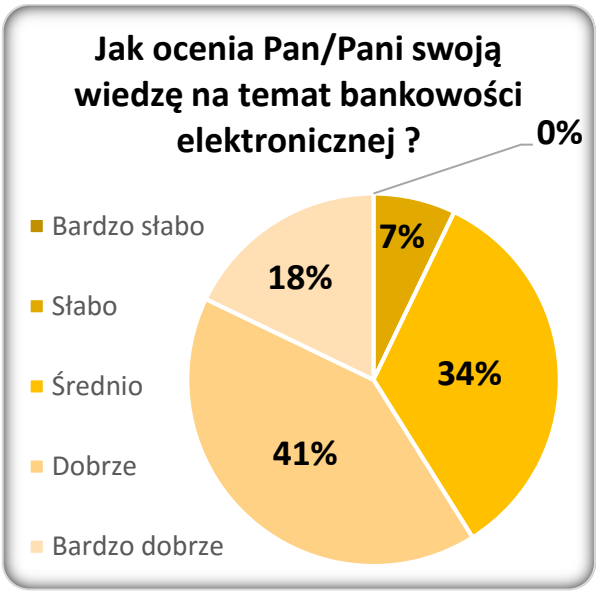

*Rysunek 16. Jak często korzysta Pan/Pani z usług bankowości elektronicznej?*
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

46% (30 respondentów) z nich to osoby, które korzystają z niej codziennie bądź kilka razy w tygodniu. 35% (23 respondentów) odpowiadających – kilka razy w miesiącu bądź raz w tygodniu. Raz w miesiącu lub rzadziej to 5% (3 osoby) ankietowanych korzystających z bankowości elektronicznej.




*Rysunek 17. W jakich miejscach najczęściej korzysta Pan/Pani z usług bankowości elektronicznej?*
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

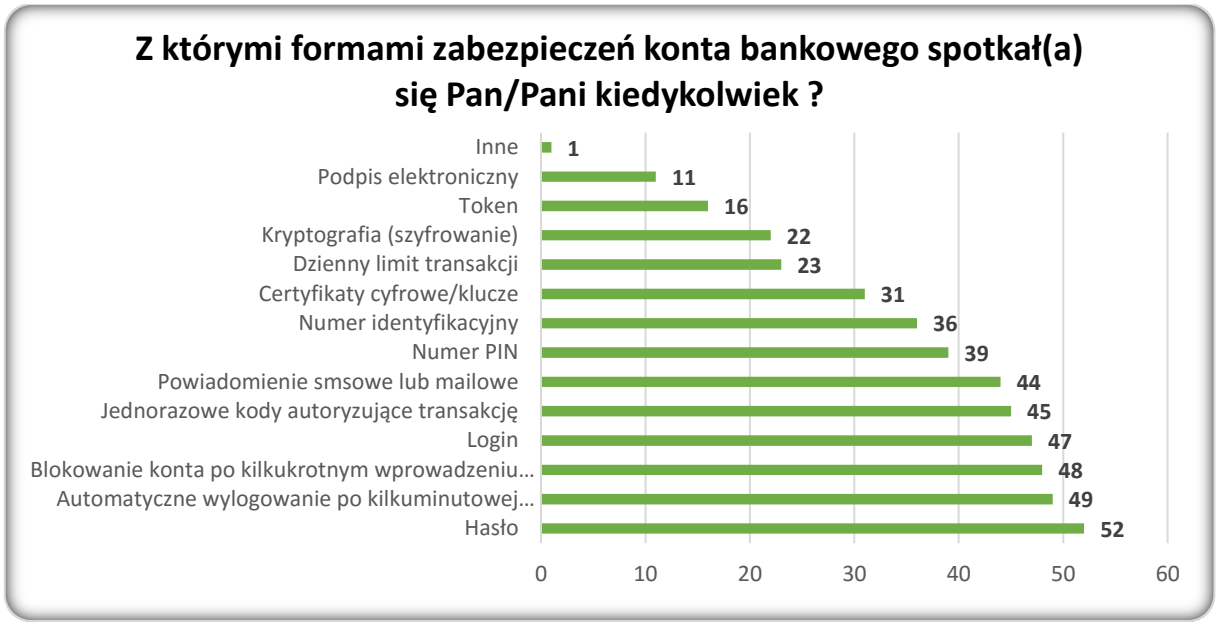
Najczęstszym miejscem sprzyjającym takim działaniom jest dom. Następnie praca bądź uczelnia. Najrzadziej korzysta się z bankowości elektronicznej w samochodzie i innych tego typu miejscach. Zaledwie 14% respondentów (9 osób) nie posługuje się taką bankowością. Wynika to z braku przekonania, dotychczasowego braku potrzeby, obawą przed oszustwem, brakiem zaufania, skomplikowanej obsługi jak również w przypadku osób starszych jest to brak niezbędnych narzędzi typu: komputer lub Internet. Natomiast większość z nich deklaruje chęć skorzystania z bankowości elektronicznej w przyszłości. Wynika to z faktu, iż korzyści, które czerpane są przez aktualnych użytkowników, jak najbardziej zachęcają do korzystania z takich udogodnień. Wśród wspomnianych cech, użytkownicy wymieniają przede wszystkim: wygodę, szybkość działania, oszczędność czasu i pieniędzy, bezpieczeństwo, brak kolejek, a tym samym uniknięcie narzekań innych, często starszych osób oczekujących na swoją kolej, dostępność do wszelkich informacji, usług i dokonywania transakcji o każdej porze i w każdym miejscu, bez konieczności wychodzenia z domu i poszukiwania oddziałów banku. Zwrócono uwagę także na łatwość kontroli swoich wydatków, darmowe usługi internetowe, mnogość dostępnych operacji możliwych do przeprowadzenia samemu, możliwość realizacji zakupów przez Internet a także brak styczności z personelem. Pomimo przedstawionego ogromu profitów wynikających z takiej formy, znalazły się także osoby, dla których sam fakt udostępnienia im takiej możliwości, zdalnego dostępu do swojego konta, jest jedynym i wystarczającym argumentem przemawiającym za jego użytkowaniem.




*Rysunek 18. Jak ocenia Pan/Pani swoją wiedze na temat bankowości elektronicznej?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

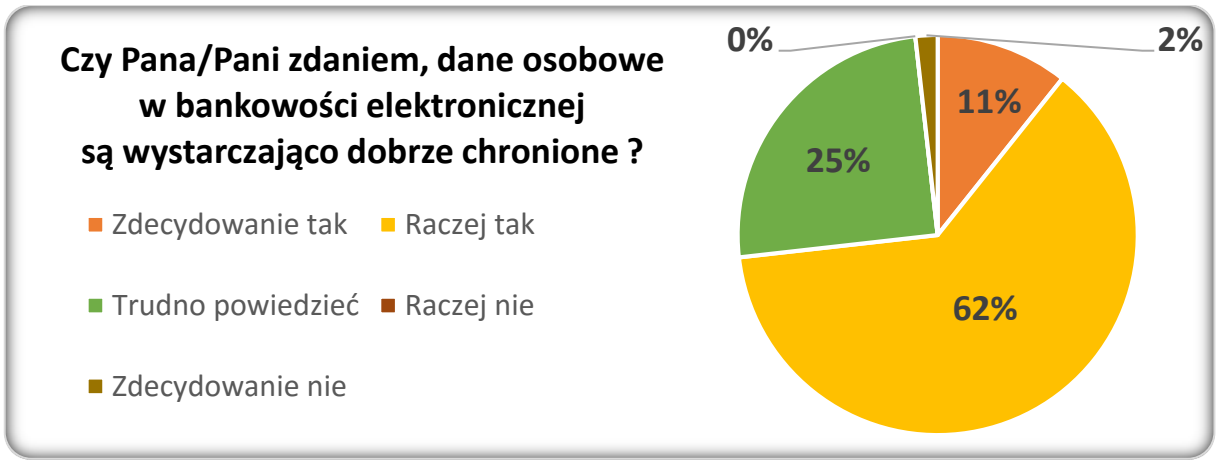

*Rysunek 19. Czy ma Pan/Pani pełne zaufanie do środków bezpieczeństwa stosowanych przez Pana/Pani bank?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Aż 80% (42 osoby) ankietowanych uważa, że ich wiedza na temat bankowości elektronicznej jest średnia lub dobra. Tylko 18% (10 osób) twierdzi, że ich wiedza jest bardzo dobra. Pozostała część ankietowanych deklaruje słabą bądź bardzo słabą znajomość tej tematyki. Te same osoby w 64% (36 osób) przejawiają pełne zaufanie do środków bezpieczeństwa używanych przez ich bank. Pozostałe 36% (20 osób) nie prezentuje już tak optymistycznego podejścia.



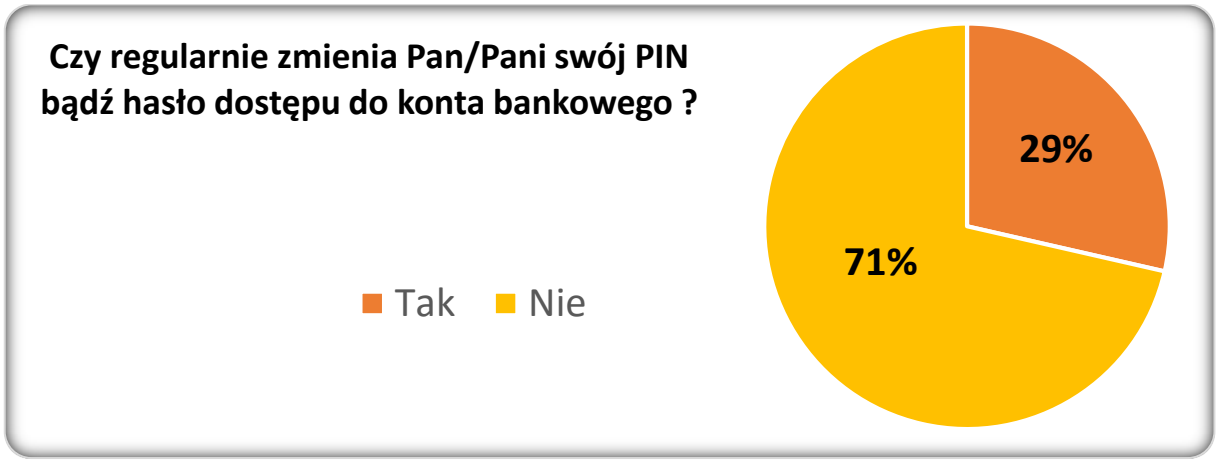

*Rysunek 20. Z którymi formami zabezpieczeń konta bankowego spotkał(a) się Pan/Pani kiedykolwiek?*
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Najczęstszymi formami zabezpieczeń z jakimi spotkali się odpowiadający są: hasło, zamknięcie sesji, czyli automatyczne wylogowanie się po kilkuminutowej bezczynności klienta, blokowanie konta po kilkukrotnym wprowadzeniu błędnych danych logowania, login, jednorazowe kody autoryzujące transakcję oraz powiadomienie sms'owe lub mail'owe o przeprowadzanych działaniach. Były to elementy wymieniane najczęściej. W odrobinę mniejszym stopniu, lecz również przytrafiającymi się metodami ochrony wymienia się: numer PIN, numer identyfikacyjny, certyfikaty i klucze cyfrowe, dzienny limit transakcji, szyfrowanie z wykorzystaniem kryptografii, token oraz podpis elektroniczny. Zawierzając w całości lub po części staraniom banków, warto również samemu zachować minimum ostrożności w zakresie wykorzystywanych urządzeń i własnego zachowania. Zdecydowanie najważniejszą i najbardziej zagrożoną informacją o użytkowniku są jego dane osobowe.




Rysunek 21. Czy Pana/Pani zdaniem, dane osobowe w bankowości elektronicznej są wystarczająco dobrze chronione?
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

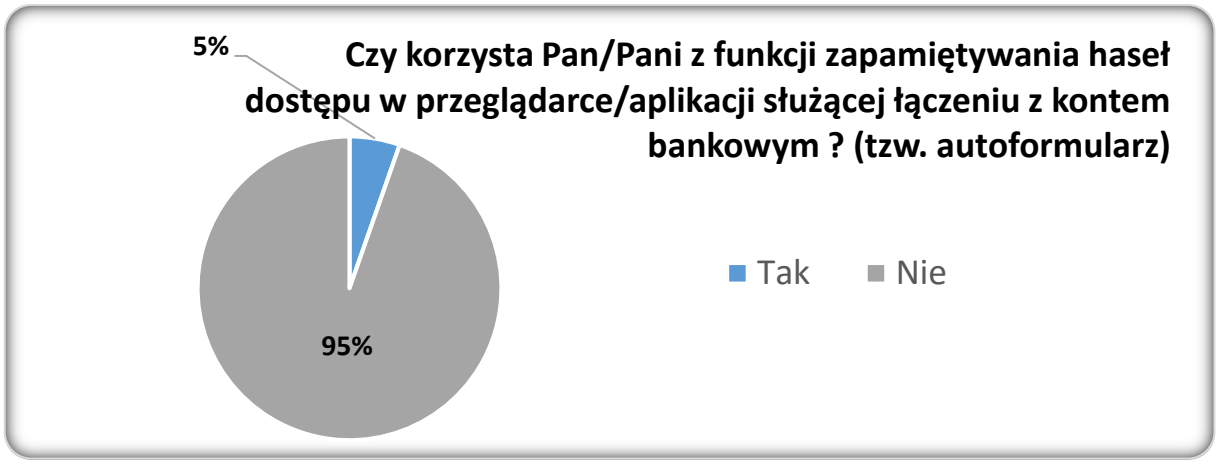
Większość ankietowanych (63%; 35 osób) uważa, że ich dane są raczej dobrze chronione, 25% (14 osób) nie ma zdania na ten temat, a zaledwie 11% (6 osób) uważa, że ochrona ich danych osobowych jest zdecydowanie właściwa. Są to stanowczo alarmujące wyniki. Minimalną formą zabezpieczenia, którą można zastosować we własnym zakresie jest odpowiednio zadbane hasło.




Rysunek 22. Czy regularnie zmienia Pan/Pani swój PIN bądź hasło dostępu do konta bankowego?
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

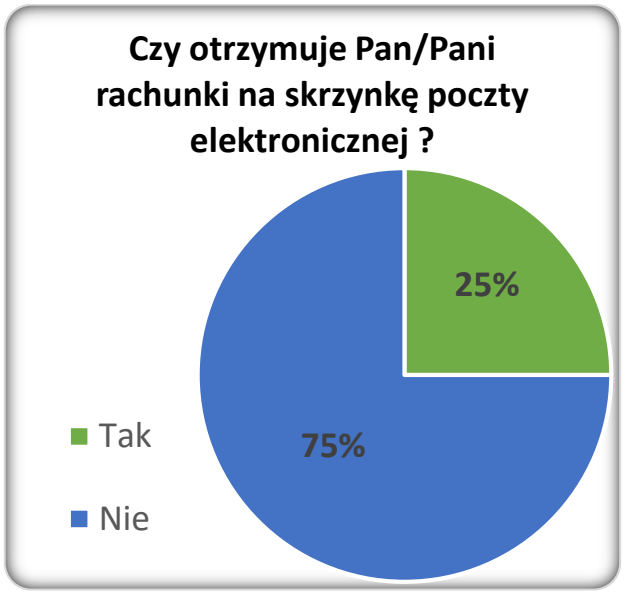
Aż 71% ankietowanych (40 osób) nie zmienia regularnie swojego hasła, co stwarza oczywiste zagrożenie dla dostępu do ich prywatnych treści. Istotnym jest także miejsce przechowywania haseł. Najczęściej są one zapamiętywane bez konieczności ich zapisywania. Jest to możliwie najbezpieczniejsza forma ochrony hasła. Niestety znalazła się również dość liczna grupa osób, które zapisują swoje dane dostępowe w notesach, trzymając w domu, w sejfie lub z innymi ważnymi dokumentami. Nie są to zbyt bezpieczne formy, choć wśród ankietowanych znalazła się garstka osób, które stosują niesłownikowe hasła, ukryte w ciągu znaków i zapisanych

w pliku .txt. Stanowi to już jakąś sensowną ochronę i daje odrobinę nadziei dla wiedzy użytkowników bankowości elektronicznej.

