Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 375 · 2018

Informatyka i Ekonometria 14

Edyta Abramek

Uniwersytet Ekonomiczny w Katowicach
Wydział Informatyki i Komunikacji
Katedra Informatyki
edyta.abramek@ue.katowice.pl

BEZPIECZEŃSTWO W SIECIACH SPOŁECZNOŚCIOWYCH – KLUCZOWE OBSZARY BADAWCZE

Streszczenie: W artykule omówiono kwestie bezpieczeństwa serwisów społecznościowych, które powinny zostać uwzględnione w formułowaniu strategii rozwoju firmy z wykorzystaniem sieci społecznościowych. Coraz więcej firm dostrzega popularność serwisów społecznościowych wśród ludzi, dlatego starają się one włączać je w swoją strategię rozwoju, aby wzmocnić przewagę konkurencyjną. Jednocześnie coraz więcej ludzi aktywnie korzysta z tego typu serwisów, zamieszczając informacje o sobie i o pracy, często nie zdając sobie sprawy z zagrożeń, jakie taka aktywność za sobą niesie. Celem poznawczym artykułu jest analiza znaczenia serwisów i sieci społecznościowych w biznesie. Część empiryczna ma pomóc zidentyfikować zagrożenia wynikające z komunikacji za pośrednictwem serwisów społecznościowych. Jej celem jest również identyfikacja kluczowych tematów i rekomendacji do dalszych badań.

Słowa kluczowe: bezpieczeństwo, serwis społecznościowy, sieć społecznościowa, zagrożenia.

JEL Classification: L1, L2, M1, O3.

Wprowadzenie

Portale internetowe to **serwisy internetowe wielotematyczne**, skierowane do szerokiego grona odbiorców, wymagające zaangażowania dużej grupy osób zarówno przy ich tworzeniu, jak i w zarządzaniu nimi. Oprócz serwisów wielotematycznych tworzone są także wortale, czyli **serwisy internetowe tematyczne**, skierowane do odbiorców zainteresowanych określonym tematem i wymagające zaangażowania grupy osób, podobnie jak w przypadku portali, ze względu na

potrzebę ich aktualizacji. Współcześnie w kręgu zainteresowania ludzi znajdują się **serwisy społecznościowe**. Są to serwisy internetowe, które oprócz firmy będącej ich właścicielem, są także współtworzone przez internautów. Od tradycyjnych serwisów internetowych odróżnia je to, że umożliwiają one budowanie sieci społecznych między użytkownikami, a dzięki temu – kontaktowanie się z innymi osobami i dzielenie się z nimi informacjami, zainteresowaniami, pomysłami, problemami itp. W tradycyjnych serwisach internetowych użytkownik był odbiorcą treści, a w serwisach społecznościowych może on pełnić podwójną rolę – być odbiorcą oraz twórcą treści. W serwisach tego rodzaju użytkownik tworzy i posiada własny profil użytkownika. Warto zauważyć, że współcześnie użytkownicy mogą posiadać tylko jeden profil, który może służyć do pracy w wielu różnych serwisach społecznościowych.

Artykuł koncentruje się na technicznych oraz społecznych aspektach bezpieczeństwa i ochrony danych w serwisach społecznościowych. Celem opracowania jest:

- analiza znaczenia serwisów i sieci społecznościowych dla biznesu;
- ukazanie zagrożeń dla firm, których pracownicy posiadają profile w serwisach społecznościowych i mogą tym samym narazić je na utratę dobrego wizerunku lub wyciek danych firmowych;
- przedstawienie zasad bezpiecznego korzystania z serwisów społecznościowych przez pracowników firmy;
- określenie rekomendacji dla firm budujących społeczność wokół swojej marki z wykorzystaniem serwisów społecznościowych;
- analiza aktywności badawczej naukowców w obszarze bezpieczeństwa sieci społecznościowych w latach 2010-2017;
- wyłonienie tematów istotnych dla dalszej eksploracji tematu.

Jako metody badawcze zastosowano: analizę literatury, analizy studiów przypadków firm budujących społeczność wokół swojej marki (Comarch, Frugo, Lenovo) oraz zaawansowane metody wyszukiwania.

1. Sieciowy model organizacji

Charakterystykę typowych modeli e-biznesu przedstawiono m.in. w pracach: [Afuach, Tucci, 2003; Nojszewski, 2007; www 1]. Modele klasyfikuje się według takich kryteriów, jak: funkcjonalność, nowatorstwo rozwiązania, złożoność, rynek działania, podmiot prowadzenia działalności i relacje z innymi podmiotami. Wśród modeli biznesu znajduje się także **model sieciowy** (*network business model*), tworzony przez społeczności internetowe.

Tradycyjne modele biznesu opierały się na hierarchii, natomiast współcześnie firmy zaczynają dostrzegać znaczenie sieci relacji społecznych. Dla podkreślenia zalet modelu sieciowego w tabeli 1 przedstawiono porównanie tradycyjnego, czyli hierarchicznego i sieciowego modelu organizacji.

Tabela 1. Porównanie modeli organizacji – hierarchicznego i sieciowego

Atrybut	Model hierarchiczny organizacji	Model sieciowy organizacji
Cel	wydajność produktywność	zwinność innowacyjność
Priorytet	sterowanie kontrola	zdolności adaptacyjne płynność
Działanie	przewidywalność	wyłanianie się (emergencja)
Wartość	referencje miejsce w hierarchii	wkład (np. umiejętności) równość
Elementy struktury	jednorodność upodabnianie się (konwergencja)	różnorodność rozbieżność (dywergencja)
Typ struktury	sztywna	sprężysta
Dążenie	perfekcja	poprawa, ulepszanie
Zakres	mała skala	duża skala (międzynarodowe sieci kontaktów)
Współpraca	kolaboracja	kooperacja
Odporność	mała	duża (redundantne połącznia, powtarzalność informacji, pośrednia komunikacja)

Źródło: Opracowano na podstawie: [Jarche, 2011].

