# BEZPIECZEŃSTWO I BIOMETRIA URZĄDZEŃ MOBILNYCH W POLSCE

## BADANIE UŻYTKOWNIKÓW 2016

Wojciech Wodo
Hanna Ławniczak

**Recenzja**
Damian Derlukiewicz

**Współpraca**
Zespół badawczy *Design Thinking – Biometry*, działajacy w ramach
Laboratorium Interdyscyplinarnosci i Kreatywnego Projektowania
Centrum Wiedzy i Informacji Naukowo-Technicznej Politechniki Wrocławskiej

*Wojciech Wodo, Hanna Ławniczak, Marta Tarapata, Agnieszka Andrzejewska, Joanna Mirocha, Irmina Krawczyk i Łukasz Liebersbach*

**Partnerzy**

Politechnika Wrocławska

VCN trzymaj nadzór

CWINT CENTRUM WIEDZY I INFORMACJI NAUKOWO-TECHNICZNEJ POLITECHNIKI WROCŁAWSKIEJ



ISBN 978-83-7493-970-6
DOI: 10.5277/Y03.2017.01

# Spis treści

# O Autorach

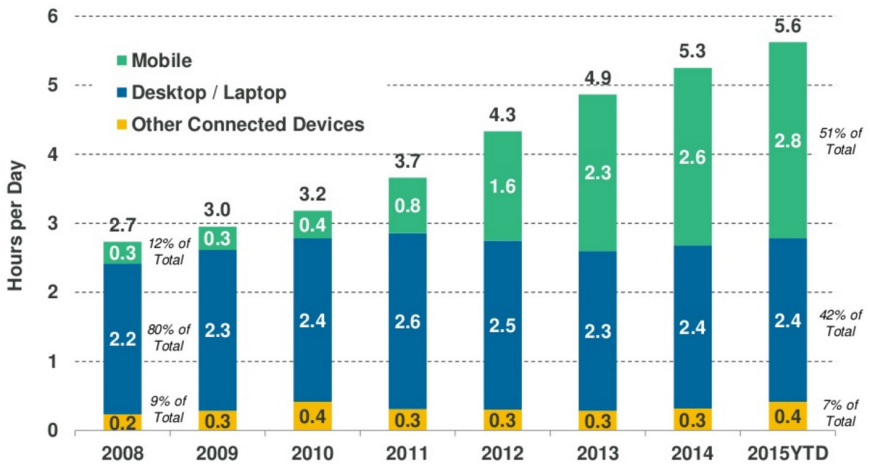
**Wojciech Wodo** jest asystentem naukowym na Politechnice Wrocławskiej w Katedrze Informatyki, doktoryzuje się również tam w obszarze nauk ścisłych. Polami zainteresowań Wojtka są bezpieczeństwo komputerowe, w tym szczególnie biometria, a także innowacje i przedsiębiorczość. Wojciech Wodo jest absolwentem specjalnego programu MNiSW *Top 500 Innovators* w *Haas School of Business* na Uniwersytecie Kalifornijskim w Berkeley dotyczącego zarządzania zespołami naukowymi, transferem technologii, komercjalizacji wyników badań naukowych oraz współpracy uczelni i przemysłu. Swoje doświadczenia w zakresie transferu technologii Wojtek zdobywał podczas pracy we Wrocławskim Centrum Badań EIT+ oraz jako wiceprezes Fundacji MANUS.

**Hanna Ławniczak** jest absolwentką Uniwersytetu Ekonomicznego we Wrocławiu, gdzie ukończyła studia magisterskie na wydziale Zarządzania Informatyki i Finansów ze specjalnością Project Management. Hania w 2013 roku była stypendystką na francuskiej uczelni *Ecole de Commerce Européenne* w Lyonie. W kręgu jej zainteresowań leżą obszary takie jak innowacyjność, komercjalizacja wiedzy, przedsiębiorczość, czy współczesne narzędzia marketingowe. Obecnie pracuje jako Project Manager w jednej z wiodących firm branży IT. Raport "Bezpieczeństwo i biometria urządzeń mobilnych w Polsce– Badanie użytkowników 2016" jest jej pierwszą publikacją naukową, której jest współautorką.

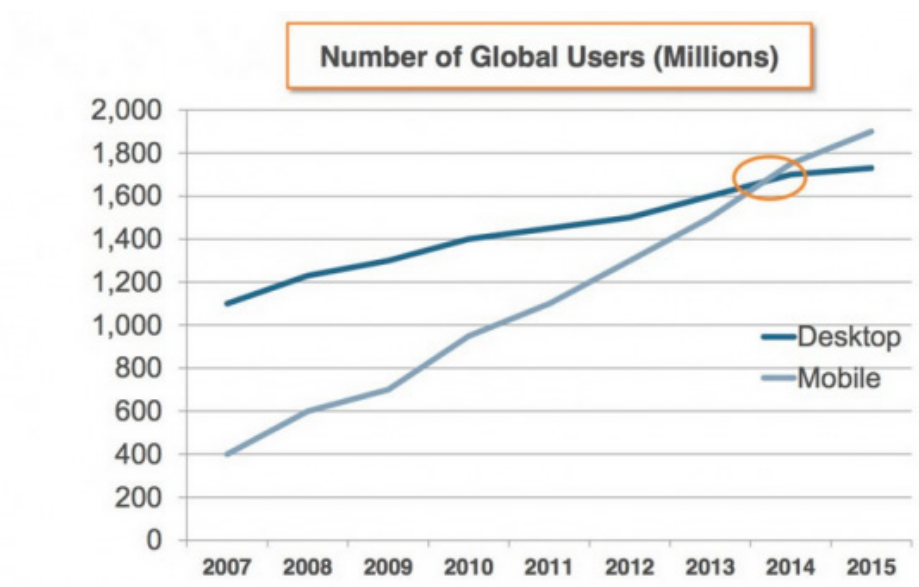
# 1 Wprowadzenie

Urządzenia mobilne zastępują coraz częściej komputery osobiste, ich rola w ostatnim czasie zyskała bardzo na znaczeniu. Użytkownicy wykorzystują urządzenia mobilne jako przenośne centra dowodzenia, zarówno w ich życiu prywatnym, jak i zawodowym. Smartfony i tablety są użytkowane w trybie ciągłego podłączenia do sieci, umożliwiając odbieranie i wysyłanie poczty elektronicznej, podejmowanie rozmów nie tylko w formie głosowej, ale także hangoutów tekstowych i wizualnych. Dokonywane są przez nie także operacje finansowe, wykorzystywane portale społecznościowe czy tworzone i edytowane dokumenty. Porównanie wyników badań pokazujących procent czasu spędzonego na wykonywaniu tych czynności na różnych urządzeniach dostępowych prezentuje **Rysunek 1**. Każdego dnia miliony ludzi na całym świecie używa urządzeń mobilnych, doskonale obrazuje to raport *comScore* – **Rysunek 2**. Relatywnie nie dawno, bo w 2014 roku liczba użytkowników mobilnych przerosła liczbę tradycyjnych użytkowników laptopów, czy komputerów stacjonarnych. Tendencja ta nadal się zachowuje, przy czym należy zaznaczyć, że krzywa obrazująca aktywność globalnych użytkowników mobilnych pnie się liniowo w górę, natomiast krzywa zwolenników urządzeń tradycyjnych zmniejsza swoje nachylenie i powoli ulega stagnacji.

Urządzenia mobilne wykorzystuje się do coraz bardziej skomplikowanych i wysublimowanych zadań. Tradycyjne przeznaczenie telefonu komórkowego już dawno zatraciło swoje pierwotne znaczenie. Obecnie telefonu używa się już nie tylko w celach kontaktu głosowego z drugą osobą, a jego dodatkowe funkcje zaczynają odgrywać już nie drugorzędną, a podstawową rolę. Dziś większość użytkowników urządzeń mobilnych zapewne nie wyobraża sobie już życia bez możliwości sprawdzenia




**Rysunek 1** – Zestawienie Ilości czasu spędzonego z mediami cyfrowymi na różnych urządzeniach dostępowych
Źródło: Internet Trends 2015 – Code Conference, Mary Meeker, 27 Maj 2015




**Rysunek 2** – Liczba globalnych użytkowników urządzeń mobilnych oraz stacjonarnych w latach 2007–2015.
Źródło: http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

najnowszych informacji z kraju i świata (w czasie rzeczywistym), sprawdzenia prognoz pogody, rozkładu jazdy komunikacji miejskiej (automatycznie wliczając estymowany czas opóźnień ze względu na korki), natychmiastowego dostępu do swojej skrzynki mailowej, różnego rodzaju portali społecznościowych, aplikacji muzycznych, filmowych, a coraz częściej również wykonywania operacji finansowych, czy zarządzania własnymi bądź firmowymi danymi. To wszystko zbudowało część rzeczywistości, w której żyjemy. Nie dziwi więc fakt, że spędzamy coraz więcej czasu pochylając się nad dorobkiem nowych technologii, bowiem czerpiąc z ich zalet po prostu ułatwiamy sobie życie.

Taka zmiana sposobu wykorzystania urządzeń mobilnych generuje nowe zagrożenia w obszarze bezpieczeństwa danych i prywatności. Wymiar dyskutowanej

zmiany jest globalny i nie ulega wątpliwości, że się nie cofnie, a wręcz przeciwnie – nabierze na znaczeniu. Mówiąc o bezpieczeństwie, mamy na myśli zarówno tożsamość elektroniczną użytkownika, przeniesioną niejako do sfery elektronicznej i dającą olbrzymie możliwości funkcjonalne, jak i same dane przechowywane na urządzeniu czy serwerach w chmurze. Sytuacja staje się jeszcze poważniejsza, jeśli uzmysłowimy sobie jak skonstruowane są obecne aplikacje mobilne oraz jakie mechanizmy zabezpieczeń oferują urządzenia mobilne.