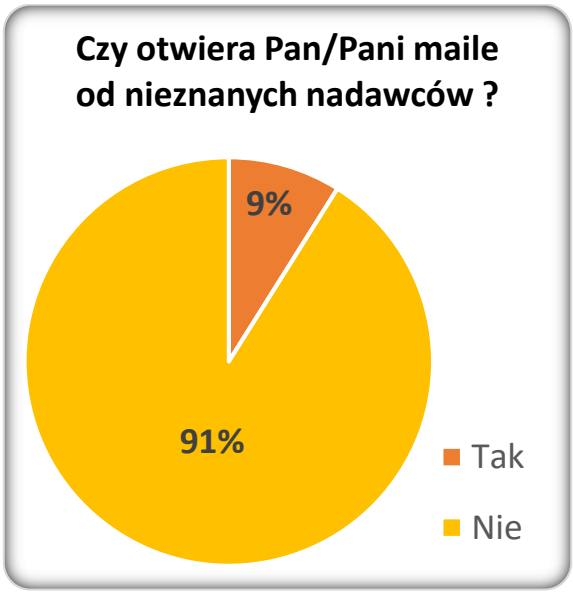



Rysunek 23. Czy korzysta Pan/Pani z funkcji zapamiętywania haseł dostępu w przeglądarce/aplikacji służącej łączeniu z kontem bankowym? (tzw. autoformularz)
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Ponadto 95% respondentów (53 osoby) nie zapamiętuje swoich haseł w przeglądarkach. Jest to mało wygodne, choć bezpieczne rozwiązanie. Ważnym aspektem są także rachunki, które otrzymywane na skrzynkę pocztową, stwarzają zagrożenie, w momencie zyskania nieuprawnionego dostępu przez osoby niepożądane, będąc źródłem dość pokaźnego zasobu informacji na temat odbiorcy.

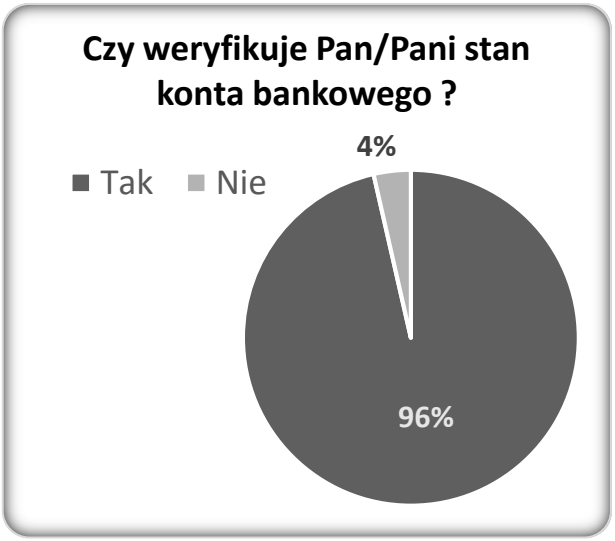



Rysunek 24. Czy otrzymuje Pan/Pani rachunki na skrzynkę poczty elektronicznej?
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

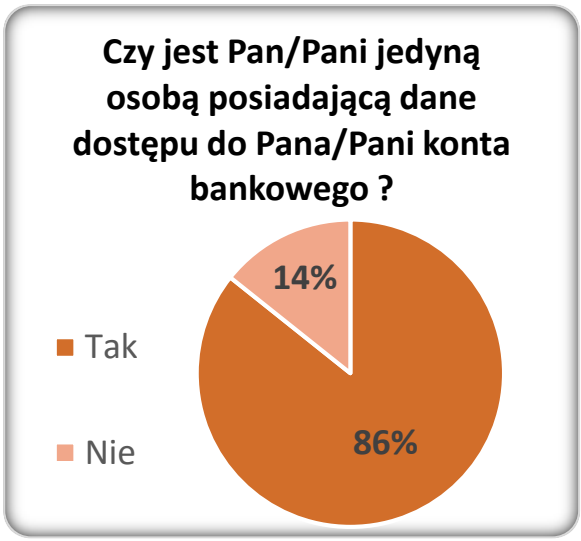



Rysunek 25. Czy otwiera Pan/Pani maile od nieznanych nadawców?
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

25% respondentów (14 osób) otrzymuje rachunki na swoją skrzynkę poczty elektronicznej. Natomiast zadowalająca liczba, 91% odpowiadających (51 osób) nie otwiera maili od nieznanych nadawców. I chociaż jako funkcjonujące w zakresie bankowości elektronicznej wymienia się bankowość internetową, telefoniczną, mobilną (przenośną), terminalową, telewizyjną i dedykowaną bankowość komputerową, to ich egzystencja nie byłaby możliwa bez konta bankowego.



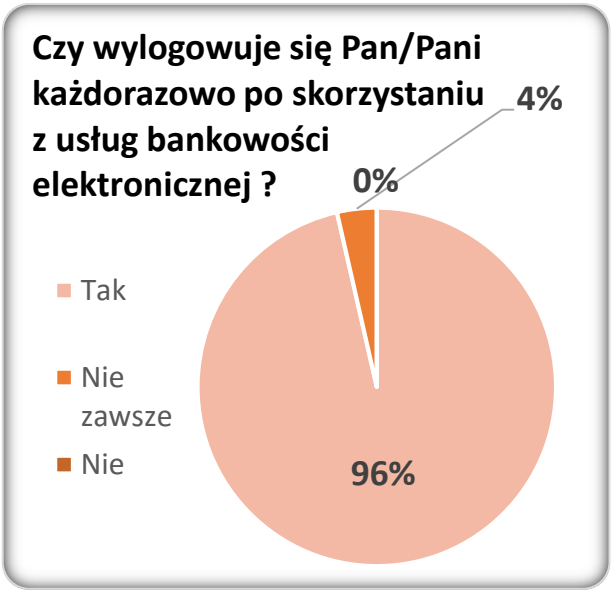

*Rysunek 27. Czy weryfikuje Pan/Pani stan konta bankowego?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*




*Rysunek 26. Czy jest Pan/Pani jedyna osoba posiadającą dane dostępu do Pana/Pani konta bankowego?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Ważne jest przede wszystkim cykliczne sprawdzanie stanu swojego konta i kontrola dokonywanych na nim działań, co praktykowane jest przez 96% ankietowanych (54 osoby). Najczęściej podejmowane czynności to: sprawdzanie salda rachunku, wykonywanie przelewów na rachunki własne i obce, dokonywanie płatności za pomocą karty płatniczej (również w sklepach internetowych bezpośrednio z konta), sprawdzanie historii wykonywanych operacji, wypłacanie i wpłacanie pieniędzy za pośrednictwem bankomatu. Odrobinę mniejszym zainteresowaniem cieszą się: doładowania telefonów, definiowanie przelewów do realizacji w przyszłości, dokonywanie operacji za pośrednictwem telefonu, ustalanie zleceń stałych płatności, zakładanie i likwidowanie lokat czy sprawdzanie ofert i promocji. Zdecydowanie najmniejsze zainteresowanie przypadło składaniu wniosków o kredyty i pożyczki oraz korzystanie z serwisu informacyjnego i doradztwa. Równie ważnym jest, aby nie podawać swoich danych dostępowych do konta, a także być jego jedynym właścicielem. Aż 14% ankietowanych (8 osób) to osoby nie będące jedynymi właścicielami konta, a zatem, bezpieczeństwo ich pieniędzy może być zagrożone, ponieważ o ile oni sami mogą przestrzegać

wszystkich znanych sobie zasad ochrony, nie ma już tej pewności co do poczynań współwłaściciela konta.



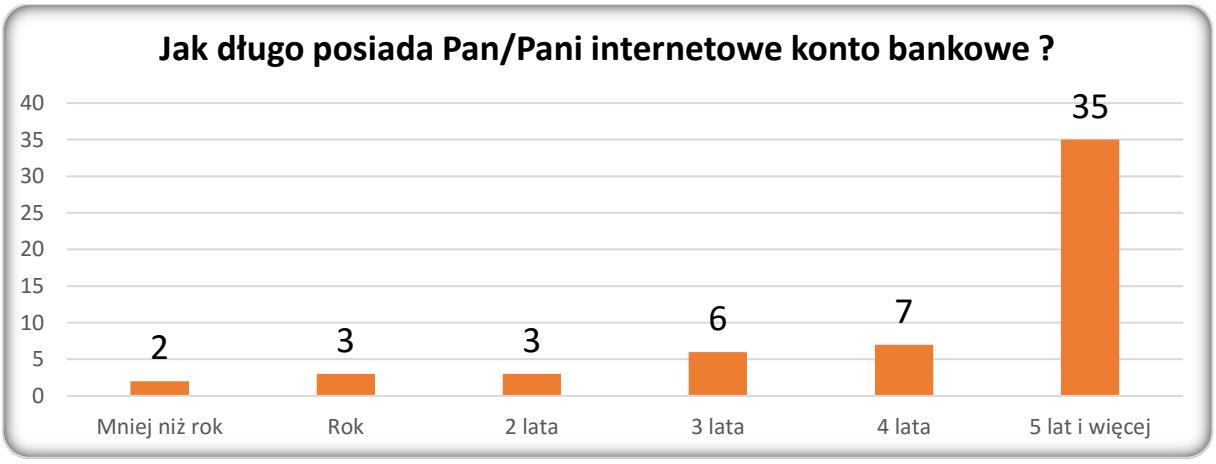

*Rysunek 28. Czy wylogowuje się Pan/Pani każdorazowo po skorzystaniu z usług bankowości elektronicznej? Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*


*Rysunek 29.Czy zawsze używa Pan/Pani znanych sobie, zaufanych urządzeń do korzystania z bankowości elektronicznej? Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Obiecującym jest fakt, iż 96% ankietowanych pamięta o każdorazowym wylogowaniu się ze stron bankowości elektronicznej. 95% respondentów (53 osoby) zwracają uwagę na istotną kwestię jaką jest korzystanie z dobrze znanych, zaufanych urządzeń, podczas łączenia się do swojego rachunku bankowego. Niezbędny jest także program antywirusowy, którego posiadanie deklaruje pozytywna liczba 86% respondentów (48 osób) i każdy z nich pamięta o dokonywaniu bieżących aktualizacji oprogramowania ochronnego.

Idąc z duchem czasu, postępem nauki i rosnącymi potrzebami, jak również wymaganiami, bankowość znacznie rozwinęła się, dzięki czemu każdy posiadacz konta bankowego może posługiwać się powszechnie udostępnianymi kanałami dystrybucji bankowości. Na potrzeby przeprowadzenia analizy, ankietowani zostali poproszeni o podzielenie się swoimi poglądami i przyzwyczajeniami zaledwie w zakresie trzech najpopularniejszych i najbardziej dostępnych w codziennym życiu kanałów dystrybucji, stanowiących główne komponenty bankowości elektronicznej i jest to bankowość: internetowa, mobilna i terminalowa. Bankowość internetowa bardzo często mylona jest z bankowością elektroniczną, choć nie jest to pojęcie tożsame. Bankowość internetowa to jedna z wielu

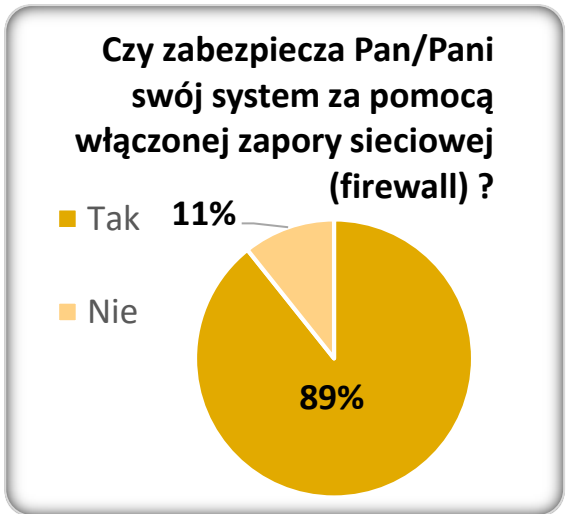
możliwości udostępnienia funkcjonalności bankowości elektronicznej. Jest to najstarsze narzędzie bankowej pracy zdalnej, którego działanie w pełni oparte jest o przeglądarkę stron www.




*Rysunek 30. Jak długo posiada Pan/Pani internetowe konto bankowe?*
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

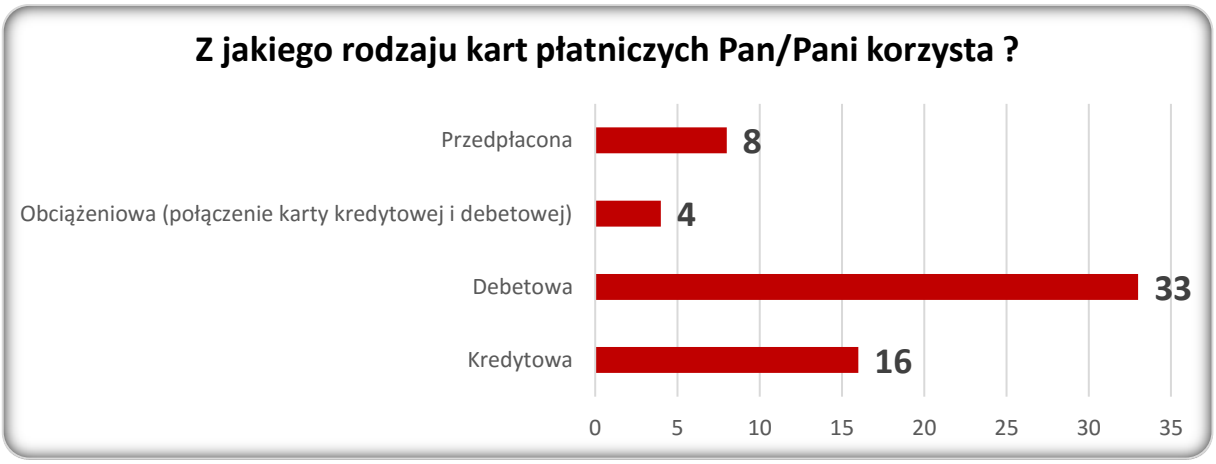
Wszyscy ankietowani korzystają z tego rodzaju bankowości i zdecydowana większość z nich, bo aż 63% (35 osób) posiada takie konto od ponad 5 lat. Zaledwie 9% (5 osób) posiada je od roku lub poniżej roku. Jak prezentują zebrane wyniki, jest to z pełną stanowczością najpopularniejsza forma bankowości elektronicznej.