Jeżeli firma dostrzega korzyści w sieciowym modelu prowadzenia biznesu, to powinna rozważyć zmiany w dotychczasowej strukturze organizacyjnej i wdrożyć narzędzia umożliwiające budowanie społeczności wokół własnej marki. Trudno jest wymienić wszystkie wartości, jakich firmom dostarcza model sieciowy. Dla przykładu, w tabeli 1 nie uwzględniono charakterystycznych dla modelu sieciowego metod generowania dochodu dzięki społeczności, czyli tzw. crowdfundingu. Wartość, jaką sieć generuje dla biznesu, jest szczególnie dostrzegalna w modelach aplikacji: gier społecznościowych, sprzedaży produktów lub usług czy też uwzględniających lokalizację użytkownika [LeBlanc, 2013, s. 46]. Na ich podstawie możliwe jest określenie zaangażowania, zainteresowań czy preferencji użytkowników i wykorzystanie tych informacji w celach biznesowych.

2. Znaczenie serwisów i sieci społecznościowych w biznesie

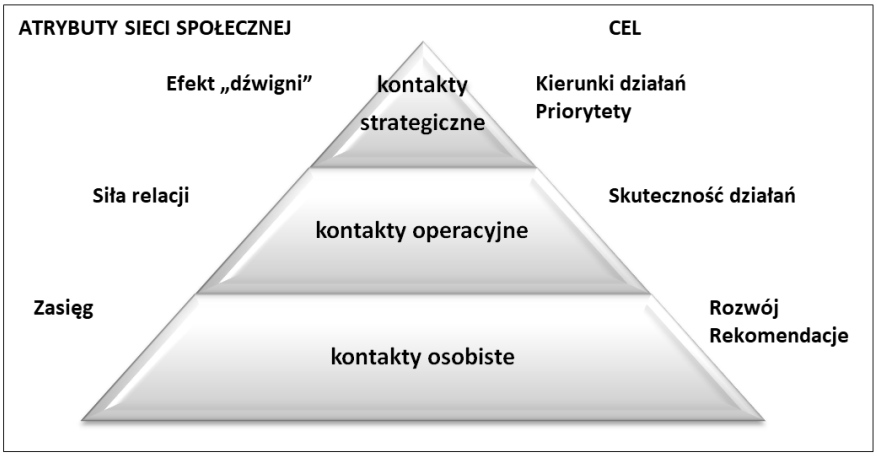
Aktualnie obowiązującym modelem koncepcji marketing-mix jest 4C (*Customer value*, *Cost*, *Convenience*, *Communication*), zaproponowany przez R. Lauterborna, zgodnie z którym przedsiębiorcy powinni myśleć o wygodzie zakupu produktów lub usług przez konsumenta i jego preferencjach. W związku

z tym najważniejszy w marketingu jest obecnie konsument i jego potrzeby. Promocja ustąpiła miejsca komunikacji. Wzrosło również znaczenie uczestnictwa oraz zaangażowania konsumentów w działania na rzecz firmy, czyli prosumpcji. Istotna stała się interaktywna, dwustronna komunikacja pomiędzy kupującymi i sprzedającymi. Z tego powodu firmy skoncentrowały swoją uwagę na serwisach społecznościowych i korzyściach, jakie dzięki nim mogą pozyskać (np. zdobycie przewagi konkurencyjnej).

Na podstawie danych z platformy NapoleonCat. [www 2] do zarządzania komunikacją marketingową w mediach społecznościowych w listopadzie 2018 r. z serwisu społecznościowego Facebook korzystało w Polsce ponad 16 mln użytkowników. Popularność serwisów społecznościowych wynika stąd, że stanowią one środowisko sprzyjające budowaniu kontaktów oraz komunikowaniu się. Obecnie powstają programy, za pomocą których ludzie mogą samodzielnie (bez pomocy programisty i konieczności kodowania) zbudować swój własny serwis społecznościowy. P. Frankowski i A. Juneja [2009] wymieniają dla przykładu takie narzędzia, jak: Elgg, Dolphin, Joomla!, Buddy Press czy SocialEngine.

Dzięki serwisom społecznościowym powstają społeczności internetowe, czyli grupy osób o wspólnych zainteresowaniach, które komunikując się ze sobą, dzielą się informacjami, doświadczeniem, zainteresowaniami i pasjami. Najczęściej są to społeczności: transakcyjne, hobbystyczne, związane relacjami opartymi na doświadczeniach życiowych (praca, podróże, sztuka, choroby i inne) czy też społeczności świata wirtualnego (świata fikcji) [Vossen, Hagemann, 2007, s. 80].