Większość aplikacji do obsługi poczty elektronicznej (np. *Gmail*) czy systemów społecznościowych (np. *Facebook*) daje natychmiastowy dostęp do konta użytkownika (bez konieczności dodatkowego uwierzytelniania), wystarczy jedynie uruchomić taką aplikację na urządzeniu mobilnym – koncepcja bezpieczeństwa opiera się jedynie o bezpieczeństwo dostępu do samego urządzenia mobilnego. Oczywiście takie rozwiązanie jest niezwykle wygodne dla użytkownika: będąc wciąż w stanie zalogowania do systemów otrzymuje się na bieżąco wszystkie notyfikacje i bez jakichkolwiek utrudnień wykonuje wszystkie czynności. Taki komfort trwa do momentu utraty kontroli nad urządzeniem mobilnym w wyniku jego kradzieży bądź po prostu zgubienia. Wtedy te same przywileje zyskuje znalazca urządzenia, jeśli tylko uda mu się je odblokować, co jak pokażemy w dalszej części, wcale nie jest trudne.

Należy pamiętać, że rozwiązania bezpieczeństwa, które producent implementuje standardowo najczęściej nie zostają przez użytkownika zmienione. Dotyczy to zarówno oprogramowania samego telefonu, jak i konfiguracji aplikacji. Stąd tak istotne jest to, aby ustawienia fabryczne dawały wysoki poziom bezpieczeństwa, który to dopiero użytkownik może świadomie zmienić na własną odpowiedzialność. Niestety, większość producentów stawia na wygodę i łatwość użytkowania produktu, pozostawiając sferę bezpieczeństwa daleko w tyle [9].

Standardowe zabezpieczenia urządzeń mobilnych opierają się na odblokowywaniu ekranu dotykowego poprzez nakreślenie określonej sekwencji punktów na ekranie, bądź podanie po prostu hasła nazywanego PIN (*ang. Personal Identyfication Number*) – **Rysunek 3**. Niektórzy użytkownicy wyłączają te mechanizmy całkowicie bądź ustawiają trywialne wzory czy hasła, jest to proces stawiający wygodę ponad jakiekolwiek wartości bezpieczeństwa. Więcej na ten temat można znaleźć w pracy [6].

Oczywiście niektóre systemy informatyczne oferują bardziej zaawansowane mechanizmy bezpieczeństwa. Przykładem mogą być rozwiązania wykorzystujące kody jednorazowe wysyłane wiadomością tekstową SMS na telefon komórkowy (np. systemy bankowe czy dostęp do Gmaila). Rozważmy przypadek, w którym właśnie został skradziony smartfon, na którym korzystano z takiego systemu – wszystkie SMSy nadal przychodzą na niego (oczywiście do momentu zastrzeżenia karty SIM). Ponadto użytkownicy często ustawiają w tego typu systemach pewne urządzania za zaufane – oznacza to, że dostęp z ich wykorzystaniem nie będzie wymagał wprowadzania takiego jednorazowego kodu. W każdej z przytoczonych sytuacji użytkownik zostaje pozbawiony ochrony i dostępu do swoich kont.

W świetle przytoczonych powyżej informacji, biorąc jednocześnie pod uwagę zachodzące zmiany w czasie spędzanym z różnymi urządzeniami mobilnymi, należy zwrócić uwagę na budujące się zagrożenia, jakie przynosi społeczeństwu ta wygodna zmiana. Mowa tutaj przede wszystkim o zagrożeniach w strefie bezpieczeństwa zarówno danych, jak i prywatności użytkowników. W takich właśnie dwóch aspektach będziemy rozumieć *„bezpieczeństwo"* w dalszej części pracy:

a) po pierwsze w aspekcie tzw. „tożsamości elektronicznej" użytkownika – czyli przetransferowanej tożsamości w sferę „elektronicznej rzeczywistości", co oferuje w konsekwencji znakomite możliwości funkcjonalne (np. nasze istnienie w sieci na portalach społecznościowych, gdzie uzupełniamy osobiste profile, często o bardzo szczegółowe, a czasem nawet dyskretne dane, posiadając jednocześnie możliwość dalszego uzupełniania informacji osobistych oraz wyrażania swoich opinii)
b) po drugie, w aspekcie danych *sensu stricte* – które są przechowywane na urządzeniu mobilnym lub w zsynchronizowanej z naszym kontem chmurze.

Sytuacja bezpieczeństwa naszych danych staje się tym bardziej poważna, gdy uświadamiamy sobie sposób, w jaki aplikacje mobilne są zbudowane, jak wygląda ich struktura, czy też oferowane przez nie mechanizmy bezpieczeństwa. Niniejszy raport stanowi znaczące rozszerzenie pracy naukowej [11] przyjętej do publikacji i prezentacji podczas międzynarodowej konferencji **FTC 2016 – Future Technologies Conference 2016** odbywającej się w San Francisco, USA.


**Rysunek 3** – Przykłady najpopularniejszych sposobów odblokowywania urządzenia mobilnego. Źródło: http://www.prophethacker.com/

## 1.1 Motywacja

Przytoczone wzorce zachowań użytkowników wskazują jednoznacznie na brak świadomości o konsekwencjach wynikających z przechwycenia dostępu do urządzenia mobilnego przez osoby trzecie. Okazuje się, że coraz więcej kradzieży urządzeń mobilnych nie jest powodowane chęcią pozyskania samego urządzenia (tj. tabletu czy telefonu), a właśnie tożsamości i danych użytkownika oraz dalszych możliwości nadużyć wynikających z ich użycia [7][8].

Naszym celem jest uczulenie użytkowników na kwestie bezpieczeństwa ich danych, tożsamości oraz prywatności, związanych z wykorzystywaniem urządzeń mobilnych na szeroką skalę. Pragniemy wskazać najczęstsze grzechy użytkowników, a także zaproponować alternatywne rozwiązania zapewniające pewien poziom bezpieczeństwa, który jednocześnie uwzględnia ergonomię rozwiązania. W naszej opinii systemy oparte o biometrię łączą te dwa aspekty, stąd chcemy poddać je badaniom w różnych konfiguracjach (tj. różne biometrie w zastosowaniach mieszanych) z uwzględnieniem opinii użytkowników. Dużą wartością dodaną opracowania jest również zestaw rekomendacji wraz z właściwościami czy parametrami systemów zabezpieczeń w urządzeniach mobilnych. Są to rozwiązania nastawione na realne problemy odbiorców, bowiem poznanie przekrojowych opinii użytkowników na temat różnych funkcjonalności telefonów (wliczając w to ich nawyki i sposoby zachowań w różnych okolicznościach) pozwoliło jednocześnie uniknąć błędów czy niedogodności, które przeszkadzają na co dzień użytkownikom. Sugestie te zostały także opracowane w adekwatnym przyporządkowaniu do wyróżnionych grup użytkowych. Na tej podstawie zostało zarekomendowanych kilka nowych podejść do kwestii bezpieczeństwa urządzeń mobilnych, wliczając w nie ciągłą weryfikację i udoskonalanie oraz wykorzystanie inżynierii biometrycznej.