Minimalne zabezpieczenie jakie można zastosować to włączona zapora sieciowa (tzw. Firewall), którą posiada 89% respondentów (50 osób). Drugim co do poziomu popularności kanałem dystrybucji jest bankowość terminalowa, której obsługa możliwa jest wyłącznie za pomocą bankomatów, kiosków samoobsługowych lub terminali POS *(ang. Point of sale).* Wśród ankietowanych 89% (50 osób) korzysta z takiej formy. Pozostała część licząca 6 osób i stanowiąca 11% respondentów nie korzysta z tego kanału dystrybucji ze względu na brak okazji, brak potrzeby skorzystania, przywiązanie do płatności gotówką lub przelewem. Znalazła się również osoba, która nie wie czym jest bankowość terminalowa, co w obecnych czasach wydaje się być dość mocno zaskakujące. Wśród tych osób, większość




*Rysunek 31. Czy zabezpiecza Pan/Pani swój system za pomocą włączonej zapory sieciowej (firewall)?*
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

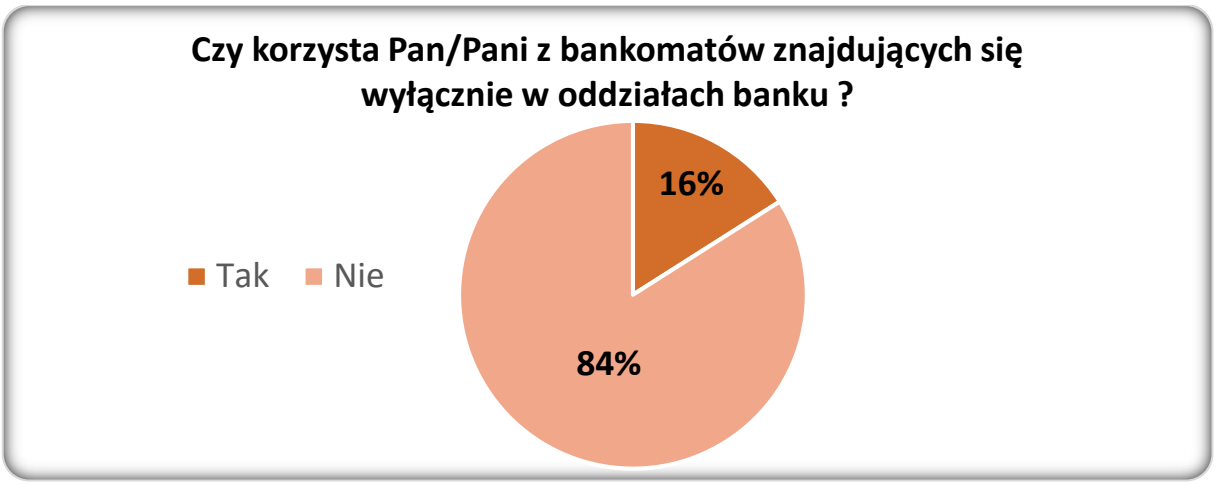
nie zamierza korzystać z tego kanału dystrybucji w przyszłości. Obsługa początkowo wymienionych narzędzi nie byłaby możliwa bez posiadania niezbędnej do tego karty płatniczej.




*Rysunek 32. Z jakiego rodzaju kart płatniczych Pan/Pani korzysta?*
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Ponad połowa odpowiadających posługuje się kartą debetową (54%), 26% respondentów to użytkownicy kart kredytowych, pozostali korzystają z możliwości kart obciążeniowych, będących połączeniem karty kredytowej i debetowej oraz kart przedpłaconych. Każda z tych kart dzięki indywidualnym cechom i funkcjonalnościom, posiada swój odrębny charakter płatniczy, dlatego też każda z nich powinna być chroniona z uwzględnieniem ich jednostkowych zagrożeń. Najczęstszym sposobem płatności jaki wybierają respondenci jest płatność zbliżeniowa (do 50zł) i ciesząca się niewiele mniejszym zainteresowaniem płatność z potwierdzeniem kodem PIN. Ważne jest również, aby korzystanie z bankomatów odbywało się w granicach rozsądku i z zachowaniem wszelkich możliwych zasad bezpieczeństwa, gdyż jest to narzędzie niezwykle narażone na ataki.


*Rysunek 33. Jaki jest najczęstszy sposób dokonywania przez Pana/Panią płatności kartą?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*




*Rysunek 34. Czy korzysta Pan/Pani z bankomatów znajdujących się wyłącznie w oddziałach banku?*
*Źródło: Opracowanie własne na podstawie ankiety pt.:*
*„Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Za najbezpieczniejsze uznaje się bankomaty znajdujące się w oddziałach banku, niestety przeważająca większość, bo aż 84% ankietowanych korzysta z bankomatów zlokalizowanych poza oddziałami banków.

Co zatem w sytuacji często zdarzających się kradzieży bądź zgubienia karty płatniczej? Większość respondentów deklaruje podjęcie natychmiastowych działań pod postacią zgłoszenia sprawy do banku za pomocą bankowości internetowej, osobistej wizyty w oddziale bądź połączenia przez infolinię, zablokowanie karty, a następnie zgłoszenie sprawy na policję. Często też pojawiały się odpowiedzi, zgodnie z którymi ofiary kradzieży karty, w pierwszej kolejności dzwoniłyby na policję, a dopiero w drugiej – powiadamiały bank. Prawidłowo należałoby najpierw zablokować złodziejowi dostęp do pieniędzy, tym samym umożliwiając sobie uratowanie własnych pieniędzy, a dopiero następnie zgłosić sprawę dotyczącą zaginionej karty, którą zawsze można wyrobić na nowo w późniejszym czasie.

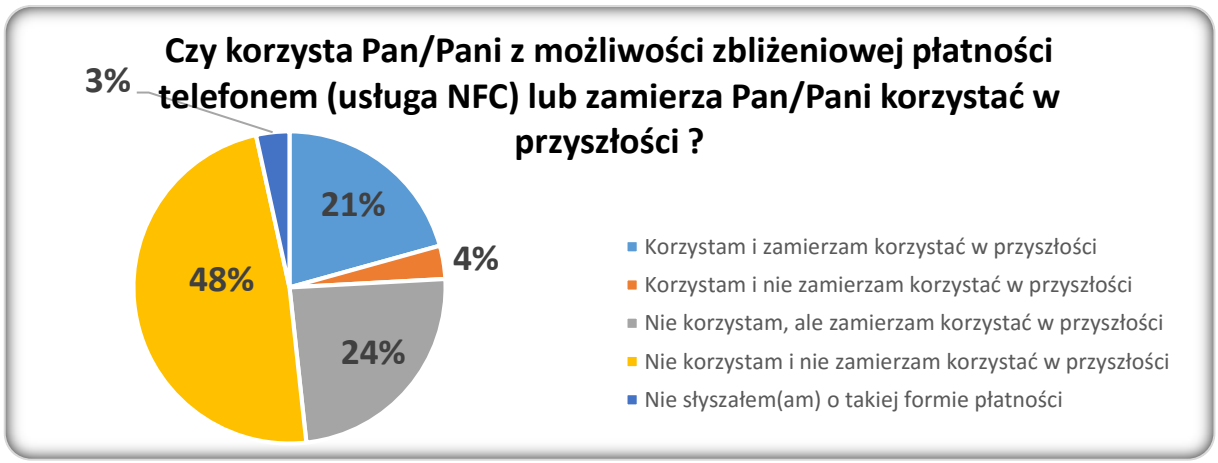
Ostatnim z najpopularniejszych kanałów dystrybucji, który jest jednym z najmłodszych i dzięki ciągłemu rozwojowi wciąż zyskuje nowych zwolenników jest bankowość mobilna, będąca niegłosową komunikacją, wykorzystującą technologię WAP, SMS i aplikacje klienckie. Wśród ankietowanych 52% (29 osób) Klientów to zwolennicy takiej formy bankowości. Pozostała, niemała grupa 48% (27 osób) obawia się przede wszystkim zgubienia bądź kradzieży telefonu oraz niewystarczających zabezpieczeń stosowanych w bankowości mobilnej. Dodatkowo osoby te nie czują takiej potrzeby, gdyż są usatysfakcjonowane funkcjonalnością bankowości internetowej, przejawiają brak zaufania, nie posiadają odpowiedniego sprzętu bądź

bank nie udostępnia im takiej możliwości. Zdecydowana większość przeciwników bankowości mobilnej nie zamierza skorzystać z jej usług w przyszłości.


*Rysunek 35. Na jakim urządzeniu najczęściej korzysta Pan/Pani z usług bankowości mobilnej?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*


*Rysunek 36. W jaki sposób korzysta Pan/Pani z usług bankowości na urządzeniach mobilnych?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Najczęściej wykorzystywanym urządzeniem są poręczne i ogólnodostępne smartfony (93% ankietowanych). Dostęp u 66% respondentów (19 osób) dokonuje się przez aplikację udostępnioną przez bank, natomiast 34% (10 osób) wykorzystuje w tym celu stronę internetową. Wśród bardziej interesujących nowoczesnych udogodnień wprowadzono płatność zbliżeniową telefonem, jest to tzw. Usługa NFC.



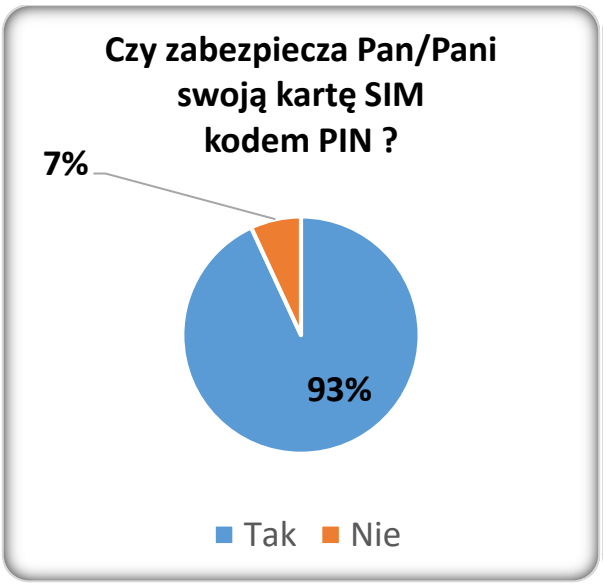

*Rysunek 37. Czy korzysta Pan/Pani z możliwości zbliżeniowej płatności telefonem (usługa NFC) lub zamierza Pan/Pani korzystać w przyszłości?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Większość w wymiarze 48% ankietowanych (14 osób) nie korzysta i nie zamierza korzystać z tej funkcjonalności w przyszłości. 24% respondentów (7 osób) nie korzysta, ale zamierza zacząć korzystać w przyszłości. Natomiast na chwilę obecną, rzeczywistych użytkowników, którzy przekonali się do tej usługi i planują kontynuować jej użytkowanie także w przyszłości jest 21 % (6 osób). Jest to bardzo ryzykowna pod względem bezpieczeństwa możliwość. Równie niebezpiecznymi mogą okazać się wszelkiego rodzaju widgety, dzięki którym, w łatwy sposób, osoby nieuprawnione mogą wejść w posiadanie ważnych informacji.

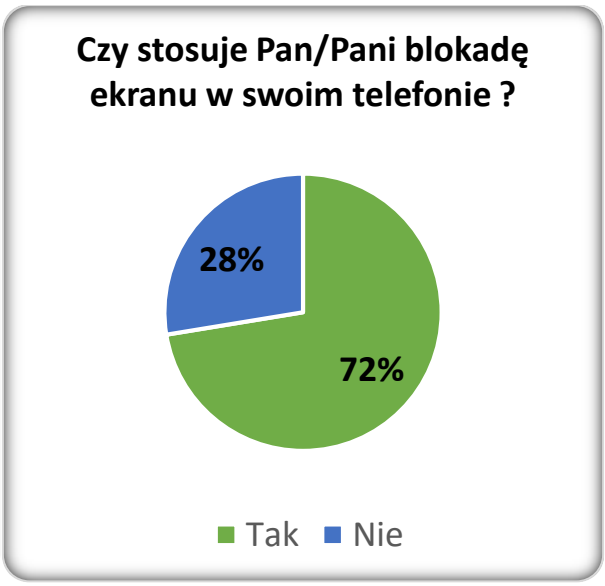

*Rysunek 38. Czy korzysta Pan/Pani z widgetu wyświetlania dostępnych środków na koncie, bez konieczności logowania się do systemu transakcyjnego? Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*


*Rysunek 39. Czy korzysta Pan/Pani z widgetu "szybkiego doładowania telefonów"? Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Jedna z takich aplikacji daje możliwość wyświetlania na ekranie telefonu środków dostępnych na koncie, bez konieczności każdorazowego logowania się do systemu transakcyjnego. Zdecydowana większość (93% ankietowanych) nie korzysta z tej aplikacji. Podobnym typem aplikacji jest widget „szybkiego doładowania telefonu", z którego niemal wszyscy (97%) respondenci nie korzystają. Posiadanie różnego rodzaju oprogramowania, a w tym przypadku aplikacji bankowych na swoich telefonach również może być pewnego rodzaju zagrożeniem, w momencie oddawania telefonu do naprawy. Nigdy nie wiadomo w czyje i jak uczciwe ręce mogą trafić. 83% ankietowanych (24 osoby) to szczęśliwi posiadacze telefonów, których oddanie do serwisu nie było nigdy konieczne. Wśród pozostałej grupy, większość pamięta o odinstalowaniu aplikacji bankowych. W przypadku bankowości mobilnej na smartfonach, podstawową formą zabezpieczenia jest kod PIN chroniący kartę SIM.

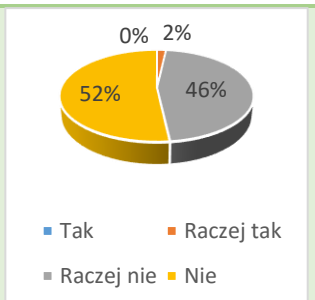
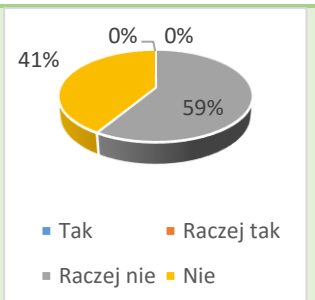
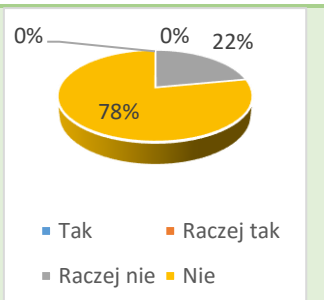



*Rysunek 40. czy zabezpiecza Pan/Pani swoją kartę SIM kodem PIN?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*




*Rysunek 41. czy stosuje Pan/Pani blokadę w swoim telefonie?*
*Źródło: Opracowanie własne na podstawie ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością".*

Wydawałoby się, że jest to niezbędne minimum ochrony, a ze względu na domyślnie ustawianie tego kodu, wszyscy będą z niego korzystali. Okazuje się jednak, że 7% ankietowanych (2 osoby) nie posiada takiej blokady. Również przydatna i niewymagająca jest blokada ekranu, która znacząco utrudnia dostanie się do zawartych w telefonie informacji. Można ją spotkać zaledwie u 72% ankietowanych (21 osób). Na podstawie zadanych pytań, została stworzona tabela porównawcza trzech wybranych rodzajów bankowości.

| | **Bankowość internetowa** | **Bankowość mobilna** | **Bankowość terminalowa** |
|---|---|---|---|
| **Czy korzystanie z usług bankowości jest skomplikowane?** |   |   |   |
| **Zalety** | • Łatwość i dostępność operacji<br>• Wygoda<br>• Płatność za zakupy internetowe<br>• Oszczędność czasu i pieniędzy<br>• Szybkość<br>• Unikanie kolejek<br>• Brak konieczności szukania oddziału | • Dostępność większa niż przy bankowości internetowej<br>• Oszczędność czasu i pieniędzy<br>• Brak kolejek<br>• Nie potrzeba komputera<br>• Łatwość obsługi | • Wygoda<br>• Wypłacenie pieniędzy o każdej porze<br>• Prostota obsługi<br>• Nie trzeba posiadać gotówki, wystarczy karta<br>• Szybkość płacenia<br>• Oszczędność czasu i pieniędzy |