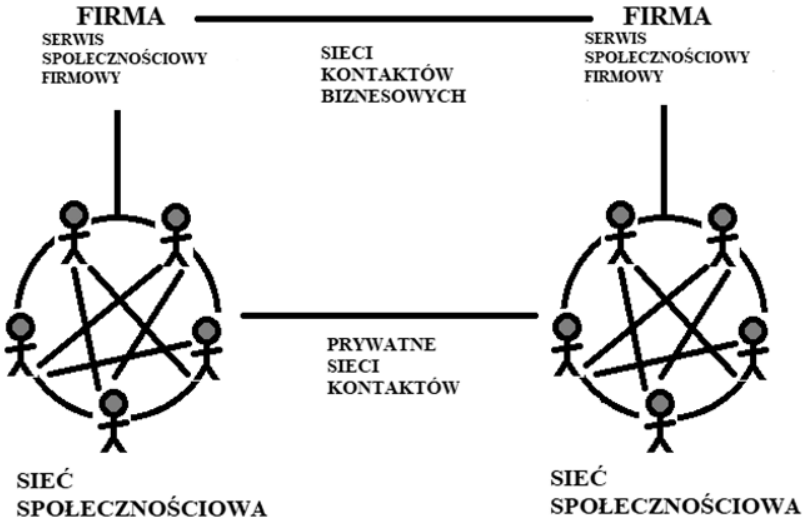
Serwisy społecznościowe zmieniają sposób, w jaki ludzie kontaktują się ze sobą. Sieci, jakie dzięki nim powstają, ułatwiają ludziom funkcjonowanie. Nawiązywanie czy też wzmacnianie relacji społecznych jest istotne ze względów osobistych, operacyjnych, ale także strategicznych. H. Ibarra i M. Hunter [2007] zwracają uwagę na to, że kontakty osobiste wpływają na rozwój osobisty pracownika, kontakty o charakterze operacyjnym pomagają pracownikom na szczeblu kierowniczym wywiązywać się ze swoich obowiązków, a kontakty o znaczeniu strategicznym pozwalają spojrzeć na biznes z innej perspektywy i tym samym lepiej dostrzec nowych interesariuszy czy też nowe trendy (rys. 1).



Rys. 1. Rodzaje relacji w sieciach społecznych

Źródło: Na podstawie: [Ibarra, Hunter, 2007, s. 185].

Rola kontaktów sieciowych jest szczególnie ważna w procesie zarządzania wiedzą [Vossen, Hagemann, 2007; Waszczuk, 2008], np. gdy w firmie trzeba odnaleźć pracowników o określonej wiedzy lub posiadających określone umiejętności i nawiązać z nimi współpracę. Jak podkreśla P. Waszczuk [2008, s. 16], „narzędzia społecznościowe dają możliwość wpływania na sposób funkcjonowania firmy nawet pracownikom niższych szczebli”.



Rys. 2. Idea budowania strategii firmy z udziałem społeczności

Zasięg sieci społecznościowych tworzonych z wykorzystaniem serwisów społecznościowych nie musi się ograniczać tylko i wyłącznie do firmy. Firmowe sieci społecznościowe mogą swoim zasięgiem obejmować relacje z klientami spoza firmy (rys. 2) – indywidualnymi czy instytucjonalnymi – i stanowić tym samym już nie tylko narzędzie do zarządzania wiedzą, ale także narzędzie do zarządzania relacjami z klientami.

2.1. Strategie społecznościowe

Dotychczas firmy realizowały strategie biznesowe w Internecie z wykorzystaniem serwisów internetowych (portale korporacyjne, wortale) czy stron internetowych. M. Piskorski [2012] określa je jako **strategie cyfrowe**. Współczesne firmy realizują także strategie biznesowe z udziałem serwisów społecznościowych i ich społeczności, tj. **strategie społecznościowe**. Nowym trendem jest już nie tylko realizowanie strategii biznesowych z udziałem społeczności własnych, ale również społeczności partnerów biznesowych. Działania w zakresie biznesu sieciowego (*network business*) polegają w tym przypadku na obopólnym rekomendowaniu przez firmy swoich usług wśród własnych społeczności. Korzyści, jakie z tego wynikają, to: nowe kontakty, większa widoczność (lepszy zasięg), bycie „na bieżąco", sprawniejsze rozwiązywanie problemów, łatwiejsze dzielenie się wiedzą i doświadczeniem oraz lepsze zaufanie i morale [Ward, 2017].

Z tego względu, że serwisy społecznościowe stają się coraz ważniejsze dla ludzi, firmy muszą weryfikować swoje strategie rozwoju i uwzględnić w nich miejsce dla strategii społecznościowych opartych na wykorzystaniu serwisów społecznościowych. M. Piskorski [2012, s. 111] pisze o czterech sposobach na budowanie strategii społecznościowej przez firmy:

- ułatwianie klientom nawiązywania relacji przy jednoczesnym redukowaniu dzięki temu kosztów,
- ułatwianie klientom nawiązywania relacji przy jednoczesnym zachęcaniu klientów do zwiększania wydatków,
- wzmacnianie relacji społecznych przy jednoczesnym redukowaniu dzięki temu kosztów,
- wzmacnianie relacji społecznych przy jednoczesnym zachęcaniu klientów do zwiększania wydatków.

Dzięki społeczności można rozwijać markę oraz pracowników, angażować pracowników, poszukiwać nowych i zatrudniać ich, wykorzystując przy tym informacje z serwisów społecznościowych (np. LinkedIn). Jak uważa M. Dutko [2010, s. 119-134], sposobów na sukces firmy w e-biznesie jest wiele. Te spo-

śród nich, które mogą być realizowane z udziałem społeczności, to np.: doskonalenie produktów i usług, dzielenie się pomysłami (wymyślanie nowych rzeczy), skanowanie otoczenia w celu znajdowania niszy na rynku, budowanie marki i wizerunku firmy, „chwalenie się" opiniami, dzielenie się pomysłami, zapewnianie dodatkowych świadczeń, udzielanie tzw. bonusów, informowanie o nowościach itp.

2.2. Przykłady firm współpracujących ze społecznością serwisu społecznościowego

Przykładem firmy, która buduje swoją strategię we współpracy ze społecznością serwisu społecznościowego, jest producent napojów owocowych – Frugo (posiada 813 tys. „polubień" na Facebooku, stan na listopad 2018 r.). Firma działa zgodnie z oczekiwaniami, życzeniami lub pomysłami jej fanów. Zdaniem dotychczasowego prezesa firmy konieczne jest ciągłe utrzymywanie zaangażowania społeczności utworzonej wokół marki (np. poprzez różnego rodzaju konkursy w serwisach społecznościowych), ale także aktywizowanie społeczności w realnym świecie [Włodarski, 2012].