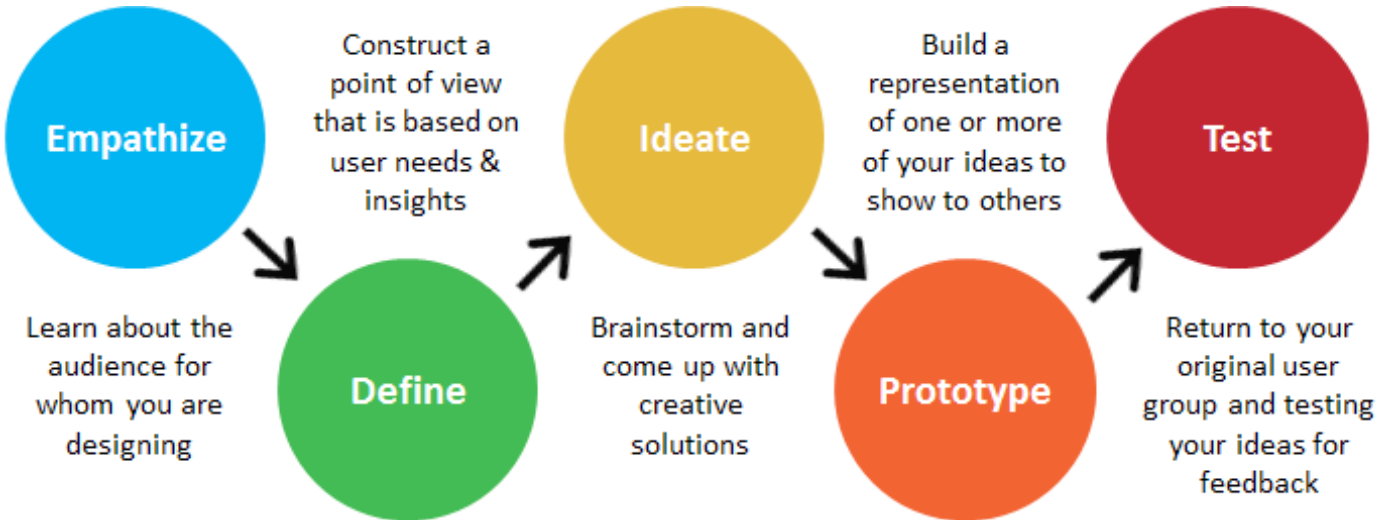
## 1.2 Dotychczasowe badania

Prace badawczo-rozwojowe w obszarze zabezpieczeń dostępu do urządzeń elektronicznych zaowocowały powstaniem poważnych systemów biomerycznych. Przykładami mogą być rozwiązania **Touch ID**[1] firmy *Apple* oparte o odcisk linii papilarnych czy **FastAcces** firmy *Sensible Vision*[2] oparte o biometrię twarzy użytkownika. Niedawno Apple wprowadził również technologię dotyku trójwymiarowego **3D Touch** umożliwiającą nowe zastosowania ekranu dotykowego (dzięki mierzeniu siły nacisku), również w kontekście biometrii dotyku. Konkurencyjne rozwiązania jedynie symulują dotyk trójwymiarowy.
Kwestiami bezpieczeństwa urządzeń mobilnych interesowali się również naukowcy. Autorzy pracy [1] pokazali, że za pomocą analizy sposobu korzystania z ekranu dotykowego (wykorzystanie pięciu ruchów) można ze skutecznością 80% rozpoznać konkretnych użytkowników z niezbyt dużego zbioru (do 5 osób). Jest to potwierdzenie, że behawioralna biometria *keystrokingu* (sposobu pisania na klawiaturze) przekłada się na ekrany dotykowe. W pracy [2] można przeczytać o porównaniu mechanizmów dostępowych do telefonu z wykorzystaniem głosu, biometrii twarzy i gestów oraz tradycyjnego hasła. Okazuje się, że niejednokrotnie rozwiązanie biometryczne wymagało od użytkownika mniej czasu niż wpisywanie hasła. Pojawiały się oczywiście czasami błędy klasyfikacji **FAR (False Acceptance Rate)** i **FRR (False Rejection Rate)**, jednakże ostateczna ocena użyteczności przytoczonych systemów (odsetek badanych wskazujących daną technologię za użyteczną) została zakwalifikowana na poziomie 78% (hasło), 66% (głos), 75%(twarz), 77% (gesty). Daje nam to istotną informację, że rozwiązania biometryczne są akceptowalne przez użytkowników, a ich ergonomia nie odbiega znacząco od przyjętych standardów. Bardzo ciekawe wyniki w kwestii wykorzystania dotyku wielopunktowego uzyskali autorzy publikacji [3]. Opracowali oni technikę autoryzacji użytkowników w oparciu o złożony model gestów wykorzystujących wszystkie pięć palców dłoni. W efekcie badań osiągnęli skuteczność 90% poprawnie zidentyfikowanych użytkowników. Praca wykazuje, że popularne rozwiązania polegające na odwzorowaniu wymyślonego przez użytkownika kształtu nie wykorzystują w pełni możliwości ekranu dotykowego i biometrii dotyku. Interesującą analizę porównawczą wykorzystania *touchpada* na podobnej zasadzie jak ekranu dotykowego przeprowadzili badacze w pracy [4]. Okazuje się, że również zachowania biometryczne podczas korzystania z *touchpada* można skutecznie zastosować do autoryzacji użytkowników. Jedne z najciekawszych wyników są w pracy Christiana Holza z laboratoriów Yahoo [5]. Opracował on rozwiązanie wykorzystujące ekran pojemnościowy do autentykacji użytkowników telefonu m.in. za pośrednictwem ucha rozmówcy. Dokonuje on swoistego skanu ucha i innych części ciała za pomocą ekranu dotykowego z dokładnością 75–150 DPI (standardowe rozdzielczości używanych ekranów dotykowych) i na tej podstawie buduje profil biometryczny.
Przy zastosowaniach biometrii do celów zabezpieczania danych i dostępów do zasobów należy zwrócić szczególną uwagę na *testy żywotności* przedstawianych próbek, tak aby dane biometryczne nie mogły być wykorzystywane bez połączenia z ich żywym posiadaczem. Zagadnieniami z tego obszaru zajmowali się autorzy prac [12][13]. Wykazali oni szereg metod, które można zastosować do odróżnienia autentycznej próbki biometrycznej od jej podrobionej wersji (wliczając martwą próbkę).
Na podstawie przytoczonych powyżej badań można bezsprzecznie stwierdzić, że zastosowanie metod biometrycznych do celów zapewnienia bezpieczeństwa na mobilnych urządzeniach jest racjonalne. Co więcej, okazuje się, że ergonomia tych rozwiązań niejednokrotnie nie odstaje od standardowo stosowanych, zapewniając jednocześnie dużo skuteczniejszą ochronę i większy próg odporności na ataki.

1 https://support.apple.com/en-us/HT204587
2 http://www.sensiblevision.com/en-us/technology/overview.aspx

# 2 Badanie użytkowników

Przed przystąpieniem do fazy analizy sytuacji w obszarze technologii bezpieczeństwa urządzeń mobilnych przeprowadzono badania eksploracyjne rynku użytkowników urządzeń mobilnych z wykorzystaniem metodyki *Design Thinking*. Jest to metoda tworzenia innowacyjnych produktów i usług w oparciu o głębokie zrozumienie problemów i potrzeb użytkowników. Design Thinking to usystematyzowane podejście do procesu innowacji opracowanego na Uniwersytecie Stanforda w Kalifornii, a więcej na jej temat można znaleźć w pracy [10]. **Rysunek 4** przedstawia pierwszy cykl życia procesu tworzenia rozwiązania w oparciu o metodę DT. Aby projektowane rozwiązanie osiągnęło dojrzałość powinno przejść kilka cykli projektowych, podczas których dojdzie do weryfikacji podjętych decyzji i obranych kierunków pracy, a przede wszystkim zderzy się ono ze swoim finalnym odbiorcą – użytkownikiem. Głównym założeniem tej metody jest koncentracja na użytkowniku, bowiem to właśnie on ma przynieść odpowiedź na przewodnie pytania związane ze świadomością i podejściem do systemów zabezpieczania danych na urządzeniach mobilnych. Zgodnie z metodyką, na samym początku został powołany interdyscyplinarny zespół badawczy, który ze względu na różnorodne doświadczenie osób należących do niego, już na początku mógł spojrzeć na problem badawczy z wielu perspektyw. W związku z tym, zdywersyfikowana wiedza i doświadczenie osób z zespołu interdyscyplinarnego, pomogło stworzyć taki rodzaj kwestionariusza, który w jak największym stopniu pozwoliłby uzyskać odpowiedź na interesujące grupę badawczą pytania.




**Rysunek 4** – Etapy procesu Design Thinking. Źródło: http://www.irdg.ie/

## 2.1 Budowa kwestionariusza i jego podstawowe cechy

Kwestionariusz badania został skonstruowany w pierwszej fazie procesu, na który wskazuje Design Thinking – czyli w fazie empatyzacji. To właśnie na samym początku, wychodząc od naszego celu badań, próbujemy stworzyć taki kwestionariusz, który w jak największym stopniu odpowiadałby jego osiągnięciu. Należy jednak przy tym również pamiętać o regułach i wskazówkach dotyczących wywiadu w ramach procesu Design Thinking. Rzeczywiście, kwestionariusz ma swój pewien określony wcześniej schemat, jednak nie można zapominać o istocie wywiadu pogłębionego, podczas którego to właśnie największą wartość dodaną tworzy eksploracja potrzeb i obaw respondenta. Należy również zwrócić uwagę na aspekty behawioralne – czyli zachowania, gestykulację podczas udzielanych odpowiedzi oraz wiążące się z tym nierozerwalnie wyrażanie emocji chociażby poprzez ton głosu, prędkość mówienia, czy mimikę twarzy. Generalnie podczas trwania wywiadu o pogłębionej formie, należy przez cały czas pamiętać o czterech filarach, które mogą determinować cały bieg rozmowy:

- co mówi udzielający wywiadu,
- co myśli,
- co robi,
- oraz co odczuwa.

Powyższe aspekty powinny tak naprawdę stanowić ramy wywiadu, a kwestionariusz powinien być jedynie wskazówką dla

przeprowadzającego wywiad – bowiem to od jego percepcji, umiejętności dostrzegania detalu oraz umiejętnie zadanych pytań zależy przebieg rozmowy, a co za tym idzie wydobycie od respondenta wartościowych informacji. Cztery filary wywiadu, o których mowa powyżej, oceniamy w ramach jednej płaszczyzny: naszej obserwacji oraz wnioskowania. Dlatego tak ważne jest, aby na kartce papieru z kwestionariuszem, na której się opieramy, czy też edytorze tekstu, bądź jakiejkolwiek innej formie – notować wszystkie nasze spostrzeżenia i od razu kategoryzować je jako nasze konkretne obserwacje (względem danego aspektu) bądź wnioski. Sposób przeprowadzania wywiadu jest zdecydowanie jednym z najważniejszych elementów całości procesu, to właśnie tutaj, mówiąc kolokwialnie, „wchodzimy w skórę użytkownika", próbujemy utożsamić się z jego potrzebami, poglądami, starając się niejako wyzbyć myśli o osiągnięciu naszego celu badań, bowiem to właśnie wypowiedzi respondentów będą stanowić podstawę do wyciągania wniosków, następnie określania potrzeb użytkowników, a w konsekwencji projektowania rozwiązań.