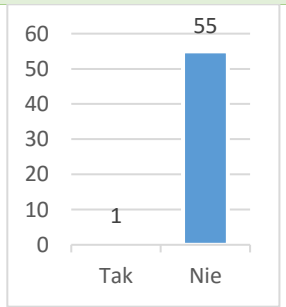
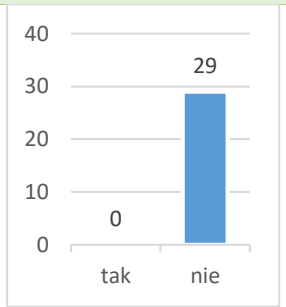
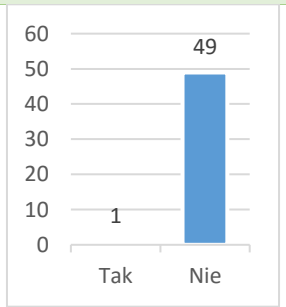
| | | | |
|---|---|---|---|
| | • Bezpośredni dostęp<br>• Finanse na bieżąco<br>• Dostęp o każdej porze | • Korzystanie w dowolnym miejscu i czasie | • Łatwy sposób blokady karty<br>• Nie trzeba szukać bankomatu/oddziału aby mieć dostęp do pieniędzy |
| **Wady** | • Włamania i kradzież pieniędzy<br>• Główne przeznaczenie dla osób 18-60 (problem z obsługą dla osób starszych)<br>• Niezbędny dostęp do Internetu<br>• Niektóre dyspozycje wymagają obsługi w oddziale<br>• Brak możliwości poprawy błędu w razie pomyłki<br>• Wirusy na urządzeniach<br>• Możliwość utraty danych<br>• Awaria systemu | • Wciąż słabe zabezpieczenia<br>• Niedostępna dla starszych ludzi<br>• Kradzież telefonu<br>• Włamania na konto<br>• Brak możliwości poprawy błędu<br>• Złośliwe oprogramowanie<br>• Łatwość włamania przy ustawionym automatycznym logowaniu | • Plastikowy pieniądz<br>• Podejrzenie PINu<br>• Kradzież karty<br>• Nie każdy sklep obsługuje terminal płatniczy<br>• Przypadkowe zniszczenie karty<br>• Brak kontroli nad wydatkami<br>• Nakładki w bankomatach<br>• Zeskanowanie karty<br>• Kradzież środków na koncie<br>• Brak możliwości szybkiego zwrotu karty po wciągnięciu przez bankomat<br>• Awarie terminali<br>• Dodatkowe opłaty za korzystanie z bankomatów innych banków<br>• Płatności zbliżeniowe<br>• Sprzedawca może np. 2 krotnie naliczyć opłaty |
| **Liczba ofiar korzystających z bankowości** |  |  |  |

Tabela 4. Porównanie bankowości internetowej, mobilnej i terminalowej.
*Źródło: Opracowanie własne na podstawie przeprowadzonej ankiety pt.: „Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością”.*

Zaprezentowana tabela pozwala zauważyć bardzo dużo wspólnych elementów wszystkich trzech rodzajów bankowości elektronicznej. Zdaniem ankietowanych, obsługa nie należy do zbyt skomplikowanych, jedynie w przypadku bankowości internetowej znalazło się 2% respondentów, uważających jej obsługę za raczej skomplikowaną. Biorąc pod uwagę

przedstawione wyniki zbiorcze, jest to zdecydowanie nikła liczba. Zalety i wady każdej z tych bankowości bardzo często się powtarzają, zdarza się także, że część z nich się wręcz uzupełnia.

Przeważającymi cechami występującymi we wszystkich trzech typach są: łatwość obsługi, wygoda, szybkość przeprowadzonych transakcji oraz niższe opłaty dodatkowe. Również część wad jest taka sama dla każdej z tych bankowości i wymienia się wśród nich: strach przed niepożądanym dostępem osób trzecich do konta i kradzieżą pieniędzy, złośliwe oprogramowania, brak możliwości poprawy błędu czy awarie systemu bądź urządzeń. Mimo wielu podobieństw, wynikających z faktu, że każda z tych bankowości jest podrzędnym elementem bankowości elektronicznej, są również cechy wyszczególnione przez respondentów, które jednoznacznie charakteryzują każdą z nich.

Bankowość internetowa pozwala na uniknięcie kolejek, bieżącą kontrolę finansów oraz dokonywanie transakcji w zaciszu swojego mieszkania bez konieczności poszukiwania oddziałów banku. Bankowość mobilna pozwala na realizację transakcji w dowolnym miejscu i czasie bez konieczności użycia komputera, lecz bardziej poręcznego smartfonu lub tabletu. Bankowość terminalowa z kolei, pozwala ograniczyć posiadanie gotówki przy sobie, za pomocą karty możliwa jest bezgotówkowa płatność w sklepach, a także wpłacanie i wypłacanie niezbędnej gotówki w dowolnej porze, korzystając na przykład z bankomatu.

Wśród ankietowanych znalazły się również ofiary tych nowoczesnych udogodnień. W jednej z takich sytuacji bankomat nie wypłacił wszystkich należytych pieniędzy klientowi. Natomiast w drugiej dokonano kradzieży karty, którą następnie dokonano zbliżeniowej płatności. Wbrew pozorom są to jedne z częstszych zdarzeń, na które trzeba uważać. Zdecydowana większość ankietowanych obawia się przede wszystkim kradzieży środków z rachunku bankowego, fałszywych zleceń płatniczych oraz wirusów rozsyłanych drogą elektroniczną. W dużo mniejszym stopniu, ale w dalszym ciągu, użytkownikom towarzyszy strach przed kradzieżą haseł lub kodów jednorazowych oraz wydobyciem danych osobowych. Jest to oczywiście w pełni uzasadniony lęk i mało kto w kwestii ochrony swojego majątku nie boi się niczego.

## 3.5. Podsumowanie

Przeprowadzone badanie zostało podzielone na kilka modułów, dzięki którym możliwe było zebranie informacji z zakresu bankowości tradycyjnej, bankowości elektronicznej wraz z jej wybranymi elementami, uzupełnione o codzienne przyzwyczajenia użytkowników.

Analiza zgromadzonych wyników pozwoliła stworzyć profil przeciętnego klienta bankowości, który bazuje na wiedzy i zachowaniu użytkowników. Zdecydowana większość ankietowanych uważa bankowość tradycyjną za bezpieczniejszą od bankowości elektronicznej, lecz biorąc pod uwagę mnogość dostępnych funkcji i operacji możliwych do przeprowadzenia we własnym zakresie, prostotę obsługi oraz łatwość dostępu, przy jednoczesnym zadowoleniu z używanych innowacyjnych usług, pomimo mniejszego zaufania w kontekście bezpieczeństwa, ankietowani częściej wybierają korzystanie z bankowości elektronicznej. Taka sytuacja podkreśla fakt, iż własny komfort wraz z oszczędnością czasu i pieniędzy stawiany jest ponad bezpieczeństwem. Widać to również na przykładzie kryteriów wyboru banku, gdzie zdecydowana większość respondentów zwraca uwagę przede wszystkim na ceny usług i produktów bankowych, a dopiero po następnych kilku kryteriach, wymienia się oferowane możliwości ochrony konta.

Z elektronicznej bankowości korzysta się aktualnie w przeróżnych miejscach i przy użyciu rozmaitych urządzeniach, których zabezpieczenia bardzo często pozostawiają wiele do życzenia. Podobnie jest również w kwestii zachowania bezpieczeństwa przez samych użytkowników. Orientują się w ramach podstawowego zakresu zasad bezpieczeństwa, lecz nie zawsze się do nich stosują. Słusznie obawiają się kradzieży środków z rachunku bankowego, fałszywych zleceń płatniczych, wirusów rozsyłanych drogą elektroniczną czy wydobycia danych osobowych. Wszystkie te działania prowadzą do pozbawienia klienta jego własnych pieniędzy, które powierza się bankowi, wierząc w całkowite zachowanie ich bezpieczeństwa.

Warto jednak pamiętać, iż wszędzie tam, gdzie występuje niezwykle istotny czynnik ludzki, techniczne zabezpieczenia bankowe nigdy nie stanowią ochrony absolutnej. Człowiek jest jednostką z natury podatną na wszelkiego rodzaju czynniki negatywne, począwszy od chęci realizacji różnych działań przy możliwie najmniejszym nakładzie własnej energii, zapoczątkowane własnym lenistwem, kończąc na socjotechnicznych metodach stosowanych w celu wyłudzenia niezbędnych danych. Chwilowa nieuwaga wystarczy, by przysporzyć sobie wielu uporczywych problemów.

Podstawową i najmniej wymagającą formą ochrony, jaką klient może zastosować jest silne, regularnie zmieniane hasło, znane tylko jemu oraz program antywirusowy, aktualizowany na bieżąco i stale działający na urządzeniu, z którego dochodzi do zdalnego połączenia z rachunkiem bankowym. Wydawałoby się, że są to najprostsze sposoby, powszechnie stosowane, dzięki którym każdy przeciętny użytkownik może zachować przynajmniej minimalny poziom ochrony ze swojej strony. Niestety rzeczywistość rysuje się odrobinę inaczej. Ponad to, że szary Kowalski nie przywiązuje większej wagi do swoich danych dostępowych i oprogramowania chroniącego, to wciąż w świecie wirtualnego pieniądza funkcjonują osoby otwierające maile od nieznanych nadawców, udostępniające swoje dane dostępu, zapominające o wylogowaniu się po skorzystaniu z usług bankowości elektronicznej. Co więcej, są również osoby, które nie blokują swoich kart SIM żadnym kodem, a ponadto nie stosują blokady ekranu w swoich telefonach, przy jednoczesnym korzystaniu z usług bankowości mobilnej. Są to mocno niepokojące wyniki, tym bardziej, że zdecydowana większość ankietowanych nie ma pełnego zaufania do środków bezpieczeństwa stosowanych przez bank, więc osobiste starania użytkownika, aby dopełnić te zabezpieczenia i zachować należytą ochronę rachunku bankowego są niezbędne.

Rezultat przeprowadzonego badania wskazuje na dość dobrą świadomość i orientację w tematyce zagrożeń występujących w bankowości elektronicznej, lecz zwraca również uwagę na brak wyobraźni użytkowników w kontekście efektu ich zachowania w sieci, zaniżone poczucie wartości indywidualnych danych osobowych i wciąż niską wiedzę w zakresie minimalizowania ryzyka utraty własnych środków.

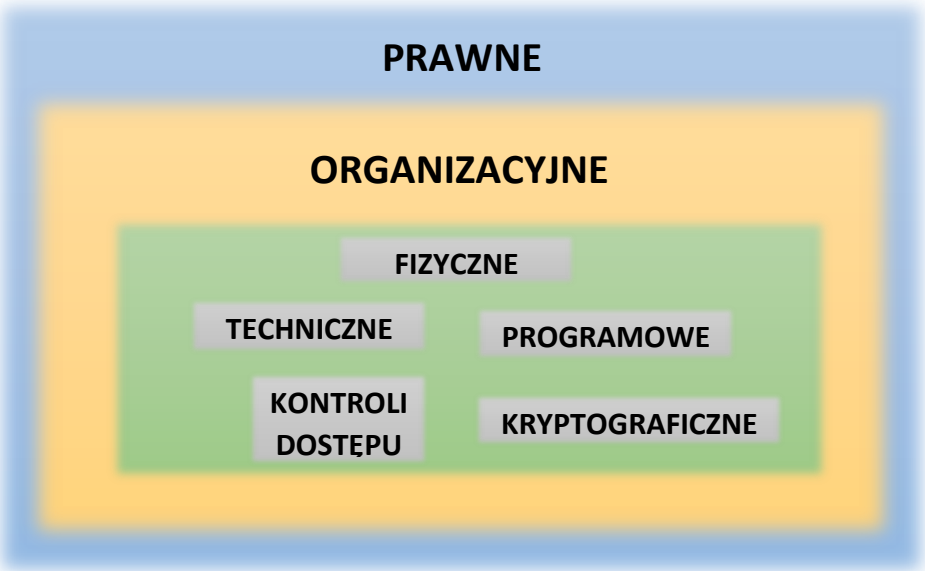
# Rozdział IV
# Zapobieganie naruszeniom bezpieczeństwa w bankowości elektronicznej

Bezpieczeństwem bankowego systemu informatycznego określa się poziom zabezpieczeń, który gwarantuje bezbłędną realizację usług z zachowaniem ich adekwatności do zaistniałych sytuacji, gwarantuje ustalone prawa kontrahentów, a ponad to, jest akceptowalny przez klientów i instytucję bankową[201]. Współczesne systemy informatyczne zabezpieczane są na kilku poziomach, do których należą[202]:

- *Komputer osobisty (terminal, klient) i jego system operacyjny* – stosowane przede wszystkim różne metody identyfikacji i uwierzytelnienia, wśród których znajdują się hasła dostępu oraz określenie konkretnych zadań dla poszczególnych komputerów w sieci bankowej.
- *Sieciowy system operacyjny* – jest kluczowym elementem funkcjonowania oraz zabezpieczenia, najważniejsze mechanizmy ochrony to: hasła i prawa dostępu, grupy użytkowników, programy śledzące, ślady audytowe, usługi bezpiecznej transmisji. Na tym poziomie, stosowane są także mechanizmy sprzętowo-programowe jak np. zapory ogniowe oraz implementacje metod kryptograficznych.
- *System zarządzania bazą danych* – zabezpieczenia w tym zakresie powinny regulować zakres praw dostępu w obrębie pól bazy danych i zezwalać na dostęp do szczegółowych lub przekrojowych informacji w zależności od potrzeb.
- *Oprogramowanie aplikacyjne* – powinno opierać się o mechanizmy identyfikacji, uwierzytelniania oraz ograniczania praw dostępu względem konkretnych zasobów i funkcjonalności zawartych w systemie.
- *Poziom fizyczny* – to głównie urządzenia, które podtrzymują napięcie oraz zapobiegają zdarzeniom losowym takim jak np.: włamania, powodzie, pożary.
- *Poziom organizacyjny* – są to wszelkie działania, które wyrażają się późniejszą efektywnością zastosowanych środków bezpieczeństwa.

[201] Witold Chmielarz, *Op. Cit.*, s. 174.
[202] Dariusz Wawrzyniak, *Op. Cit.*, s. 46-47.

Wszystkie zagrożenia wymienione we wcześniejszych rozdziałach, podlegają przeciwdziałaniu określonych środków ochrony, wśród których wyróżnia się następujące kategorie: prawne, fizyczne, techniczne, programowe, organizacyjne, kontroli dostępu oraz kryptograficzne[203]. Ich hierarchia widoczna jest na rysunku nr 42.




Rysunek 42. Hierarchia środków ochrony danych
*Źródło: Opracowanie własne na podstawie Dariusz Wawrzyniak, Zarządzanie bezpieczeństwem systemów informatycznych*

**Środki prawne** to kategoria, do której zaliczają się wszelkie unormowania prawne, dotyczące ochrony danych, które przetwarzane są w systemach informatycznych. Najważniejsze unormowania zawarte są w: ustawie o ochronie danych osobowych, prawie bankowym, kodeksie pracy, kodeksie karnym, ustawie o elektronicznych instrumentach płatniczych, ustawie o podpisie elektronicznym czy normalizacji[204].

**Środki fizyczne** to grupa funkcjonująca w otoczeniu systemu informatycznego, nie będąca jego elementem składowym. Środki te, nie wpływają bezpośrednio na dostępność, poufność czy integralność danych, lecz bez nich, optymalna praca systemu informatycznego byłaby niemożliwa. Zalicza się do nich między innymi: urządzenia przeciwwłamaniowe oraz przeciwpożarowe, alarmy, sejfy, pomieszczenia odpowiednio przystosowane do pracy komputerów, architektoniczne rozwiązania oraz urządzenia klimatyczne[205].