Innym przykładem firm zaangażowanych w rozwój własnych społeczności, a przy tym korzystających z mechanizmów grywalizacji, są: firma informatyczna Lenovo (posiada ponad 6 mln „polubień" na Facebooku, a Lenovo Polska – ponad 400 tys., stan na listopad 2018 r.) i jej serwis społecznościowy LenovoZone (zawiera takie elementy, jak: Blog, Wideo, Produkty, Konkursy, Dyskusje, Aplikacje) oraz dostawca oprogramowania komputerowego – firma Comarch (ponad 3 tys. „polubień" na Facebooku, stan na listopad 2018 r.). Firma Comarch udostępniła swojej społeczności własny, autorski serwis społecznościowy Comarch ERP Społeczność [www 3]. Dzięki niemu społeczność ta może zadawać pytania i otrzymywać odpowiedzi, dzielić się pomysłami, rozwiązywać problemy, a także otrzymywać informacje o nowościach.

3. Bezpieczeństwo i ochrona danych z perspektywy serwisów społecznościowych

Pracownicy będący członkami społeczności serwisu społecznościowego mogą narazić na wyciek poufnych danych lub utratę dobrego wizerunku nie tylko siebie, ale także firmę, w której są zatrudnieni. Dlatego firmy korzystające w sposób świadomy z serwisów społecznościowych nie zapominają o „uzgodnieniu" ze swoimi pracownikami zasad, jakich powinni oni przestrzegać w związ-

ku z użytkowaniem serwisów społecznościowych. Opracowanie **dokumentu polityki bezpieczeństwa** polega na zdefiniowaniu zasad i norm, których powinni przestrzegać pracownicy, aby zapewnić firmie bezpieczeństwo i nie narazić jej na utratę dobrego imienia.

Kwestie bezpieczeństwa w firmach, związane m.in. z użytkowaniem serwisów społecznościowych, są bardzo ważne [Hiatt, Choi, 2016], nie tylko ze względu na regulacje o ochronie danych osobowych RODO, która weszła w życie 25 maja 2018 r., ale także w kontekście rozporządzenia ePrivacy, dotyczącego prywatności i łączności elektronicznej (e-mail, SMS, telefon, komunikator itp.), określanego jako rozszerzenie RODO.

Odnośnie do bezpieczeństwa w kontekście serwisów społecznościowych należy pamiętać o następujących kluczowych aspektach:

- technicznych, czyli o bezpieczeństwie gwarantowanym przez serwis społecznościowy i prawidłowej konfiguracji profilu użytkownika w serwisie,
- społecznych, czyli o zasadach użytkowania serwisu społecznościowego (o czym sami użytkownicy serwisów społecznościowych najczęściej zapominają).

Rozważając kwestie bezpieczeństwa gwarantowane przez serwis społecznościowy, należy mieć na uwadze udostępnianie danych użytkowników oraz relacje pomiędzy użytkownikami. J. LeBlanc [2013] rozróżnia dwa modele udostępniania danych użytkownika w serwisach społecznościowych. Ich porównanie przedstawiono w tabeli 2.

Tabela 2. Porównanie modeli udostępniania danych użytkownika w serwisach społecznościowych

Kryteria	Model opt-in	Model opt-out
Sposób udostępniania danych użytkowników	udostępnienie danych za zgodą użytkownika	udostępnianie danych ustawione jest domyślnie; użytkownik musi pamiętać o zmianie ustawień
Zalety rozwiązania	po stronie użytkownika	po stronie serwisu
Podmiot, który odnosi korzyści	użytkownik	bezpośrednio – serwis, pośrednio – użytkownik (im więcej informacji o użytkownikach, tym więcej interakcji między nimi)
Zmiana ustawień	modyfikacja ustawień przez użytkownika lub udzielenie odpowiedzi na pytanie	modyfikacja ustawień przez użytkownika
Ochrona	użytkownika	interesów serwisu

Źródło: Na podstawie: [LeBlanc, 2013, s. 63-64].

Oprócz tego, w jaki sposób skonfigurujemy profil użytkownika, ważny jest sposób użytkowania serwisu. Ludzie, którzy korzystają z serwisów społecznościowych, komunikują się z innymi na trzy różne sposoby. Są to: model śledzenia, model połączeń i model grupowy [LeBlanc, 2013, s. 65]. W **modelu śle-**

dzenia, charakterystycznym np. dla Twittera, komunikacja odbywa się w relacji jeden do wielu. Prywatność użytkownika jest zagrożona, gdyż wiadomość w kilka chwil może uzyskać globalny zasięg. Ponadto wiadomości są rozsyłane do osób, których często nie znamy. W tym modelu to użytkownik musi podjąć czynności mające na celu ochronę wysyłanych przez siebie komunikatów. W **modelu połączeń**, charakterystycznym np. dla Facebooka, dużo ważniejsze niż zasięg są relacje. Użytkownik kontaktuje się jednocześnie tylko z jednym użytkownikiem. Profil użytkownika jest tu dużo bardziej złożony i szczegółowy niż w modelu śledzenia. Wkrótce, zgodnie z polityką serwisu społecznościowego Facebook, relacje międzyludzkie i ich pogłębianie staną się jeszcze ważniejsze niż dotychczas. Przedmiotem zainteresowania firmy ma być także technologia blockchain oparta na kryptografii (z założenia odporna na cyberataki czy awarie systemów informatycznych). Problemem modelu połączeń jest poprawne skonfigurowanie profilu przez użytkownika. Trzecim modelem jest **model grupowy**, w którym użytkownik jednocześnie komunikuje się z wybraną grupą użytkowników. Model ten jest najbardziej złożony, poczynając od ustawień profilu, a kończąc na sposobach podziału na grupy i dlatego też – najbardziej wymagający spośród wymienionych pod względem bezpieczeństwa.