Badania eksploracyjne realizowane w ramach procesu Design Thinking opierają się na wywiadach pogłębionych, są to zdecydowanie badania jakościowe, wykonywane na niezbyt szerokim zbiorze ludzi. W naszym przypadku przebadaliśmy 60 użytkowników z przedziału wiekowego 14 – 84 lat, o zrównoważonej strukturze płciowej. Przygotowany został skrypt rozmowy z uczestnikiem badania, w którym szczególny nacisk położony został na dociekanie przyczyn zaistniałych stanów faktycznych, ich emocjonalne tło, zachowanie osoby poddanej badaniu oraz próbie zrozumienia podejmowanych decyzji, a przede wszystkim identyfikacji obaw i lęków użytkownika wobec różnych aspektów wykorzystywania urządzeń mobilnych. Wywiad składał się z 14 otwartych pytań, których celem była eksploracja obszaru użytkowania urządzeń mobilnych i poglądów dotyczących kwestii bezpieczeństwa. Kwestionariusz powstał z naciskiem na zbadanie obecnych doświadczeń użytkowników związanych z korzystaniem z telefonu oraz ich przyczyn, towarzyszącego im tła emocjonalnego wyrażającego się w zachowaniu respondentów oraz chęci zrozumienia motywacji podejmowania przez nich decyzji. Niemniej jednak przede wszystkim kwestionariusz miał wydobyć potrzeby, obawy czy niepokój użytkowników związany z różnymi aspektami korzystania z urządzeń mobilnych. Poszczególne elementy wywiadu dotyczyły:

- zakresu użytkowania urządzenia mobilnego, zarówno prywatnego jak i zawodowego;
- rodzaju danych i sposobie ich przechowywania na urządzeniu mobilnym;
- poczucia bezpieczeństwa wynikającego z użytkowania urządzenia mobilnego;
- doświadczeń i emocji związanych z utratą urządzenia (kradzieży, zgubienia, zniszczenia);
- identyfikacji największych obaw związanych z utratą urządzenia mobilnego;
- znajomości i wykorzystania form zabezpieczania urządzenia mobilnego;
- znajomości i stosunku do metod biometrycznych i ich zastosowania w stosunku do urządzeń mobilnych;
- idealnego wg. badanego systemu zabezpieczania urządzenia mobilnego.

## 2.2 Interpretacja wyników i dyskusja

Przeprowadzone badania pozwoliły zrozumieć szerzej problematykę użytkowników urządzeń mobilnych i wyszczególnić wśród nich *cztery główne persony*, łączące podobne cechy, potrzeby i obawy:

1. *Wygodnicka Wanda* (nie stosuje żadnych zabezpieczeń, najważniejszy jest szybki dostęp do telefonu/danych i łatwość obsługi, nie obawia się kradzieży i utraty danych [bo nie są one ważne], *nie stresuję się tym*). Potrzeba: niezakłócony niczym sposób użytkowania urządzenia mobilnego. Ból: dostępne rozwiązania wymagające ciągłego wprowadzania danych weryfikacyjnych, które przeszkadzają w łatwym, natychmiastowym dostępie do pożądanych treści/aplikacji.
2. *Nieufna Natalia* (nie wierzy w skuteczność i sens zabezpieczeń – *nie ma idealnego systemu zabezpieczeń*, obawia się inwigilacji oraz ingerencji zewnętrznej siły, absorbuje informacje z massmediów i przyjmuje je jako swoje poglądy). Potrzeba: możliwość odpowiedniego szkolenia/edukacji z zakresu działania/funkcjonowania systemów zabezpieczeń, dostarczenie na tyle przemyślanego i nieskomplikowanego systemu zabezpieczenia urządzeń mobilnych, które zapewniałoby personalną ochronę użytkownika, poczucie pewności o braku inwigilacji. Ból: brak wiary i chęci do głębszego poznania dostępnych rozwiązań w zakresie bezpieczeństwa danych i prywatności.
3. *Zagubiony Zbig* (nie rozumie o co chodzi [tak jak osoby starsze], nie wie co to backup, chmura itp., nie potrafi korzystać z podstawowych/popularnych aplikacji, *one-button clicker*). Potrzeba: przewodnik, edukator, który pomógłby w wyjaśnieniu podstawowych mechanizmów funkcjonowania urządzeń mobilnych, wyjaśniłby elementarne zagrożenia dotyczące naruszenia danych i prywatności oraz w prosty sposób pokazał, jak tych zagrożeń unikać. Ból: brak wiedzy na temat nowych technologii, a związku z tym uczucie ciągłego zagubienia w kwestii użytkowania urządzeń mobilnych.
4. *Obawiający się Olek* (użytkownik o dużej świadomości i sporej wiedzy z zakresu technologii, *IT Guy*, obawia się utraty danych, inwigilacji itp., stosuje zabezpieczenia, szyfruje dane, foldery prywatne, persona podzielona na dwie kategorie: świadomie nie przetrzymuje w telefonie danych, które może stracić; bo obawia się ich utraty / wycieku bądź stosuje zabezpieczenie, ponieważ obawia się utraty danych). Potrzeba: jak najlepsza możliwa ochrona danych na urządzeniach mobilnych. Ból: obawa niedostatecznego zabezpieczenia danych, poprzez co możliwy byłby wyciek danych, coraz to nowe, udoskonalone sposoby łamania zabezpieczeń i ustawień prywatności celem dostania się do osobistych danych.

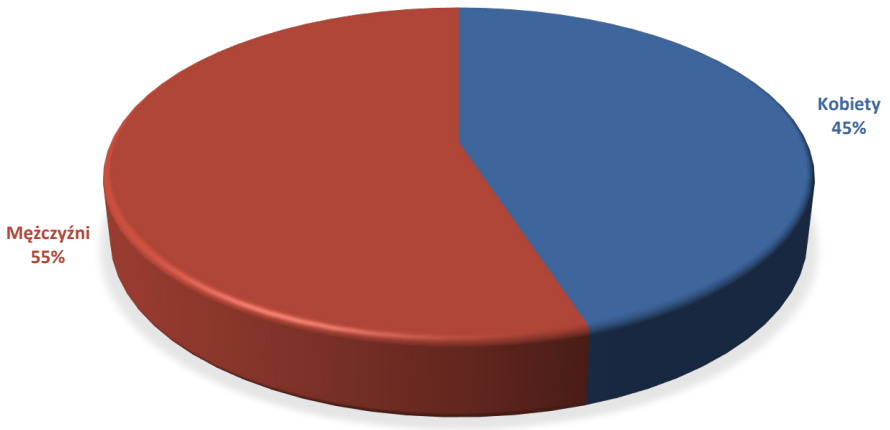
Należy jednak podkreślić, iż wyróżnione *persony* stanowią jednak swojego rodzaju ujednolicenie. Trudno bowiem o pełne utożsamienie danego użytkownika z konkretną grupą (chociaż takie przypadki miały miejsce). Dlatego przy szczegółowej analizie danych, każdy wywiad był brany pod uwagę indywidualnie. W przypadku, gdy dana osoba przejawiała najwięcej cech typowych dla danej persony – zostawała kwalifikowana właśnie do tej grupy. W dalszej części tej sekcji zaprezentujemy uzyskane przez nas wyniki badań, w tym liczne obserwacje zachowań użytkowników i ich uzasadnienia, jak również sposoby podejścia do kwestii użytkowania urządzeń mobilnych.
W zdecydowanej większości wypadków widać brak edukacji użytkowników w obszarze technologii bezpieczeństwa i zagrożeń wynikających z ryzykownych zachowań oraz braku stosowania mechanizmów ochrony. W odpowiedziach respondentów pojawiają się liczne opinie stereotypowe dotyczące technologii biometrycznych, istnieje silna obawa wobec utraty prywatności, inwigilacji, wejścia w posiadanie zbyt osobistych danych. Część opinii jest zaczerpnięta wręcz bezpośrednio z wizerunku biometrii wykreowanej w popkulturze czy kulturze masowej *science-fiction* włączając w to obawy przed próbami ekstrakcji organów celem uzyskania dostępu przez atakujących.
Osoby, które posiadają telefony na abonament obawiają się, że po utracie telefonu ktoś będzie z niego korzystał na ich koszt. Pozostali użytkownicy telefonów martwią się o to, że w przypadku kradzieży ktoś może wziąć na nich kredyt lub o inne sytuacje związane z tym, że kradzież telefonu pociągnie ich do dodatkowych kosztów. Użytkownicy telefonów, z którymi przeprowadzane były wywiady posiadają swoje karty SIM od wielu lat, obawiają się więc o stratę swojego numeru, ale również o stratę kontaktów, które były zbierane latami. Respondenci chcieliby bardziej zabezpieczać się przed kradzieżą telefonu, ale z drugiej strony nie chcą, aby zabezpieczenia dotyczyły wszystkich. Zależy im na takich rozwiązaniach, które będą uwzględniać zaufane osoby (takie jak członkowie rodziny) oraz sytuacje wyjątkowe, np. wypadki.