[203] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 80.
[204] *Ibidem*, s. 81-83.
[205] Dariusz Wawrzyniak, *Op. Cit.*, s. 47.

**Środki techniczne** to rozwiązania sprzętowe, bezpośrednio związane z informatyką i wpływające na bezpieczeństwo systemu. Wymienia się wśród nich: urządzenia podtrzymujące zasilanie, karty mikroprocesorowe i magnetyczne, urządzenia biometryczne służące do identyfikacji osób na podstawie linii papilarnych, siatkówki oka, głosu, urządzenia wykorzystywane do tworzenia kopii zapasowych, serwery Proxy, sprzętowe blokady dostępu do klawiatur, napędów dysków itp., rozwiązania i urządzenia chroniące przed emisją ujawniającą, optymalizacja konfiguracji sprzętowej komputerów, dublowanie okablowania oraz centrów obliczeniowych i baz danych[206].

**Środki programowe** obejmują wszelkiego rodzaju, dostępne oprogramowania systemowe oraz aplikacyjne wśród których wymienia się: dzienniki systemowe, programy śledzące, mechanizmy rozliczenia, oprogramowania antywirusowe, antyspamowe czy antyszpiegowskie, personalne zapory ogniowe (ang. *personal firewall*), programy wykrywające słabe hasła w systemie, systemy monitorujące, narzędzia wspomagające pracę administratorów, mechanizmy zabezpieczenia statystycznych baz danych, kody korekcyjne oraz wirtualne sieci prywatne[207].

**Środki organizacyjne** skupiają się na kontroli zarządzania i procedurach, którymi są[208]:

- *Analiza ryzyka*, polegająca na określeniu wszelkich przypadków ryzyka, a następnie nadanie mu rangi jego wielkości (w sposób jakościowy lub ilościowy), co sprawdza się w przypadku wykrywania potencjalnych zdarzeń, negatywnie ingerujących w funkcjonalność instytucji.
- *Polityka bezpieczeństwa* obejmująca przede wszystkim: podział funkcji operacyjnych pomiędzy różnymi osobami, odpowiedzialność za rozwój systemu powierzona grupom osób, ograniczając tym samym możliwość posiadania pełnej władzy w systemie przez jedną osobę, prowadzenie dokumentacji zmian systemowych, nadzorowanie modyfikacji oprogramowania, testowanie systemu, analiza ryzyka, szkolenia użytkowników a także monitoring systemu i wykrywanie anomalii.

[206] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 84.
[207] *Ibidem*.
[208] *Ibidem*, s. 85-86.

**Środki kontroli dostępu**[209] opierają się głównie o uwierzytelnienie użytkownika, którym nazywa się proces zapewnienia jednej ze stron, o tożsamości drugiej. Odbywa się za pomocą systemu przez:

- *Identyfikację* (ustalenie: kim użytkownik jest)
- *Uwierzytelnienie* (ustalenie: czy użytkownik jest tym, za kogo się podaje)
- *Autoryzację* (ustalenie: co użytkownik może zrobić w danej chwili)

Nazwa „uwierzytelnienie" używana jest zamiennie z „identyfikacja". Wyróżnia się 3 rodzaje:

- *Słabe* – oparte na hasłach będących ciągiem minimum 6 znaków, niezmiennych w czasie i łatwych do zapamiętania dla użytkownika
- *Silne* – oparte na hasłach jednorazowych, kluczach symetrycznych oraz kluczach publicznych
- *Oparte na metodach o wiedzy zerowej* – wykorzystujące specjalnie zaprojektowane protokoły wykorzystujące liczby losowe.

Uwierzytelnianie użytkowników to najprostsza forma logowania użytkownika do systemu bankowości za pomocą loginu i hasła. Dzięki temu, ma on możliwość przeglądania stanu swojego konta. Dokonywanie jakichkolwiek zmian, bardzo często połączone jest z dodatkowymi zabezpieczeniami rachunku. Wyróżnia się cztery podstawowe metody uwierzytelniania:

- **Weryfikacja wiedzy użytkownika** (ang. *by something you know*) – w oparciu o to, co użytkownik zna
- **Weryfikacja przedmiotu posiadanego przez użytkownika** (ang. *by something you have - SYH*) – w oparciu o to, co użytkownik posiada
- **Weryfikacja cech fizycznych użytkownika** (ang. *by something you are - SYA*) – w oparciu o to, kim lub czym użytkownik jest
- **Weryfikacja czynności wykonywanych przez użytkownika** (ang. *by something you do - SYD*) – w oparciu o to, co użytkownik robi

Środki kontroli dostępów są zagadnieniem o wiele bardziej obszernym, zwracają uwagę na ściśle z nią związaną kontrolę do zasobów, kontrolę dyskrecjonalną, kontrolę obowiązkową czy też kontrolę zależną od zadań, lecz w kontekście poruszanych zagrożeń bankowości

[209] *Ibidem*, s. 86-88.

elektronicznej, powyższe przedstawienie tegoż zagadnienia, wydaje się być w zupełności wystarczające[210].

**Kryptografia** jest nauką o metodach przesyłania wiadomości w zaszyfrowanej postaci, którą przeczytać będzie mógł tylko prawowity odbiorca. Tekst jawny, zwany także tekstem otwartym, przekształca się w tzw. *szyfrogram*, będący zaszyfrowaną wersją oryginalnego tekstu[211]. Natomiast algorytmem bądź szyfrem kryptograficznym nazywa się funkcję matematyczną lub proces z elementami matematycznymi, który ze zwykłego tekstu tworzy ciąg znaków. Nowoczesne algorytmy zapewniają bezpieczeństwo poprzez klucze: algorytmy symetryczne i algorytmy z kluczem jawnym[212]. Funkcjonalność algorytmów symetrycznych opiera się o klucz szyfrujący będący identycznym z kluczem deszyfrującym lub jeden z nich wyznaczony jest z drugiego. Algorytmy z kluczem jawnym są zupełnie odmienna grupą. Klucz szyfrujący (zwany kluczem jawnym) posiada spora liczba nadawców, aby mogli zaszyfrować swoje wiadomości. Z kolei odczytanie wiadomości, możliwe jest tylko w sytuacji użycia klucza deszyfrującego (zwanym kluczem prywatnym), będącego w posiadaniu adresata wiadomości. Oba te klucze różnią się od siebie i nie wynikają jeden z drugiego[213]. Klucz utrzymany w tajemnicy stanowi gwarancję bezpiecznej wymiany danych. Kryptograficzne systemy posiadają różne poziomy zabezpieczenia. Rozważając zagadnienie pod kątem teoretycznym: każdy algorytm można złamać. Praktycznie jednak, nie zawsze jest to możliwe. Jeśli konkretny algorytm możliwy jest do złamania wyłącznie w teorii, wtedy mówi się o nim, że jest bezpieczny[214].

**Systemy biometryczne**[215], ze względu na swoje cechy, są coraz częściej wybieranymi metodami weryfikacji. Wynika to z czynników technologicznych (dokładność i elastyczność), finansowych (koszty namacalne, aktywa nie materialne), organizacyjnych (poparcie kadry zarządczej, dostępność zasobów) oraz prawnych i etnicznych (konieczność dostosowania się do regulacji prawnych i przepisów, kwestie społeczne i psychologiczne). Metody te, badają:

- Cechy fizyczne – tęczówka oka, siatkówka (dno oka), kształt linii zgięcia wnętrza dłoni, kształt dłoni, układ naczyń krwionośnych na dłoni lub przegubie

[210] Dariusz Wawrzyniak, *Op. Cit.*, s. 48-52.
[211] Mirosław Kutyłowski, *Kryptografia: teoria i praktyka zabezpieczenia systemów komputerowych*, Warszawa 1998, s. 3-4.
[212] Dariusz Wawrzyniak, *Op. Cit.*, s. 52.
[213] Andrzej Gospodarowicz, *Op. Cit.*, s. 84.
[214] Dariusz Wawrzyniak, *Op. Cit.*, s. 52-53.
[215] Sylwia Wojciechowska-Filipek, *Op. Cit.*, s. 88-91.

ręki, linie papilarne, twarz, rozkład temperatur na twarzy, kształt ucha, kształt i rozmieszczenie zębów, DNA, zapach itp.

- Cechy behawioralne – wiążące się z zachowaniem, jak np.: sposób chodzenia, sposób pisania na klawiaturze, podpis odręczny, głos.

Są to niezwykłe zabezpieczenia ze względu na fakt, iż każda z tych cech charakteryzuje się:

- Niepowtarzalnym charakterem, specyficznym dla każdego człowieka np.:
  - Ludzka tęczówka posiada około 260 unikatowych cech, które z reguły nie ulegają zmianie w trakcie życia
  - Biometryka rogówki funkcjonuje na podstawie analizy charakterystycznego wzoru naczyń krwionośnych umiejscowionych na dnie oka
  - Układ żył, przez całe życie pozostaje taki sam
- Nie ma możliwości wypożyczenia ani kradzieży którejś z tych cech innej osobie
- Nie ma możliwości zgubienia bądź zapomnienia którejś z tych cech.

Warto również przedstawić proces metod biometrycznych. Zamyka się on w trzech następujących krokach:

- **Pobranie zwane także utrwaleniem** (ang. *capture*) próbek fizycznych od użytkowników i zapisanie ich w formie szablonów
- **Porównanie** (ang. *comparison*) zapisanego szablonu z kolejną, nową próbką użytkownika
- **Dopasowanie** (ang. *matching*), które odbywa się w ramach systemu, decyduje on czy uzyskana próbka zgadza się z szablonem – jeśli tak, zezwala na dostęp użytkownika do systemu.

Systemy biometryczne uważane są za bezpieczne, a także wygodne rozwiązanie, dzięki czemu, zgodnie z badaniami przeprowadzonymi przez firmę Unisys, 66% klientów na świecie wybiera te instytucje finansowe, które z nich korzystają.

Proponując usługi bankowości elektronicznej swoim klientom, bank powinien przestrzegać jednej z podstawowych zasad bankowości, jaką jest obowiązek zapewnienia bezpieczeństwa środków pieniężnych, gromadzonych przez jego klientów na swoich rachunkach bankowych. Jednak, każdy użytkownik bankowości elektronicznej, powinien być świadomym faktu, iż bezpieczeństwo jego finansów w dużej mierze zależy od niego samego.

## 4.1. Ochrona bankowości terminalowej

Obraz bezpieczeństwa w bankowości terminalowej bardzo często zniekształcony jest przez medialne doniesienia. W rzeczywistości jednak, utrata karty płatniczej wiąże się z nieporównywalnie większym prawdopodobieństwem odzyskania pieniędzy niż w przypadku utraty gotówki. Wynika to między innymi z faktu, iż transakcje z użyciem kart podlegają ciągłemu monitorowaniu przez banki[216].

**Bezpieczeństwo kart płatniczych** przede wszystkim zależy od rodzaju urządzenia wykorzystywanego do przeprowadzenia transakcji oraz od budowy samej karty. Związek Banków Polskich opublikował na swojej stronie 27 zasad, którymi każdy posiadacz karty płatniczej powinien kierować się podczas przeprowadzania transakcji. Większość z nich wynika również z przepisów prawa polskiego oraz obowiązków jakie spoczywają na posiadaczu karty płatniczej[217].

1. 828 828 828 – to numer telefonu, pod który dzwoniąc można zastrzec kartę w przypadku jej utraty. Dodatkowo strona *www.zastrzegam.pl* stanowi Informacje o Systemie Zastrzegania Kart wraz z listą banków, które w nim uczestniczą.
2. W czasie transakcji nie należy spuszczać karty z oczu, a po jej dokonaniu należy bezzwłocznie ją odebrać.
3. Nie należy udostępniać numeru karty nikomu, podczas połączenia telefonicznego, nawet w sytuacji, gdy dzwoniąca osoba podaje się za pracownika banku i prosi o weryfikację.
4. Nie należy odpowiadać na maile lub sms'y, których nadawca prosi o udostępnienie informacji o karcie. Również nie należy odpowiadać na wiadomości zachęcające do weryfikacji swoich danych, za pomocą strony internetowej.
5. Nie należy podawać informacji na temat karty na stronach, które nie są bezpieczne.
6. Należy sprawdzać, czy strona, na której podawane są dane, jest szyfrowana (adres strony rozpoczyna się „https://")
7. Wskazanym jest aktywacja i korzystanie z mechanizmów wzmocnionego uwierzytelniania transakcji (np. 3D Secure).
8. Kartę należy podpisać od razu po jej otrzymaniu.
9. Należy całkowicie niszczyć wszelką korespondencję z bankiem, zawierającą różnego rodzaju wnioski, dane czy zestawienia transakcji przed jej wyrzuceniem.

[216] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 18.
[217] Związek Banków Polskich, *Karty bankowe – 27 zasad korzystania z kart bankowych*, [data dostępu: 3 maja 2016], <https://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe>.

10. Nie należy zapisywać kodu PIN na karcie, niewskazane jest także przechowywanie go wraz z kartą.
11. Karty oraz pokwitowania transakcji nie powinny być zostawiane bez nadzoru. Pokwitowania transakcji powinny być niszczone przed wyrzuceniem.
12. Należy bezwzględnie chronić numer karty oraz inne, poufne kody, dzięki którym możliwe jest wykonanie transakcji (jak np.: numer PIN, numer CVV2 lub CVC2)
13. Należy nosić przy sobie wyłącznie karty, których używa się na co dzień.
14. Transakcje kartowe należy traktować z taką samą rozwagą jak wszystkie inne operacje wykonywane na rachunku bankowym. Ważne jest, aby tak samo weryfikować wyciągi otrzymane od banku pod kątem dokonanych transakcji.
15. Należy zasłonić klawiaturę podczas autoryzacji transakcji kodem PIN (np. podczas wypłacania gotówki z bankomatu lub płacąc używając terminalu)
16. Jakiekolwiek rozbieżności powinny zostać natychmiastowo zgłoszone do banku, który wydał kartę, poprzez złożenie pisemnej reklamacji.
17. Nieprawidłowe pokwitowania transakcji należy zniszczyć, natomiast pokwitowania transakcji, które nie doszły do skutku należy zachować, na wypadek konieczności złożenia reklamacji.
18. Przed wyrzuceniem należy zniszczyć wszystkie dokumenty zawierające pełny numer karty.
19. Nie należy podpisywać pokwitowań in blanco. W przypadku transakcji w imprinterze, należy nakreślić linie w czystej części blankietu, aby nie było możliwe dopisanie dodatkowych opłat.
20. Aktualnie bardzo rzadko wykorzystuje się kalkę do transakcji, lecz jeśli została użyta, należy ją zniszczyć.
21. Otrzymując wydruk z terminala z miejscem na wpisanie napiwku (np. w restauracji), należy wpisać kwotę lub przekreślić to miejsce kreską poziomą.
22. Nie należy zapisywać numeru swojej karty w miejscach dostępnych dla niepowołanych osób (np. na pocztówce).
23. Dobrym pomysłem jest noszenie kart poza portfelem, np. w oddzielnej zamykanej przegródce lub etui.
24. Nie należy udostępniać kart osobom niepowołanym.
25. W razie przeprowadzki, należy jak najszybciej poinformować bank, który wydał kartę o zmianie adresu.

26. Nie należy zabierać karty ze sobą w sytuacjach, gdzie bardziej prawdopodobne jest zgubienie karty niż jej użycie np. zakupy w miejscach o wzmożonym zagrożeniu na kradzież kieszonkową.
27. W sytuacjach sprzyjających kradzieży, należy mieć na uwadze posiadanie swoich kart, np. w przedziale pociągu.