Rozważając bezpieczeństwo serwisów społecznościowych pod względem zasad ich użytkowania, należy mieć na uwadze przestrzeganie **zasady poufności**, **zasady integralności** i **zasady dostępności**. Poufność to ochrona gromadzonych w serwisach społecznościowych danych i informacji przed nieautoryzowanym dostępem. Dotyczy ona danych i informacji niejawnych oraz stanowiących tajemnicę. Integralność i dostępność, w porównaniu do poufności, odnoszą się zarówno do jawnych, jak i niejawnych danych oraz informacji. Nienaruszalność (integralność) oznacza ochronę przed zmodyfikowaniem lub zniszczeniem danych i informacji. Dostępność danych i informacji stanowi zapewnienie, aby dane lub informacje były dostępne na żądanie uprawnionemu (autoryzowanemu) do tego podmiotowi we właściwym miejscu i czasie.

3.1. Zagrożenia wynikające z użytkowania serwisów społecznościowych

Serwisy społecznościowe powodują, że ich użytkownicy są narażeni na zagrożenia:

- jako jednostka, np. na kradzież tożsamości, zainfekowanie profilu społecznościowego, podszywanie się pod konta, aktywne linki lub przyciski w oprogramowaniu, niechciane treści (spam) i inne;

– jako organizacja, np. na kradzież własności intelektualnej, tajemnicy handlowej, oszustwa, wycieku danych.

Skutkiem tego może być np. przypadkowe ujawnienie danych osobowych czy też chronionych danych firmowych. Dla firmy może się to zakończyć utratą renomy i wiarygodności, zaufania do marki, a co za tym idzie – utratą klientów. Propozycję kategoryzacji zagrożeń odnośnie do bezpieczeństwa i prywatności sieci społecznościowych przedstawili w swoich badaniach m.in. R. Kamatchi i K. Minocha [2015]. Ochrona tożsamości użytkownika jest współcześnie tak samo ważna, jak bezpieczeństwo sprzętu. Jak wspomniano we wprowadzeniu, problemy dotyczące bezpieczeństwa mogą leżeć nie tylko po stronie nieprawidłowego skonfigurowania oprogramowania (błędnie skonfigurowany profil, uzupełnienie i udostępnianie danych, które nie są niezbędne do funkcjonowania serwisu, błędy w oprogramowaniu), ale mogą też wynikać z niewłaściwego sposobu jego użytkowania (możliwość zakładania fałszywych profili, ujawnianie danych ze swojego życia prywatnego, a przy okazji także innych osób, naruszając przy tym dobra osobiste tych osób, niewylogowanie się z serwisu np. na komputerze w pracy lub na uczelni). Istotnym problemem związanym z utrzymaniem prywatności i bezpieczeństwa danych użytkownika jest też ich przetwarzanie w sposób nieautoryzowany przez osoby trzecie oraz udostępnianie ich w szczególności w postaci multimedialnej (zdjęcia, filmy, nagrania audio), czyli nieustrukturalizowanej. Do najistotniejszych i najczęściej wymienianych w literaturze zagrożeń związanych z sieciami społecznościowymi, oprócz kradzieży tożsamości (zakładania fikcyjnych profili), kradzieży własności intelektualnej, utraty danych wrażliwych, należy wykorzystywanie tych sieci jako miejsca ataku przez cyberprzestępców. Związane z tym rodzaje zagrożeń to, np.:

– phishing w serwisie społecznościowym (wyłudzanie danych polegające na podszywaniu się pod inną osobę lub instytucję w celu podania hasła i loginu),
– spear phishing (phishing ukierunkowany na konkretną grupę, np. pracowników danej firmy),
– whaling (jak wyżej, ale celem są w firmie tzw. grube ryby),
– malware (szkodliwe oprogramowanie), które zawiera wirusy i oprogramowanie szpiegowskie (spyware),
– watering hole („taktyka wodopoju", która polega na zaatakowaniu konkretnej grupy czy organizacji poprzez zaobserwowanie, z jakich stron najczęściej korzysta, a następnie na zainfekowaniu jej szkodliwym oprogramowaniem),
– ataki na urządzenia mobilne oraz urządzenia IoT (Internet of Things) [Kumar i in., 2013; Alguliyev, Aliguliyev, Yusifov, 2018].

Hakerzy zawsze wykorzystują najsłabsze ogniwo bezpieczeństwa, czyli ludzi. W związku z tym firmy stoją przed trzema głównymi wyzwaniami [Hekkala, Väyrynen, Wiander, 2012] będącymi konsekwencjami działań pracowników lub ich nieświadomości, wynikającymi z mieszania przez nich prywatnych i zawodowych ról oraz dotyczących komunikacji pomiędzy pracownikami, która nie jest kontrolowana przez firmę.

3.2. Zasady bezpiecznego korzystania z serwisów społecznościowych

Trudno jest nie dzielić się informacjami na swój temat, jeżeli chce się funkcjonować w społeczności. Użytkownicy serwisów społecznościowych muszą wyrazić zgodę na udostępnianie swoich danych, aby budowanie takich relacji w serwisie było w ogóle możliwe. Jeżeli użytkownicy rejestrują się w serwisie i udostępniają swoje dane oraz dodatkowo oprogramowanie może śledzić ich działania w serwisie, to z założenia interakcje między użytkownikami mogą być wówczas częstsze, wzrasta też skuteczność takiego serwisu oraz doskonalone są jego funkcjonalności. Jednocześnie udostępnienie danych przez użytkowników w serwisie nie pozostaje bez wpływu na ich bezpieczeństwo. Wielu użytkowników nie zmienia ustawień w zakresie zabezpieczeń sieci społecznościowych, co oznacza pozostawienie ogromnych ilości danych podatnych na działania przestępcze [Foltz, Newkirk, Schwager, 2016]. Ujawnienie przez użytkownika serwisu społecznościowego dodatkowych danych czy informacji nawet w sposób świadomy, również może pociągać za sobą poważne konsekwencje.