Z przeprowadzonych przez nas badań wynika, że duża część użytkowników potrzebuje autorytetu w obszarze urządzeń mobilnych: jeśli otrzymają rekomendację dotyczącą użycia bądź nie pewnych funkcjonalności bądź aplikacji to się do niej zastosują. W takim wypadku chętnie skorzystają z nowych możliwości i przetestują nieznane dotąd opcje. Pokłosiem powyższego jest to, że znacząca grupa badanych korzysta jedynie z fabrycznych ustawień urządzenia (w tym obszaru bezpieczeństwa i prywatności), bądź co najwyżej wykorzystują domyślne profile. Niezwykle dużą dozą nieufności badani wykazują się w stosunku do bankowości elektronicznej realizowanej za pomocą tabletu czy smartfona. Mają oni poczucie zagrożenia przejęcia konta bankowego i wykonywania przez osoby trzecie transakcji bez ich autoryzacji. Ponadto problematycznym jest zbyt mały ekran tych urządzeń, by w sposób wygodny wprowadzać dane logowania, a następnie transakcji finansowych. Sytuacja ta dotyczy również płatności z wykorzystaniem technologii *NFC (ang. Near Field Communication)*. Jest to powodem wciąż niezbyt wielkiej popularności płatności za pośrednictwem telefonu w porównaniu do płatności bezstykowej kartą bankomatową z możliwością *PayPass*. Pojawia się w tym obszarze również głos rozsądku, mówiący o korzystaniu jedynie z zaufanych sieci WiFi, nigdy publicznych, przy wykonywaniu czynności związanych z finansami.
Spora część osób uważa również, że zagrożenia nie dotyczą ich. Uważają się za osoby mniej ważne, twierdzą, że włamania do telefonów dotyczą jedynie dyrektorów. Użytkownicy w większości są zgodni co do jednej rzeczy. Uważają, że najlepsze rozwiązanie w zabezpieczeniu telefonów byłoby, gdyby telefon sam wiedział, że jest w rękach swojego właściciela, mówią: *urządzenie będzie zadawać pytania, które zna tylko właściciel* lub *urządzenie wyczuwałby go poprzez fale*. Jest to sytuacja, w której użytkownicy poproszeni o wymyślenie ich zdaniem najlepszego sposobu zabezpieczenia urządzenia mobilnego sięgają właśnie po rozwiązania biometryczne, do których wykazują tak dużą nieufność. Sprzeczność ta wynikać może z braku świadomości tego czym są biometryki i jaki może być zakres ich zastosowań.
Bardziej świadoma część osób używających mobilnych urządzeń reprezentuje pogląd, że połączenie telefonu czy tabletu z Internetem jest immanentnym zagrożeniem dla urządzenia. Podążając za tym poglądem uprawiają tak zwany *lurking*, który polega na zakładaniu fikcyjnych kont w różnych serwisach celem korzystania z funkcjonalności bez ujawniania żadnych informacji o sobie. Stosują również prostą zasadę: *skoro telefon, to komputer, a skoro komputer, to antywirus i antispyware*. Naturalnym jest dla nich potrzeba instalowania oprogramowania przeciwdziałającego złośliwym aktywnościom z sieci. Niestety, często z uwagi na obawę utraty danych, rezygnują oni z wielu funkcjonalności i przechowywania cennych informacji na urządzeniu mobilnym. Niezwykle istotą kwestią poruszaną przez tę grupę użytkowników był dostęp zdalny do urządzenia i możliwość kasowania danych, czy ich blokady.
Interesującym poglądem jest zabezpieczanie poszczególnych obszarów urządzenia mobilnego już po jego odblokowaniu. Polegać to miałoby na tym, że dostęp do poszczególnych aplikacji, folderów czy ustawiań wymagałby odrębnej weryfikacji. Możliwym rozwiązaniem byłoby również utworzenie tak zwanych prywatnych folderów, które zawierałyby wrażliwe dane.
Jednym z dominujących problemów okazał się back-up danych zgromadzonych na urządzeniu mobilnym. Wciąż w świadomości użytkowników pokutują obawy związane z przechowywaniem danych w sieci, nie wykazują oni zaufania do połączenia z chmurą. Obawiają się braku odpowiedzialności właścicieli chmur przed wyciekiem ich prywatnych danych. Kluczowym krokiem jest zapewnienie odbiorców usług o ich poziomie bezpieczeństwa, wyjaśnienia procedur kontrolnych i krytycznych. Rzetelne zapewnienie o zakresie odpowiedzialności dostawcy usług może być zasadniczym argumentem działającym na wyobraźnię, a w efekcie na decyzję użytkownika. Dodatkowo zapewnienie mechanizmów automatycznej synchronizacji i dbania w imieniu użytkownika o aktualizację danych powinno przekonać nawet najbardziej nieufne osoby.

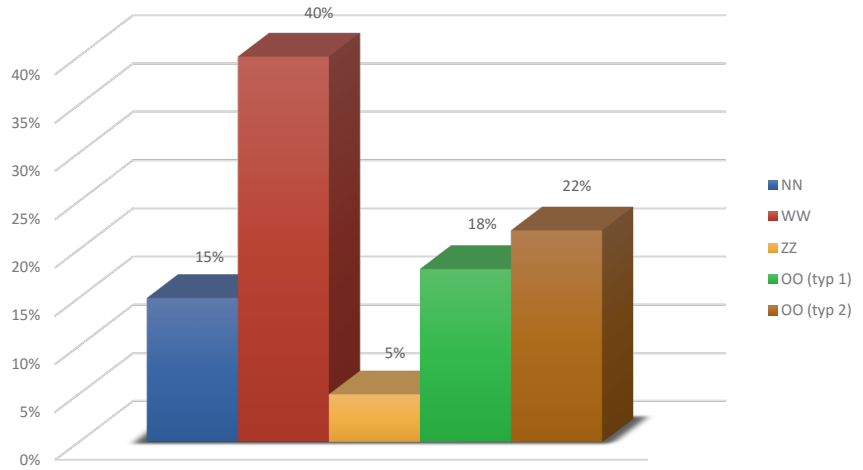
Z drugiej strony, wydaje się, że tak radykalne rozwiązanie jak udostępnienie operatorowi / dostawcy usług wszelkich danych w zamian za możliwość wykonania repliki telefonu i jego zawartości w postaci 1:1 satysfakcjonowałoby wielu użytkowników.
Chcąc przygotować odpowiedni system zabezpieczający, należy zaadresować odpowiednią grupę użytkowników, czyli odpowiedzieć na problemy konkretnej frakcji reprezentowanej przez persony. Próby zainteresowania osób o profilu *Wygodnickiej Wandy* czy *Zagubionego Zbiga* będą wymagały olbrzymich nakładów, zarówno finansowych jak i edukacyjnych. Stąd w pierwszej kolejności zdecydowaliśmy się na przygotowanie rozwiązań mogących zaspokoić potrzeby użytkowników o profilu *Nieufnej Natalii* i *Obawiającego się Olka*. Upatrujemy w nich najsilniejszej potrzeby bezpieczeństwa i ochrony danych oraz widzimy potencjał do dotarcia z odpowiednią informacją i rozwiązaniem, które może ich przekonać.

## 2.3 Statystyczne ujęcie zebranych danych

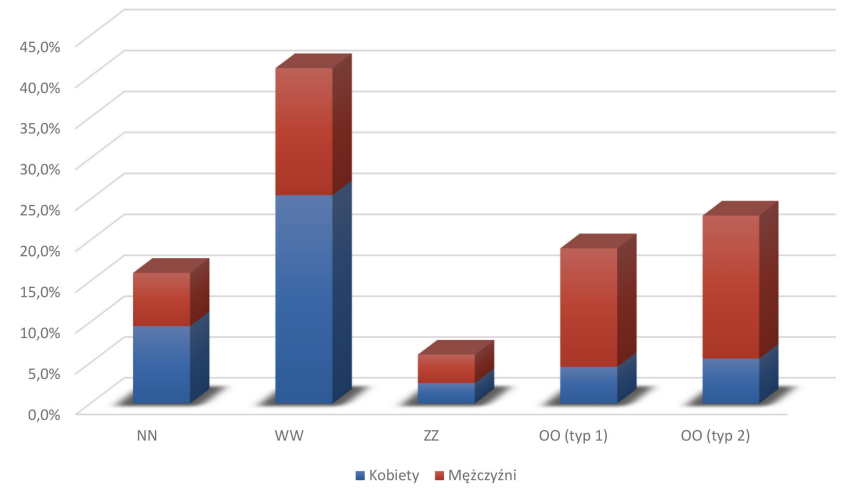
W dalszej części pracy zostaną zaprezentowane dane zebrane podczas wywiadów w ujęciu ilościowym. Przedstawione zestawienia stanowią jedynie część wywiadu – nie sposób bowiem ująć wszystkich zależności w postaci graficznej, niemniej jednak zostały zaprezentowane te, które najlepiej obrazują cel badań.
W badaniu wzięło udział 60 osób stanowiących próbę badawczą, w tym 33 mężczyzn oraz 27 kobiet w wieku od 14 do 84 lat – **Rysunek 5**.
Wszyscy respondenci zostali skategoryzowani i przydzieleni do wymienionych już wcześniej grup użytkowych – **Rysunek 6**. Statystycznie najwięcej wywiadów przeprowadzono z osobami o cechach charakterystycznych dla persony *Wygodnicka Wanda* – prawie połowa respondentów (24 osoby) przejawiała takie właśnie nastawienie. Już ta podstawowa kategoryzacja, w kontekście przytoczonego wcześniej opisu tej właśnie grupy użytkowej wskazuje na sceptyczny stosunek względem chociażby zabezpieczeń telefonu. Najmniej z kolei można było wyróżnić osób, które zaliczają się do grupy typu *Zagubiony Zbig*. Liczba osób zaliczających się do grupy użytkowników świadomych podzieliła się mniej więcej równo między dwie wyróżnione kategorie.
Przy dokonaniu podziału na grupy użytkowe z uwzględnieniem płci (**Rysunek 7**), można zauważyć, że większość kobiet buduje persony: *Wygodnicka Wanda* oraz *Nieufna Natalia*, natomiast okazuje się, że mężczyźni stanowią zdecydowaną większość uświadomionych