W sytuacji utraty karty, należy bezzwłocznie ją zablokować, poprzez skontaktowanie się z bankiem lub organizacją, która ją wydała. Można zadzwonić pod numer 828 828 828, gdzie ofiara zostanie zapytana o bank, w którym posiada kartę, a następnie do niego przekierowana. Można również skontaktować się z centrum autoryzacji kart, które czynne jest przez 24h. Jego numer umieszczany jest na rewersie karty płatniczej, można go także otrzymać wraz z przesyłką, w momencie dostarczenia karty. Dobrą praktyką jest zapisanie tego numeru np. w pamięci telefonu. Warto pamiętać, że zgodnie z polskim prawem, od momentu zgłoszenia utraty karty, to jej wydawca ponosi odpowiedzialność za przeprowadzone transakcje. Dodatkowo, ustawa o usługach płatniczych określa maksymalną odpowiedzialność właściciela karty, za transakcje przeprowadzone przed zgłoszeniem jej utraty, do 150 €, a w przypadku transakcji zbliżeniowych jest to równowartość 50 €[218].

**Bezpieczeństwo podczas korzystania z bankomatu** oparte jest głównie o proces autoryzacji, czyli tryb komunikacji bankomatu z główną bazą danych banku. Warto jednak mieć na uwadze[219]:

- Elementy wyposażenia bankomatu, które mogą być używane przez oszustów, jak np.:
  - Pogrubiona klawiatura lub nakładka na klawiaturę
  - Dodatkowy daszek nad okienkiem bankomatu
  - Nakładka na okienko do wsuwania karty płatniczej
- Zaleca się korzystanie z tych samych bankomatów, ponieważ kwestia przyzwyczajenia sprzyja łatwiejszemu zauważeniu jakiekolwiek różnic w jego wyglądzie, a w przypadku dostrzeżonych niezgodności należy natychmiastowo poinformować o tym fakcie właściciela bankomatu lub bank

[218] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 97-101.
[219] Credit Agricole, Korzystanie z bankomatu, [data dostępu: 3 maja 2016], <http://www.credit-agricole.pl/bezpieczenstwo/korzystanie-z-bankomatu>.

- Należy upewnić się, że podczas korzystania z bankomatu, nikt nie obserwuje przeprowadzanych transakcji. Zaleca się dodatkowe przysłanianie klawiatury dłonią, podczas wprowadzania kodu PIN
- Zaleca się także regularne sprawdzanie swoich wyciągów bankowych i wszelkich przeprowadzanych transakcji na rachunku bankowym.

Jakiekolwiek wątpliwości powinny być zgłaszane w banku lub u wydawcy karty.

## 4.2. Ochrona bankowości internetowej

„Podstawą funkcjonowania bankowości internetowej jest niezaprzeczalność transakcji, która jest autoryzowana kodem znanym jedynie posiadaczowi rachunku bankowego”[220]. Co oznacza, że identyfikacja klienta odbywa się wyłącznie na podstawie danych, wprowadzonych przez niego do systemu bankowości internetowej. W związku z tym, na bezpieczeństwo transakcji internetowych największy wpływ ma poufność haseł dostępu wraz z bezpieczeństwem narzędzi, które służą do ich generowania. Głównymi metodami zapewniającymi bezpieczeństwo transakcji internetowych są[221]:

- *Szyfrowana transmisja danych* – realizowana z wykorzystaniem protokołu SSL
- *Proste uwierzytelnianie* - identyfikator, hasło, PIN
- *Silne uwierzytelnianie* - token, certyfikat użytkownika, klucz prywatny
- *Kwalifikowany podpis elektroniczny*

Protokół SSL (ang. *Secure Socket Layer*) jest podstawą zabezpieczeń współczesnej bankowości internetowej i służy do bezpiecznej transmisji zaszyfrowanych danych. Wykorzystuje się go do ochrony transmisji, która realizowana jest protokołem *http*. Korzysta z metody tzw. klucza publicznego oraz szyfrowania symetrycznego. Jako jego główne funkcje wymienia się[222]:

- **Uwierzytelnienie** – weryfikacja tożsamości klienta i banku
- **Poufność** – szyfrowanie przesyłanych informacji, czytelnych jedynie dla komunikujących się stron
- **Integralność** – zabezpieczenie przed modyfikacją treści przesyłanego komunikatu

[220] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 29.
[221] *Ibidem*.
[222] *Ibidem*, s.30.

Skuteczność i dostępność standardu SSL przyczyniła się do aktualnej jego obsługi przez wszystkie przeglądarki internetowe oraz zdecydowaną większość systemów bankowości internetowej. Pojawienie się zamkniętej kłódki wraz z literką „s" przy adresie internetowej strony, sygnalizuje nawiązanie bezpiecznego połączenia (SSL). Kliknięcie symbolu zamkniętej kłódki umożliwia zidentyfikowanie banku, z którym zostało nawiązane połączenie. Również klient otrzymuje swój indywidualny identyfikator użytkownika, który jest niezbędnym elementem następujących metod uwierzytelnienia[223]:

- Hasło stałe
- Hasło jednorazowe
    - lista haseł jednorazowych,
    - karta TAN (ang. Transaction Authorisation Number),
    - token sprzętowy,
    - token w postaci aplikacji w telefonie,
    - wiadomość SMS
- Certyfikaty skojarzone z numerami PIN lub hasłem

Metody te stosowane są w zależności od wykonywanej operacji i systemu bankowości internetowej. Na przestrzeni ostatnich 15 lat i zebranych doświadczeń, zabezpieczenia systemów w Polsce są coraz lepsze. W związku z tym, głównym celem ataków jest człowiek, będący najsłabszym ogniwem systemu zabezpieczeń bankowości internetowej. Powinien więc, kierować się w swoich działaniach głównie rozsądkiem i mieć na uwadze ciągłą ochronę poufności swoich danych autoryzacyjnych[224]. Związek Banków Polskich prezentuje informacje i zasady postępowania, o których warto pamiętać podczas korzystania z bankowości internetowej.

Zasady ogólne[225]:

1. Pamiętaj, żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.
2. Sprawdź na stronie Twojego Banku jakie zabezpieczenia stosowane są w serwisie internetowym.

[223] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 191.
[224] *Ibidem*, s. 191-192.
[225] Związek Banków Polskich, *Bankowość internetowa. Zasady ogólne*, [data dostępu: 3 maja 2016], <https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=1>.

3. Komputer lub telefon komórkowy podłączony do Internetu musi posiadać zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany.
4. Dokonuj płatności internetowych tylko z wykorzystaniem zaufanych komputerów.
5. Skontaktuj się ze swoim dostawcą Internetu w celu upewnienia się, ze korzysta on z bezpiecznych kanałów dystrybucji tej usługi.
6. Instaluj na swoim komputerze tylko legalne oprogramowanie.
7. Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę banku i wykonaniem jakiejkolwiek transakcji.
8. Aktualizuj system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe.
9. Nie otwieraj wiadomości i dołączonych do nich załączników nieznanego pochodzenia.
10. Unikaj stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje.

Zasady dotyczące płatności z internetowego konta bankowego[226]:

11. Po zalogowaniu do systemu transakcyjnego nie odchodź od komputera, a po zakończeniu pracy wyloguj się i zamknij przeglądarkę.
12. Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodanie pola z pytaniem o hasła do autoryzacji, natychmiast zgłoś problem do swojego banku.
13. Nie wchodź na stronę internetową Twojego banku za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach (Phishing).
14. Nigdy nie używaj wyszukiwarek internetowych do znalezienia strony z logowania Twojego banku.
15. Przed zalogowaniem sprawdź, czy połączenie z bankiem jest bezpieczne.
16. Sprawdzaj prawidłowość certyfikatu.
17. Nigdy nie udostępniaj osobom trzecim identyfikatora ani hasła dostępu.
18. Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie.
19. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.
20. Korzystaj z infolinii udostępnionej przez Twój bank.
21. Odwiedzaj regularnie Portal „Bezpieczny Bank" na stronie internetowej ZBP (*www.zbp.pl*)

[226] Związek Banków Polskich, *Bankowość internetowa. Zasady dotyczące płatności z internetowego konta bankowego*, [data dostępu: 3 maja 2016], <https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=3>.

Zasady dotyczące płatności kartami płatniczymi przez Internet[227]:

22. Zachowaj rozwagę przy przekazywaniu numeru karty
23. Nigdy nie odpowiadaj na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie – zgłoś taką sprawę w swoim banku.
24. Nigdy nie podawaj informacji o karcie na stronach, które nie są bezpieczne.
25. Nie zapisuj kodu PIN na karcie, ani nie przechowuj go razem z kartą.
26. Chroń swój numer karty i inne poufne kody umożliwiające dokonanie transakcji np. numer PIN, numer CVV2 lub CVC2
27. Dokonuj transakcji w znanych i zweryfikowanych przez siebie sklepach internetowych. W przypadku mniejszych serwisów zbadaj ich wiarygodność, na przykład dzwoniąc do takiego serwisu i weryfikując jego ofertę, warunki dokonania transakcji oraz reklamacji.

Biorąc pod uwagę wszystkie powyższe zasady, niezwykle ważnym jest należyte dbanie o dane wrażliwe, którymi są: dane osobowe, numery kart płatniczych, hasła czy dokumenty elektroniczne zawierające bankowe dane. Są one głównym przedmiotem zainteresowania w cyberprzestępczości.

## 4.3. Ochrona bankowości telefonicznej

Zachowanie bezpieczeństwa w bankowości telefonicznej sprowadza się do korzystania wyłącznie z oficjalnych numerów telefonów, dostępnych w oficjalnych materiałach reklamowych, na oficjalnych stronach internetowych banków, oficjalnych wizytówkach lub wyciągach bankowych przesłanych na adres klienta (w przypadku bankowości telefonicznej) oraz spełnieniu minimalnych wymagań względem zabezpieczenia wykorzystywanego telefonu i praktyki jego użytkowania (w przypadku bankowości mobilnej)[228]. Najczęstsze zagrożenia wynikają z podszywania się oszustów pod przedstawicieli konkretnych banków, powiązanych z danym klientem. Również i w tej dziedzinie, Związek Banków Polskich opublikował podstawowe zasady bezpiecznych kontaktów telefonicznych z bankiem.

[227] Związek Banków Polskich, *Bankowość internetowa. Zasady dotyczące płatności kartami płatniczymi przez Internet,* [data dostępu: 3 maja 2016], <https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=4>.

[228] Grażyna Szwajkowska, Piotr Kwaśniewski, Kamil Leżoń, Filip Woźniczka, *Op. Cit.*, s. 43-44.

Prezentują się następująco[229]:

1. Bank musi Cię zidentyfikować i uwierzytelnić Twoją tożsamość.
2. Swoją tożsamość możesz potwierdzić u konsultanta lub wykorzystując udostępnione przez bank systemy i urządzenia.
3. Opis metod identyfikacji i autoryzacji znajdziesz w dokumentacji bankowej.
4. Żądaj informacji o aktualnych numerach serwisów bankowych.
5. Zawsze masz prawo sprawdzić, czy telefonuje do Ciebie bank.
6. Bank nigdy nie pyta telefoniczne o dane wrażliwe nie służące do bezpośredniej identyfikacji tożsamości.
7. Podczas rozmowy bank może posługiwać się Twoimi danymi osobowymi.
8. Nie dzwoń na numery, których autentyczności nie jesteś pewien.
9. Nie każda rozmowa z bankiem wymaga uwierzytelnienia.
10. Twoja rozmowa z bankiem może być nagrywana.
11. Telefonu z banku spodziewaj się w dni robocze i godzinach dziennych.
12. Starannie przechowuj swoje dane identyfikacyjne i uwierzytelniające.
13. Dbaj o poufność danych w trakcie kontaktu z bankiem.
14. Wprowadź do swojego telefonu komórkowego telefony do swojego banku.

Ponadto warto pamiętać o unikaniu prowadzenia rozmów z bankiem w miejscach publicznych, nie zapewniających prywatności. Aplikacja banku, ściągana na telefon powinna pochodzić z zaufanego źródła i być podpisaną cyfrowo przez dostawcę. Jak w przypadku bankowości internetowej, należy pamiętać o instalowaniu i bieżącej aktualizacji oprogramowania antywirusowego na swoim telefonie. Należy także unikać zapisywania haseł w telefonie w formie jawnej oraz unikać sytuacji, w których występuje większe zagrożenie kradzieży telefonu niż przeciętnie[230].

Powyższy rozdział w całości odniósł się do rozdziału drugiego, związanego z zagrożeniami w bankowości elektronicznej. Chcąc przyciągnąć większą liczbę klientów i wzbudzać ich zaufanie, banki przywiązują bardzo dużą uwagę do zagadnień związanych z ochroną pieniędzy zgromadzonych na kontach ich klientów. Również wciąż rozwijająca się technologia oraz ciągle rosnąca przestępczość, skłania do stosowania wzmożonej ochrony. Warto jednak pamiętać, iż przede wszystkim bezpieczeństwo środków finansowych zależy od ich właścicieli.

[229] Związek Banków Polskich, *Bankowość telefoniczna*, [data dostępu: 3 maja 2016], <https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-telefoniczna>.
[230] Jerzy Gąsiorowski, Piotr Podsiedlik, *Op. cit.*, s. 213-215.

Klienci bankowości elektronicznej poprzez swoje codzienne zachowanie weryfikują potencjalny poziom niebezpieczeństwa, jakim mogą zostać obarczeni. Dlatego też, niezwykle istotna jest przynajmniej podstawowa świadomość występujących zagrożeń i możliwości ich zapobiegania, które przedstawione zostały w powyższym rozdziale.

# Zakończenie

Ciągły postęp technologiczny przyczynia się do rozwoju i zmian zachodzących w bankowości. Rosnącą popularnością cieszą się usługi z zakresu bankowości elektronicznej, szczególnie pod postacią bankowości internetowej, terminalowej i telefonicznej. Pomimo, iż bankowość tradycyjną uważa się za bardziej bezpieczną, to jednak bankowość elektroniczna wybierana jest częściej podczas wykonywania codziennych czynności. Na tak liczne zainteresowanie wpływają przede wszystkim: wygoda, oszczędność czasu i pieniędzy, szybkość, łatwość i prostota obsługi, a także brak kolejek i dostęp o każdej porze. Wskazuje to jednoznacznie, iż własny komfort w połączeniu z oszczędnością czasu i pieniędzy, stawiany jest ponad bezpieczeństwem. Również podczas wyboru banku potencjalny klient kieruje się przede wszystkim cenami usług i produktów bankowych, a dopiero po wymienieniu kilku pośrednich kryteriów, pojawia się kwestia ochrony konta i znajdujących się na nim środków. Klienci mają do dyspozycji system bankowy, elektroniczne instrumenty płatnicze oraz dowolne kanały dystrybucji usług bankowości elektronicznej, wciąż przez bank dostosowywane do ich aktualnych potrzeb. Możliwe jest korzystanie z tych udogodnień w dowolnie wybranym miejscu, czasie i urządzeniach. Zgodnie z przeprowadzonym badaniem, klienci bankowości elektronicznej najbardziej obawiają się kradzieży środków z rachunku bankowego, fałszywych zleceń płatniczych, wirusów rozsyłanych drogą elektroniczną oraz wydobycia danych osobowych. Są to jak najbardziej uzasadnione obawy, gdyż przestępczość bankowa, w oparciu o nowe technologie oraz pomysłowość atakującego, również ciągle się rozwija. Wszelkie podjęte działania przestępcze mają na celu przejęcie środków finansowych zgromadzonych na rachunku bankowym. W związku z tym, warto pamiętać, że techniczne zabezpieczenia bankowe, choć rzeczywiście są niezwykle istotne, to nigdy nie stanowią ochrony absolutnej, tym bardziej, jeśli jednym z czynników zachowania bezpieczeństwa jest człowiek. Z natury ufny, naiwny, a także leniwy i podatny na wszelkiego rodzaju czynniki negatywne, w bardzo łatwy sposób wykorzystywane przez atakującego. Chwilowa nieuwaga wystarczy, by przysporzyć sobie wielu uporczywych problemów.