Pierwszym krokiem do zwiększenia bezpieczeństwa jest przeszkolenie pracowników i partnerów firmy. Należy pamiętać o tym, aby udostępniać w serwisie społecznościowym tyle danych, ile jest niezbędne, aby korzystając z niego nie zapominać o wylogowaniu się oraz stosować uwierzytelnianie wielopoziomowe, np. dwuetapowe (2FA, *two-factor authentication*). Użytkownicy mogą korzystać z oprogramowania antywirusowego, które blokuje dostęp do poufnych danych użytkownika oraz zapewnia ochronę w chmurze (np. Panda Cloud Antivirus). Pracodawcy mogą też korzystać z oprogramowania pozwalającego na kontrolowanie, z jakich serwisów ich pracownik korzysta w godzinach pracy lub na blokowanie dostępu do serwisów społecznościowych w godzinach pracy, zarówno na komputerach, jak i smartfonach (np. oprogramowanie Samsung KNOX – jedyne, jak do tej pory na rynku) lub tabletach służbowych. Blokowanie pracownikom dostępu do serwisów społecznościowych w godzinach pracy nie zagwarantuje poufności firmowych danych i informacji. Ważnym elementem

ochrony jest w związku z tym odpowiednia polityka bezpieczeństwa firmy [Banday, Mattoo, 2013].

Konieczne zatem wydaje się opracowanie wytycznych dla firm budujących społeczność wokół swojej marki z wykorzystaniem serwisów społecznościowych:

- aby **jako jednostka** ustrzec się przed udostępnianiem oraz upowszechnianiem firmowych danych i informacji, a w konsekwencji przed utratą tajemnicy służbowej, reputacji czy swojej renomy lub zaufania do marki; firmy powinny szkolić pracowników w tym zakresie, a pracownicy powinni mieć świadomość tego, czego im nie wolno robić lub jakich danych nie wolno im udostępniać;
- aby **jako organizacja** ustrzec się przed zagrożeniami wynikającymi z korzystania z oprogramowania społecznościowego, a zarazem przed spadkiem efektywności pracy spowodowanym korzystaniem z serwisów społecznościowych w godzinach pracy; firmy powinny opracowywać i uwzględniać w politykach bezpieczeństwa oraz odrębnych regulaminach zasady korzystania z serwisów społecznościowych przez pracowników.

4. Metodyka badawcza

Artykuł podzielono na dwie części. Przedmiotem rozważań pierwszej części, teoretycznej, jest bezpieczeństwo sieci społecznościowych. Natomiast w części drugiej, badawczej, zawarto wyniki badań mające zidentyfikować kluczowe tematy i rekomendacje dla dalszych badań nad bezpieczeństwem sieci społecznościowych. W ramach badań zaproponowano:

1. Przeprowadzenie analizy liczby publikacji dedykowanych pojęciu „bezpieczeństwo sieci społecznościowych" z wykorzystaniem wyszukiwarek wybranych katalogów bibliotecznych. Badanie to miało na celu ocenę dotychczasowego stanu analiz naukowych dotyczących tematu bezpieczeństwa serwisów społecznościowych w latach 2010-2017 i ukazanie frekwencyjności źródeł literaturowych.
2. Przeprowadzenie analizy hasła przedmiotowego „bezpieczeństwo sieci społecznościowych" przy pomocy internetowych wyszukiwarek kontekstowych. Badanie to miało na celu rozpoznanie związków frazeologicznych – powiązań hasła z innymi wyrazami lub inaczej, jego odniesień semantycznych, co pozwoliło na ukazanie kontekstu analizowanego pojęcia.

W związku z tym pytania badawcze sformułowano następująco:

RQ1. Czy występuje i jaki jest trend występowania frazy „social networking security" z perspektywy wyszukiwarek obecnych w katalogach bibliotecznych?

RQ2. W jakim kontekście najczęściej występuje analizowane pojęcie z perspektywy internetowych wyszukiwarek kontekstowych?

5. Wynik badania

Stosując metodę analizy bibliometrycznej liczby publikacji, prowadzonej wokół z góry założonego hasła przedmiotowego – frazy „social networking security" – oceniono częstotliwość jego występowania w literaturze przedmiotu. Badaniem objęto źródła literaturowe opublikowane w języku angielskim w latach 2010-2017. Wyszukiwanie frazy prowadzono z wykorzystaniem wyszukiwarek z polami wyboru wybranych katalogów bibliotecznych. Badanie pozwoliło określić wielkość zbioru (tabela 3) oraz przyrost publikacji (tabela 4).

Tabela 3. Liczba publikacji zawierających frazę „social networking security" w wybranych bazach bibliotecznych*

Baza biblioteczna	Pełnotekstowe publikacje recenzowane
EBSCOhost	191
ProQuest	7062
Scopus	34
SpringerLink	178697
Web of Science	3331
BazEkon	7
BazTech	1

* Przedział od 2010 r. do 2017 r.; pełne teksty recenzowane.

Źródło: Na podstawie analizy katalogów bibliotecznych (dostęp: marzec 2018).

Tabela 4. Przyrost publikacji zawierających frazę „social networking security" w bazach ProQuest i Scopus od 2010 r. do 2017 r.