**Rysunek 5** – Udział kobiet i mężczyzn w badaniu




**Rysunek 6** – Procent osób przyporządkowanych do stworzonych kategorii użytkowników

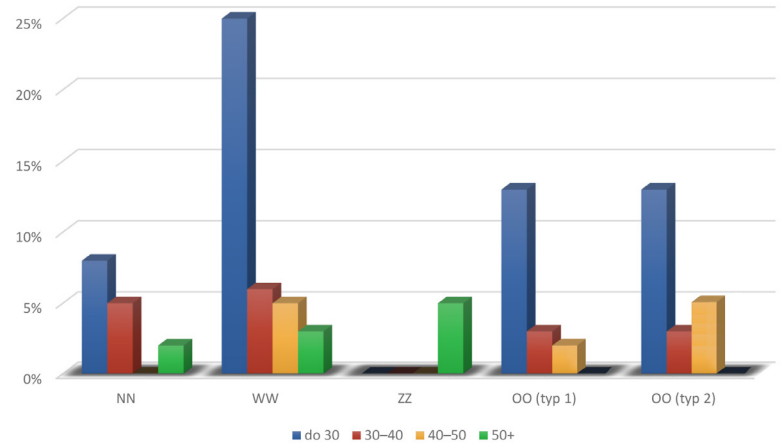



**Rysunek 7** – Udział kobiet i mężczyzn w poszczególnych kategoriach użytkowników

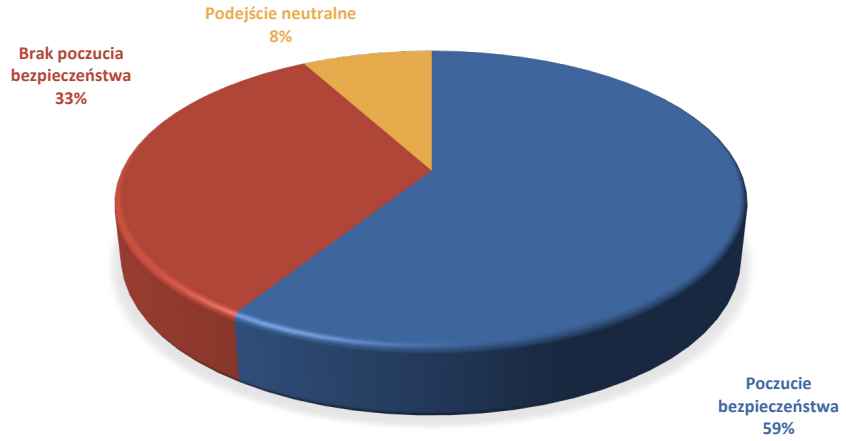
użytkowników, którzy dbają o bezpieczeństwo danych przechowywanych na swoich urządzeniach. Nasuwa się w związku z tym wniosek, mówiący o tym, iż większy nacisk na obszar edukacji w zakresie świadomego użytkowania urządzeń mobilnych należy kierować w stronę kobiet.

Użytkownicy zostali również podzieleni na cztery kategorie wiekowe. Pierwszą jest grupa do lat 30, następnie grupa wiekowa od 30 do 40 lat, 40 – 50 oraz powyżej 50 roku życia – **Rysunek 8**. Dzięki podziałowi grup użytkowników ze względu na grupy wiekowe możemy zauważyć, iż osoby młode (do 30 roku życia) stanowią większość w grupach: *Nieufna Natalia*, *Wygodnicka Wanda*, oraz dwóch typów *Obawiającego się Olka*. Zestawiając te dane z wykresem zaprezentowanym powyżej, można wywnioskować, że młode kobiety w wieku do 30 lat przejawiają stosunek ambiwalentny względem bezpieczeństwa użytkowania urządzeń mobilnych. Z kolei młodzi mężczyźni przede wszystkim tworzą grupę użytkowników świadomych. Ciekawym jest fakt, iż 50% osób z kategorii wiekowej 50+ przejawiają cechy *Zagubionego Zbiga*. Kategoria wiekowa 30–40 rozkłada się mniej więcej równomiernie po wszystkich grupach użytkowników. Powstaje pewien dyskurs w stosunku do osób w wieku 40–50, które przejawiają zarówno bardzo świadomą postawę, jak i zupełnie odwrotną, zaliczając się tym samym do persony typu *Wygodnicka Wanda*.

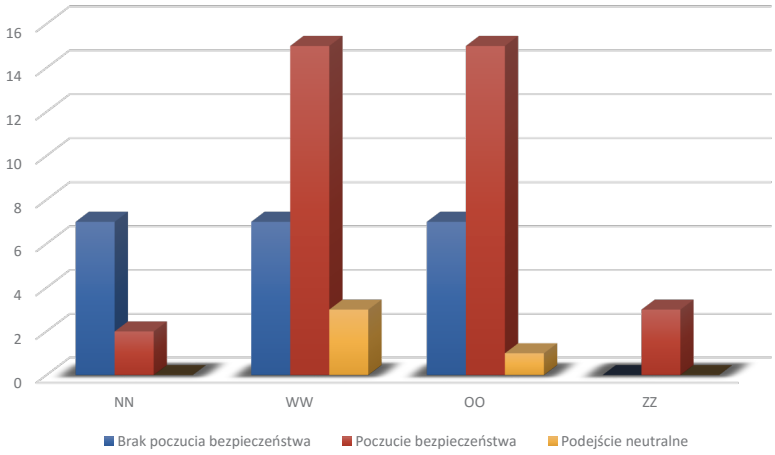
Jednym z najważniejszych celów było zbadanie poczucia bezpieczeństwa próby badawczej, związanego z użytkowaniem telefonów. Co ciekawe, większość respondentów zadeklarowała, że czuje się bezpiecznie używając na co dzień swojego telefonu. Nieco ponad 20% takiego poczucia nie ma, natomiast ok 6% deklaruje podejście neutralne (np. brak poczucia bezpieczeństwa, ale zupełna akceptacja tego stanu rzeczy, bądź brak zdania w tym temacie) – **Rysunek 9**. Ciekawi również fakt, że osoby deklarujące poczucie bezpieczeństwa związanego z użytkowaniem urządzeń mobilnych często w dalszej części wywiadu wyjawiały również brak posiadania jakichkolwiek systemów zabezpieczeń