Przeprowadzone badanie podkreśla dość dobrą świadomość i orientację w tematyce zagrożeń występujących w bankowości elektronicznej, lecz zwraca również uwagę na brak wyobraźni użytkowników w kontekście efektu ich zachowania w sieci, zaniżone poczucie wartości indywidualnych danych osobowych i wciąż niską wiedzę w zakresie minimalizowania ryzyka utraty własnych środków.

Warto zatem, przynajmniej zapoznać się z podstawowymi zagrożeniami, a także zasadami poprawnego zachowania. Kilka drobiazgów, na które dzięki tej wiedzy uda zwrócić się uwagę, mogą znacznie przyczynić się do niepowodzeń atakujących, co w przypadku indywidualnych korzyści klienta bankowości elektronicznej, bezsprzecznie - zawsze się opłaca i warte jest poświęconej energii.

# Załącznik 1. Kwestionariusz ankiety

*Bankowość elektroniczna w świecie zagrożonym cyberprzestępczością*

*Ankieta skierowana głównie do Klientów bankowości elektronicznej. Jej celem jest zebranie informacji, które przyczynią się do stworzenia ogólnego wizerunku przeciętnego Klienta bankowości elektronicznej z uwzględnieniem wrażliwości na zagrożenia związane z bezprawną kradzieżą pieniędzy z prywatnego konta.*

*Ankieta jest anonimowa.*

## Metryczka

1. **Przedział wiekowy:**
   - 16 – 25 lat
   - 26 – 45 lat
   - 46 – 65 lat
   - Powyżej 65 lat

2. **Płeć:**
   - Kobieta
   - Mężczyzna

3. **Miejsce zamieszkania:**
   - Wieś
   - Miasto: mniej niż 50 000 mieszkańców
   - Miasto: między 50 000 a 100 000 mieszkańców
   - Miasto: między 100 000 a 300 000 mieszkańców
   - Miasto: między 300 000 a 500 000 mieszkańców
   - Miasto: powyżej 500 000 mieszkańców

4. **Wykształcenie:**
   - Podstawowe
   - Zawodowe
   - Średnie
   - Niepełne wyższe
   - Wyższe

## Bankowość

Tradycyjna oraz elektroniczna

1. **Która forma usług bankowych jest Pana/Pani zdaniem bardziej bezpieczna ?**
   - Bankowość tradycyjna (np. kontakt z pracownikiem banku, wizyta w oddziale)
   - Bankowość elektroniczna (np. bankowość internetowa, bankowość mobilna)

2. **Jakie kryteria są dla Pana/Pani najważniejsze przy dokonaniu wyboru banku?**
   Proszę wybrać co najmniej 3 odpowiedzi. Alfabetyczna kolejność odpowiedzi.
   - ☐ Ceny usług i produktów bankowych
   - ☐ Innowacyjne usługi
   - ☐ Jakość obsługi Klienta
   - ☐ Kraj pochodzenia banku
   - ☐ Oferowane możliwości zabezpieczeń konta
   - ☐ Opinia znajomych (pozytywna bądź negatywna) o banku
   - ☐ Położenie oddziałów banku
   - ☐ Renoma banku
   - ☐ Wysokie oprocentowanie lokat
   - ☐ Inne, …

3. **Jaki rodzaj kontaktu z bankiem Pan/Pani preferuje?**
   - Dostęp poprzez Internet
   - Osobista wizyta w oddziale banku
   - Telefoniczny kontakt z konsultantem (call center)
   - Telefoniczna obsługa przez system automatyczny (IVR)
   - WAP/SMS
   - Inne, …

4. **W jaki sposób najczęściej wypłaca Pan/Pani gotówkę ?**
   - Bankomat
   - Oddział banku
   - Urząd pocztowy
   - Inne, …

5. **Czy wie Pan/Pani z jakich zabezpieczeń korzysta Pana/Pani bank ?**
   - Tak
   - Nie

6. **Co Pana/Pani zdaniem bank powinien zrobić/wprowadzić/ulepszyć, aby zwiększyć bezpieczeństwo finansów i danych osobowych swoich Klientów ?**
   - ➢ Pytanie otwarte.

## Bankowość elektroniczna

Wszystkie formy zdalnego zarządzania pieniędzmi: bankowość internetowa, dedykowana bankowość komputerowa, bankowość telefoniczna, bankowość mobilna (przenośna), bankowość terminalowa, bankowość telewizyjna.

1. **Czy korzysta Pan/Pani z usług bankowości elektronicznej ?**
   - Tak
   - Nie

2. **Dlaczego nie korzysta Pan/Pani z usług bankowości elektronicznej ?**
   - Pytanie otwarte

3. **Czy zamierza Pan/Pani skorzystać z bankowości elektronicznej w przyszłości ?**
   - Tak
   - Nie

4. **Jak często korzysta Pan/Pani z usług bankowości elektronicznej ?**
   - Codziennie
   - Kilka razy w tygodniu
   - Raz w tygodniu
   - Kilka razy w tygodniu
   - Raz w miesiącu
   - Rzadziej niż raz w miesiącu

5. **W jakich miejscach najczęściej korzysta Pan/Pani z usług bankowości elektronicznej ?**
   Proszę wybrać co najwyżej 2 odpowiedzi. Alfabetyczna kolejność odpowiedzi.
   - ☐ Na uczelni
   - ☐ W domu
   - ☐ W pracy
   - ☐ W samochodzie
   - ☐ Inne, …

6. **Dlaczego korzysta Pan/Pani z usług bankowości elektronicznej ? Jakie czerpie Pan/Pani korzyści ?**
   - Pytanie otwarte

7. **Jak ocenia Pan/Pani swoją wiedzę na temat bankowości elektronicznej ?**

8. **Czy ma Pan/Pani pełne zaufanie do środków bezpieczeństwa stosowanych przez Pana/Pani bank ?**
   - o Tak
   - o Nie

9. **Z jakiej formy bankowości elektronicznej Pan/Pani korzysta ?**
   Alfabetyczna kolejność odpowiedzi.
   - ☐ Bankowość mobilna (komunikacja niegłosowa wykorzystująca technologię WAP, SMS i aplikacje klienckie)
   - ☐ Bankowość internetowa (dostęp poprzez przeglądarkę stron internetowych)
   - ☐ Bankowość telefoniczna (komunikacja głosowa z call center lub IVR)
   - ☐ Bankowość telewizyjna (dostęp przez telewizję cyfrową)
   - ☐ Bankowość terminalowa (za pomocą bankomatów, kiosków samoobsługowych)
   - ☐ Dedykowana bankowość komputerowa (dostęp poprzez specjalistyczne oprogramowanie, lokalnie zainstalowane na komputerze)

10. **Z jakich usług bankowości elektronicznej Pan/Pani korzysta ?**
    Alfabetyczna kolejność odpowiedzi.
    - ☐ Definiowanie przelewów do realizacji w przyszłości
    - ☐ Dokonywanie operacji za pośrednictwem telefonu
    - ☐ Dokonywanie płatności w sklepach internetowych bezpośrednio z konta
    - ☐ Dokonywanie płatności za pomocą karty płatniczej (na pin, na podpis, zbliżeniowo)
    - ☐ Doładowania telefonu
    - ☐ Serwis informacyjny i doradztwo
    - ☐ Składanie wniosków o kredyty/pożyczki
    - ☐ Sprawdzanie historii wykonywanych operacji
    - ☐ Sprawdzanie ofert i promocji
    - ☐ Sprawdzanie salda rachunku
    - ☐ Ustalanie zleceń stałych płatności
    - ☐ Wykonywanie przelewów na rachunki własne i obce
    - ☐ Wypłacanie/wpłacanie pieniędzy za pośrednictwem bankomatu
    - ☐ Zakładanie i likwidowanie lokat
    - ☐ Inne, …

11. **Czy weryfikuje Pan/Pani stan konta bankowego ?**
    - o Tak
    - o Nie

12. **Czy Pana/Pani zdaniem, dane osobowe w bankowości elektronicznej są wystarczająco dobrze chronione ?**
    - Zdecydowanie tak
    - Raczej tak
    - Trudno powiedzieć
    - Raczej nie
    - Zdecydowanie nie

13. **Czy otrzymuje Pan/Pani rachunki na skrzynkę poczty elektronicznej ?**
    - Tak
    - Nie

14. **Czy otwiera Pan/Pani maile od nieznanych nadawców ?**
    - Tak
    - Nie

15. **Czy regularnie zmienia Pan/Pani swój PIN bądź hasło dostępu do konta bankowego ?**
    - Tak
    - Nie

16. **W jaki sposób przechowuje Pan/Pani swoje hasło lub PIN umożliwiające dostęp do konta?**
    - Pytanie otwarte

17. **Czy korzysta Pan/Pani z funkcji zapamiętywania haseł dostępu w przeglądarce/aplikacji służącej łączeniu z kontem bankowym ? (tzw. autoformularz)**
    - Tak
    - Nie

18. **Czy jest Pan/Pani jedyną osobą posiadającą dane dostępu do Pana/Pani konta bankowego ?**
    - Tak
    - Nie

19. **Czy wylogowuje się Pan/Pani każdorazowo po skorzystaniu z usług bankowości elektronicznej ?**
    - Tak
    - Nie zawsze
    - Nie

**20. Czy posiada Pan/Pani program antywirusowy na urządzeniu, z którego dochodzi do połączenia z kontem bankowym ?**

- o Tak
- o Nie

**21. Czy aktualizuje Pan/Pani swój program antywirusowy na bieżąco ?**

- o Tak
- o Nie
- o Nie dotyczy

**22. Czy zawsze używa Pan/Pani znanych sobie, zaufanych urządzeń do korzystania z bankowości elektronicznej ?**

- o Tak
- o Nie

**23. Z którymi formami zabezpieczeń konta bankowego spotkał(a) się Pan/Pani kiedykolwiek ?**

Alfabetyczna kolejność odpowiedzi.

- ☐ Automatyczne wylogowanie po kilkuminutowej nieaktywności Klienta
- ☐ Blokowanie konta po kilkukrotnym wprowadzeniu błędnych danych logowania
- ☐ Certyfikaty cyfrowe/klucze
- ☐ Dzienny limit transakcji
- ☐ Hasło
- ☐ Jednorazowe kody autoryzujące transakcję
- ☐ Kryptografia (szyfrowanie)
- ☐ Login
- ☐ Numer identyfikacyjny
- ☐ Numer PIN
- ☐ Podpis elektroniczny
- ☐ Powiadomienie smsowe lub mailowe
- ☐ Token
- ☐ Inne, …

**24. Jakich zagrożeń w bankowości elektronicznej obawia się Pan/Pani najbardziej?**

Proszę wybrać co najwyżej 3 odpowiedzi. Alfabetyczna kolejność odpowiedzi.

- ☐ Fałszywe zlecenia płatnicze
- ☐ Kradzież haseł lub kodów jednorazowych
- ☐ Kradzież środków z rachunku bankowego
- ☐ Niczego się nie obawiam
- ☐ Wirusy rozsyłane drogą elektroniczną
- ☐ Wydobycie danych osobowych
- ☐ Inne, …

25. **Czy w ciągu najbliższych 12 miesięcy zamierza Pan/Pani skorzystać z usług bankowości elektronicznej ?**
    - Tak
    - Nie

## Bankowość internetowa

Użytkowanie bankowości w oparciu o przeglądarkę stron WWW.

1. **Czy korzysta Pan/Pani z usług bankowości internetowej ?**
    - Tak
    - Nie

2. **Dlaczego nie korzysta Pan/Pani z usług bankowości internetowej ?**
    - Pytanie otwarte

3. **Czy zamierza Pan/Pani skorzystać z usług bankowości internetowej w przyszłości ?**
    - Tak
    - Nie

4. **Jak długo posiada Pan/Pani internetowe konto bankowe ?**
    - Mniej niż rok
    - Rok
    - 2 lata
    - 3 lata
    - 4 lata
    - 5 lat i więcej

5. **Czy według Pana/Pani korzystanie z usług bankowości internetowej jest skomplikowane ?**
    - Tak
    - Raczej tak
    - Raczej nie
    - Nie

6. **Jakie korzyści dostrzega Pan/Pani w użytkowaniu bankowości internetowej ?**
    - Pytanie otwarte

7. **Jakie wady dostrzega Pan/Pani w użytkowaniu bankowości internetowej ?**
    - Pytanie otwarte

8. **Czy zabezpiecza Pan/Pani swój system za pomocą włączonej zapory sieciowej (firewall) ?**
    - Tak
    - Nie

9. **Czy kiedykolwiek został(a) Pan/Pani ofiarą kradzieży z rachunku bankowego ?**
    - Tak
    - Nie

10. **Proszę o krótki opis zdarzenia.**
    - Pytanie otwarte

## Bankowość mobilna

Komunikacja niegłosowa wykorzystująca technologię WAP, SMS i aplikacje klienckie

1. **Czy korzysta Pan/Pani z usług bankowości mobilnej ?**
    - Tak
    - Nie

2. **Dlaczego nie korzysta Pan/Pani z usług bankowości mobilnej ?**
    - Pytanie otwarte

3. **Czy zamierza Pan/Pani skorzystać z bankowości mobilnej w przyszłości ?**
    - Tak
    - Nie

4. **Na jakim urządzeniu najczęściej korzysta Pan/Pani z usług bankowości mobilnej ?**
    - Na smartfonie
    - Na tablecie
    - Inne, …

5. **W jaki sposób korzysta Pan/Pani z usług bankowości na urządzeniach mobilnych ?**
    - Przez stronę internetową
    - Przez aplikację udostępnioną przez bank

6. **Czy korzysta Pan/Pani z możliwości zbliżeniowej płatności telefonem (usługa NFC) lub zamierza Pan/Pani korzystać w przyszłości ?**
    - Korzystam i zamierzam korzystać w przyszłości
    - Korzystam i nie zamierzam korzystać w przyszłości
    - Nie korzystam, ale zamierzam korzystać w przyszłości
    - Nie korzystam i nie zamierzam korzystać w przyszłości
    - Nie słyszałem(am) o takiej formie płatności

7. **Czy zabezpiecza Pan/Pani swoją kartę SIM kodem PIN?**
    - Tak
    - Nie

8. **Czy stosuje Pan/Pani blokadę ekranu w swoim telefonie ?**
    - Tak
    - Nie

9. **Czy korzysta Pan/Pani z widgetu wyświetlania dostępnych środków na koncie, bez konieczności logowania się do sytemu transakcyjnego ?**
    - Tak
    - Nie

10. **Czy korzysta Pan/Pani z widgetu „szybkiego doładowania telefonów" ?**
    - Tak
    - Nie

11. **Czy oddając telefon do serwisu, dokonuje Pan/Pani deinstalacji aplikacji bankowych ?**
    - Tak
    - Nie
    - Nie oddawałem(am) telefonu do serwisu

12. **Czy według Pana/Pani korzystanie z usług bankowości mobilnej jest skomplikowane ?**
    - Tak
    - Raczej tak
    - Raczej nie
    - Nie

13. **Jakie korzyści dostrzega Pan/Pani w bankowości mobilnej ?**
    - Pytanie otwarte

14. **Jakie wady dostrzega Pan/Pani w bankowości mobilnej ?**
    - Pytanie otwarte

15. **Czy kiedykolwiek został(a) Pan/Pani okradziony(a) przy dokonaniu płatności za pomocą urządzenia mobilnego ?**
    - Tak
    - Nie

16. **Proszę o krótki opis zdarzenia**
    - Pytanie otwarte.