Lata	2010	2011	2012	2013	2014	2015	2016	2017	Razem
Pełne teksty recenzowane – baza Scopus	**1**	**2**	**6**	**3**	**5**	**3**	**11**	**3**	**34**
Przyrost publikacji recenzowanych	–	1	4	–3	2	–2	8	–8	–
Pełne teksty recenzowane – baza ProQuest	**745**	**817**	**888**	**909**	**942**	**1047**	**1167**	**547**	**7062**
Przyrost publikacji recenzowanych	–	72	71	21	33	105	120	–620	–

Źródło: Na podstawie analizy katalogów bibliotecznych (dostęp: marzec 2018).

Liczba publikacji łącznie oraz w poszczególnych latach pozwala ocenić aktywność badawczą na danym polu, wyznaczyć linię trendu oraz prognozę na najbliższe lata. Pojęcie „social networking security" jest obecne w źródłach literaturowych. W latach 2010-2016 zaobserwowano rosnące zainteresowanie tematem, a w 2017 r. – widoczny spadek (RQ1). W bazie ProQuest, biorąc pod uwagę pełnotekstowe i recenzowane prace w latach 2000-2009, zostało zarejestrowanych 3938 rekordów, natomiast już w marcu 2018 r. liczba publikacji wynosiła 7098.

W celu analizy związków frazeologicznych pojęcia „social networking security" skorzystano z wyszukiwarek internetowych kontekstowych. Uzyskano następujące wyniki:

a) z wykorzystaniem wyszukiwarki Soovle, która wyświetla również podpowiedzi, sugestie związane z danym tematem (tabela 5),
b) z wykorzystaniem wyszukiwarki Answer The Public (tabela 6), która prezentuje wyniki wyszukiwania zarówno w sposób tekstowy, jak i graficzny.

Tabela 5. Wyniki wyszukiwania frazy „social networking security" z wykorzystaniem wyszukiwarki Soovle

Google	**Answers.com**
Social networking security Social networking security and privacy Social networking security awareness Social networking security awareness pdf Social networking security concerns Social networking security issues Social networking security issues pdf Social networking security risks Social networking security threats Social networking security tips	Are social networking antisocial Disadvantage of social networking Is bloging social networking Is social networking dangerous Is social networking useful Social networking sites Upcoming social networking site What drives social networking What is social networking Who uses social networking
WIKIPEDIA	**Bing**
Brak danych	Brak danych
YAHOO!	**YouTube**
Social networking security Social networking security and privacy Social networking security for teens Social networking security in the workplace Social networking security issues Social networking security risks Social networking security threat Social networking security threats Social networking security tips Social networking security tools	Social networking security
Amazon.com	
Brak danych	

Źródło: [www 4].

Tabela 6. Wyniki wyszukiwania frazy „social networking security" z wykorzystaniem wyszukiwarki Answer The Public

Answer The Public
social networking security risks
social networking security tips
social networking security issues pdf
social networking security awareness
social networking security
social networking security issues
social networking security threats
social networking security ppt
social networking security awareness ppt
social networking security issues ppt
social networking security problems
social networking security concerns
social networking security protection
social networking security flaws
social network security pdf
social network security and privacy
social network security research paper
social network security vulnerabilities
social network security tools
social network security project

Źródło: [www 5].

Wykorzystanie wyszukiwarek kontekstowych ułatwia wyłonienie luki badawczej w danym temacie. Na podstawie wyszukiwarki Soovle, siedmiu serwisów, z których ta wyszukiwarka korzysta, oraz wyszukiwarki Answer The Public można stwierdzić, że najczęściej wyszukiwanymi tematami były (RQ2):

a) bezpieczeństwo w sieciach społecznościowych (i prywatność),
b) zagrożenia bezpieczeństwa sieci społecznościowych,
c) problemy z bezpieczeństwem sieci społecznościowych,
d) porady dotyczące bezpieczeństwa sieci społecznościowych,
e) narzędzia i znajomość zabezpieczeń sieci społecznościowych,
f) zabezpieczanie sieci społecznościowych oraz błędy zabezpieczeń, luki w zabezpieczeniach,
g) świadomość w zakresie bezpieczeństwa sieci społecznościowych i obawy dotyczące ich zabezpieczeń,
h) projekty zabezpieczeń i dokumentacja związana z problematyką bezpieczeństwa w sieciach społecznościowych.

6. Wnioski

Wstępna analiza bibliometryczna publikacji na podstawie wybranych baz bibliotecznych pozwoliła ocenić ze względu na poszukiwaną frazę, czyli „social networking security", wielkość zbiorów publikacji, a także ich dynamikę. Z kolei

badanie związków frazeologicznych pojęć wpisywanych w wyszukiwarkach wyłoniło najbardziej istotne tematy w analizowanym obszarze badawczym. Otrzymane wyniki uzasadniają potrzebę rozwijania badań w tym obszarze. Należy podkreślić, że badania tego rodzaju nie są pozbawione ograniczeń. Ograniczeniem jest zasięg baz bibliotecznych i zawężenie do źródeł w języku angielskim. Jednakże już nawet wstępna ocena danych ilościowych uzyskanych na podstawie pełnotekstowych, recenzowanych oraz opublikowanych artykułów, pozwala ustalić stan rzeczy i jest niezbędna do dalszego prowadzenia badań zgodnie z metodyką systematycznego przeglądu literatury.