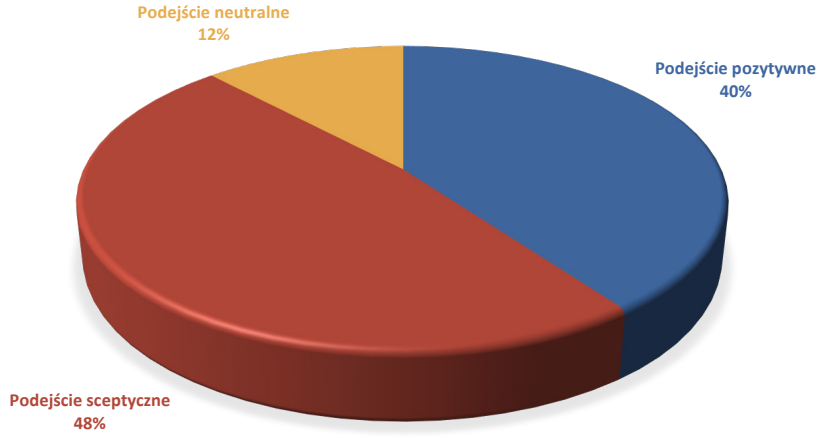

**Rysunek 8** – Podział grup użytkowników ze względu na grupy wiekowe



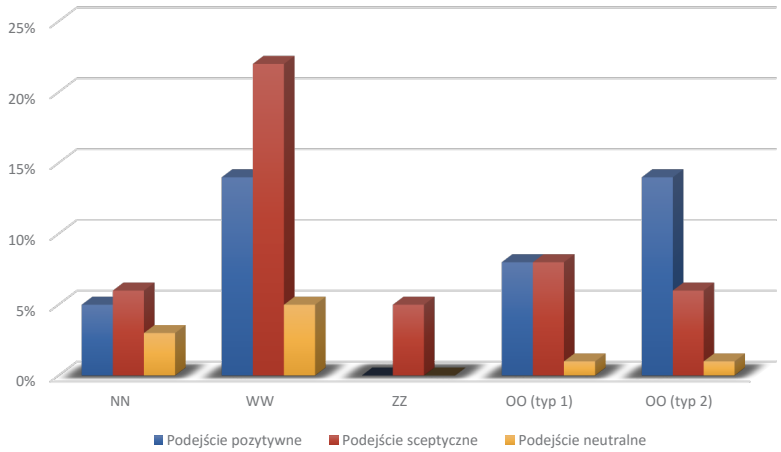

**Rysunek 9** – Poczucie bezpieczeństwa użytkowników związane z użytkowaniem telefonów



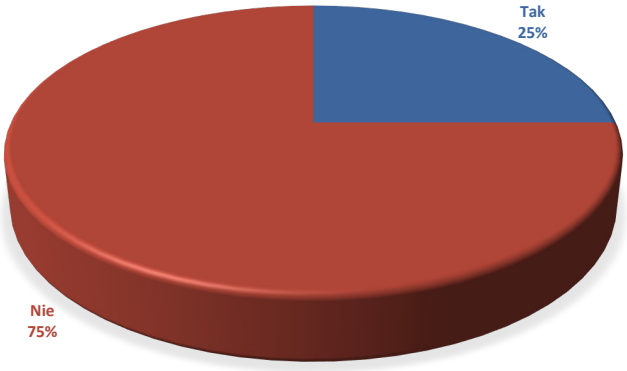

**Rysunek 10.** Poczucie bezpieczeństwa związane z użytkowaniem telefonów w rozbiciu na persony



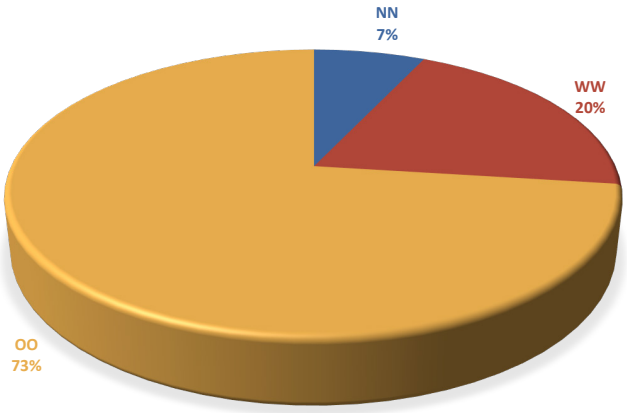

**Rysunek 11** – Nastawienie użytkowników do biometrycznych sposobów zabezpieczeń urządzeń mobilnych




**Rysunek 12** – Nastawienie użytkowników do biometrycznych sposobów zabezpieczeń z podziałem na grupy użytkowe




**Rysunek 13.** Wykonywanie operacji finansowych na urządzeniu mobilnym




**Rysunek 14.** Wykonywanie operacji finansowych na urządzeniu mobilnym w rozbiciu na persony

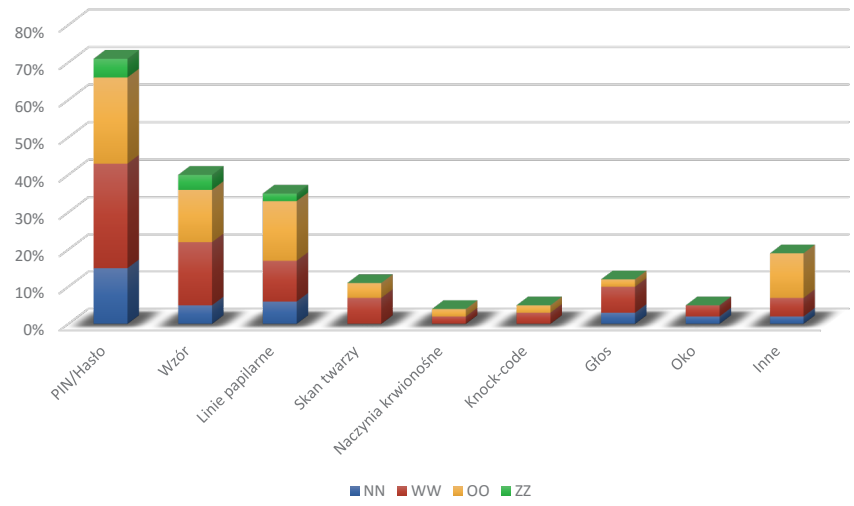
na swoich telefonach. Drugą frakcją osób wykazującą poczucie bezpieczeństwa byli użytkownicy bardzo świadomi, używający różnego rodzaju systemów zabezpieczających ich urządzenia. Jeśli chodzi o osoby nie mające takiego poczucia – często byli to respondenci, którzy i tak stosowali różne (mniej lub bardziej skomplikowane) systemy zabezpieczeń, jednak mimo wszystko nie mieli do nich zaufania i oceniali swój stan poczucia bezpieczeństwa jako bardzo niski.

Parząc na **Rysunek 10** widać, że zgodnie ze swoim profilem *Nieufna Natalia* przejawia raczej brak poczucia bezpieczeństwa związanego z użytkowaniem telefonu. *Wygodnicka Wanda*, z kolei czuje się bezpiecznie, co może wynikać m.in. z jej beztroskiego i nieprzemyślanego podejścia do bezpieczeństwa danych, bądź braku edukacji w tym zakresie. Co ciekawe, struktura odpowiedzi układa się podobnie w przypadku persony *Obawiający się Olek*, jednak ze względu na dużą świadomość tych osób oraz stosowanie zabezpieczeń odpowiedzi są z pewnością bardziej przemyślane i umotywowane nieco innymi przesłankami. Ciekawostką z kolei jest fakt, iż respondenci o bardzo niskiej świadomości i nie mający często pojęcia o działaniu podstawowych funkcji, czy aplikacji telefonu okazali jednoznacznie poczucie bezpieczeństwa związane z użytkowaniem telefonu.

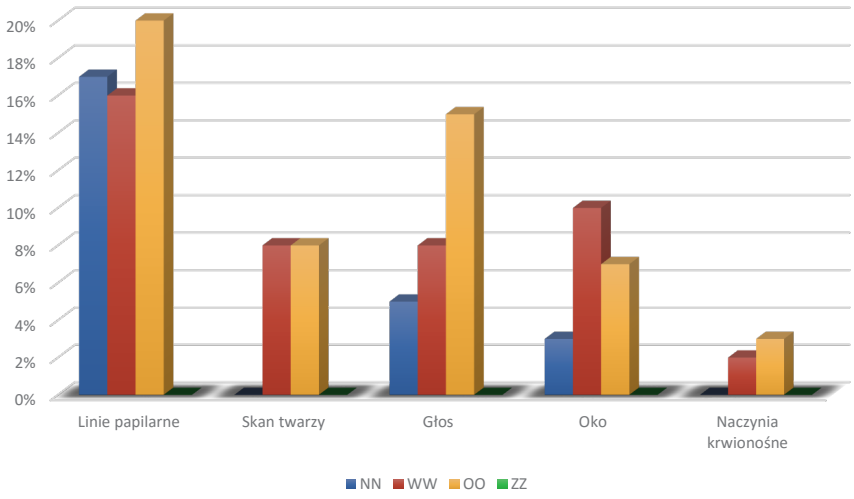
Wspomniany został już wcześniej temat podejścia użytkowników do biometrycznych rozwiązań zabezpieczania urządzeń mobilnych. Jak pokazuje **Rysunek 11**, większość respondentów otwarcie przejawia podejście sceptyczne lub neutralne do biometrycznych rozwiązań. Tylko 40% badanych jest pozytywnie nastawiona do stosowania tego typu rozwiązań na co dzień. Fakt ten skłania do głębokich przemyśleń w zakresie podstawowej edukacji użytkowników urządzeń mobilnych dotyczących uświadomienia zasad działania biometrii w kontekście zabezpieczeń technologicznych.

Nastawienie użytkowników do rozwiązań biometrycznych zostało również zmierzone z uwagi na przydział do poszczególnych grup użytkowych. Jak pokazuje **Rysunek 12**, najbardziej sceptycznie nastawione są osoby, które można utożsamić z *Wygodnicką Wandą*. Ciekawym jest również fakt, iż cała grupa osób zaliczających się do persony *Zagubionego Zbiga* nie ufa zabezpieczeniom wykorzystującym rozwiązania biometryczne. Podejście pozytywne można zauważyć zasadniczo w każdej grupie użytkowej, jednak sumarycznie najbardziej pozytywne podejście ma grupa użytkowników świadomych.

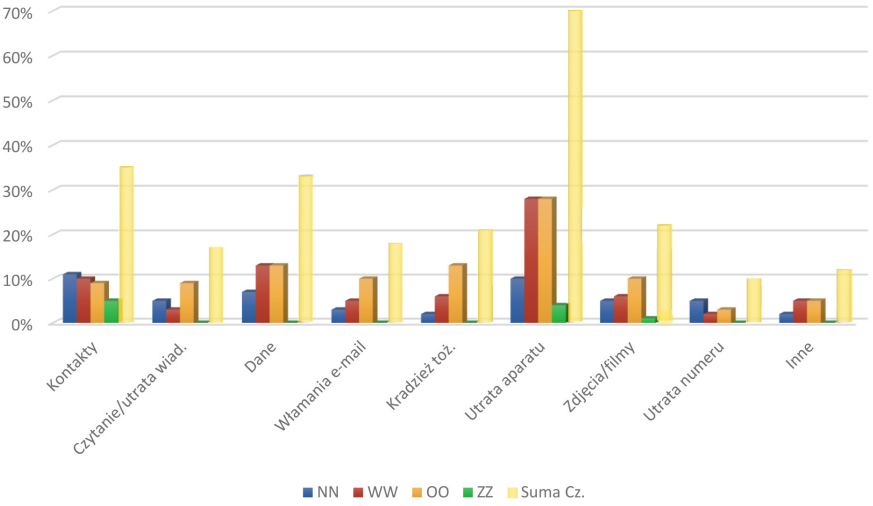
Ciekawym obszarem, który udało się wyeksplorować podczas badania było wykorzystanie urządzeń mobilnych do wykonywania operacji finansowych, w tym obsługi płatności online i korzystania z systemów bankowości elektronicznej. Spośród wszystkich przebadanych osób jedynie 20% korzysta w jakiejś formie z usług finansowych za pośrednictwem technologii mobilnych. Swoje obawy użytkownicy motywują faktem, że nie podoba im się sposób w jaki się to robi – *bo trudno się wprowadza wszystkie dane w telefonie*, uważają że usługi te są słabo zabezpieczone – *nie korzystam bo brak jest pełnych haseł, a PINy, do których nie mam zaufania*, podnoszą również




**Rysunek 15** – Rozpoznane formy zabezpieczeń w rozbiciu na persony




**Rysunek 16** – Znajomość biometrycznych formy zabezpieczeń w rozbiciu na persony




**Rysunek 17** – Obawy związane z utratą urządzenia mobilnego w rozbiciu na persony

kwestie wygody i ergonomii – *nie robię przelewów, bo jest to mało wygodne, telefon obsługuje tylko jeden ekran przeglądarki, a często potrzebuję zobaczyć nr faktury, jest mi to wygodniej zrobić na laptopie, a nie przeskakiwać pomiędzy widokami*. Ci, którzy decydują się na korzystanie z takich usług twierdzą, że częstokroć strona bankowości elektronicznej jest na tyle dobrze zrobiona, że nie potrzebują dedykowanej aplikacji. Ponadto motywują ten sposób faktem, że nie chcą przechowywać hasła na telefonie. Użytkownicy podkreślają, że realizują w ten sposób raczej małe transakcje. Zapytani o dedykowaną aplikację, odpowiadają – *tak, byłbym chętny, ale mój bank nie daje prostego dostępu, trzeba zrobić kilka rzeczy i to mnie zniechęca*. Strukturę użytkowników korzystających z operacji finansowych i bankowości elektronicznej na urządzeniach mobilnych ilustrują **Rysunek 13** oraz **Rysunek 14**.