## Bankowość terminalowa

Bankomaty, kioski samoobsługowe, POS-y

1. **Czy korzysta Pan/Pani z bankowości terminalowej ?**
   - Tak
   - Nie

2. **Dlaczego nie korzysta Pan/Pani z bankowości terminalowej ?**
   - Pytanie otwarte

3. **Czy zamierza Pan/Pani skorzystać z usług bankowości terminalowej w przyszłości ?**
   - Tak
   - Nie

4. **Z jakiego rodzaju kart płatniczych Pan/Pani korzysta ?**
   - ☐ Kredytowa
   - ☐ Debetowa
   - ☐ Obciążeniowa (połączenie karty kredytowej i debetowej)
   - ☐ Przedpłacona

5. **Jaki jest najczęstszy sposób dokonywania przez Pana/Panią płatności kartą ?**
   - Płatność z potwierdzeniem kodem PIN
   - Płatność zbliżeniowa (do 50zł)
   - Na podpis

6. **Czy korzysta Pan/Pani z bankomatów znajdujących się wyłącznie w oddziałach banku ?**
   - Tak
   - Nie

7. **Jakie korzyści dostrzega Pan/Pani w bankowości terminalowej ?**
   - Pytanie otwarte

8. **Jakie wady dostrzega Pan/Pani w usługach bankowości terminalowej ?**
   - Pytanie otwarte

9. **Czy według Pana/Pani korzystanie z usług bankowości terminalowej jest skomplikowane ?**
   - Tak
   - Raczej tak
   - Raczej nie
   - Nie

10. **Jak zareagowałby(aby) Pan/Pani w sytuacji zgubienia bądź kradzieży karty bankowej ?**
    - Pytanie otwarte

11. **Czy kiedykolwiek został(a) Pan/Pani okradziony(a) przy dokonaniu płatności kartą płatniczą lub przy wypłacaniu bądź wpłacaniu pieniędzy za pośrednictwem bankomatu ?**
    - Tak
    - Nie

12. **Proszę o krótki opis sytuacji**
    - Pytanie otwarte

## Dziękuję serdecznie za wszelkie udzielone odpowiedzi !

# Bibliografia

## Literatura


1. Adamiec J.: *Bankowość elektroniczna*, Warszawa: Społeczeństwo informacyjne, D.Grodzka (red.), „Studia BAS", nr 3(19) 2009.
2. Banasikowska J.: *Rodzaje płatności i systemy płatności na rynku elektronicznym*, Systemy wspomagania organizacji, Katowice: Akademia Ekonomiczna 2004.
3. Bednarek J., Andrzejewska A.: *Cyberświat: możliwości i zagrożenia*, Warszawa: Wydawnictwo Akademickie ŻAK 2009.
4. Białas A.: *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa: Wydawnictwo Naukowo-Techniczne 2006, 2007.
5. Bury A.: *Karty płatnicze w Polsce*, Warszawa: CeDeWu 2002.
6. Bliźniuk G., Nowak S.J.: *Społeczeństwo informacyjne*, Katowice: Wyd. PTI 2005.
7. Chinowski B.: *Elektroniczne metody płatności. Istota, rozwój, prognoza*, Warszawa: Komisja Nadzoru Finansowego 2013.
8. Chmielarz W.: *Systemy elektronicznej bankowości*, Warszawa: Centrum Doradztwa i Informacji Difin 2005.
9. Chmielarz W.: *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa: Wyższa Szkoła Ekonomiczno-Informatyczna w Warszawie 1999.
10. Cialdini R.: *Wywieranie wpływu na ludzi. Teoria i praktyka*, Gdańsk: Gdańskie Wydawnictwo Psychologiczne 2000.
11. Gąsiorowski J., Podsiedlik P.: *Przestępstwa w bankowości elektronicznej w Polsce – próba oceny z perspektywy prawno-kryminalistycznej*, Dąbrowa Górnicza: Wydawnictwo Naukowe, Wyższa Szkoła Biznesu w Dąbrowie Górniczej 2015.
12. Generalny Inspektor Ochrony Danych Osobowych: *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, Warszawa: GIODO 2009.
13. Gospodarowicz A.: *Bankowość elektroniczna*, Warszawa: Polskie Wydawnictwo Ekonomiczne 2005.
14. Górnisiewicz M., Obczyński R., Pstruś M.: *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną*, Warszawa: Komisja Nadzoru Finansowego 2014.
15. Guzik A.: *Zagrożenia socjotechniczne, a bezpieczeństwo informacji*, „Hakin9", nr 7/2007.
16. Hadnagy C.: *Socjotechnika – sztuka zdobywania władzy nad umysłami*, Gliwice: Helion 2011.
17. Jakubski J. K., *Przestępczość komputerowa – podział i definicja*, Przegląd Krymianlistyki: Nr 2/7 1997.
18. Janowicz R.: *Pieniądz elektroniczny w wybranych krajach – charakterystyka, główne funkcje i zastosowanie*, Narodowy Bank Polski, „Bank i kredyt", 2005.
19. Jurkowski A.: *Bakowość Elektroniczna, Zeszyt 125*, Warszawa: Narodowy Bank Polski 2001.
20. Korenik D.: *Innowacyjne usługi banku*, Warszawa: Wydawnictwo PWN 2006.
21. Korzeń K.: *Bankowość elektroniczna jako kanał dystrybucji usług bankowych*, Warszawa: Intelgraf – Anna Dygas 2007.

22. Kosiński J.: *Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych*, III Międzynarodowa Konferencja Naukowa, Szczytno: Wyższa Szkoła Policji w Szczytnie 2003.
23. Kossecki J.: *Cybernetyka kultury*, Warszawa: Państwowy Instytut Wydawniczy 1974.
24. Kossecki J.: *Cybernetyka społeczna*, Warszawa: Państwowe Wydawnictwo Naukowe 1981.
25. Kutyłowski M.: Strothmann W.: *Kryptografia: teoria i praktyka zabezpieczenia systemów komputerowych*, Warszawa: Wydawnictwo Lupus, 1998.
26. Lukatsky A.: *Wykrywanie włamań i aktywna ochrona danych*, Gliwice: Helion 2005.
27. Mikoś M.: *SPAM – metody walki i obrony*, CBKE e-biuletyn 1/2005.
28. Mitnick K., Simon W.: *Sztuka podstępu*, Gliwice: Helion 2003.
29. Niedźwiedzka-Małecka M.: Przestępstwa związane z wykorzystaniem kart płatniczych, „Studia Iuridica" 2001.
30. Polasik M.: *Bankowość elektroniczna, istota-stan-perspektywy*, Warszawa: CeDeWu 2012.
31. Podsiedlik P., Czylok T.: *Przestępczość w bankowości elektronicznej – Skimming karty bankomatowej*, Katowice: Wydawnictwo Szkoły Policji w Katowicach 2010.
32. Polasik M., Maciejewski K.: *Innowacyjne usługi płatnicze w Polsce i na świecie*, Materiały i studia, Zeszyt nr 241, Warszawa: Narodowy Bank Polski 2009.
33. Ryznar Z.: *Informatyka bankowa – prób syntezy*, Poznań: Wydawnictwo Wyższej Szkoły Bankowej w Poznaniu 1998.
34. Ryznar Z.: *Multichannelling, czyli wielokanałowość*, Czasopismo BANK, nr 7-8 2003.
35. Shinder L. D., Tittel E.: *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice: Wydawnictwo Helion 2004.
36. Sienkiewicz P., Nowak S.J.: *Społeczeństwo informacyjne – krok naprzód, dwa kroki wstecz*, Katowice: Polskie Towarzystwo Informatyczne. Oddział Górnośląski: Polskie Towarzystwo Społeczeństwa Informacyjnego 2008.
37. Siwicki M.: *Cyberprzestępczość*, Warszawa: Wydawnictwo C.H.Beck 2013.
38. Skowron A.: *Phishing, czyli jak się łowi hasła w Internecie*, Wrocław: Politechnika Wrocławska 2006.
39. Smykla I.: *Analiza form zastosowania bankowości elektronicznej dla obsługi przedsiębiorstw*, Warszawa: Intelgraf – Anna Dygas 2005.
40. Stallings W.: *Kryptografia i bezpieczeństwo sieci komputerowych – Koncepcje i metody bezpiecznej komunikacji*, Gliwice: Helion 2012.
41. Stallings W.: *Systemy operacyjne – Struktura i zasady budowy*, Warszawa: Wydawnictwo Naukowe PWN 2006.
42. Szwajkowska G., Kwaśniewski P., Leżoń K., Woźniczka F.: *Usługi bankowości elektronicznej dla klientów detalicznych – charakterystyka i zagrożenia*, Warszawa: Urząd Komisji Nadzoru Finansowego 2010.
43. Ślązak E., Guzek E.: *Innowacyjna bankowość internetowa*, Warszawa: Wolters Kluwer Polska 2012.
44. Świecka B.: *Bankowość elektroniczna*, Warszawa: CeDeWu 2004.
45. Trejderowski T.: *Socjotechnika, podstawy manipulacji w praktyce*, Warszawa: ENETEIA Wydawnictwo Psychologii i Kultury 2009.
46. Waglowski P.: *Ochrona dóbr osobistych i danych osobowych*, Warszawa: Polska Agencja Rozwoju Przedsiębiorczości 2009.
47. Wang W.: *Tajemnice Internetu, hackingu, i bezpieczeństwa*, Gliwice: Helion 2005.

48. Wawrzyniak D.: *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości*, Warszawa: Oficyna Wydawnicza „Zarządzanie i Finanse" 2002.
49. Wojciechowska-Filipek S.: *Technologia informacyjna w usługach bankowości elektronicznej*, Warszawa: Difin 2010.
50. Wrona M.: *Niebezpieczeństwo komputerowe*, Warszawa: RM 2000.
51. Zalesińska A., Rodziewicz P., Pęcherzewski P., Kotecka S., Goździaszek Ł., Cieślak Ł., Burdziak A., *Technologia informacyjna dla pracowników*, Wrocław: Prawnicza i Ekonomiczna Biblioteka Cyfrowa 2011.

## Akty prawne

1. Ustawa Prawo Bankowe, DzU 1997r. nr 140.
2. Ustawa Prawo Bankowe, DzU 2002r. nr 72.

Źródła sieciowe


1. Besala J., *Historia banków i bankierów*, http://www.polityka.pl/tygodnikpolityka/historia/1523347,1,historia-bankow-i-bankierow.read, data dostępu: 9 maja 2016.
2. Credit Agricole, *Korzystanie z bankomatu*, http://www.credit-agricole.pl/bezpieczenstwo/korzystanie-z-bankomatu, data dostępu: 3 maja 2016.
3. Cyberwojna, http://securelist.pl/analysis/26,analiza_mentalnosci_hakera.html, data dostępu: 17.03.2016.
4. *Definicja i budowa karty płatniczej*, http://www.kartyplatnicze.info/definicja.php, data dostępu: 20 listopada 2015.
5. *Definicja i budowa karty płatniczej*, http://www.kartyplatnicze.info/typologia.php, data dostępu: 22 listopada 2015.
6. Gajewski M.: *Phishing – łowienie naiwnych, http://www.chip.pl/artykuly/trendy/2009/11/phishing-lowienie-naiwnych*, data dostępu: 19 kwietnia 2016.
7. *Kolejna kampania ataków na routery klienckie*, http://www.cert.pl/news/tag/man-in-the-middle, data dostępu: 9 kwietnia 2016.
8. Merritt M., *Kradzież tożsamości – podstawowe informacje*, http://pl.norton.com/identity-theft-primer/article, data dostępu: 10 kwietnia 2016.
9. Mikołajczyk K., *Przestępstwa związane z wykorzystaniem bankowości elektronicznej*, http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-1/1008,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-10-6-2014.html, data dostępu: 4 kwietnia 2016.
10. Norton, *Słownik bezpieczeństwa internetowego*, http://pl.norton.com/security-glossary/article#p, data dostępu: 16 kwietnia 2016.
11. Policja podlaska, *Oszustwa bankomatowe*, http://www.podlaska.policja.gov.pl/pod/dzialania-policji/przestepczosc-gospodar/struktura-wydzialu/zespol-ii/oszustwa-bankomatowe/28417,Oszustwa-bankomatowe.html, data dostępu: 3 kwietnia 2016.
12. Siwicki M., *Kradzież tożsamości – pojęcie i charakterystyka zjawiska. Część 1*, http://www.edukacjaprawnicza.pl/artykuly/artykul/a/pokaz/c/artykul/art/kradziez-tozsamosci-pojecie-i-charakterystyka-zjawiska-czesc-i.html, data dostępu: 10 kwietnia 2016.
13. Słownik Języka Polskiego PWN: *hasło: pogotowie kasowe*, http://sjp.pwn.pl/sjp/pogotowie-kasowe;2503263.html, data dostępu: 17 listopada 2015.
14. Słownik pojęć internetowo-reklamowych, *serwer DNS*, https://slownik.intensys.pl/definicja/36/serwer-dns/, data dostępu: 19 kwietnia 2016.
15. Szymkiewicz R.: *Czym jest carding?*, http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298323,Czym-jest-carding.html, data dostępu: 9 kwietnia 2016.
16. *Oszustwa rekrutacyjne*, http://www.oszustwsieci.pl/oszustwa_rekrutacyjne.php, data dostępu: 19 kwietnia 2016.
17. Wikipedia, *Inżynieria społeczna*, https://pl.wikipedia.org/wiki/In%C5%BCynieria_spo%C5%82eczna_(informatyka), data dostępu: 14 kwietnia 2016.

18. Wikipedia, *Pharming*, https://pl.wikipedia.org/wiki/Pharming, data dostępu: 19 kwietnia 2016.
19. *Wireless Application Protocol,* https://pl.wikipedia.org/wiki/Wireless_Application_Protocol, data dostępu: 5 grudnia 2015.
20. Wydział Wsparcia Zwalczania Cyberprzestępczości Biura Kryminalnego Komendy Głównej Policji, *Ochrona informatyczna danych – „Phishing" i kradzież tożsamości*, http://www.policja.pl/pol/kgp/bsk/dokumenty/cyberprzestepczosc/58792,Ochrona-informatyczna-danych-phishing-i-kradziez-tozsamosci.html, data dostępu: 10 kwietnia 2016.
21. Związek Banków Polskich: *Bankowość internetowa. Atak słownikowy*, https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=10, data dostępu: 3 maja 2016.
22. Związek Banków Polskich: *Bankowość internetowa. Zasady dotyczące płatności kartami płatniczymi przez Internet*, https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=4, data dostępu: 3 maja 2016.
23. Związek Banków Polskich: *Bankowość internetowa. Zasady dotyczące płatności z internetowego konta bankowego*, https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=3, data dostępu: 3 maja 2016.
24. Związek Banków Polskich: *Bankowość internetowa. Zasady ogólne*, https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa?edytor_311=1, data dostępu: 3 maja 2016.
25. Związek Banków Polskich: *Bankowość telefoniczna*, https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-telefoniczna, data dostępu: 3 maja 2016.
26. Związek Banków Polskich: *Karty bankowe. 27 zasad korzystania z kart bankowych*, https://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe, data dostępu: 3 maja 2016.
27. Związek Banków Polskich: *Raport NetB@nk: Dostęp do e-bankowości – kolejny rekord*, https://zbp.pl/dla-prasy/informacje-prasowe/raport-netb-nk-dostep-do-e-bankowosci-kolejny-rekord, data dostępu: 24 października 2015.

# Spis rysunków

# Spis tabel



# Spis załączników