Podsumowanie

Tematyka bezpieczeństwa w serwisach społecznościowych czy też bezpieczeństwa widzianego z perspektywy sieci społecznościowych wymaga dalszych, pogłębionych badań zarówno w aspekcie teoretycznym, jak i praktycznym, m.in. po to, aby ich użytkownicy znali zagrożenia z nimi związane oraz sposoby dbania o bezpieczeństwo i ochronę danych osobowych czy danych firmowych. Zadaniem oprogramowania społecznościowego jest budowanie relacji. Jednakże korzystanie z serwisów społecznościowych przez pracowników firmy oznacza jednocześnie oddanie im kontroli nad przepływem informacji. Dlatego analizowana tematyka będzie dla badaczy coraz większym wyzwaniem ze względu na rosnącą liczbę zagrożeń z tym związanych. Blokowanie pracownikom dostępu do serwisów społecznościowych nie jest rozwiązaniem. Rozwijanie relacji z wykorzystaniem serwisów społecznościowych ma bowiem istotne znaczenie dla sukcesu w biznesie, dlatego muszą za tym podążać inne metody. Rozwiązaniem w zakresie bezpieczeństwa w sieciach społecznościowych powinny być: zabezpieczenia na poziomie serwisu społecznościowego (regulamin serwisu, ustawienia profilu, oprogramowanie antywirusowe), edukowanie pracowników w zakresie zasad bezpiecznego użytkowania (zakres podawanych danych i zasada adekwatności, zasady dodawania znajomych, udostępniania haseł, publikowania informacji, świadomość zagrożeń) oraz regulacje prawne i polityka bezpieczeństwa firmy w tym obszarze.

Literatura

Afuach A., Tucci Ch. (2003), *Internet Business Models and Strategies*, McGraw-Hill, Nowy Jork – Boston.

Alguliyev R., Aliguliyev R., Yusifov F. (2018), *Role of Social Networks in E-government: Risks and Security Threats*, "Online Journal of Communication and Media Technologies", Vol. 8(4), s. 363-376.

Banday M.T., Mattoo M. (2013), *Social Media in e-Governance: A Study with Special Reference to India*, "Social Networking", Vol. 2, s. 47-56.

Dutko M. (2010), *e-Biznes. Poradnik praktyka*, Helion, Gliwice.

Foltz C.B., Newkirk H.E., Schwager P.H. (2016), *An Empirical Investigation of Factors that Influence Individual Behavior toward Changing Social Networking Security Settings*, "Journal of Theoretical and Applied Electronic Commerce Research", Vol. 11(2), s. 1-15.

Frankowski P., Juneja A. (2009), *Serwisy społecznościowe. Budowa, administracja i moderacja*, Helion, Gliwice.

Hekkala R., Väyrynen K., Wiander T. (2012), *Information Security Challenges of Social Media for Companies*, ECIS 2012 Proceedings, Paper 56, http://aisel.aisnet.org/ecis2012/56 (dostęp: luty 2018).

Hiatt D., Choi Y.B. (2016), *Role of Security in Social Networking*, "International Journal of Advanced Computer Science and Applications", Vol. 7, No. 2, s. 12-15.

Ibarra H., Hunter M. (2007), *W jaki sposób liderzy budują i wykorzystują sieci kontaktów*, „Harvard Business Review Polska", nr 7/8(53/54), s. 182-191.

Jarche H. (2011), *Network Thinking*, http://jarche.com/2011/12/network-thinking/ (dostęp: luty 2018).

Kamatchi R., Minocha K. (2015), *A Modus Operandi for Social Networking Security Solutions Based on Varied Usages* [w:] J. Abawajy, S. Mukherjea, S. Thampi, A. Ruiz-Martínez (eds.), *Security in Computing and Communications*. SSCC 2015. Communications in Computer and Information Science, Vol. 536. Springer, Cham, s. 317-328.

Kumar A., Gupta S.K., Rai A.K., Sinha S. (2013), *Social Networking Sites and Their Security Issues*, "International Journal of Scientific and Research Publications", Vol. 3(4), s. 1-5.

LeBlanc J. (2013), *Programowanie aplikacji na serwisy społecznościowe*, Helion, Gliwice.

Nojszewski D. (2007), *Przegląd modeli e-biznesowych (cz. II)*, „e-mentor", nr 2(19), http://www.e-mentor.edu.pl/artykul/index/numer/19/id/414 (dostęp: luty 2018).

Piskorski J. (2012), *Skuteczne strategie społecznościow*e, „Harvard Business Review Polska", kwiecień, s. 102-111.

Vossen G., Hagemann S. (2007), *Serwis Web 2.0. Od pomysłu do realizacji*, Helion, Gliwice.

Ward S. (2017), *What Is Business Networking & What Are the Benefits? Why Business Networking Is Essential for Success*, https://www.thebalance.com/what-is-business-networking-and-what-are-the-benefits-2947183 (dostęp: luty 2018).

Waszczuk P. (2008), *Biznes w społeczności*, „Computerworld", nr 36/830.

Włodarski W. (2012), *Frugo: reaktywacja marki na Facebooku*, „Harvard Business Review Polska", nr 111 , s. 28-33.

[www 1] www.infobiz.pl/Internetowe_modele_biznesowe-1-119-20-.html (dostęp: luty 2018).

[www 2] https://napoleoncat.com/pl/ (dostęp: listopad 2018).

[www 3] https://spolecznosc.comarch.pl (dostęp: listopad 2018).

[www 4] https://soovle.com (dostęp: listopad 2018).

[www 5] https://answerthepublic.com (dostęp: listopad 2018).

SECURITY IN SOCIAL NETWORKS – KEY RESEARCH AREAS

Summary: The paper discusses the security issues of social networking sites, which should be included in the formulation of the company's development strategy with the use of social networks. More and more companies are recognizing the popularity of social networking sites among people. Therefore, companies try to incorporate them into their development strategy in order to strengthen their competitive advantage. At the same time, more and more people actively use these types of services by posting on them information about themselves and their work, often unaware of the risks that such activity entails. The cognitive goal of the paper is to analyze the importance of social networking sites and social networks in business. The empirical part aims to identify threats arising from communications using social networking sites. Its goal is also to identify key topics and recommendations for further research.

Keywords: security, social networking sites, social networks, threats.