Podczas badań chcieliśmy poznać również wiedzę i świadomość istnienia różnych form zabezpieczania urządzeń mobilnych i nowoczesnych technologii bezpieczeństwa – **Rysunek 15**. Do kategorii *inne* zaliczone są następujące, wymienione nielicznie przez użytkowników formy zabezpieczeń: antywirus, szyfrowanie, blokowanie aplikacji, folia zaciemniająca oraz zdalny dostęp. Użytkownicy zapytani o znane im biometryczne metody bezpieczeństwa wymienili jedynie pięć z nich (**Rysunek 16**), pomimo, że we wcześniejszym pytaniu pojawiło się ich więcej. Najwyraźniej nie do końca w świadomości użytkowników metody te funkcjonują jako *biometryczne*.

Ponadto chcieliśmy poznać obawy użytkowników związane z utratą urządzenia mobilnego, przy czym utratę zdefiniowaliśmy trojako: zniszczenie urządzenia, jego kradzież bądź zagubienie. Do kategorii *inne* zaliczone są następujące, wymienione nielicznie przez użytkowników obawy: włamanie do banku, utrata poziomu doświadczenia w grach, nuda, utrata dostępu do sieci – **Rysunek 17**.

# 3 Wnioski

Edukacja użytkownika jest jednym z ważniejszych elementów wdrażania nowych produktów i usług na rynek. Niejednokrotnie wymaga ona olbrzymich nakładów zarówno finansowych jak i organizacyjnych. Przeprowadzone badania wykazały jednoznacznie, że w obszarze technologii mobilnych, a w szczególności w aspekcie ich bezpieczeństwa istnieje olbrzymia luka świadomościowa użytkowników. Podczas przeprowadzania badań można zauważyć wiele poziomów świadomości korzystania z urządzeń mobilnych, a co za tym idzie zróżnicowanej wiedzy z zakresu funkcjonalności czy bezpieczeństwa użytkowania smartfonów i tabletów. W trakcie wywiadów badacze mieli okazję rozmawiać z ludźmi, którzy nie potrafili korzystać z funkcji, jakie dają smartfony, poza tymi najbardziej podstawowymi, w ogóle nie utożsamiali się w jakikolwiek sposób z zagrożeniami względem użytkowania tzw. „mobile devices". Jednocześnie grupa badawcza rozmawiała również z osobami o średniej, dużej oraz bardzo dużej świadomości użytkowania tychże urządzeń. Niestety takie osoby stanowiły mniejszość próby badawczej. Przeprowadzone badania wykazały brak podstawowej edukacji w zakresie bezpieczeństwa i prywatności danych na urządzeniach mobilnych oraz świadomości zagrożeń płynących z ryzykownych zachowań. Respondenci nie odczuwali również potrzeby autoryzacji w dostępach do poszczególnych aplikacji czy programów. Z drugiej strony, można było jednak zauważyć otwarte postawy użytkowników, którzy chętnie nabyliby taką wiedzę, jednak okazało się, że potrzebują do tego swojego rodzaju „autorytetu" – kogoś, kto w sposób jasny i klarowny wytłumaczy i przedstawi różne funkcjonalności telefonu, aplikacji, czy w końcu istoty systemów zabezpieczeń. W takim przypadku jest bardzo prawdopodobnym, że użytkownicy tacy zaczęliby najpierw testować, a potem korzystać z poszerzonych funkcjonalności telefonu, nieodkrytych przez nich do tej pory. Przy omawianiu wyników badań okazało się również, że większość udzielających wywiadu korzysta z domyślnych funkcji zabezpieczeń telefonu i nie myśli o tym, by je zmienić i dostosować do swoich potrzeb. Odpowiednia edukacja w tym zakresie mogłaby przynieść odpowiednie rezultaty.

Nawiązując więc do całego tematu edukacji użytkowników w zakresie świadomego korzystania z urządzeń mobilnych – na pewno ważną konkluzją jest fakt zapewnienia użytkowników o poziomie bezpieczeństwa danych usług – wyeliminowałoby to z pewnością obawy względem korzystania z usług tzw. „chmury". Wyjaśnienie kontroli i procedur krytycznych pomogłoby zrozumieć jak wygląda system zabezpieczania naszych danych. Jest to bardzo cenna informacja m.in. dla wspomnianej już wcześniej branży bankowości elektronicznej, która może wykorzystać te informacje do tworzenia swoich aplikacji. Kluczem jest tutaj zapewnienie użytkownika o poziomie bezpieczeństwa świadczonej usługi czy serwisu. Wiarygodne zapewnienie o odpowiedzialności usługodawcy może być niezbędnym elementem wpływającym ostatecznie na decyzję klienta. Dodatkowo, dostarczając mechanizmów automatycznej synchronizacji danych przy jednoczesnym dbaniu o informowanie użytkownika o wszystkich wprowadzanych usprawnieniach w sposób dla niego zrozumiały, powinno przekonać nawet tych najbardziej sceptycznych. Połączenie umiejętnej i przemyślanej edukacji użytkowników z gruntownym przemyśleniem i przepracowaniem technologicznym w kierunku bardziej użytkowym aplikacji związanych z bankowością mobilną powinno przynieść pozytywne rezultaty dla tego właśnie obszaru.

Wnioskiem płynącym z niniejszego opracowanie jest fakt, że niemożliwym jest stworzenie jednego uniwersalnego rozwiązania odpowiadającego na wszelkie potrzeby bezpieczeństwa użytkowników urządzeń mobilnych. Systemy bezpieczeństwa powinny być projektowane z myślą o określonej grupie odbiorców łączących podobne cechy, poglądy i potrzeby. Aby zidentyfikować te dane, należy przeprowadzić rzetelne badania rynku, które pozwolą wyeksplorować takie jego obszary, których na początku prac nie przewidywano. Niejednokrotnie okazuje się, że wybrane sposoby komunikacji nowych funkcjonalności nie trafiają do odbiorców i nie wzbudzają ich zaufania. Utrwalone stereotypy (jak w wypadku metod biometrycznych) biorą górę nad rozwojem technologii. W takich wypadkach należy postawić na aspekt ludzki i przeprowadzić użytkownika przez nieznaną dotąd drogę dając mu poczucie bezpieczeństwa. Nie jest to zadanie łatwe, ale bez wykonania tej pracy nie można liczyć na wysokie wskaźniki adaptacji nowych technologii bezpieczeństwa.

# Literatura


[1]. Sarah Martina Kolly, Roger Wattenhofer, and Samuel Welten. *A personal touch: recognizing users based on touch screen behavior*. In Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones (PhoneSense '12). ACM, New York, NY, USA, Article 1, 5 pages, 2012.

[2]. Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. *Biometric authentication on a mobile device: a study of user effort, error and task disruption*. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). ACM, New York, NY, USA, 159–168, 2012.

[3]. Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister, and Nasir Memon. *Biometric-rich gestures: a novel approach to authentication on multi-touch devices*. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12). ACM, New York, NY, USA, 977–986, 2012.

[4]. Saevanee, H.; Bhatarakosol, P. *User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device*. In Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on , vol., no., pp.82–86, 20–22 Grudzień 2008.

[5]. Christian Holz, Senaka Buthpitiya, and Marius Knaust. *Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts*. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 3011–3014, 2015.

[6]. EY Report – Insights on governance, risk and compliance series, *Mobile device security*. Understanding vulnerabilities and managing risks, Styczeń 2012, http://www.ey.com/Publication/vwLUAssets/EY_Mobile_security_devices/$FILE/EY_Mobile%20security%20devices.pdf [dostęp: 11.05.2016 r.].

[7]. *Confessions of a smartphone thief*, http://www.cnet.com/news/smartphone-thief/ [dostęp: 11.05.2016 r.].

[8]. *Phone Theft In America*, https://www.lookout.com/resources/reports/phone-theft-in-america [dostęp: 11.05.2016 r.].

[9]. Madzima, Kudakwashe; Moyo, Moses; Dzawo, Gilbert; Mbodila, Munienge. *Mobile Security Threats: A survey of how Mobile Devices Users are Protecting Themselves From new Form of Cybercrimes International Conference on Cyber Warfare and Security* (ICCWS): 178–187. Reading: Academic Conferences International Limited. 2015.

[10]. Tim Brown, *Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation,* HarperBusiness. 2009.

[11]. Wojciech Wodo and Lucjan Hanzlik, *Biometrics safety engineering in mobile devices,* Proceedings of FTC 2016 – Future Technologies Conference, San Francisco, USA, Grudzień 2016.

[12]. Martin Drahansky, *Liveness Detection in Biometrics*, Advanced Biometric Technologies, Intech 2011.

[13]. Andrzej Pacut, Adam Czajka, *Aliveness detection for iris biometrics*, 2006 IEEE International Carnahan Conference on Security Technology, 40th Annual Conference, 17–19 Wrzesień 2006, Lexington, Kentucky, IEEE.